

idp

idp

MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA

**AVALIAÇÃO DO NÍVEL DE MATURIDADE EM GESTÃO DE
RISCOS NA DIRETORIA DE ASSISTÊNCIA AO PESSOAL DO
EXÉRCITO BRASILEIRO (DAP)**

PAOLLA CRISTINA DE MOURA E SILVA

Brasília-DF, 2023

PAOLLA CRISTINA DE MOURA E SILVA

**AVALIAÇÃO DO NÍVEL DE MATURIDADE EM GESTÃO
DE RISCOS NA DIRETORIA DE ASSISTÊNCIA AO
PESSOAL DO EXÉRCITO BRASILEIRO (DAP)**

Dissertação apresentada ao Programa de Pós Graduação em Administração Pública, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito parcial para obtenção do grau de Mestre.

Orientador

Professor Mestre Weder de Oliveira

Brasília-DF 2023

PAOLLA CRISTINA DE MOURA E SILVA

AVALIAÇÃO DO NÍVEL DE MATURIDADE EM GESTÃO DE RISCOS NA DIRETORIA DE ASSISTÊNCIA AO PESSOAL DO EXÉRCITO BRASILEIRO (DAP)

Dissertação apresentada ao Programa de Pós Graduação em Administração Pública, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, como requisito parcial para obtenção do grau de Mestre.

Aprovado em 25 / 06 / 2024

Banca Examinadora

Prof. Me.. Weder de Oliveira. - Orientador

Prof. Dr. Felipe Lopes da Cruz - IDP

Prof. Dr. André Castro Carvalho - Examinador externo

S586a Silva, Paolla Cristina de Moura
Avaliação do nível de maturidade em gestão de riscos na diretoria de assistência ao pessoal do exército brasileiro (DAP) / Paolla Cristina de Moura e Silva. – Brasília: IDP, 2024.

96 p.
Inclui bibliografia.

Dissertação – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP, Mestrado em Administração Pública, Brasília, 2024.
Orientador: Prof. Mestre. Weder de Oliveira.

1. Gestão de Riscos. 2. Governança Pública. 3. Maturidade em Gestão de Riscos. I. Título.

CDD: 341

Ficha catalográfica elaborada pela Biblioteca Ministro Moreira Alves
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

RESUMO

Com o advento do paradigma da governança pública, no final do século XX, a gestão de riscos ganhou maior relevância na administração pública. No Brasil, em 2016, a Instrução Normativa Conjunta nº 01 estabeleceu que órgãos do Poder Executivo Federal deveriam sistematizar suas ações relacionadas à gestão de riscos. Um desses órgãos foi o Exército Brasileiro, que, em 2017, publicou a 1ª edição da sua política de gestão de riscos. Entre as organizações militares que seguem essa política, encontra-se a Diretoria de Assistência ao Pessoal (DAP), responsável pelas áreas de pessoal civil, veteranos, pensionistas e assistência social e religiosa do Exército. Embora a referida política cite a avaliação da maturidade em gestão de riscos como uma ferramenta de identificação de áreas vulneráveis que possam afetar os objetivos organizacionais, o documento não apresenta um modelo de mensuração. Desse modo, o objetivo deste trabalho é mensurar a maturidade em gestão de riscos na DAP, conforme metodologia do Tribunal de Contas da União (TCU), e emitir sugestões. Para isso, foi realizada uma pesquisa descritiva e qualitativa, por meio de entrevista, análise documental e aplicação de questionário. A partir dos dados coletados, utilizou-se os parâmetros de mensuração do TCU para identificar o nível de maturidade da gestão de riscos nas dimensões ambiente, processos, parcerias e resultados e, aplicando pesos para cada dimensão, concluiu-se que o nível de maturidade global da DAP é o “aprimorado”. Após a identificação das possibilidades de melhoria, sugestões foram emitidas, a fim de aperfeiçoar o nível de maturidade da diretoria.

Palavras-chaves: Gestão de Riscos. Governança Pública. Maturidade em Gestão de Riscos.

ABSTRACT

With the advent of the public governance paradigm at the end of the 20th century, risk management gained greater relevance in public administration. In Brazil, in 2016, Joint Normative Instruction No. 01 established that entities of the Federal Executive Branch should systematize their actions related to risk management. One of these entities was the Brazilian Army, which, in 2017, published the 1st edition of its risk management policy. Among the military organizations that follow this policy is the Personnel Assistance Directorate (DAP), responsible for the areas of civilian personnel, veterans, pensioners and social and religious assistance of the Army. Although the aforementioned policy cites the assessment of risk management maturity as a tool for identifying vulnerable areas that may affect organizational objectives, the document does not present a measurement model. Therefore, the objective of this work is to measure maturity in risk management at DAP, according to the methodology of the Federal Court of Accounts (TCU), and issue recommendations. For this, a descriptive and qualitative research was carried out, through interviews, document analysis and questionnaire application. From the data collected, the TCU measurement parameters were used to identify the level of maturity of risk management in the dimensions environment, processes, partnerships and results and, applying weights to each dimension, it was concluded that the DAP's level of overall maturity is "enhanced". After identifying possibilities for improvement, recommendations were issued in order to improve the board's maturity level.

Keywords: Risk Management. Public Governance. Maturity in Risk Management.

SUMÁRIO

1	INTRODUÇÃO	9
1.1.	Contextualização.....	9
1.2.	Apresentação do problema e hipótese de pesquisa.	14
1.3.	Enunciação dos Objetivos.	15
1.3.1.	Geral.	15
1.3.2.	Específicos.	15
2.	REFERENCIAL TEÓRICO	18
2.1.	Gestão de riscos.	18
2.1.1.	Introdução à gestão de riscos.	18
2.1.2.	Modelos e normas de referência.	21
2.1.3.	Processo de gestão de riscos.	25
2.2.	Maturidade em Gestão de Riscos.	29
2.2.1.	RMM – <i>Risk Maturity Model</i>	29
2.2.2.	Modelo do Instituto Brasileiro de Governança Corporativa (IBGC)	33
2.2.3.	Modelo do Tribunal de Contas da União.	38
3.	GESTÃO DE RISCOS NO EXÉRCITO BRASILEIRO	42
4.	METODOLOGIA	49
5.	A GESTÃO DE RISCOS NA DAP	55
6.	RESULTADOS E DISCUSSÕES	61
7	CONSIDERAÇÕES FINAIS	75
	REFERÊNCIAS BIBLIOGRÁFICAS	80
	ANEXO A	88
	ANEXO B	94



1

INTRODUÇÃO

1.1 Contextualização

Ao longo dos anos, a administração pública passou por diversos paradigmas, que são um conjunto de crenças, valores e práticas que orientam a forma como a gestão pública é pensada e implementada.

Os paradigmas da administração pública têm evoluído ao longo dos tempos, indo da Administração Patrimonial, do início e meados do século passado, até a Nova Gestão Pública (NGP), que reinou quase absoluta nas décadas 1980/1990, passando pela Administração Burocrática. E a partir do final do século passado, surge um novo paradigma, genericamente denominado de Governança Pública, com foco na colaboração e na coordenação dos entes públicos e destes com a sociedade civil (Neves; Guimarães; Júnior, 2017, p. 2).

Segundo os mesmos autores, essa evolução não foi dada de forma segmentada, pois os paradigmas se sobrepõem, coexistindo todos, em algum grau, até os dias atuais. Assim, a linha do tempo mostra apenas o paradigma predominante do momento, desde o patrimonialismo até a governança pública.

No Brasil, o Decreto nº 9.203, de 22 de novembro de 2017, em seu inciso I do Art. 2º, define governança pública como um “conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade” (Brasil, 2017a).

Dentro desse conceito, no âmbito dos mecanismos de estratégia e controle, temos a gestão de riscos e controles internos, sendo riscos eventos que podem gerar impactos negativos na organização, impossibilitando a criação de valor ou destruindo o valor já existente (COSO, 2007), enquanto gestão de riscos é definida no art. 2º, inciso IV, do Decreto nº 9.203, como:

[...] processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que

contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos (Brasil, 2017a).

Nesse contexto, o então Ministério do Planejamento, Orçamento e Gestão e a Controladoria-Geral da União (CGU) emitiram a Instrução Normativa Conjunta nº 01, que estabeleceu que órgãos e entidades do Poder Executivo Federal deveriam sistematizar suas ações relacionadas à gestão de riscos, aos controles internos e à governança (Brasil, 2016).

Nesse momento, a necessidade de metodizar o gerenciamento de riscos se materializa de forma amplamente impositiva no âmbito do Poder Executivo Federal, o que, até então, era feito pontualmente a partir de acórdãos do Tribunal de Contas da União, a exemplo do acórdão 1517/2010, que apresentou “os riscos da copa do mundo de futebol de 2014 nas áreas de construção ou reforma de estádios, infraestrutura aeroportuária e mobilidade urbana, bem como na sistemática de gerenciamento das ações a cargo do governo federal” (Brasil, 2010, p. 1) e do acórdão 1739/2015, que identificou riscos relevantes em contratações de serviços de tecnologia da informação, sob o modelo de computação em nuvem (Brasil, 2015).

Entre os diversos órgãos que devem cumprir as imposições constantes na Instrução Normativa Conjunta nº 01 encontra-se o Exército Brasileiro (EB).

Segundo o art. 142 da Constituição Federal, as Forças Armadas “destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem” (Brasil, 1988). Como Força Terrestre, o Exército Brasileiro tem prestado diversos serviços à sociedade brasileira, além dos já previstos constitucionalmente. Esses serviços são formalizados por meio normativos próprios, como a Lei nº 10.826/2003 (Brasil, 2003), que trata, entre outras coisas, da fiscalização de produtos controlados; a Portaria Normativa nº 62/2019 (Brasil, 2019a), que dispõe sobre o Projeto Soldado-Cidadão, que oferece qualificação profissional aos militares temporários¹ carentes ou em situação de risco social; a Lei Complementar nº 97/1999 (Brasil, 1999), que atribui, subsidiariamente, ao Exército, a execução de obras e serviços de engenharia, a exemplo da construção de pontes e estradas; ou através de operações conjuntas

¹ Militares que prestam serviço militar, obrigatório ou voluntário, podendo permanecer na Força pelo prazo máximo de 8 anos.

do Ministério da Defesa (MD), sem normativos específicos, como no apoio à vacinação contra a COVID-19 e nas ações de combate à dengue.

Assim, buscando acompanhar os novos valores da administração pública e cumprindo as imposições constantes na Instrução Normativa Conjunta nº 01, o Exército Brasileiro elaborou, em 2017, a 1ª edição da Política de Gestão de Riscos do Exército Brasileiro, revogada pela 2ª edição, em 2018 (Brasil, 2018a).

Anteriormente à elaboração desse normativo, a gestão de riscos era feita de forma independente e sem unicidade metodológica, realizada quase que exclusivamente em áreas técnicas e/ou de alto risco, como na gestão de projetos e na aviação do Exército.

A referida política procurou sistematizar o tema no âmbito de toda Força Terrestre por meio da exposição de conceitos, princípios, estruturação da governança, gestão de riscos e controles internos da gestão, competências, responsabilidades e diretrizes. O documento apresenta de forma clara e detalhada como a gestão de riscos será implementada em todas as organizações militares (OM) do Exército.

Entretanto, cada OM possui características particulares, como sua cultura organizacional, sua atividade-fim (técnica ou operacional) e o efetivo de pessoal dedicado à área de gestão. Todos esses fatores, entre outros, podem influenciar direta ou indiretamente na excelência com qual a organização militar gere seus riscos. Desse modo, algumas unidades podem possuir níveis mais maduros de gestão de riscos e outras menos, sendo necessário compreender os pontos sensíveis que precisam de aprimoramento.

Uma dessas OM é a Diretoria de Assistência ao Pessoal, objeto de estudo desta pesquisa, que se encontra diretamente subordinada ao Departamento-Geral do Pessoal (DGP), composto por 6 (seis) diretorias e responsável pela gestão da dimensão humana da Força (promoção, movimentação, serviço militar, assistência ao pessoal, saúde e a gestão orçamentária dessas cinco áreas).

Segundo seu regulamento, a DAP tem como finalidade gerir o sistema de pessoal civil do Exército (SiPeC-EB), o serviço de veteranos e pensionistas do Exército (SvVPEEx) e o sistema de assistência social do Exército (SASEx) (Brasil, 2019b), sendo também incorporada a gestão do serviço de assistência religiosa do Exército (SAREx), em 2023.

A DAP possui quatro macroprocessos finalísticos demasiadamente distintos entre si, o que amplia a complexidade da sua missão, dos seus ambientes interno e externo, dos seus clientes e, conseqüentemente, da sua gestão de riscos.

Por atuar em áreas sensíveis, como processos de aposentadoria, de passagem para a reserva e todo o sistema de assistência social e religiosa do Exército, é primordial que a DAP possua ferramentas para gerir seus riscos de processos - como a concessão indevida de direitos e danos ao erário/usuário por erro de cálculo de benefícios -, seus riscos de integridade - como fraudes nos processos de habilitação à pensão ou concessão de reforma - e seus riscos estratégicos².

A gestão de riscos na Diretoria visa, especialmente, reduzir impactos negativos na gestão orçamentária, na gestão dos recursos humanos que compõem todos os quatro sistemas e serviços da Diretoria e na gestão dos diversos processos executados e/ou normatizados pela DAP, contribuindo, assim, para a melhoria da qualidade de vida da família militar³, uma vez que assistência ao pessoal será fornecida com maior excelência.

A gestão de riscos madura pode evitar fraudes, desvio de verbas, danos ao erário em geral, irregularidades, entre outros efeitos nocivos à boa gestão. É necessário não apenas implementar políticas de gerenciamento de riscos, mas também avaliar o seu nível de maturidade no órgão. Essa avaliação propiciará aos gestores informações relevantes para a tomada de decisão, na medida em que seu diagnóstico aponta quais áreas do gerenciamento de riscos podem ser aprimoradas, podendo indicar, também, que políticas expressas documentalmente não estão sendo implementadas na prática pela organização.

No âmbito de EB, a Diretriz Reguladora da Política de Gestão de Riscos do Exército (Brasil, 2019c), menciona, entre outras coisas, a avaliação da maturidade de gestão de riscos. Apesar de possuir orientações relevantes sobre gestão de riscos, no que concerne à avaliação da maturidade, a metodologia apresentada é insuficiente para uma boa mensuração, pois considera apenas duas dimensões - a observância às normas e metodologias formais e a quantidade de áreas

² Por determinação do alto comando, os riscos estratégicos não podem ser divulgados.

³ A família militar é composta por todos os militares e servidores civis integrantes do Exército Brasileiro, bem como seus dependentes legais e pensionistas.

relevantes para o atingimento do objetivo da organização militar em que as práticas são implementadas -, resultando em quatro possíveis níveis:

Art. 17 [...]

I - inicial: as práticas são inexistentes, não implementadas, não funcionais ou são realizadas de maneira informal e esporádica em algumas áreas relevantes para consecução dos objetivos da OM;

II - básico: as práticas são realizadas de acordo com as normas e metodologias definidas em algumas áreas relevantes para consecução dos objetivos da OM;

III - intermediário: as práticas são realizadas de acordo com normas e metodologias definidas na maior parte das áreas relevantes para os objetivos da OM; e

IV - aprimorado: as práticas são realizadas de acordo com normas e metodologias definidas em todas as áreas relevantes para consecução dos objetivos da OM (Brasil, 2019c).

A diretriz ressalta que a mensuração será realizada por meio de uma autoavaliação diagnóstica da gestão organizacional do EB, sem explicitar a metodologia que deverá ser utilizada (ferramentas de coleta, modelo de questionário, etc.).

O enquadramento dos níveis proposto pela diretriz é demasiadamente simples, pois avalia apenas duas dimensões, que se resumem ao cumprimento de normas e à quantidade de áreas relevantes em que essas normas são aplicadas, ignorando questões como cultura organizacional e o processo de gerenciamento de risco.

Para avaliar os níveis de maturidade, existem diversos modelos, como o *Risk Maturity Model* (RMM), o modelo do Instituto Brasileiro de Governança Corporativa (IBGC) e o do TCU. Os dois primeiros modelos apresentam apenas os ambientes a serem avaliados e os possíveis níveis de maturidade, enquanto o modelo do TCU fornece uma metodologia de mensuração, com um questionário a ser aplicado e métricas definidas.

Desse modo, diante da inexistência de metodologia de mensuração própria do Exército, esta pesquisa utilizará a metodologia de avaliação de maturidade de gestão de riscos do TCU, por possuir variáveis e métricas bem definidas, por ser direcionada a órgãos públicos e por ser o Tribunal o órgão de controle externo que fiscaliza a atuação e gestão do Exército Brasileiro.

1.2. Apresentação Do Problema E Hipótese De Pesquisa

A gestão de riscos é uma atividade a ser realizada por todas as organizações do Poder Executivo Federal. Essas organizações necessitam emitir, anualmente, relatórios de gestão, para fins de prestação de contas ao TCU (Brasil, 2020a), sendo a avaliação dos riscos um dos elementos de conteúdo desse relatório (Brasil, 2022a). Uma boa gestão de riscos contribui para uma maior eficácia das entregas feitas à sociedade, uma vez que tende a minimizar erros, atrasos, fraudes e aplicação ineficiente e ineficaz de recursos.

Embora muitas organizações públicas possuam uma metodologia de gestão de riscos definida, como é o caso do Exército e da sua Diretoria de Assistência ao Pessoal (DAP), isso por si só não garante que a gestão seja feita de forma madura, sendo necessário avaliar, além da existência da metodologia, como ela é implementada na prática. A mensuração do nível de maturidade em gestão de riscos permite essa avaliação, contribuindo, ainda, para a identificação de possíveis melhorias. Apesar de o Exército possuir uma política de gestão de riscos que menciona a mensuração de sua maturidade, esse documento não apresenta um modelo aplicável de mensuração.

Em uma organização como a DAP, diretoria responsável por gerir a assistência social, a assistência religiosa, o quadro de pessoal civil, de veteranos e pensionistas do Exército, áreas com impacto orçamentário considerável e que, de um modo geral, trata de pessoas em situação de vulnerabilidade social e/ou emocional (idosos, portadores de necessidades especiais, viúvos), faz-se necessário identificar qual é o nível de maturidade de gestão de riscos da diretoria, uma vez que uma maturidade baixa tende a facilitar a concretização de eventos negativos, como fraudes nos processos de pensão e reforma, insuficiência de recursos orçamentários para prover as ações socioassistenciais e erros na geração de direitos remuneratórios. A ocorrência desses e de outros eventos pode resultar em um baixo nível de assistência aos militares, servidores civis e seus dependentes.

Desta forma, pretende-se investigar nesta pesquisa a seguinte questão: **Qual o nível de maturidade da gestão de riscos da Diretoria de Assistência ao Pessoal do Exército Brasileiro a partir da metodologia de mensuração do Tribunal de Contas da União?**

A metodologia do TCU possui 4 dimensões a serem avaliadas (ambiente, processos, parcerias e resultados) e 5 possíveis níveis de maturidade (inicial, básico, intermediário, aprimorado e avançado). O modelo não apresenta uma definição genérica para cada nível, o enquadramento é feito por meio de pontuação obtida em questionário.

A hipótese de pesquisa é que o nível de maturidade global em gestão de riscos da DAP, de acordo com a metodologia do TCU, seja o nível intermediário. Isso porque a dimensão “processos” tende a obter um bom índice, considerando a existência de um manual técnico que orienta todo o processo de gestão de riscos, com a disponibilidade de ferramentas para serem utilizadas nas diversas etapas do processo (identificação, avaliação, respostas a riscos, monitoramento e comunicação), enquanto a existência de uma política de gestão de riscos e de sua diretriz contribuem para um bom índice na dimensão “ambiente”. Entretanto, na dimensão “parcerias”, o índice pode ser baixo, pois não há formalização da gestão de riscos no acordo de cooperação entre a DAP e sua parceira. Por fim, a dimensão “resultados”, tende a apresentar um nível intermediário de maturidade, uma vez que o ambiente e os processos estão bem estruturados, contribuindo para o alcance dos objetivos organizacionais.

1.3. Enunciação dos Objetivos

1.3.1. Geral

O objetivo geral desta pesquisa é mensurar o nível de maturidade em gestão de riscos da Diretoria de Assistência ao Pessoal do Exército Brasileiro, seguindo os critérios estabelecidos pelo Tribunal de Contas da União, e emitir sugestões.

1.3.2. Específicos

- a) apresentar a legislação vigente no Brasil sobre o tema;
- b) apresentar modelos de avaliação da maturidade em gestão de riscos, com destaque para o modelo do TCU;
- c) identificar e descrever a estrutura da gestão de riscos no Exército e, em particular, na Diretoria de Assistência ao Pessoal;

d) coletar dados sobre as práticas de gestão de riscos na Diretoria de Assistência ao Pessoal;

e) calcular o índice de maturidade global em gestão de riscos da DAP conforme o modelo do TCU; e

f) propor ações que possam aumentar o índice de maturidade global em gestão de riscos da DAP.



2

REFERENCIAL TEÓRICO

2.1. Gestão De Riscos

2.1.1. Introdução À Gestão De Riscos

De acordo com o *Committee of Sponsoring Organizations of the Treadway Commission (COSO)* (2007), riscos são eventos que podem gerar impactos negativos na organização, impossibilitando a criação de valor ou destruindo o valor já existente.

O COSO (2020, p.1) trouxe uma definição atualizada de riscos ao excluir a afirmação de que são apenas eventos negativos. Assim, a nova definição passou a ser “risco é a possibilidade de ocorrência de eventos que podem afetar a realização da estratégia e dos objetivos do negócio”. Desse modo, tanto eventos negativos como positivos, que afetem a estratégia e os objetivos, podem ser vistos como riscos.

O comitê também define gerenciamento de riscos, sendo ele:

[...] um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. (COSO II, 2007, p. 10)

Segundo Dionne (2013), a gestão de riscos passou a ser estudada após a Segunda Guerra Mundial e os primeiros livros acadêmicos sobre o tema foram publicados apenas na década de 1960.

Przetacznik (2022) afirma que o conhecimento sobre probabilidade produzidos no período do Renascimento contribuíram para o desenvolvimento real do campo de estudo sobre a gestão de riscos no século XX.

Ainda segundo a autora, até a década de 1970, a gestão de riscos no setor privado era focada em riscos puros e seguráveis. Após esse período, as empresas passaram a utilizar métodos de gestão de riscos

de forma mais ampla, como no controle de perdas e nas estratégias para evitar, reduzir ou transferir riscos.

Um divisor de águas quanto ao tema foi o surgimento, no início do século XXI, do *Enterprise Risk Management* (ERM). Diferenciando-se da abordagem tradicional, que tratava os riscos de forma segmentada na empresa, o ERM opta por uma abordagem holística, incorporando-se ao nível estratégico da organização (Carvalho, 2021). A tabela abaixo apresenta as principais diferenças entre as duas abordagens:

Tabela 1: Comparativo entre as abordagens ERM e tradicional	
Características do ERM	Características da gestão de riscos tradicional
Gestão consistente e abrangente de todos os riscos aos quais a organização está exposta, levando em conta as ligações que possam existir entre eles. Gestão conjunta da carteira de riscos.	Os riscos individuais são tratados de forma independente e analisados separadamente, sua gestão é apenas uma de muitas funções que ocorrem na empresa. Nem todos os riscos são levados em consideração.
Atitude proativa em relação ao risco. Risco visto tanto como uma ameaça quanto uma oportunidade.	Atitude ativa ou reativa em relação ao risco. O risco é visto apenas como uma ameaça.
A gestão de riscos é um processo contínuo constantemente melhorado, implementado em toda a empresa, parte integrante de todos os processos que ocorrem na organização, enquadrados em uma estrutura organizacional de uma determinada empresa.	A gestão de riscos é uma função isolada e única, as ações tomadas são muitas vezes desestruturadas e descoordenadas.
Cultura adequada de gestão de risco, há o envolvimento de todos os funcionários e há responsabilidade por risco em todos os locais de trabalho.	Não há cultura de gestão de risco.
Infraestrutura de gerenciamento de risco bem desenvolvida (política, procedimentos, indicadores de risco, relatórios, sistemas de tecnologia da informação).	Fraco desenvolvimento da infraestrutura da gestão de riscos.
Divisão claramente definida de responsabilidades, deveres e competências. Os proprietários de risco são designados e existe o cargo de gerente de riscos.	Não há um gerente de riscos.
A gestão de riscos faz parte do planejamento estratégico e é parte integrante da gestão e da tomada de decisão	O impacto do risco na implementação da estratégia não é considerado.
O objetivo é otimizar o nível de risco.	O objetivo é minimizar a exposição ao risco.

Fonte: Przetacznik, 2022, p. 103

Embora a gestão de riscos tenha iniciado no setor privado, ela se estendeu ao setor público, recebendo maior atenção com o surgimento da governança pública. De acordo com a *International Federation of Accountants* (IFAC) (2013, p. 8) a “governança compreende os mecanismos implementados para garantir que os resultados pretendidos pelas partes interessadas sejam definidos e alcançados”.

Para Vieira e Araújo (2020, p. 407) “a governança e a gestão de uma organização são fortalecidas quando a gestão de riscos é integrada ao planejamento e à execução das estratégias, pois permite o alinhamento de estratégias e desempenho com sua missão institucional e propósitos fundamentais”. Nesse sentido, a IFAC (2013) cita que gerir riscos e desempenho, por meio de um controle interno eficaz e de um sólido gerenciamento de recursos públicos, é um dos princípios para o alcance de uma boa governança.

De acordo com o TCU (Brasil, 2020b), a governança pública abrange mecanismos de liderança, estratégia e controle. A gestão de riscos é uma prática do mecanismo de estratégia, como mostra a figura a seguir.

Figura 1: Práticas relacionadas aos mecanismos de governança



Fonte: Brasil, 2020b, p. 52

Para Vieira e Barreto (2019, p. 105), a sistematização da gestão de riscos dentro de uma organização também “se relaciona diretamente com os mecanismos de governança e controle interno que visam aprimorar a direção e o controle e assegurar maior responsividade (*accountability*), transparência (*openness*) e a integridade (*integrity*) das agências públicas”. Percebe-se que a prática de gestão de riscos se comunica com outras práticas de governança, representando a visão holística trazida pelo ERM.

Embora a metodologia de gestão de riscos seja similar em organizações públicas e privadas, a sua implementação no setor público enfrenta desafios adicionais, como: i) mudança frequente de lideranças ou vacância de cargos de liderança; ii) líderes com pouco conhecimento em gestão de riscos; iii) divisão entre o orçamento operacional e o orçamento dos programas; iv) cultura e mentalidade de risco limitadas (Ahmeti; Vladi, 2017).

Ainda que encontre desafios, a gestão de riscos é uma ferramenta crucial de governança no setor público, auxiliando os gestores a cumprir suas responsabilidades de gerar, preservar e fornecer valor público à sociedade (Vieira; Barreto, 2019).

Os mesmos autores ressaltam que a principal vantagem da adoção de um sistema de gestão de riscos é aumentar a probabilidade de alcançar os objetivos da organização pública, realizando ações que visam priorizar iniciativas públicas, melhorar decisões de investimento e operacionais, proteger a reputação e garantir o cumprimento do propósito institucional.

2.1.2 Modelos E Normas De Referência

De acordo com Viana (2021, p. 40), “a gestão de riscos é trabalhada e conceituada por normas padronizadas e adotadas em nível mundial”.

Além das normas, que serão apresentadas mais a frente, existem modelos que trazem práticas de referência em gestão de riscos, a exemplo do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO).

Esse comitê foi criado em 1985 nos Estados Unidos, composto por cinco grandes associações profissionais norte americanas e tinha

como objetivo inicial patrocinar a Comissão Nacional de Fraude de Relatório Financeiro, que tinha a finalidade de compreender o porquê de tantas fraudes nas demonstrações contábeis dos Estados Unidos (MAFFI, 2018).

Inicialmente, focado apenas no controle interno, o comitê elaborou, em 1992, o modelo COSO *Report*, também conhecido como *Control-Integrated Framework* (COSO-IC ou COSO I). Sua edição mais recente define controle interno como “um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade” e descreve a avaliação de riscos como um dos cinco componentes integrados do controle interno (COSO, 2013, p. 6).

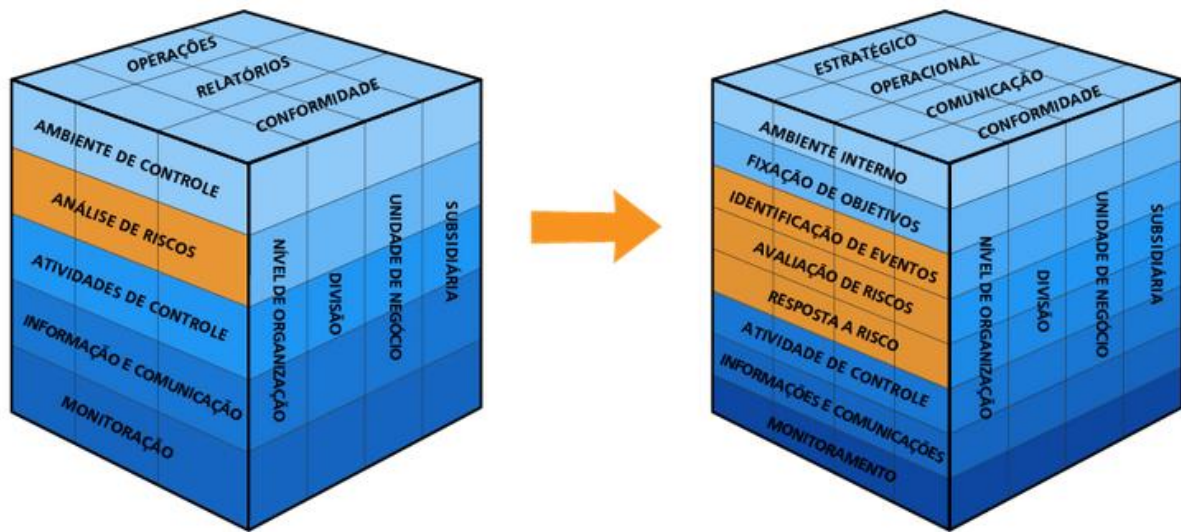
A versão elaborada em 1992 foi remodelada em 2004, criando o COSO ERM - *Enterprise Risk Management - Integrated Framework*, também denominado COSO II, com enfoque na gestão de riscos corporativos e fraude (Gattringer; Marinho, 2020).

De acordo com Dutra et al.:

Para a realização dos objetivos estabelecidos na missão e visão da organização, o modelo estrutural sugerido no relatório Enterprise Risk Management (ERM) [...] estabelece que a gerência de riscos precisa definir: as estratégias (*Estrategic*); utilizar eficazmente seus recursos (*Operations*); reproduzir por meio de relatórios as decisões e resultados (*Reporting*); respeitar as leis e regulamentos impostos pela gestão (*Compliance*) (2009, p. 94).

O COSO ERM promoveu um aumento do número de componentes que constituem o modelo. Na área da gestão de riscos, acrescentou a identificação de eventos e a resposta a riscos, mantendo o componente de avaliação de riscos já previstos no modelo COSO-IC. A figura a seguir apresenta os componentes do COSO I e COSO II, destacando os relacionados à gestão de riscos.

Figura 2: Comparativo entre os componentes dos COSO I e II



Fonte: Coso, 2007; Coso, 2013

Em 2017, o COSO ERM passou por uma reformulação, sendo criado o *Enterprise Risk Management – Integrating with Strategy and Performance* (Gerenciamento dos Riscos Corporativos – Integrado com Estratégia e Performance). Esse novo modelo “realça a importância do gerenciamento de riscos corporativos no planejamento estratégico e da sua incorporação em toda a organização – porque o risco influencia e alinha estratégia e performance em todos os departamentos e funções” (COSO, 2017, p. 6).

No COSO 2017, os seus componentes são definidos da seguinte forma:

Tabela 2: Componentes do COSO 2017

Componente	Definição
Governança e cultura	A governança dá o tom da organização, reforçando a importância e instituindo responsabilidades de supervisão sobre o gerenciamento de riscos corporativos. A cultura diz respeito a valores éticos, a comportamentos esperados e ao entendimento do risco em toda a entidade.
Estratégia e definição de objetivos	Gerenciamento de riscos corporativos, estratégia e definição de objetivos atuam juntos no processo de planejamento estratégico. O apetite a risco é estabelecido e alinhado com a estratégia; os objetivos de negócios colocam a estratégia em prática e, ao mesmo tempo, servem como base para identificar, avaliar e responder aos riscos.
Performance	Os riscos que podem impactar a realização da estratégia e dos objetivos de negócios precisam ser identificados e avaliados. Os riscos são priorizados com base no grau de severidade, no contexto do apetite a risco. A organização determina as respostas aos riscos e, por fim, alcança uma visão consolidada do portfólio e do montante total dos riscos assumidos. Os resultados desse processo são comunicados aos principais <i>stakeholders</i> envolvidos com a supervisão dos riscos.
Análise e revisão	Ao analisar sua performance, a organização tem a oportunidade de refletir sobre até que ponto os componentes do gerenciamento de riscos corporativos estão funcionando bem ao longo do tempo e no contexto de mudanças relevantes, e quais correções são necessárias.
Informação, comunicação e divulgação	O gerenciamento de riscos corporativos demanda um processo contínuo de obtenção e compartilhamento de informações precisas, provenientes de fontes internas e externas, originadas das mais diversas camadas e processos de negócios da organização.

Fonte: Elaborada pela autora a partir de COSO, 2017, p. 6.

Assim como o COSO, outra organização que buscou padronizar o processo de gestão de riscos foi a *International Organization for Standardization* (ISO), uma organização não governamental criada em 1947 (Chaves; Campello, 2016), que estabelece normas a fim de aprimorar a qualidade de produtos e serviços (Pinto; Barros, 2018) ofertados por diversas instituições.

A primeira norma ISO sobre o tema foi publicada em 2009, “devido à necessidade de harmonizações dos padrões, regulamentações e estruturas das normas relacionadas à gestão de riscos publicadas anteriormente” (Santos, 2021, p. 2). Essa norma traz princípios e orientações gerais sobre a gestão de riscos, que podem ser usados por qualquer instituição pública ou privada (ABNT, 2018).

Mesmo não tratando explicitamente sobre o tema “nível de maturidade de gestão de riscos”, a ISO 31000 cita a sua importância ao dizer que “convém que a organização avalie suas práticas e processos existentes de gestão de riscos, avalie quaisquer lacunas e aborde estas lacunas no âmbito da estrutura” (ABNT, 2018, p. 4).

Ainda que na norma não esteja incluída a mensuração do nível de maturidade em uma das 7 atividades do processo de gestão de riscos, ela pode ser enquadrada no monitoramento e análise crítica, uma vez que trata de um autodiagnóstico de quão bem estruturado é o processo de gestão de riscos na organização.

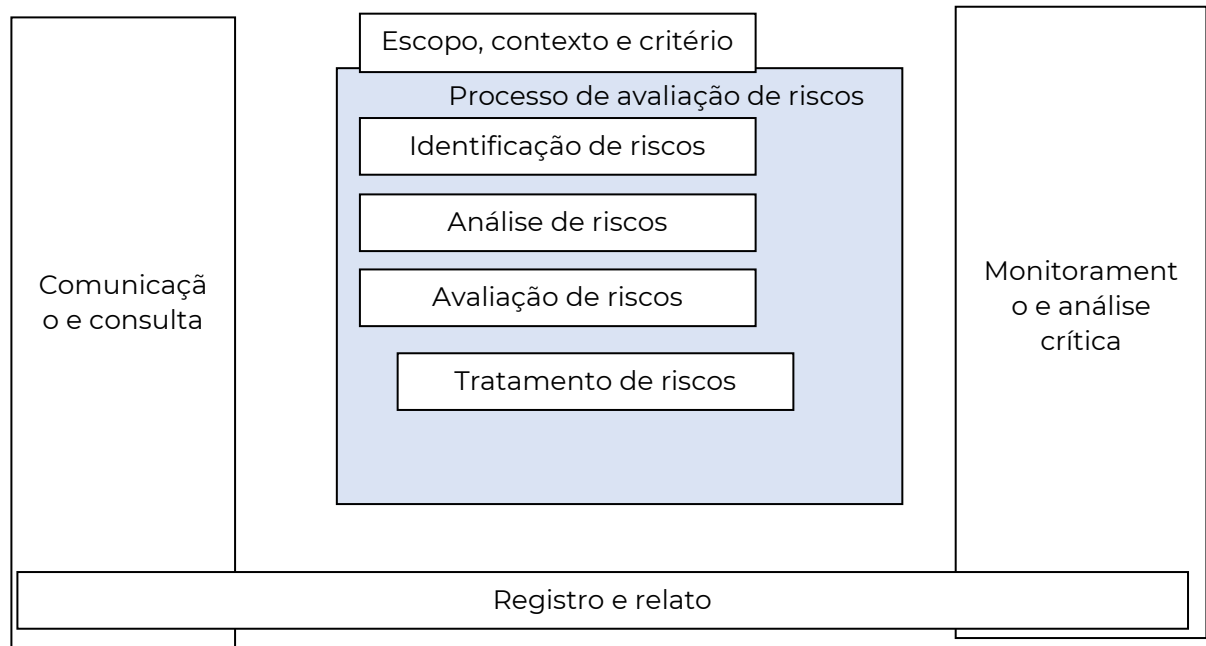
Para as atividades que compõem o processo de avaliação de riscos (identificação, análise e avaliação de riscos), existe uma ISO específica abordando o tema.

Intitulada “Técnicas para o processo de avaliação de riscos”, a ISO 31010 ressalta que a finalidade do processo de avaliação de riscos é “fornecer informações baseadas em evidências e análise para tomar decisões informadas sobre como tratar riscos específicos e como selecionar entre opções” (ABNT, 2012, p. 15).

Além das normas ISO 31000 e 31010, outras são relacionadas à gestão de riscos, sendo elas: i) ISO 31022 (2020), que fornece um guia para a gestão de riscos de natureza legal, alinhada com atividades de *compliance*, a fim de garantir a segurança jurídica na consecução das obrigações e objetivos da organização; e ii) ISO 31073 (2022), que é um vocabulário que busca alinhar entendimentos nas organizações sobre os termos e conceitos da Gestão de Riscos.

2.1.3. Processo De Gestão De Riscos

A condução da gestão de riscos é feita em todos os níveis e perpassa todas as áreas de uma organização, seja ela pública ou privada. A forma como essa condução é dada é conhecida como processo de gestão de riscos, que “envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos” (ABNT, 2018, p. 9).

Figura 3: Processo de gestão de riscos.

Fonte: ABNT, 2018

Cada atividade da figura acima apresenta ações específicas, mas que geram sinergia no processo de gestão de riscos, de modo que nenhuma deva ser negligenciada.

De acordo com o modelo proposto pelas ISO 31000 (ABNT, 2018) e 31010 (ABNT, 2012), as 6 (seis) macro atividades são definidas da seguinte forma:

1) comunicação e consulta: estabelecimento de uma comunicação e consulta eficazes com as partes interessadas do processo, a fim de facilitar uma melhor definição do contexto e identificação dos riscos, além de garantir que diferentes perspectivas sejam consideradas e que haja aprovação e apoio de todos para um plano de tratamento de riscos. Para Brasiliano (2012), essa atividade também é importante para a realização do “endomarketing”, que são ações de marketing voltadas para o público interno, visando a integração de todas as áreas da organização e a difusão da importância e objetivos da implantação da gestão de riscos. Essa ação estimula o desenvolvimento da cultura de riscos (Pereira, 2014);

2) escopo, contexto e critério: momento em que os objetivos da análise de riscos e o plano para conduzi-la são definidos e acordados entre as partes. São feitos o estabelecimento dos critérios de risco e a definição do escopo das atividades de gestão de riscos. Para a

realização dessa etapa, é necessário definir o contexto externo: como os aspectos culturais, regulatórios, econômicos; o contexto interno: cultura e valores organizacionais, estrutura de governança e de pessoal, objetivos organizacionais, entre outros; e o contexto de gestão de riscos: metodologias do processo de avaliação de riscos, estabelecimento dos critérios de risco, definição da avaliação de desempenho na gestão de riscos, por exemplo;

3) processo de avaliação de riscos: é um processo que engloba a identificação, a análise e a avaliação de riscos. Essa atividade permite compreender os riscos existentes, suas causas, consequências e probabilidades, fornecendo subsídios para a tomada de decisão quanto a necessidade de tratamento do risco, a priorização das opções de tratamento e a maximização de oportunidades;

4) tratamento do risco: envolve as ações voltadas para selecionar opções de respostas aos riscos com vistas a reduzir sua probabilidade, impacto ou ambos. Essa etapa está relacionada também com a implementação dessas ações. De acordo com o *Project Management Institute* (PMI) (2013), existem 4 opções de tratamento de riscos: i) prevenir: ação de eliminar totalmente a ameaça. Um exemplo é a exclusão de uma atividade ou um processo que seja fonte de risco; ii) transferir: é o redirecionamento do risco, e da responsabilidade por seu tratamento, para terceiros (como parceiros e empresas prestadoras de serviços); iii) mitigar: ações são realizadas para reduzir a probabilidade e/ou o impacto do risco, a fim de deixá-lo em um nível aceitável, a exemplo do *backup* de dados críticos, para a proteger contra perda de informações; e iv) aceitar: nessa opção nenhuma medida é tomada para o enfrentamento do risco. Essa estratégia é utilizada quando não há viabilidade técnica ou financeira para tratar o risco.

É uma atividade cíclica, que deve ser revista periodicamente, uma vez que o nível do risco (probabilidade x impacto) pode ser alterado no decorrer do tempo e, assim, exigir nova forma de tratamento;

5) monitoramento e análise crítica: tem por objetivo garantir e aprimorar a qualidade e a eficácia do processo de gestão de riscos. Deve ocorrer de forma contínua, planejada e em todas as etapas do processo; e

6) registro e relato: trata da documentação e do relato de todo o processo de gestão de riscos. Visa a comunicação das atividades e

resultados da gestão de riscos na organização, o fornecimento de informações para embasar a tomada de decisão, o aperfeiçoamento das práticas de gestão de riscos e o auxílio na interação com as partes interessadas.

O COSO (2007, p. 4) também discorre sobre o tema e define o gerenciamento de riscos como:

[...] um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

Esse processo é composto por 8 (oito) componentes, que são inter-relacionados. O modelo de processo de gestão de riscos do COSO é apresentado pela tabela a seguir:

Tabela 3: Componentes do processo de gestão de riscos no COSO 2007.	
Componente	Definição
Ambiente Interno	Compreende o tom de uma organização e fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, inclusive a filosofia de gerenciamento de riscos, o apetite a risco, a integridade e os valores éticos, além do ambiente em que estes estão.
Fixação de Objetivos	Os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização. O gerenciamento de riscos corporativos assegura que a administração disponha de um processo implementado para estabelecer os objetivos que propiciem suporte e estejam alinhados com a missão da organização e sejam compatíveis com o seu apetite a riscos.
Identificação de Eventos	Os eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização devem ser identificados e classificados entre riscos e oportunidades. Essas oportunidades são canalizadas para os processos de estabelecimento de estratégias da administração ou de seus objetivos.
Avaliação de Riscos	Os riscos são analisados, considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser administrados. Esses riscos são avaliados quanto à sua condição de inerentes e residuais.
Resposta a Risco	A administração escolhe as respostas aos riscos - evitando, aceitando, reduzindo ou compartilhando - desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite a risco.
Atividades de Controle	Políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos sejam executadas com eficácia.

Tabela 3: Componentes do processo de gestão de riscos no COSO 2007.

Componente	Definição
Informações e Comunicações	As informações relevantes são identificadas, colhidas e comunicadas de forma e no prazo que permitam que cumpram suas responsabilidades. A comunicação eficaz também ocorre em um sentido mais amplo, fluindo em todos níveis da organização.
Monitoramento	A integridade da gestão de riscos corporativos é monitorada e são feitas as modificações necessárias. O monitoramento é realizado através de atividades gerenciais contínuas ou avaliações independentes ou de ambas as formas.

Fonte: Elaborada pela autora a partir de COSO, 2007, p. 6

2.2 Maturidade em Gestão de Riscos

De acordo com De Bruin et al. (2005), modelos de maturidade são desenhados para avaliar a maturidade (ou seja, competência, capacidade, nível de sofisticação) de um tema determinado, com base em um conjunto mais ou menos abrangente de critérios.

De acordo com Wieczorek-Kosmala (2014, p. 138):

A abordagem estratégica para o gerenciamento de riscos requer que as organizações conduzam adequadamente atividades de gerenciamento de riscos e introduzam práticas adequadas de gerenciamento de riscos, especialmente no nível do conselho administrativo. Para esses fins, os Modelos de Maturidade de Risco são aplicáveis, pois sua ideia e estrutura permitem uma sequência lógica de implementação de avanços no gerenciamento de riscos. Consequentemente, tais modelos podem ser usados para avaliar o estágio atual da implementação e prática de gerenciamento de riscos de uma organização.

2.2.1. RMM – Risk Maturity Model

O *Risk Maturity Model* (RMM) - Modelo de Maturidade de Riscos - foi criado por Hillson (1997), com o objetivo de proporcionar às organizações em geral uma ferramenta de autoanálise em relação à sua gestão de riscos e de identificação de possíveis pontos de melhoria. Foi um dos primeiros modelos criados e, portanto, serviu de base para vários outros modelos mais desenvolvidos (Novais, 2016).

O RMM possui quatro níveis de maturidade: i) ingênuo; ii) principiante; iii) normalizado; e iv) natural. O modelo apresenta quatro atributos a serem analisados: i) cultura; ii) processo; iii) experiência; e iv)



aplicação. A identificação dos atributos dentro de cada nível é apresentada na **Tabela 4**.



Tabela 4: Relacionamento entre níveis e áreas do modelo RMM

	Nível 1 (Simples)	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.

Tabela 4: Relacionamento entre níveis e áreas do modelo RMM				
	Nível 1 (Simples)	Nível 2 (Principiante)	Nível 3 (Normalizado)	Nível 4 (Natural)
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.

Fonte: Hillson, 1997 apud Novais, p. 23, 2016

2.2.2. Modelo do Instituto Brasileiro de Governança Corporativa (IBGC)

O Instituto Brasileiro de Governança Corporativa é uma organização que busca criar e difundir conhecimentos na área de governança corporativa, a fim de influenciar gestores na aplicação de melhores práticas (IBGC, s.d.).

O IBGC produz cadernos de governança corporativa, onde trata de variados assuntos relacionados ao tema. O Caderno 19 é traz informações relativas ao gerenciamento de riscos corporativos.

É nesse caderno que o IBGC (2017) apresenta seu próprio modelo de mensuração de maturidade em gestão de riscos, elencando cinco níveis: i) inicial; ii) fragmentado; iii) definido; iv) consolidado; e v) otimizado.

O instituto entende que há diversas maneiras de se alcançar um nível de maturidade desejado e que cada organização deverá traçar seu caminho de acordo com suas particularidades, como a cultura organizacional.

Nesse modelo são analisadas sete componentes do gerenciamento de riscos corporativos (GRCorp): i) estratégia de GRCorp, ii) governança de GRCorp, iii) política de GRCorp, iv) processo de GRCorp e interação desse processo com os demais ciclos de gestão, v) linguagem de riscos e métodos de avaliação, vi) sistemas, dados e modelos de informação e vii) cultura de GRCorp, comunicação, treinamento, monitoramento (interno e externo) e melhoria contínua.

Assim, o cruzamento dos níveis de maturidade com as dimensões avaliadas se apresenta da seguinte forma:

Tabela 5: Mensurando a maturidade em relação aos componentes de GRCorp

	Estratégia de GRCorp	Governança de GRCorp	Política de GRCorp	Processo de GRCorp	Linguagem de riscos e métodos de avaliação	Sistemas, dados e modelos de informação	Cultura de GRCorp,
Otimizado	<ul style="list-style-type: none"> • Estratégia de gestão de riscos claramente definida, implementada e integrada aos demais ciclos de gestão • As metas de desempenho estão alinhadas com a estratégia e a gestão de riscos. 	<ul style="list-style-type: none"> • Os objetivos estão claramente definidos e alinhados entre as diversas funções da 2ª linha de defesa a fim de prover valor para a organização • O modelo é referência do setor 	<ul style="list-style-type: none"> • Políticas e procedimentos são regularmente referenciados por terceiros e pelo setor. As políticas têm impacto sobre o ambiente de negócios externo 	<ul style="list-style-type: none"> • Os processos de identificação e avaliação de riscos estão bem integrados aos objetivos estratégicos • Atividades de monitoramento eficientes e coordenadas 	<ul style="list-style-type: none"> • Utiliza abordagem padronizada e consistente para definir o apetite e tolerância a riscos • Cenários futuros e testes de stress são usados para explorar a análise dos riscos 	<ul style="list-style-type: none"> • Tecnologias integradas habilitam a organização a gerenciar os riscos e são consideradas altamente efetivas e reconhecidas como práticas líderes pelo mercado 	<ul style="list-style-type: none"> • A cultura de riscos e controles é efetiva em todos os níveis da organização • Programas de disseminação são aplicados para a evolução contínua da gestão de riscos

Tabela 5: Mensurando a maturidade em relação aos componentes de GRCorp

	Estratégia de GRCorp	Governança de GRCorp	Política de GRCorp	Processo de GRCorp	Linguagem de riscos e métodos de avaliação	Sistemas, dados e modelos de informação	Cultura de GRCorp,
Consolidado	<ul style="list-style-type: none"> • Estratégia de gestão de riscos claramente definida e implementada • As metas de desempenho são monitoradas 	<ul style="list-style-type: none"> • As funções da 2ª linha de defesa cobrem de forma abrangente os riscos da organização • A estrutura organizacional está bem definida e alinhada à estratégia e aos objetivos 	<ul style="list-style-type: none"> • Políticas e procedimentos são bem desenvolvidos e aplicados consistentemente em toda a organização • São continuamente atualizados de acordo com as mudanças na estratégia de negócio 	<ul style="list-style-type: none"> • Os processos de identificação e avaliação de riscos estão bem definidos, estruturados • Os gestores de negócio monitoram sistematicamente os riscos associados aos seus processos 	<ul style="list-style-type: none"> • Utiliza abordagem padronizada e consistente para definir o apetite e a tolerância a riscos • Testes de e análise stress de cenários são utilizados em nível corporativo 	<ul style="list-style-type: none"> • Tecnologias emergentes são aproveitadas para permitir que os objetivos de gestão de riscos sejam alcançados em nível corporativo 	<ul style="list-style-type: none"> • A cultura de riscos e controles está inserida nas atividades diárias da organização e os riscos são proativamente tratados nos níveis de processo e de funções
Definido	<ul style="list-style-type: none"> • Estratégia de gestão de riscos claramente definida e implementada • As metas de desempenho são definidas 	<ul style="list-style-type: none"> • As funções da 2ª linha de defesa cobrem os riscos de negócio e direcionadores de valor, podendo haver sobreposições • A estrutura organizacional 	<ul style="list-style-type: none"> • Políticas e procedimentos de GRCorp são formais e comunicadas de forma consistente em toda a organização 	<ul style="list-style-type: none"> • Uma abordagem baseada em riscos é executada de maneira sistemática e consistentemente aplicada em nível corporativo e por toda a 	<ul style="list-style-type: none"> • Há uma abordagem padronizada para definir o nível aceitável de riscos. No entanto, ela não é utilizada por todas as 	<ul style="list-style-type: none"> • Os modelos de informações e de relatórios são bem definidos e compreendidos. Os relatórios são elaborados com informações corretas, completas 	<ul style="list-style-type: none"> • Protocolos claros de comunicação existem e são abertos a todos os empregados. A comunicação de duas mãos com as partes

Tabela 5: Mensurando a maturidade em relação aos componentes de GRCorp

	Estratégia de GRCorp	Governança de GRCorp	Política de GRCorp	Processo de GRCorp	Linguagem de riscos e métodos de avaliação	Sistemas, dados e modelos de informação	Cultura de GRCorp,
		está definida		organização	funções de maneira consistente		interessadas é incentivada.
Fragmentado	<ul style="list-style-type: none"> • A organização sabe por onde começar, mesmo que não tenha claro aonde quer chegar • As metas de desempenho existem 	<ul style="list-style-type: none"> • As funções da 2ª linha de defesa focam em áreas históricas em resposta ao cumprimento das obrigações regulatórias 	<ul style="list-style-type: none"> • Políticas e procedimentos são limitados a áreas direcionadoras-chave 	<ul style="list-style-type: none"> • Os processos de identificação e avaliação de riscos são executados como atividades distintas ou separadas acontecendo sob demanda 	<ul style="list-style-type: none"> • Não há abordagem padronizada para definir o nível aceitável de riscos • Análises qualitativas e quantitativas são realizadas 	<ul style="list-style-type: none"> • Modelos de informações e relatórios são definidos pela alta direção, mas não são compreendidos pela gestão ou alinhados na organização 	<ul style="list-style-type: none"> • Existem comunicações, mas não estão formalmente definidas. • Treinamentos pontuais são realizados
Inicial	<ul style="list-style-type: none"> • A organização não sabe como, quem, quando, onde e por que implementar 	<ul style="list-style-type: none"> • As funções da 2ª linha de defesa são realizadas individualmente, não integradas à visão 	<ul style="list-style-type: none"> • Políticas e procedimentos não estão definidos e não há um processo consistente para seu 	<ul style="list-style-type: none"> • Processos e controles que dão apoio à gestão de riscos são pouco desenvolvidos • Mínimas atividades de 	<ul style="list-style-type: none"> • Não há abordagem padronizada para definir o nível aceitável de riscos 	<ul style="list-style-type: none"> • Modelos de informações e relatórios são direcionados por exigências externas e não são 	<ul style="list-style-type: none"> • Não há um plano de disseminação implementado para formalizar as principais

Tabela 5: Mensurando a maturidade em relação aos componentes de GRCorp

	Estratégia de GRCorp	Governança de GRCorp	Política de GRCorp	Processo de GRCorp	Linguagem de riscos e métodos de avaliação	Sistemas, dados e modelos de informação	Cultura de GRCorp,
	gestão de riscos · As metas de desempenho existem	estratégica.	desenvolvimento e manutenção	monitoramento ocorrem	· Análises qualitativas e quantitativas são realizadas	suficientemente definidos	decisões da companhia em relação às práticas de riscos

Fonte: Ibgc, 2017, p. 36

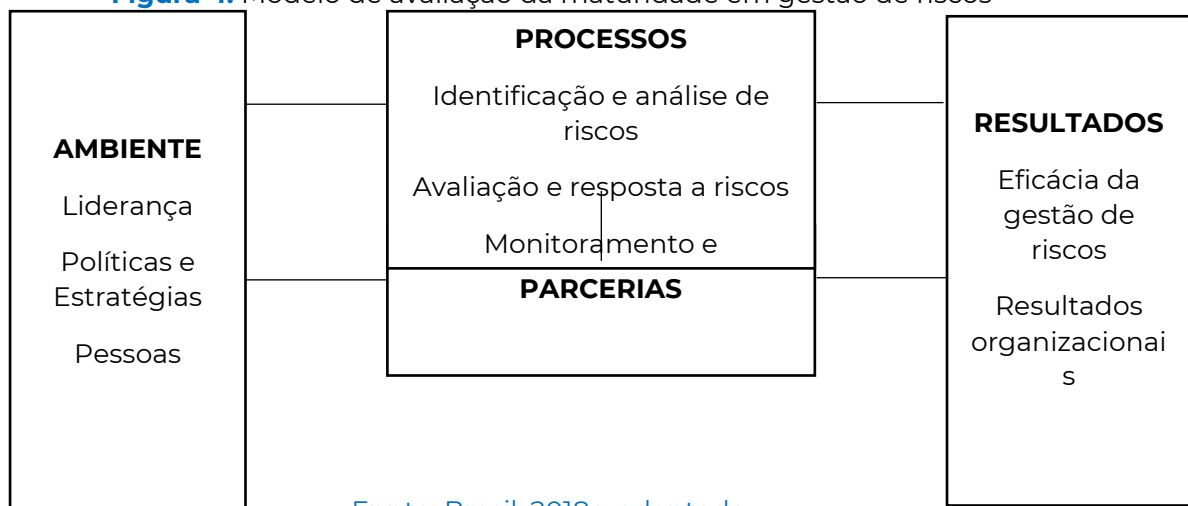
2.2.3 Modelo do Tribunal de Contas da União

O TCU, como órgão de controle externo da União, vem buscando aprimorar suas auditorias na área de gestão de riscos. Nesse sentido, uma das medidas tomadas pelo Tribunal foi a elaboração do Roteiro de Avaliação de Maturidade da Gestão de Riscos, cujo principal objetivo é auxiliar os auditores do setor público na atividade de avaliação da maturidade da gestão de riscos e identificar os pontos que necessitam de aperfeiçoamento, a fim de aprimorar a entrega de produtos e serviços à sociedade (Brasil, 2018c).

O modelo apresentado nesse roteiro é usado pelo TCU para a realização de auditoria de gestão de riscos nos órgãos da administração pública federal. Foi elaborado a partir da avaliação de diversos modelos de gestão de riscos (COSO, ISO 31000 e outros), sendo selecionados os que possuíam uma estrutura sólida de conceitos e a possibilidade de compilação de boas práticas (Brasil, 2012).

O modelo de maturidade do TCU é composto por quatro dimensões, conforme figura abaixo:

Figura 4: Modelo de avaliação da maturidade em gestão de riscos



Fonte: Brasil, 2018c, adaptado.

A dimensão “Ambiente” está relacionada à cultura, à governança de riscos e à consideração dos riscos no momento da elaboração da estratégia e dos objetivos. Busca verificar se há na organização um ambiente propício para a gestão de riscos avaliando três aspectos: (i) liderança, que busca verificar qual o nível de assunção de

responsabilidades da área de governança e da alta administração com a gestão de riscos, buscando alcançar o comprometimento de todos os níveis da organização; (ii) políticas e estratégias: avalia em que grau a organização possui políticas e estratégias de gestão de riscos definidas, divulgada e postas em prática, além de analisar se os riscos são considerados na definição de estratégias, planos e objetivos; e (iii) pessoas: busca avaliar em que nível as pessoas da organização estão informadas e capacitadas para exercerem seus papéis no gerenciamento de riscos.

A dimensão “Processos” trata dos processos de gestão de riscos, buscando identificar em que medida a organização possui processo formal, com métodos e critérios bem definidos para: (i) identificação e análise de riscos, de modo que sejam priorizados os riscos mais significativos para posterior tratamento; (ii) avaliação e resposta a riscos, a fim de analisar se essas atividades são aplicadas de forma consistente para garantir um tratamento adequado aos riscos identificados; e (iii) monitoramento e avaliação, que busca avaliar em que medida essas atividades estão definidas e são aplicadas de forma consistente para assegurar que a gestão de riscos e controles seja eficiente e eficaz.

A dimensão “Parcerias” está relacionada aos arranjos colaborativos estabelecidos entre o órgão avaliado e outras entidades públicas ou privadas. Aborda como os riscos são geridos nessas relações, buscando avaliar se a definição dos riscos e da responsabilidade por cada um deles é feita de forma clara e se há um canal de comunicação estabelecido para tratar o tema entre as partes.

Por fim, na dimensão “Resultados”, é avaliado como as práticas da gestão de riscos trazem resultados eficazes para a melhoria dos processos de governança, dos produtos e serviços entregues à sociedade, da transparência e prestação de contas, além do cumprimento de leis e regulamentos.

Nesse modelo, é possível avaliar o índice de maturidade de cada dimensão ou o índice global, que considera todas as dimensões. Assim:

O cálculo dos índices de maturidade para cada aspecto da gestão de riscos é realizado atribuindo-se quatro pontos para a presença integral e consolidada da prática ou característica de gestão enfocada, um, dois ou três, quando a presença é parcial, de acordo com sua intensidade, e zero ponto à ausência total [...]. No caso de questões que admitem respostas sim/não, atribuiu-se quatro pontos ao 'sim' e zero ponto ao 'não' (Brasil, 2018c, p. 57).

Nas situações em que cada questão se desdobra em itens, cada item vale um número decimal, resultante da divisão da pontuação máxima possível (quatro) pela quantidade de itens, por exemplo: uma questão com 6 itens, cada item recebe no máximo 0,6 pontos (4/6). Desse modo, o índice de cada dimensão é mensurado da seguinte forma:

[...] tomando-se o somatório de pontos do conjunto de questões que a compõe e calculando-se a razão entre a pontuação alcançada e a pontuação máxima possível, expressando esse quociente com um número entre 0% e 100%. Se, por exemplo, uma dimensão obtém 40 pontos de 76 possíveis (19 questões x 4 pontos = 76 pontos), então o índice de maturidade dessa dimensão seria de 52,6% (40/76 x 100) (Brasil, 2018c, p. 58).

O índice de maturidade global é composto pela média ponderada do índice de maturidade das dimensões (IMD), a tabela abaixo apresenta os pesos de cada dimensão e um exemplo de cálculo de índice de maturidade:

Tabela 6: Pesos e exemplo de cálculo do índice de maturidade				
DIMENSÃO	PESO	EXEMPLO		
		IMD	PESO	PONDERADO
Ambiente	40	52,6	0,4	21,0
Processos	30	45,9	0,3	13,8
Parcerias	10	80,1	0,1	8,0
Resultados	20	49,5	0,2	9,9
ÍNDICE DE MATURIDADE GLOBAL				52,7

Fonte: Brasil, 2018c.

O resultado obtido no índice de maturidade global pode ser enquadrado em 5 níveis de maturidade:

Tabela 7: Níveis de maturidade da gestão de riscos	
ÍNDICE DE MATURIDADE APURADO	NÍVEL DE MATURIDADE
De 0% a 20%	Inicial
De 20,1 a 40%	Básico
De 40,1% a 60%	Intermediário
De 60,1% a 80%	Aprimorado
De 80,1% a 100%	Avançado

Fonte: Brasil, 2018c, adaptado.



3

3

**GESTÃO DE RISCOS NO EXÉRCITO
BRASILEIRO**

Ao longo dos anos, a administração pública passou por diversos paradigmas até chegar ao da governança pública, que deu maior atenção à colaboração e coordenação entre os órgãos públicos, bem como entre esses órgãos e a sociedade (Neves; Guimarães; Júnior, 2017). No Brasil, o Decreto nº 9.203, de 22 de novembro de 2017, definiu governança pública como um “conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade” (Brasil, 2017a, art. 2º, inciso I).

Em 2016, surgiu a Instrução Normativa Conjunta nº 01, do então Ministério do Planejamento, Orçamento e Gestão e da Controladoria-Geral da União, que estabeleceu que órgãos e entidades do Poder Executivo Federal deveriam sistematizar suas ações relacionadas à gestão de riscos, aos controles internos e à governança (Brasil, 2016).

Nesse momento, a necessidade de metodizar o gerenciamento de riscos se materializa de forma amplamente impositiva no âmbito do Poder Executivo Federal, o que, até então, era feito pontualmente por Acórdãos do Tribunal de Contas da União, como os acórdãos 1517/2010 e 1739/2015, descritos na “subseção 1.1”.

O próprio TCU aprovou a Resolução nº 287, de 12 de abril de 2017 (Brasil, 2017b), que dispõe sobre sua política de gestão de riscos.

Analisando as políticas de outros órgãos como Exército Brasileiro (BRASIL, 2018a), Instituto Nacional do Seguro Social (INSS) (Brasil, 2020c) e Agência Nacional de Saúde Suplementar (ANS) (Brasil, 2022b), elas se apresentam de forma muito semelhante à do Tribunal de Contas da União, principalmente no que tange às etapas do processo de gerenciamento. Essa similaridade se justifica, possivelmente, pelo fato de todos esses órgãos usarem como base modelos de referência internacional na gestão de riscos, sendo notável especial semelhança ao modelo proposto pela ISO 31000.

Para o TCU (Brasil, 2017b), e para os órgãos do Poder Executivo que acompanham a metodologia ISO, o processo de gerenciamento de riscos se divide em 8 etapas:

1) estabelecimento do contexto: momento em que são analisados os ambientes internos e externos no qual se insere a organização;

2) identificação do risco: percepção e descrição de um risco, bem como de suas possíveis fontes, causas e consequências;

3) análise do risco: determinação do nível do risco, geralmente calculado pelo produto da sua probabilidade e de seu impacto;

4) avaliação do risco: comparação do nível do risco com o apetite ao risco da instituição, a fim de verificar se o risco é aceitável;

5) tratamento do risco: definição e execução das ações que visam reduzir o nível do risco;

6) monitoramento: acompanhamento da situação do risco a ser gerido, assim como a análise da efetividade das ações implementadas na etapa anterior;

7) comunicação e consulta: identificação das partes interessadas no processo de gerenciamento de riscos e estabelecimento de uma comunicação efetiva com essas partes; e

8) melhoria contínua: ajuste continuado de aspectos da gestão de riscos com base nos achados da etapa de monitoramento.

O Exército Brasileiro (EB) elaborou, em 2017, a 1ª edição da Política de Gestão de Riscos do Exército Brasileiro, que foi revogada pela 2ª edição, em 2018 (Brasil, 2018a). Essa política procurou sistematizar o tema dentro do âmbito da Força Terrestre através da exposição de conceitos, princípios, estruturação da governança, gestão de riscos e controles internos da gestão, competências, responsabilidades e diretrizes.

Ela tem como referência metodológica a ISO 31000, que definiu gestão de riscos como um “processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração e pelos demais gestores, aplicável em todos os escalões que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que

possam afetar a organização” (Brasil, 2018a, art. 3º, inciso III) e risco como “possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos institucionais estabelecidos. O risco é medido em termos de probabilidade e impacto”. (Brasil, 2018a, art. 3º, inciso VI).

A Política de Gestão de Riscos do Exército, também apresenta a sua estrutura de governança, gestão de riscos e controles internos da gestão, sendo ela hierarquicamente composta por:

- 1) Alto Comando do Exército (ACE): responsável por propor a atualização da Política de Gestão de Riscos, analisar assuntos relevantes sobre a gestão de riscos, propor os níveis adequados de exposição aos riscos e deliberar sobre matérias apresentadas pelo Comitê de Governança, Riscos e Controles do Exército;
- 2) Comitê de Governança, Riscos e Controles do Exército (CGRiCEX): responsável por propor melhorias e disseminar uma cultura unificada no que tange à governança, à gestão de riscos e aos controles internos, propor matérias a serem deliberadas pelo ACE e coordenar as atividades de implantação e desenvolvimento da gestão de riscos e controles internos;
- 3) Escritório de Gestão de Riscos e Controles do Exército (EGRiCEX): responsável por apoiar o CGRiCEX em suas atividades, coordenar a atualização da metodologia de gestão de riscos, conduzir o processo de implantação da gestão de riscos, supervisionar as atividades das Assessorias de Gestão de Riscos e Controles e coordenar as ações de comunicação e monitoramento da gestão de riscos, assessorar o CGRiCEX;
- 4) Assessorias de Gestão de Riscos e Controles (AGRiC): responsáveis por implementar, operacionalizar e gerenciar as atividades relacionadas à gestão de riscos de sua organização militar; e
- 5) Proprietários de Riscos e Controles (PRisC): responsáveis pela execução das atividades que envolvam a gestão dos riscos sob sua responsabilidade.

A Política de Gestão de Riscos do Exército trata o tema de forma macro, estabelecendo conceitos, orientações e responsabilidades gerais.

Para detalhar as orientações contidas na Política, o EB instituiu a Diretriz Reguladora da Política de Gestão de Riscos (Brasil, 2019c), tendo como referências, além de normativos internos e do governo federal, o COSO ERM e a ISO 31000. Entre outras coisas, ela trata da classificação dos riscos no âmbito do Exército, sendo eles divididos em (i) estratégicos, que estão diretamente relacionados aos eventos que possam dificultar ou impossibilitar o alcance dos objetivos estabelecidos no Plano Estratégico do Exército (PEEx); (ii) operativos, que estão relacionados aos eventos que possam dificultar ou impedir a execução das atividades de natureza eminentemente militar; (iii) gestão interna, que estão voltados para os eventos que possam comprometer as atividades administrativas das OM; e (iv) integridade, que são os eventos relacionados a ações ou omissões propositais possibilitando a ocorrência de fraudes e atos de corrupção. Os riscos de integridade são tratados com mais detalhe no Programa de Integridade do Exército Brasileiro (Brasil, 2018b).

Percebe-se uma lacuna em relação a classificação explícita de alguns riscos geridos por organizações técnico-normativas dentro do Exército, uma vez que muitas delas não executam atividades eminentemente militares (segurança orgânica, preparo e emprego) – riscos operativos - e ao mesmo vão além da gestão de atividades administrativas internas – riscos de gestão interna.

A DAP, por exemplo, não gere apenas o pessoal de sua OM, mas sim os veteranos e servidores civis de todo o EB. Desse modo, seus riscos não podem ser classificados nem como operativos, tampouco como gestão interna.

Percebendo essa possível lacuna, a diretriz reguladora diz que “As Entidades Vinculadas poderão adotar ainda outros riscos de acordo com as suas especificidades” (Brasil, 2019c, art. 5º, § 1º). Cabe ressaltar que é possível o enquadramento dos riscos das OM técnico-normativas em estratégicos (caso sua atividade esteja listada no Plano Estratégico do Exército) e em riscos de integridade.

Para gerenciar todos esses riscos, a diretriz reguladora apresenta um modelo de linhas de defesa, cujo objetivo é estabelecer o diálogo entre as partes envolvidas no gerenciamento de riscos e controles,

garantindo que as competências e responsabilidades fundamentais estejam claramente definidas. As linhas de defesa estabelecidas são:

Art. 13. [...]

I - 1ª Linha: os PRisC das OM, apoiados pelas EGRiC, quando estabelecidas, e supervisionadas pelas AGRiC;

II - 2ª Linha:

a) o Escalão Superior, de acordo com o canal de comando, será a 2ª Linha para suas organizações militares diretamente subordinadas (OMDS); e

b) as OM em que, pelo canal técnico, haja subordinação em assuntos específicos.

III - 3ª Linha: o Centro de Controle Interno do Exército (CCIEEx) e as Inspetorias de Contabilidade e Finanças do Exército (ICFEx).

§ 1º Todas as OM são a 1ª Linha de Defesa de seus próprios processos. [...] (Brasil, 2019c).

Outro documento relevante é o Manual Técnico da Metodologia de Gestão de Riscos do Exército Brasileiro, que apresenta detalhadamente as ações e ferramentas para a aplicação prática da gestão de riscos no Exército, além de direcionar a identificação, a avaliação, o tratamento, o monitoramento e a comunicação dos riscos institucionais (Brasil, 2017). Nele encontram-se elencadas as seguintes opções de tratamento de riscos:

I - aceitar: não adoção de medidas para reduzir a probabilidade ou impacto do risco;

II - compartilhar: redução da probabilidade ou do impacto do risco pela transferência ou compartilhamento de uma porção do risco;

III - evitar: não execução das atividades que geram riscos; e

IV - mitigar: adoção de medidas visando a reduzir a probabilidade, o impacto dos riscos ou ambos. (Brasil, 2017, p. 8).

A avaliação da maturidade é vista pela diretriz “como parâmetro para identificação das áreas vulneráveis que possam dificultar ou comprometer o atingimento dos objetivos da OM” (Brasil, 2019c, art. 18).

Embora o Exército tenha percebido a relevância da mensuração do nível de maturidade, ele não elaborou uma metodologia para sua execução, citando apenas que será realizada através de uma autoavaliação da gestão organizacional do EB.

O manual técnico, que traz mais detalhadamente os instrumentos de operacionalização da gestão de riscos no Exército, não definiu um modelo de “autoavaliação”, tampouco foram encontrados



modelos, ainda que informais, que atestassem a prática de avaliação da maturidade em gestão de riscos na instituição.





4

4

METODOLOGIA

Segundo Bloise (2020), a metodologia estrutura a pesquisa, definindo as etapas a serem seguidas para alcançar os objetivos desejados. Ainda de acordo com a autora, a escolha da metodologia define o tipo de pesquisa a ser realizada e o percurso que essa pesquisa seguirá até sua conclusão, incluindo os instrumentos utilizados e a forma como os dados de estudo serão coletados.

Desse modo, a fim de responder o problema de pesquisa “Qual o nível de maturidade da gestão de riscos da Diretoria de Assistência ao Pessoal do Exército Brasileiro a partir da metodologia de mensuração do Tribunal de Contas da União?”, foi realizada uma pesquisa de natureza descritiva e de abordagem qualitativa.

Em relação a coleta de dados, a mesma teve como objetivo avaliar cada uma das quatro dimensões que compõem modelo de maturidade de gestão de riscos do TCU, sendo elas: Ambiente, Processos, Parcerias e Resultados. A dimensão Ambiente se divide em Liderança, Políticas e Estratégias e Pessoas; a dimensão Processos se divide em Identificação e Análise de riscos, Avaliação e Resposta a riscos e Monitoramento e Comunicação; e a dimensão Resultados se divide em Eficácia da gestão de riscos e Resultados organizacionais.

Para isso, foi aplicado, por meio da ferramenta JotForms, o questionário constante no anexo A. O questionário é o mesmo usado pelo TCU no Acórdão 2467/2013 (Brasil, 2013), com as seguintes adaptações:

- a) na “parte A”: i) para a questão 6, além das opções de resposta “sim” e “não”, foi incluída a opção “não sei”. Essa opção recebeu a mesma pontuação da resposta “não”; e ii) a questão 7 foi verificada através de pesquisa documental;
- b) na “parte B”, o modelo do TCU descreve apenas as escalas das pontas (1 e 5), não descrevendo as escalas intermediárias (2 a 4). Para facilitar o entendimento dos respondentes, as descrições para as escalas intermediárias foram criadas pela autora; e

- c) a “parte C” não compôs o questionário enviado aos membros da gestão de riscos da diretoria, uma vez que trata de aspecto muito específico que poucos respondentes teriam conhecimento. Dessa forma, as respostas desta parte do questionário foram coletadas exclusivamente com o gestor da parceria firmada pela DAP.

O questionário foi destinado aos integrantes da gestão de riscos da diretoria e ao gestor de parcerias, compondo um universo de 37 servidores (militares e civis), classificados da seguinte forma:

- a) membros da assessoria de gestão de riscos e controles (AGRIC) - 2 servidores: são responsáveis pela definição, coordenação, orientação e consolidação de dados e atividades relacionadas à gestão de riscos na diretoria;
- b) membros da equipe de gestão de riscos e controles (EGRIC) – 9 servidores: formada por todos os chefes das seções que possuem riscos formalmente identificados. São responsáveis por coordenar a gestão de riscos dentro de sua seção e reportar à AGRIC qualquer evento sobre o tema;
- c) proprietários de riscos e controles (PRisC) – 25 servidores: são os executores dos processos que possuem riscos formalmente identificados. São responsáveis por identificar, avaliar, propor tratamento e monitorar seus riscos; e
- d) gestor de parcerias - 1 servidor: responsável por gerir as parcerias existentes na sua área finalística. Embora o gestor de parcerias não componha a gestão de riscos da diretoria, ele foi selecionado para responder a parte “C” do questionário, uma vez que a DAP não possui um PRisC definido para a parceria existente.

O questionário possui quatro partes, equivalentes às dimensões em análise, e a quantidade de perguntas dentro de cada dimensão é composta da seguinte forma:

Tabela 8: Quantidade de perguntas por dimensão	
Dimensão	Quantidade de Perguntas
Ambiente de gestão de riscos	19
Liderança	5
Políticas e estratégias	6

Pessoas	8
Processos de gestão de riscos	19
Identificação e avaliação de riscos	8
Respostas a riscos	6
Monitoramento e comunicação	5
Gestão de riscos em parcerias	9
Resultados	9
Total	55

Fonte: Brasil, 2013.

As perguntas referentes às dimensões Ambiente, Parcerias e Resultados foram respondidas em uma escala de concordância de cinco pontos, conforme tabela abaixo, exceto as perguntas de número 6 e 7 da dimensão “Ambiente”, que possuem apenas a opção de resposta sim/não. A pergunta número 7 foi comprovada através de análise documental.

Tabela 9: Escala de resposta para perguntas de Ambiente, Parcerias e Resultados				
1	2	3	4	5
Discordo totalmente	Discordo mais do que concordo	Não concordo Nem concordo	Concordo mais do que discordo	Concordo totalmente

Fonte: Brasil, 2013.

As perguntas referentes à dimensão “Processos” foram respondidas também em uma escala de 1 a 5 (tabela 7), com as seguintes definições para cada escala:

Tabela 10: Escala de resposta para perguntas de Processos				
1	2	3	4	5
Prática inexistente na instituição	Prática raramente realizada na instituição	Prática às vezes realizada na instituição	Prática frequentemente realizada na instituição	Prática sistemática plenamente incorporada à cultura

Fonte: Brasil, 2013.

Assim, para efeito de cálculo do índice de maturidade, foi adotado uma correspondência de pontuação para cada nível das escalas apresentadas anteriormente, onde as primeiras opções de respostas (“discordo totalmente” ou “prática inexistente na instituição”) receberão pontuação zero, por representar completa ausência da prática, e as últimas opções (“concordo totalmente” ou “prática

sistemática plenamente incorporada à cultura”) receberão pontuação 4. Em relação às perguntas que admitem resposta sim/não, foram atribuídos 0 pontos para “não” e 4 pontos para “sim”.

Tabela 11: Critério de correspondência das escalas	
Ponto da escala	Pontuação correspondente
1, “não” ou “não sei”	0
2 ou “em partes”	1
3	2
4	3
5 ou “sim”	4

Fonte: Brasil, 2013.

O índice de maturidade de cada dimensão será definido pela razão entre a pontuação obtida nas respostas de cada questão da dimensão e a pontuação máxima possível, sendo o resultado apresentado em porcentagem (de 0% a 100%).

Nas situações em que cada questão se desdobra em itens, cada item vale um número decimal, resultante da divisão da pontuação máxima possível (quatro) pela quantidade de itens, por exemplo: uma questão com 6 itens, cada item recebe no máximo 0,6 pontos (4/6). A questão 9 da parte D do questionário, embora seja uma questão com subitens, cada subitem terá a pontuação máxima de 4 pontos, uma vez que a pergunta foi dividida em subitens apenas para evitar a repetição do enunciado da questão.

Tendo em vista que o questionário foi aplicado a diversos respondentes, o resultado foi obtido por média simples. Na questão 1 da parte C, a pontuação é obtida através da média aritmética dos pontos atribuídos à existência de gestão de conjunta de riscos nas parcerias, considerando quatro pontos para a opção “sim”, dois pontos para a opção “em parte” e nenhum ponto para a opção “não”.

Após a obtenção do nível de maturidade dentro de cada dimensão, o nível global será calculado utilizando a média ponderada desses níveis, com base nos pesos atribuídos na **Tabela 6**. Assim, o resultado alcançado foi classificado de acordo com a **Tabela 7**.

Além do questionário, foi realizada uma verificação documental nos arquivos físicos e digitais da DAP conforme critérios a seguir:

Tabela 12: Documentos verificados

Documento verificado	Objetivo da verificação
Regulamento da diretoria	Compreender a missão e a estrutura organizacional da DAP.
Política de gestão de riscos do Exército	Responder à questão 7 da parte “A” (Ambiente) do questionário e compreender como a gestão de riscos é feita no Exército.
Diretriz da política de gestão de riscos do Exército	Responder à questão 7 da parte “A” do questionário e compreender como a gestão de riscos é feita no Exército.
Manual técnico da metodologia da gestão de riscos no Exército	Responder à questão 7 da parte “A” do questionário, compreender como a gestão de riscos é feita no Exército e complementar as respostas obtidas na parte “B” (Processos) do questionário.
Plano de gestão de riscos da DAP	Compreender a estrutura da gestão de riscos na DAP.
Matrizes de riscos	Verificar os tipos de riscos geridos pela DAP e complementar as respostas obtidas na parte “B” do questionário.
Relatório anual de gestão de riscos	Complementar as respostas obtidas na parte “D” (Resultados) do questionário.
Acordo de cooperação – DAP/ANDE-Brasil	Complementar as respostas obtidas na parte “C” (Parcerias) do questionário.

Fonte: Elaborada pela autora, 2024

De forma complementar, para subsidiar o entendimento sobre a gestão de riscos na DAP, foi realizada uma entrevista com um dos membros da AGRiC, conforme perguntas constantes no “Anexo B”.

A escolha do membro entrevistado foi feita levando em consideração a posição de chefia, pois essa proporciona uma visão mais ampla da gestão de riscos na diretoria. As perguntas foram selecionadas visando obter respostas não proporcionadas pelo questionário e pela verificação documental, além de ratificar ou retificar as respostas já obtidas.

Os dados coletados utilizando os instrumentos propostos foram quantificados e confrontados os resultados com os critérios estabelecidos no Roteiro de Avaliação de Maturidade do TCU (Brasil, 2018c), a fim de calcular o nível de maturidade global de gestão de riscos da DAP.



5

5

A GESTÃO DE RISCOS NA DAP

Para compreender o histórico, a estrutura e a dinâmica da gestão de riscos na DAP, foram realizadas análise documental no acervo de gestão de riscos da diretoria e entrevista com um dos membros da assessoria de gestão de riscos e controles (AGRiC).

Constatou-se que a diretoria iniciou suas práticas de gestão de riscos, formalmente, em 2020, data de seu primeiro plano de gestão de riscos, atualmente em sua 3ª edição. Esse documento busca regular e orientar a gestão de riscos dentro da DAP, apresentando sua estrutura e as competências de cada integrante, conforme tabela a seguir:

Tabela 13: Estrutura e competências na gestão de riscos da DAP

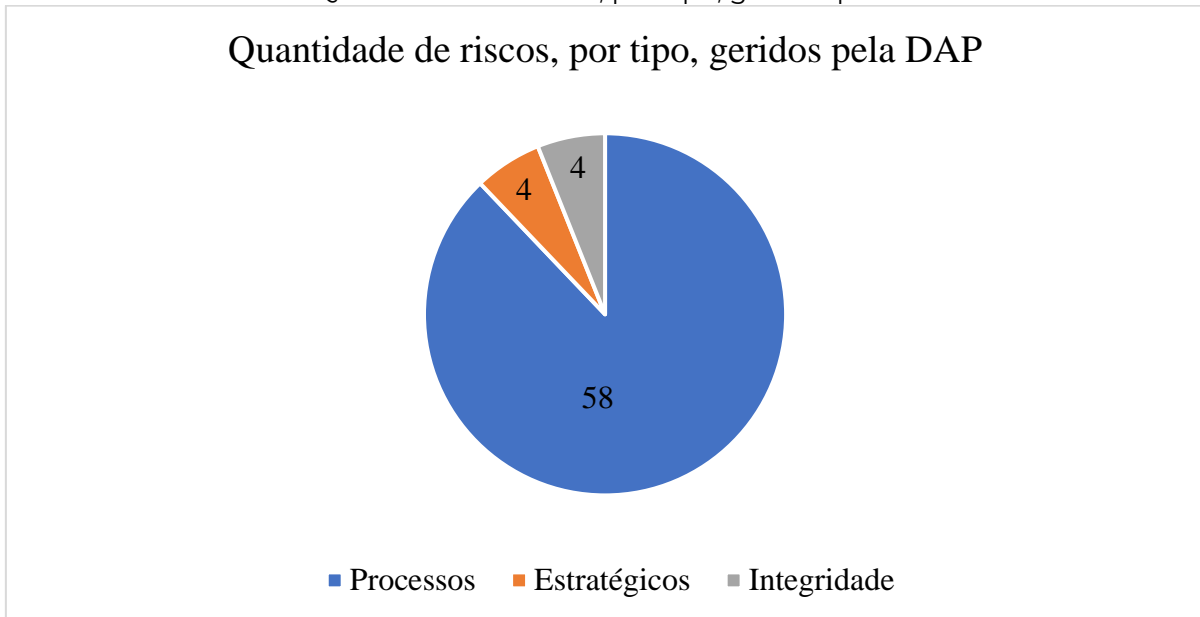
Estrutura	Composição	Competências
Assessoria de gestão de riscos e controles (AGRIC)	1) Chefe: chefe da subseção de gestão organizacional e capacitação da seção de planejamento, orçamento e gestão (SPOG); e 2) adjunto: oficial da subseção de gestão organizacional e capacitação da SPOG.	1) Assegurar que os riscos sejam gerenciados de acordo com a metodologia para a gestão de riscos do Exército Brasileiro; 2) implantar, monitorar, supervisionar e, quando for o caso, atualizar o plano de gestão de riscos; 3) orientar os proprietários de riscos e controles (PRisC) na identificação, avaliação, tratamento e monitoramento dos riscos inerentes às suas atividades; 4) monitorar e propor o aperfeiçoamento dos controles internos da gestão; 5) realizar, reuniões de análise da gestão de riscos, de acordo com o cronograma estabelecido no plano de gestão de riscos; 6) contribuir para a atualização do portfólio de riscos prioritários do Departamento-Geral do Pessoal (DGP); 7) estabelecer indicadores de desempenho de gerenciamento de riscos alinhados com a legislação em vigor; 8) supervisionar os trabalhos da EGRiC e dos PRisC; e 10) encaminhar à AGRiC do DGP o relatório anual da gestão de riscos, as atas das reuniões trimestrais de análise de riscos, o portfólio de riscos estratégicos e o portfólio de riscos prioritários da DAP.
Equipe de gestão de riscos e controles (EGRiC)	1) Chefe da seção de assistência social; 2) chefe da seção de veteranos e pensionistas; 3) chefe da seção de licença especial; 4) chefe da seção de pessoal civil; 5) chefe da assessoria de correição de servidores civis; 6) chefe da seção de apoio administrativo; 7) chefe da assessoria de apoio para assuntos jurídicos; 8) chefe da seção de planejamento orçamento e gestão; e 9) chefe do serviço de assistência religiosa.	1) Supervisionar todos os trabalhos dos PRisC; 2) coordenar o gerenciamento de riscos da sua seção; 3) coordenar o brainstorming para identificação de novos riscos; 4) garantir que o monitoramento e o tratamento dos riscos estão sendo efetivamente realizados; e 5) compilar e validar as informações contidas nas matrizes de riscos da sua seção.
Proprietários de Riscos e Controles	Todos os militares e servidores civis com responsabilidade e autoridade para	1) Identificar, avaliar, tratar e monitorar os riscos inerentes às suas atividades, de acordo com as normas em vigor, levando em consideração a probabilidade de

Tabela 13: Estrutura e competências na gestão de riscos da DAP		
Estrutura	Composição	Competências
(PRisC)	gerenciar um risco. (A designação dos PRisC é publicada em aditamento interno, com atualização periódica).	<p>ocorrência e o impacto nos objetivos;</p> <p>2) monitorar os riscos ao longo do tempo, de modo a garantir que as respostas adotadas resultem na sua manutenção em níveis adequados;</p> <p>3) implementar os planos de ação definidos para tratamento dos riscos sob sua responsabilidade;</p> <p>4) garantir que as informações sobre os riscos estejam disponíveis em todos os níveis da organização, considerando seu respectivo sigilo;</p> <p>5) operacionalizar e aperfeiçoar os controles internos da gestão;</p> <p>6) identificar e comunicar ao membro da EGRiC da sua seção as necessidades de melhoria da gestão de riscos e de controles internos sob sua responsabilidade; e</p> <p>7) preencher e manter atualizada a sua matriz de riscos.</p>

Fonte: elaborado pela autora a partir do Plano de Gestão de Riscos da DAP, 3ª edição, 2023.

Segundo o membro da AGRiC entrevistado, os tipos de riscos geridos pela DAP são de processos, projetos (quando existentes), integridade e riscos estratégicos, sendo percebido, por ele, uma ênfase maior nos riscos de processos e riscos estratégicos. No momento, não há projetos em andamento na diretoria, a quantidade dos demais tipos de riscos está dividida da seguinte forma:

Gráfico 1: Quantidade de riscos, por tipo, geridos pela DAP



.Fonte: Elaborado pela autora, 2024.

Os riscos de processos estão ligados à execução de uma atividade dentro de um processo realizado pela diretoria, como a concessão indevida de direitos e danos ao erário/usuário por erro de cálculo de benefícios; os riscos de integridade estão relacionados às ações ou omissões propositais, possibilitando a ocorrência de fraudes e atos de corrupção, a exemplo de fraudes nos processos de habilitação à pensão ou concessão de reforma; e os riscos estratégicos são aqueles que afetam diretamente um objetivo estratégico da diretoria. Os riscos estratégicos, por determinação do comando, não podem ser divulgados.

Para todos os riscos identificados existe uma matriz de riscos e um plano de ação, esses documentos apresentam dados sobre (i) a identificação do risco: nome do risco, o processo ou macroprocesso e o objetivo organizacional ao qual está vinculado; (ii) a avaliação dos riscos: a vulnerabilidade que propicia a ocorrência do evento, sua

consequência, sua probabilidade e seu impacto; (iii) o tratamento do risco: tipo de ação sobre o risco (mitigar, aceitar, compartilhar ou evitar); (iv) as atividades de controle: definição do controle preventivo (ação para reduzir a probabilidade de ocorrência do evento), definição do controle detectivo (como será detectada a ocorrência do evento) e o plano de contingência (ação para reduzir o impacto do evento já ocorrido). As atividades listadas nessa etapa geram um plano de ação, no modelo 5W2H; e (v) o monitoramento: sendo essa parte da matriz a menos detalhada, informando apenas se os controles foram efetivos ou não (porém sem um parâmetro definido) e o nível de risco residual, aquele calculado após a implementação dos controles.

Em relação ao monitoramento, foi destacada a existência de reuniões periódicas para discutir a eficácia dos controles e planos estabelecidos. Foi informado que está em fase de implementação um sistema informatizado de gestão (SIG-DAP), onde os PRisC lançam mensalmente os eventos de riscos concretizados e a eficácia dos controles e planos de contingência. O sistema será alimentado em todas as fases do processo de gestão de riscos, a fim de integrar as atividades de gestão da diretoria, facilitar o monitoramento dessas atividades e a extração de indicadores.

Ainda de acordo com o entrevistado, a alta administração participa ativamente da gestão de riscos. O diretor emite orientações quanto aos riscos que devem ser priorizados e contribui na definição dos riscos estratégicos, além disso, participa de reuniões com o escalão superior e é o responsável por emitir o relatório anual de gestão de riscos da diretoria.

Entretanto, embora haja envolvimento da alta administração e as funções sejam formalmente definidas nos demais níveis da diretoria, o entrevistado pontua que ainda não há uma cultura sólida de gestão de riscos na DAP, mas que todos os esforços realizados nos últimos anos e os esforços atuais têm contribuído para que essa cultura seja alimentada na diretoria



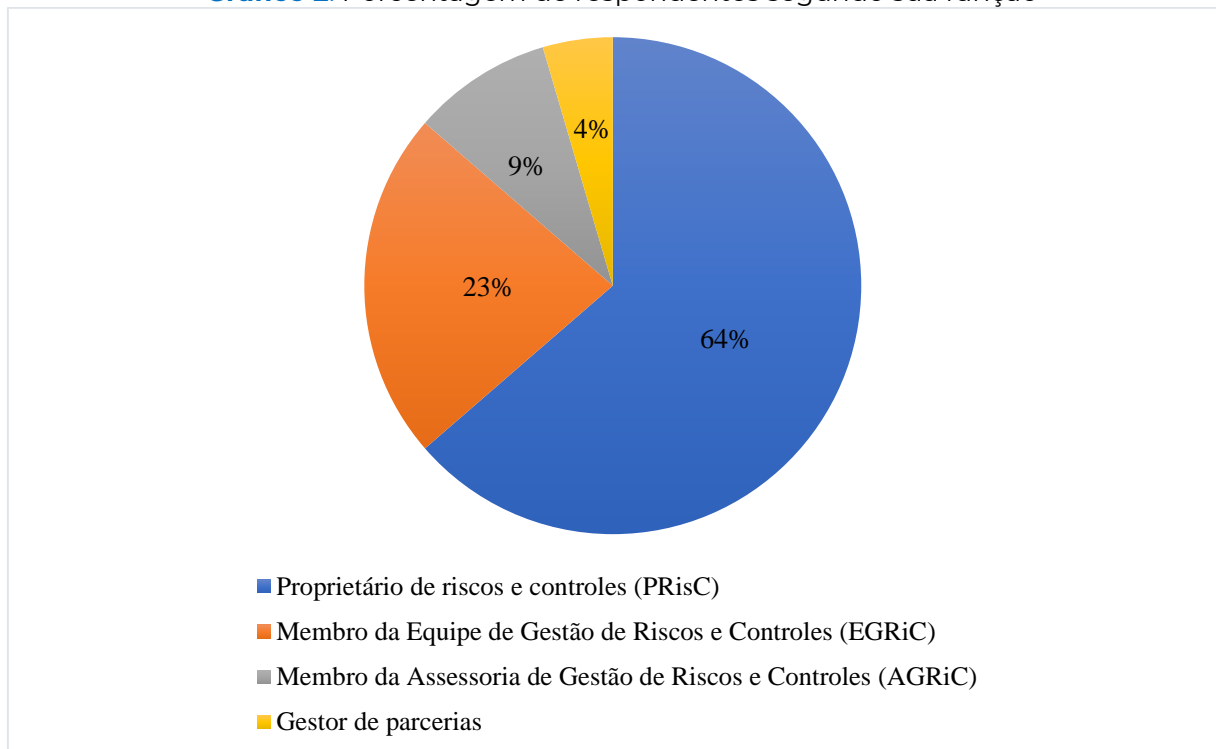
6

6

RESULTADOS E DISCUSSÕES

O questionário para avaliar o índice de maturidade das dimensões (IMD) e o índice de maturidade global (IMG) foi destinado a 37 servidores, sendo obtidas 22 respostas, conforme distribuição a seguir:

Gráfico 2: Porcentagem de respondentes segundo sua função

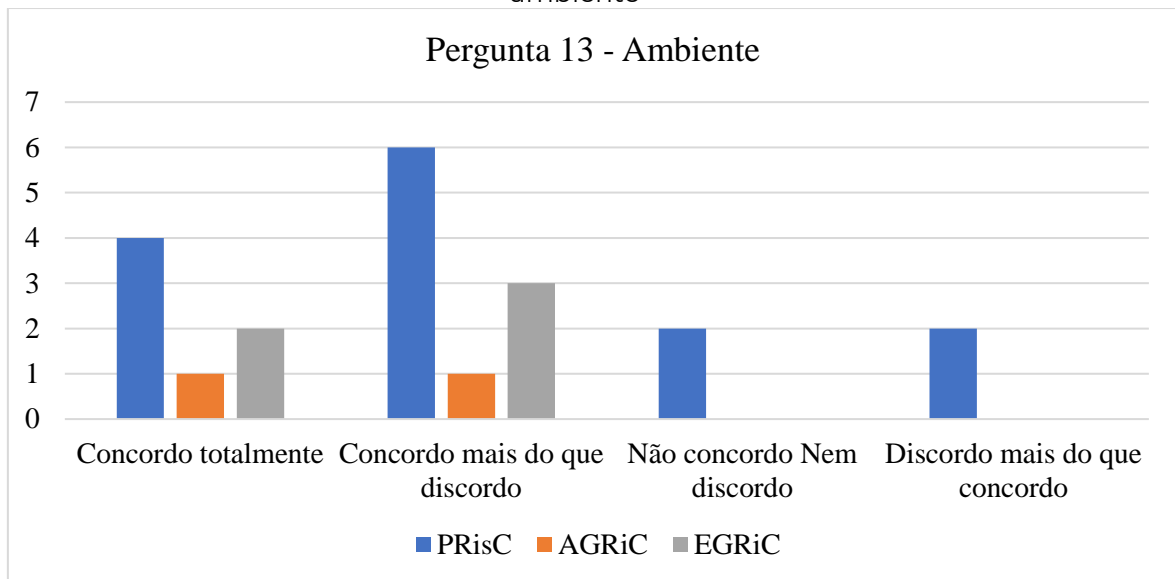


Fonte: Elaborado pela autora, 2024

A primeira dimensão avaliada foi “ambiente”, que está relacionada à cultura, à governança e à consideração dos riscos no momento da elaboração da estratégia e dos objetivos. Nessa dimensão, 19 perguntas foram realizadas, cada uma valendo 4 pontos, sendo que a questão 7, que trata da composição da política de gestão de riscos, foi avaliada exclusivamente através de análise documental.

A pergunta 13, “os servidores conhecem os principais riscos enfrentados por suas unidades?”, recebeu a menor pontuação média da dimensão, 2,85 pontos. As 21 respostas obtidas para essa questão estão distribuídas da seguinte forma:

Gráfico 3: Relação quantidade de respostas x respondentes, questão 13 - ambiente

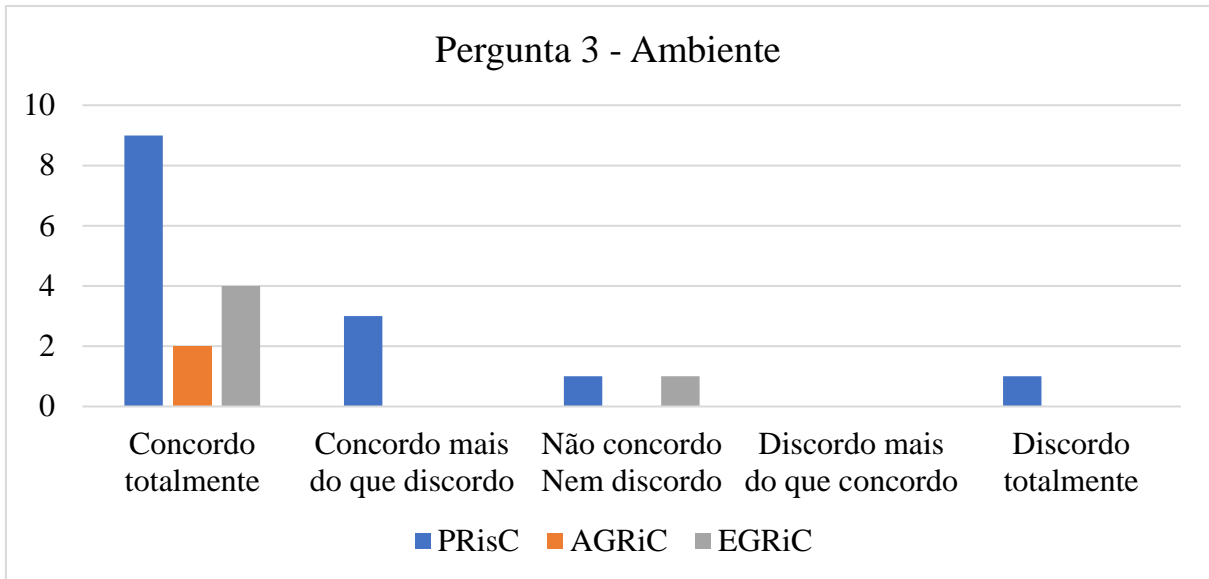


Fonte: Elaborado pela autora, 2024.

Observa-se que nos níveis mais altos da administração (membros da AGRiC e da EGRiC) as repostas foram mais positivas, esse resultado pode ser justificado pelo fato de que esses membros possuem uma visão mais holística dos riscos, devido às suas posições hierárquicas e suas funções, que englobam a consolidação de informações, enquanto os PRisC tendem a focar mais nos seus próprios riscos, tendo menor conhecimento sobre os riscos geridos por outros PRisC.

As perguntas que obtiveram maior pontuação média na dimensão “ambiente” foram a 3, com 3,4 pontos; a 6, com 3,6 pontos; e a 7, com 3,42 pontos. Com a repostas distribuídas conforme gráficos a seguir.

Gráfico 4: Relação quantidade de respostas x respondentes, questão 3 - ambiente.



Fonte: Elaborado pela autora, 2024.

Cerca de 86% dos respondentes selecionaram as opções “concordo totalmente” e “concordo mais do que discordo” para a pergunta 3, “A alta administração considera os riscos-chave que podem comprometer o alcance dos principais objetivos organizacionais e fornece direção clara para que eles sejam gerenciados?”, mostrando a percepção de que a alta administração da DAP se preocupa com os riscos-chave da organização, aqueles que podem impactar diretamente nos objetivos organizacionais, além disso, orienta os PRisC de forma clara sobre como gerenciá-los.

Na pergunta 6, “Existe uma política corporativa de gestão de riscos aprovada pela alta administração?”, 90% dos respondentes afirmaram existir uma política, enquanto 10% alegaram não saber se existe ou afirmaram não existir.

A verificação documental confirmou a existência da Política de Gestão de Riscos do Exército Brasileiro (Brasil, 2018a) e partir dela, juntamente com a Diretriz Reguladora da Política de Gestão de Riscos do Exército (Brasil, 2019c) e o Manual Técnico da Metodologia de Gestão de Riscos do Exército Brasileiro (Brasil, 2017), foram respondidos os 7 itens da questão 7. A tabela a seguir apresenta o item avaliado na questão e o enquadramento normativo na política, na diretriz ou no manual.

Tabela 14: Enquadramento normativo, questão 7 – ambiente.

Caso exista uma política corporativa de gestão de risco, indicar se ela aborda os seguintes aspectos:	Enquadramento normativo
a) Objetivos organizacionais com relação à gestão de riscos.	Política de gestão de riscos – art. 5º
b) Integração da gestão de riscos a processos e políticas organizacionais.	Política de gestão de riscos – art. 17 e 18
c) Responsabilidades para gerenciar riscos.	Política de gestão de riscos – capítulo VI
d) Diretrizes sobre como os riscos devem ser identificados, avaliados, tratados e monitorados.	Manual técnico – capítulo VII, seções III, IV, V e VIII
e) Consultas e comunicação com partes interessadas internas e externas sobre assuntos relacionados a risco.	Manual técnico – capítulo VII, seção VII
f) Diretrizes para a medição do desempenho da gestão de riscos.	Diretriz – art. 23, inciso VIII
g) Compromisso de analisar criticamente e melhorar a política e a estrutura da gestão de riscos em resposta a um evento ou mudança nas circunstâncias.	Não encontrado.

Fonte: Elaborada pela autora, 2024.

As demais questões da dimensão “ambiente” obtiveram pontuação média maior ou igual a 3, levando o cálculo do índice de maturidade da dimensão ao seguinte resultado:

Tabela 15: Índice de maturidade apurado na dimensão “ambiente”.

Total de pontos obtidos na dimensão (média simples)	60,95
Total de pontos possíveis na dimensão	76
Índice de maturidade apurado na dimensão "ambiente"	80,2%

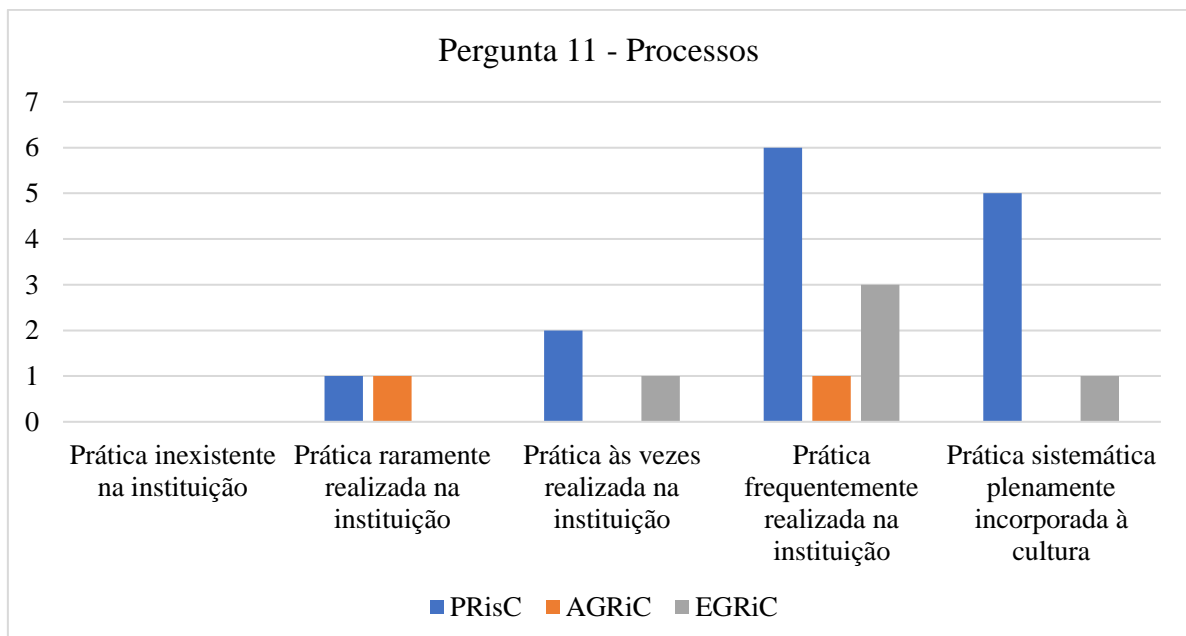
Fonte: Elaborada pela autora, 2024.

De acordo com a métrica estabelecida na tabela 7, constatamos que o nível de maturidade na dimensão “ambiente” é avançado, pois está acima de 80,1%.

A dimensão “processos” está relacionada às etapas de identificação e análise de riscos; avaliação e resposta a riscos; e monitoramento e avaliação. Nessa dimensão, 19 perguntas foram realizadas, cada uma valendo 4 pontos. 4 dessas perguntas obtiveram pontuação média abaixo de 3, conforme descrito a seguir:

a) pergunta 11: “A escolha de respostas aos riscos leva em conta a relação custo-benefício das respostas consideradas?” – recebeu 2,95 pontos;

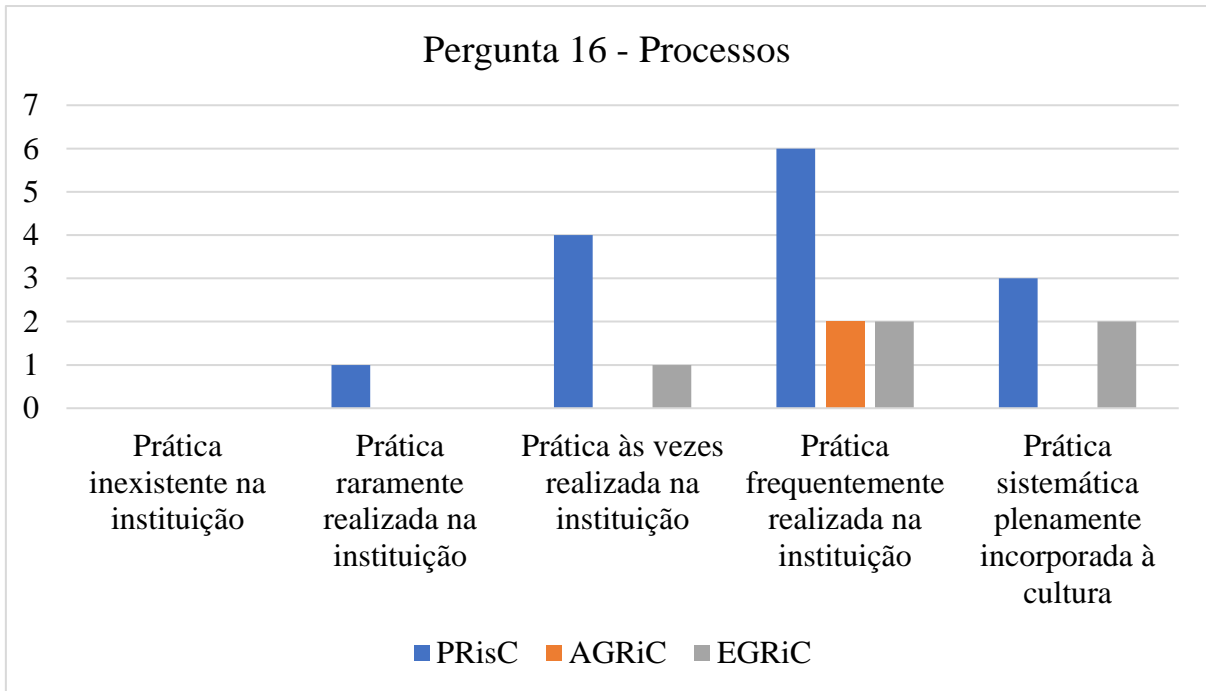
Gráfico 5: Relação quantidade respostas x respondentes, questão 11 – processos.



.Fonte: Elaborado pela autora, 2024.

b) pergunta 16: “O controle interno, ou a auditoria interna, contribui ativamente para as atividades de gestão de riscos na organização?” – recebeu 2,9 pontos;

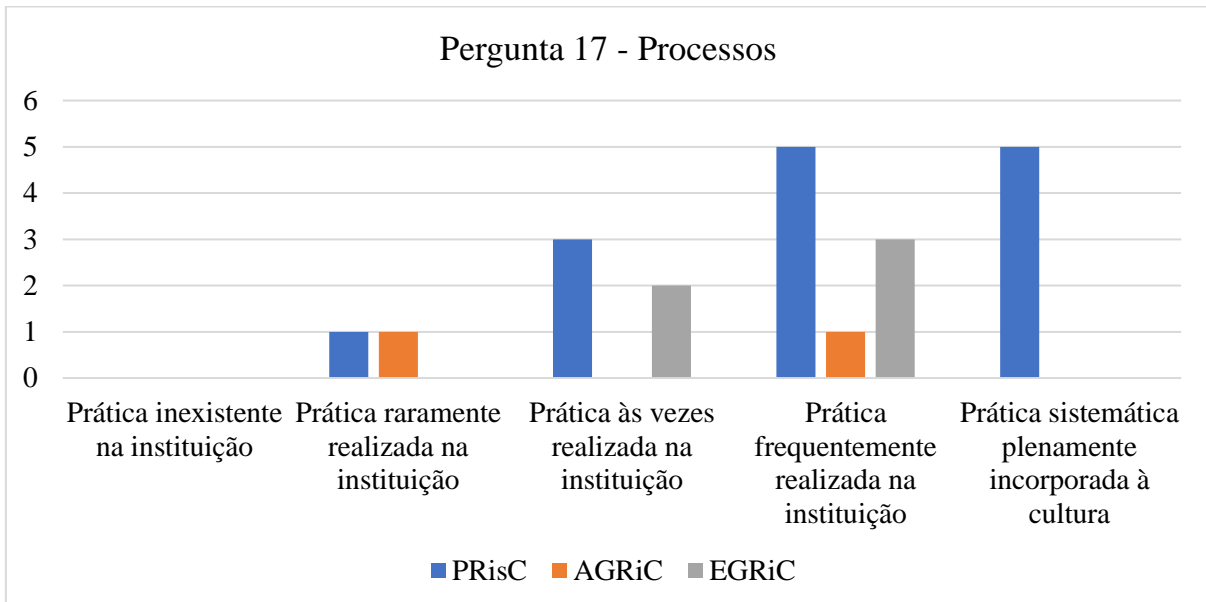
Gráfico 6: Relação quantidade de respostas x respondentes, questão 16 - processos.



Fonte: Elaborado pela autora, 2024.

c) pergunta 17: “Foram estabelecidas medidas de desempenho que permitem avaliar se as respostas a riscos adotadas foram ou não efetivas?” – recebeu 2,8 pontos; e

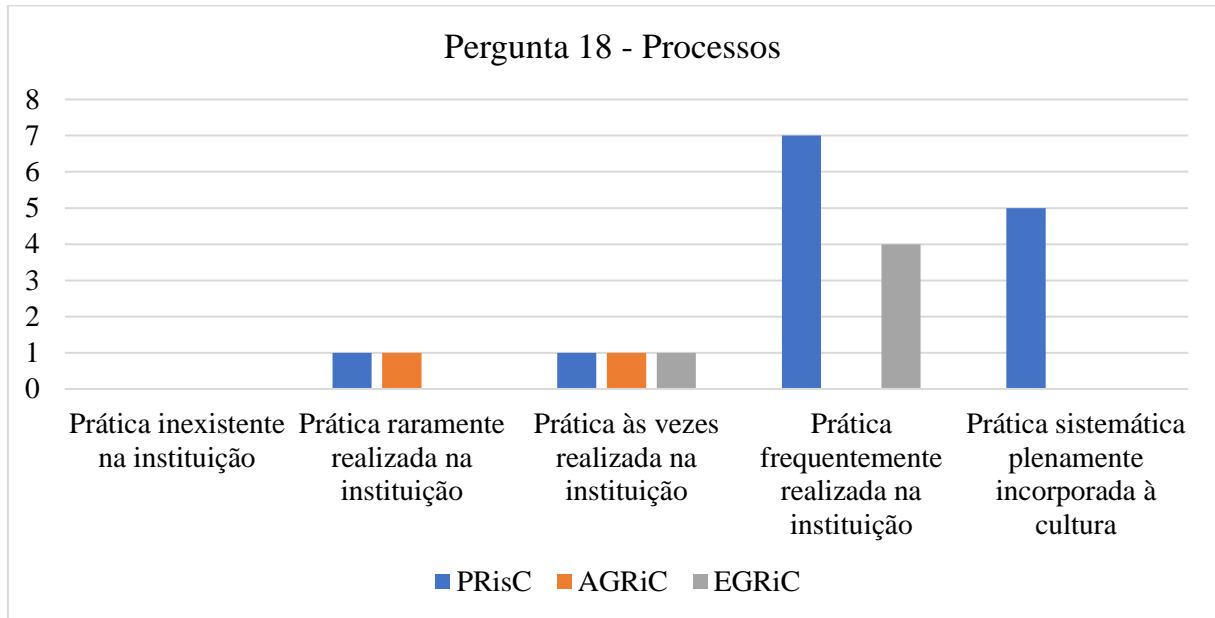
Gráfico 7: Relação quantidade de respostas x respondentes, questão 17 - processos.



Fonte: Elaborado pela autora, 2024.

d) pergunta 18: “No monitoramento do processo de gestão de riscos, são evidenciadas as oportunidades de melhoria e as lições aprendidas?” – recebeu 2,9 pontos.

Gráfico 8: Relação quantidade de respostas x respondentes, questão 18 - processos.



Fonte: Elaborado pela autora, 2024.

Observa-se que as 3 últimas perguntas estão relacionadas à fase de monitoramento e comunicação dos riscos, sugerindo a necessidade de melhoria nessa etapa do processo de gestão de riscos.

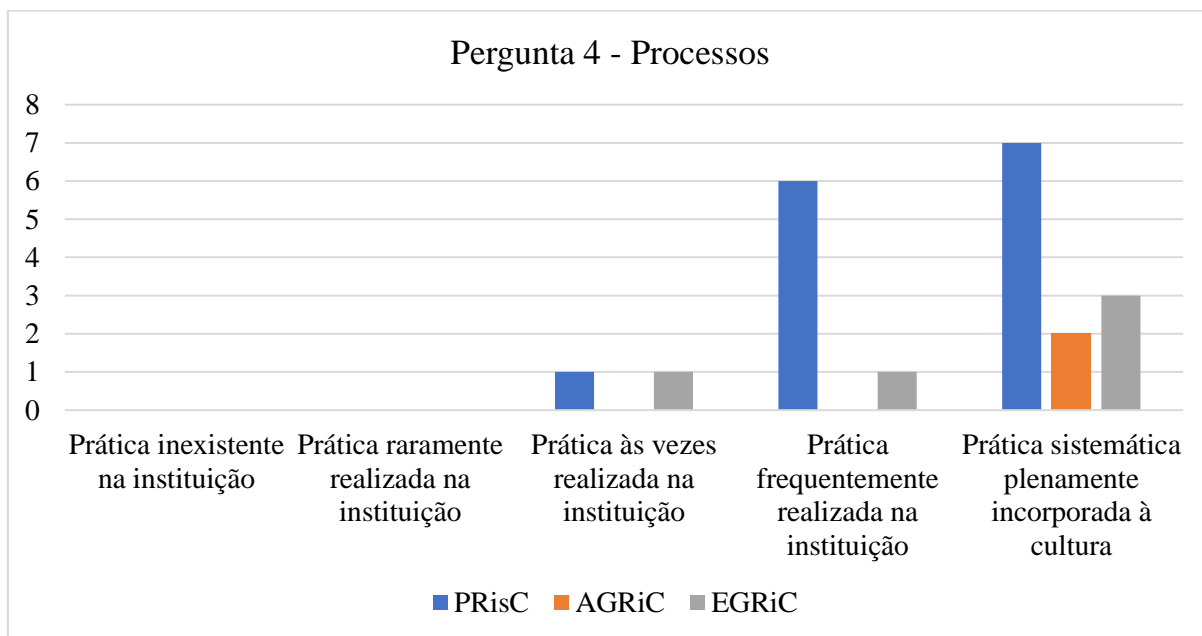
Sobre o controle interno, a análise documental constatou que ele é exercido pelo Centro de Controle Interno do Exército (CCIEEx), uma organização militar externa à diretoria, que realiza auditorias anuais na área de gestão no Departamento-Geral do Pessoal, que é o órgão imediatamente superior à DAP. Não foi verificado no regulamento da diretoria a existência de uma seção destinada à realização de auditorias.

Em relação à eficácia das respostas a riscos, questão 17, verificou-se que a diretoria elabora um relatório onde apresenta a frequência de eventos de riscos concretizados no ano e se os controles detectivos e os planos de contingência foram eficientes, entretanto essa avaliação só é formalmente realizada uma vez por ano e não há parâmetros definidos para determinar se a resposta foi eficaz ou não.

A pergunta que obteve a maior pontuação na dimensão “processos” foi a questão 4, “Os riscos identificados são levados à

consideração da instância decisória pertinente segundo critérios formalmente estabelecidos?”, com 3,47 pontos.

Gráfico 9: Relação quantidade de respostas x respondentes, questão 4 – processos.



Fonte: Elaborado pela autora, 2024.

As demais questões da dimensão “processos” obtiveram pontuação média maior ou igual a 3, levando o cálculo do índice de maturidade da dimensão ao seguinte resultado:

Tabela 16: Índice de maturidade apurado na dimensão “processos”.	
Total de pontos obtidos na dimensão (média simples)	59,52
Total de pontos possíveis na dimensão	76
Índice de maturidade apurado na dimensão "processos"	78,32%

Fonte: Elaborado pela autora, 2024.

Assim, conforme enquadramento constante na tabela 7, constatamos que o nível de maturidade na dimensão “processos” é aprimorado, pois está entre 60,1% e 80%.

A dimensão “parcerias” foi avaliada por meio de 9 perguntas, com pontuação máxima de 4 pontos cada, destinadas exclusivamente ao gestor de parcerias da diretoria.

Nessa dimensão, 3 perguntas obtiveram pontuação 1, são elas: i) “nas parcerias estabelecidas, existe clareza sobre quem é responsável por gerenciar cada risco?”; ii) “a organização estrutura com seus parceiros arranjos de contingência (incluindo a priorização de ações de mitigação) para minimizar efeitos adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falha ao entregar o serviço?”; e iii) “quando riscos são transferidos a organizações parceiras, mantém-se a capacidade de gerenciar e monitorar desempenho e de adotar tempestivamente medidas em caso de dificuldades?”.

Todas essas perguntas obtiveram a resposta “discordo mais do que concordo”. As demais perguntas receberam pontuação 3, com exceção das questões 1 e 5, que obtiveram pontuação 2.

Analisando as respostas do questionário e realizando a verificação documental, constatou-se que a DAP possui atualmente apenas 1 parceria firmada, com a Associação Nacional de Equoterapia (ANDE-BRASIL), uma entidade civil, sem fins lucrativos, que visa “oferecer a equoterapia como meio de reabilitação, de educação e de inserção social para melhorar a qualidade de vida de pessoas com deficiência ou necessidades especiais” (ANDE-BRASIL, s.d.).

A gestão de riscos conjunta é feita “em partes” entre a DAP e a ANDE-BRASIL e o instrumento que oficializa a parceria é um acordo de cooperação. Esse acordo tem por finalidade oferecer a militares, servidores civis e seus dependentes com necessidades especiais, reabilitação e inserção social através da equoterapia. Analisando o acordo de cooperação, observa-se que não há cláusula específica para a gestão de riscos, entretanto, há responsabilidades definidas quanto à gestão de alguns eventos que podem ser entendidos como riscos, a exemplo de demandas judiciais para pagamento de encargos trabalhistas.

O resultado final da dimensão é apresentado na tabela abaixo:

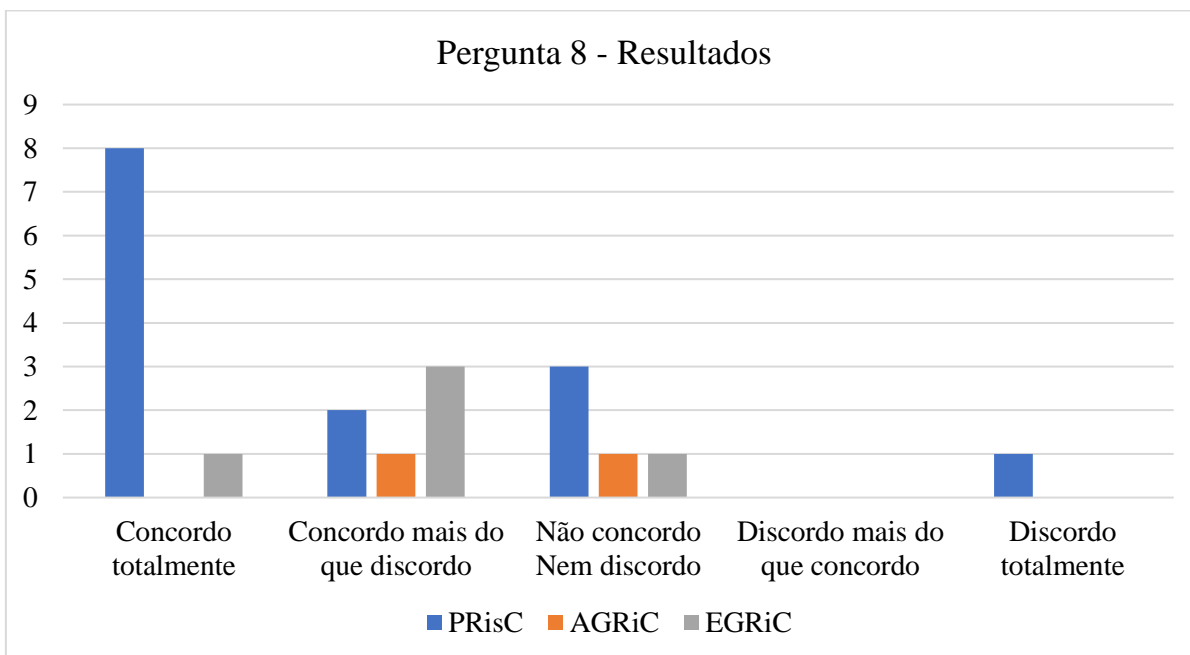
Tabela 17: Índice de maturidade apurado na dimensão “parcerias”.	
Total de pontos obtidos na dimensão	19
Total de pontos possíveis na dimensão	36
Índice de maturidade apurado na dimensão "ambiente"	52,78%

Fonte: Elaborado pela autora, 2024.

Assim, constatamos que o nível de maturidade na dimensão “parcerias” é intermediário, pois está acima entre 40,1% e 60%.

Na dimensão “resultados” nenhuma das 9 perguntas recebeu pontuação média inferior a 3 (três). A questão com menor pontuação foi a 8, “O processo de gestão de riscos tem levado os servidores a se envolverem com avaliação e controle de riscos em suas atividades cotidianas?”, com pontuação média de 3,04 e com a seguinte distribuição de respostas:

Gráfico 10: Relação quantidade de respostas x respondentes, questão 8 - resultados

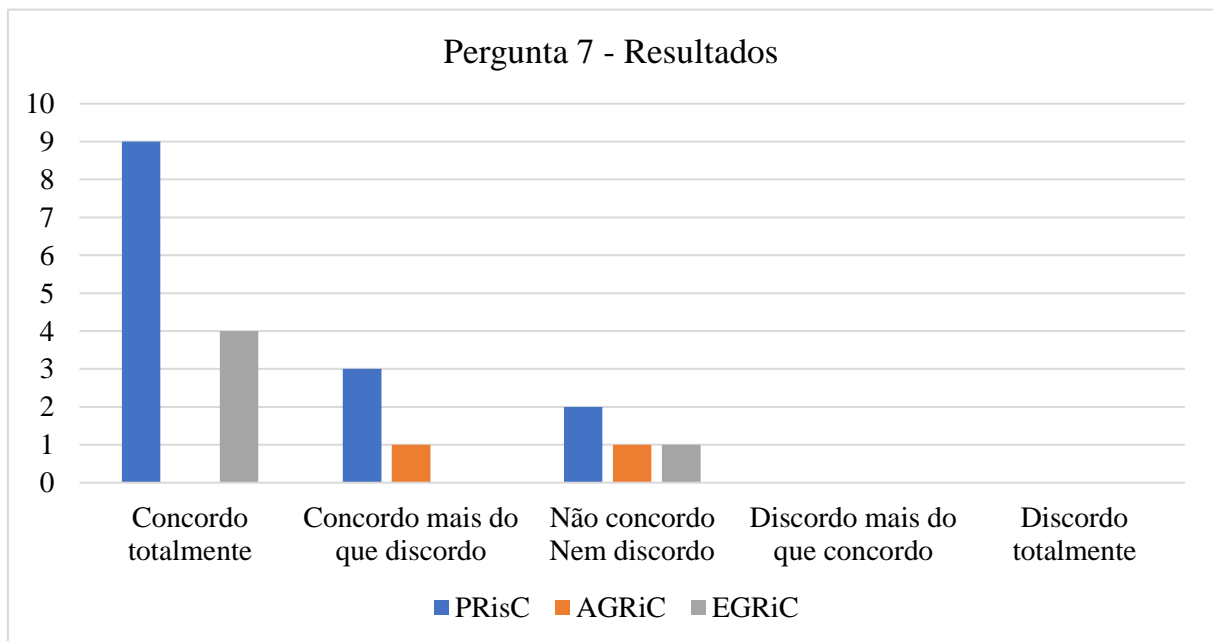


. Fonte: Elaborado pela autora, 2024.

Nessa questão é possível observar que a AGRiC apresenta maior dúvida se os servidores têm se envolvido de forma rotineira nas atividades de monitoramento e controle, possivelmente pela distância física e funcional em relação aos demais servidores, enquanto um percentual maior de membros da EGRiC e dos próprios PRiSC, que são os maiores responsáveis por essas atividades, entendem que sim, o envolvimento tem sido rotineiro.

A pergunta 7 (sete), “O processo de gestão de riscos contribuiu para a melhoria do processo decisório na organização?”, foi a que obteve maior pontuação média na dimensão, 3,42 pontos. A figura abaixo apresenta a distribuição das respostas:

Gráfico 11: Relação quantidade de respostas x respondentes, questão 7 - resultados.



Fonte: Elaborado pela autora, 2024.

O resultado final da dimensão é apresentado na tabela abaixo:

Tabela 18: Índice de maturidade apurado na dimensão “resultados”.	
Total de pontos obtidos na dimensão (média simples)	45,57

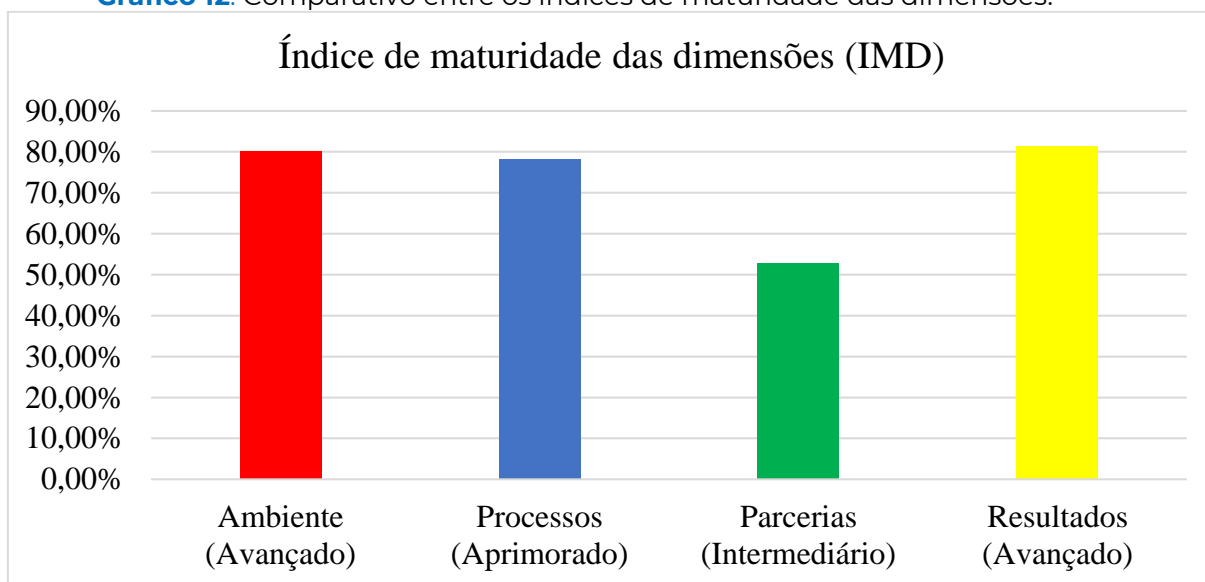
Total de pontos possíveis na dimensão	56
Índice de maturidade apurado na dimensão "ambiente"	81,38%

Fonte: Elaborado pela autora, 2024

Constatamos, desse modo, que o nível de maturidade na dimensão “resultados” é avançado, pois está entre 80,1% e 100%.

O gráfico a seguir apresenta o comparativo entre os índices de maturidade de cada dimensão:

Gráfico 12: Comparativo entre os índices de maturidade das dimensões.



Fonte: Elaborado pela autora, 2024.

É possível observar que, com exceção da dimensão “parcerias”, os IMD se apresentam quase no mesmo nível, denotando esforços equivalentes na gestão de riscos da diretoria no que concerne ao ambiente, aos processos e aos resultados.

A discrepância em relação às parcerias pode ser justificada pela baixa formalização das questões relacionadas a riscos no instrumento que firma a parceria, nesse caso, o acordo de cooperação.

Além disso, uma gestão de riscos conjunta é mais desafiadora, pois cada organização pode ter sua metodologia de gerenciamento de riscos, seu apetite a riscos e até mesmo prioridades diferentes quanto ao processo que é realizado conjuntamente.

A comunicação entre as partes é outro ponto sensível, uma vez que cada instituição carrega seus próprios valores e culturas, podendo haver interesses diversos entre os parceiros.

Assim, após avaliar a maturidade de cada dimensão, temos o resultado do índice de maturidade global, conforme tabela a seguir:

Tabela 19: Índice de maturidade global da DAP.				
DIMENSÃO	PESO	IMD	PESO	PONDERADO
Ambiente	40	80,2	0,4	32,08%
Processos	30	78,32	0,3	23,50%
Parcerias	10	52,78	0,1	5,28%
Resultados	20	81,38	0,2	16,28%
ÍNDICE DE MATURIDADE GLOBAL				77,13%

Fonte: Elaborado pela autora a partir de Brasil, 2018c.

Desse modo, constatamos que o nível de maturidade global da Diretoria de Assistência ao Pessoal é aprimorado, pois está entre 60,1% e 80%.



7

CONSIDERAÇÕES FINAIS

A presente pesquisa atingiu o seu objetivo ao encontrar o nível de maturidade em gestão de riscos da Diretoria de Assistência ao Pessoal do Exército, segundo a metodologia do TCU.

A hipótese de que o nível global de maturidade seria o intermediário não foi confirmada. Embora os índices obtidos nas dimensões “ambiente” e “processos” sejam similares aos previstos na hipótese, nas dimensões “parcerias” e “resultados” os índices foram maiores, resultando no nível de maturidade global “aprimorado”. Os dados coletados no questionário, na verificação documental e na entrevista validam a refutação da hipótese.

A diferença de resultado na dimensão “parceria” em relação à hipótese se deve ao fato de que, embora não haja formalização da gestão de riscos no acordo de cooperação entre a DAP e a ANDE-Brasil, cada responsável possui autonomia e recursos para gerenciar seus riscos, além disso, os riscos transferidos são monitorados pela DAP.

Verificou-se que um nível intermediário de maturidade na dimensão “parcerias” não impactou significativamente na dimensão “resultados”, e por isso essa dimensão também recebeu um índice maior ao previsto na hipótese. Esse achado pode ser explicado pelo fato de a diretoria possuir apenas uma parceria vigente, relacionada estritamente a um único processo, desse modo, essa dimensão possui pouca influência nos resultados organizacionais como um todo.

Os índices de maturidade apurado nas dimensões “ambiente”, “processos” e “resultados” apontaram níveis de maturidade similares entre si, com variação de apenas 3%. Na dimensão “parcerias”, houve maior discrepância em relação aos outros níveis, entretanto, isso não tem interferido na dimensão “resultados”, que recebeu a maior pontuação média.

Cabe ressaltar que o nível de maturidade em gestão de riscos não é algo estático, uma vez que melhorias podem ser realizadas em todas as dimensões a fim de aprimorar o nível atual.

Serão apresentadas a seguir sugestões de ações, dentro de cada dimensão, que podem contribuir para que a DAP eleve seu nível de maturidade para o avançado.

As sugestões foram feitas com base no referencial teórico, em especial sobre o processo de gestão de riscos, e foram consideradas as respostas com menores pontuações do questionário e oportunidades de melhoria detectadas na análise documental e na entrevista.

Tabela 20: Sugestões por dimensão avaliada.

Dimensão Responsável	Sugestão	Objetivo	
Ambiente	EGRiC	Realizar reuniões de análise de riscos em suas seções, a fim de compartilhar informações relevantes com todos os servidores e não apenas com os PRisC.	Ampliar a comunicação dos riscos e reforçar a cultura de gestão de riscos em todos os servidores.
		Identificar riscos durante o surgimento de novos processos ou atividades na seção.	Evitar que possíveis novos riscos sejam negligenciados.
	AGRiC	Analisar as boas práticas de gestão de riscos nas demais forças armadas e no Ministério da Defesa.	Identificar ferramentas e estratégias em instituições com atividades semelhantes, a fim de aperfeiçoar as práticas já existentes na DAP.
		Realizar, semestralmente, palestras sobre gestão de riscos a todos os servidores da DAP.	Ampliar a comunicação e reforçar a cultura de gestão de riscos em todos os servidores.
Processos	AGRiC	Realizar auditorias bimestrais no SIG-DAP, com vistas a avaliar a frequência de eventos ocorridos e a eficácia dos controles.	Aprimorar a resposta aos riscos, auxiliando os PRisC e os membros da EGRiC na seleção de novos controles, caso seja necessário.
		Estabelecer medida de desempenho para avaliar se as repostas a riscos e os controles foram efetivos.	Reduzir a subjetividade na fase de monitoramento. Atualmente não existe critério definido para determinar se as repostas e os controles foram efetivos, assim, cada PRisC faz uma

Tabela 20: Sugestões por dimensão avaliada.

Dimensão Responsável	Sugestão	Objetivo	
		avaliação subjetiva ou seguindo critérios diversos entre si.	
	EGRiC	Elaborar relatório de lições aprendidas, a ser lançado no SIG-DAP.	Aprimorar o monitoramento e a comunicação dos riscos.
Parcerias	Gestor de parcerias	Elaborar matriz de riscos e plano de ação, especificando a responsabilidade de cada parceiro, e incluir esses documentos como anexo ao acordo de cooperação.	Formalizar a gestão de riscos e facilitar a execução de todas as etapas do processo de gestão de riscos na parceria estabelecida.
		Estabelecer reuniões periódicas com a entidade parceira para tratar de riscos.	Melhorar a comunicação entre as partes e facilitar o monitoramento dos riscos.
Resultados	AGRiC e EGRiC	Incluir, no relatório anual de gestão de riscos, possíveis necessidades de alteração de normas e processos, levando em consideração as lições aprendidas.	Garantir que a gestão de riscos não seja um fim em si mesma, utilizando os trabalhos realizados anualmente para produzir mudanças relevantes nas diversas competências da diretoria, contribuindo para obtenção de melhores resultados organizacionais.

Fonte: Elaborado pela autora, 2024.

Quanto às recomendações para futuras pesquisas, sugere-se um estudo a fim de propor uma metodologia própria de mensuração para o Exército, uma vez que seu manual técnico de gestão de riscos não apresenta ferramentas para essa mensuração.

Embora o modelo do TCU seja facilmente aplicável em um estudo ou em uma auditoria mais minuciosa, seu questionário extensivo não é uma ferramenta prática, o que pode dificultar a aplicabilidade no EB, em especial nas unidades menores e operacionais, onde há poucos servidores dedicados à área de gestão.

Além disso, a maioria das organizações militares não trabalham com parcerias. Desse modo, essa dimensão receberia pontuação zero

em boa parte das mensurações, causando uma interferência negativa e equivocada no nível de maturidade global.

A criação de um modelo específico, considerando as particularidades do Exército, irá facilitar a mensuração do nível de maturidade em gestão de riscos em todas as unidades da Força Terrestre



REFERÊNCIAS

REFERÊNCIAS

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnica. **NBR ISO 31010:2012**. Gestão de Riscos – Técnicas para o processo de avaliação de riscos. 2012. Disponível em: <https://planejamentoestrategico.mcti.gov.br/arquivos/Gestao_Riscos_Tecnicas_%20ABNT%20NBR%20ISO-IEC%2031010-2012.pdf>. Acesso em: 24 jan. 2024.

ABNT. Associação Brasileira De Normas Técnica. **NBR ISO 31000:2018**. Gestão de Riscos – Diretrizes. 2018. Disponível em: <<https://dintegcgcin.saude.gov.br/attachments/download/23/2018-Diretrizes-Gestao-de-Riscos-ABNT-NBR-ISO-31000.pdf>>. Acesso em: 03 maio. 2023.

ABNT. Associação Brasileira De Normas Técnica. **NBR ISO 31022:2020**. Gestão de Riscos – Diretrizes para a gestão de riscos legais. 2020. Disponível em: <<https://www.abntcatalogo.com.br/pnm.aspx?Q=WkpUbDNoN24vQ0s yMIERUHFVTm1leUxXN1dmc2hjbTVma2o2Yk8yK0Nhczo=>>>. Acesso em: 25 jan. 2024.

ABNT. Associação Brasileira De Normas Técnica. **NBR ISO 31073:2022**. Gestão de Riscos – Vocabulários. 2022. Disponível em: <<https://www.abntcatalogo.com.br/pnm.aspx?Q=MXJkRzRHN2xwWnFKZGINNldhNHRHRVN2YzVSWmdmLOQrSHRHMHpBRTMIYzO=>>>. Acesso em: 25 jan. 2024.

AHMETI, Remzi; VLADI, Besarta. **Risk Management in Public Sector: A Literature Review**. 2017. Disponível em: <https://revistia.com/files/articles/ejms_v2_i5_17/Remzi.pdf>. Acesso em: 28 mar. 2024.

ANDE-BRASIL. **Nossa missão**. [s.d.]. Disponível em: <http://equoterapia.org.br/articles/index/article_detail/135/2019>. Acesso em: 24 abr. 2024

BLOISE, Denise Martins. **A importância da metodologia científica na construção da ciência. Revista Científica Multidisciplinar Núcleo do Conhecimento**. Ano 05, Ed. 06, Vol. 06, pp. 105-122. 2020. Disponível em: <<https://www.nucleodoconhecimento.com.br/educacao/metodologia-cientifica>>. Acesso em: 20 maio 2024.

BRASIL. **Constituição da República Federativa do Brasil**. 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 29 ago. 2022.

BRASIL. **Lei Complementar nº 97, de 9 de junho de 1999**. 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm>. Acesso em: 16 mar. 2024.

BRASIL. **Lei nº 10.826**, de 22 de dezembro de 2003. 2003. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2003/l10.826.htm>. Acesso em: 16 mar. 2024.

BRASIL. **Acórdão 1517/2010**, de 9 de julho de 2010. 2010. Tribunal de Contas da União. Disponível em: <<https://portal.tcu.gov.br/biblioteca-digital/relatorio-de-riscos-acordao-1517-2010-tcu-8A81881F759554350176331A25800843.htm>>. Acesso em: 2 mar. 2024.

BRASIL. **Fiscalis nº 489/2012**, de 24 de abril de 2012. Tribunal de Contas da União. Relatório de Levantamento para Avaliação da Gestão de Riscos e Controles Internos na Administração Pública Federal Indireta. 2012.

BRASIL. **Acórdão 2467/2013**, de 11 de setembro de 2013. Tribunal de Contas da União. Disponível em: <https://pesquisa.apps.tcu.gov.br/documento/acordao-completo*/NUMACORDAO:2467%20ANOACORDAO:2013%20COLEGIA DO:'Plen%C3%A1rio'/DTRELEVANCIA%20desc,%20NUMACORDAOINT%20desc/0>. Acesso em: 27 set. 2023.

BRASIL. **Acórdão 1739/2015**, de 15 de julho de 2015. Tribunal de Contas da União. Disponível em: <https://pesquisa.apps.tcu.gov.br/documento/acordao-completo*/NUMACORDAO:1739%20ANOACORDAO:2015%20COLEGIA DO:'Plen%C3%A1rio'/DTRELEVANCIA%20desc,%20NUMACORDAOINT%20desc/0>. Acesso em: 2 mar. 2024.

BRASIL. **Instrução Normativa Conjunta no 1**, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. 2016. Ministério Do Planejamento, Orçamento e Gestão. Controladoria-Geral da União. Disponível em: <<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&data=11/05/2016&pagina=14>>. Acesso em: 29 ago. 2022.

BRASIL.. **Decreto nº 9.203**, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta,

autárquica e fundacional. 2017a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9203.htm>. Acesso em: 5 dez. 2022.

BRASIL. **Resolução** - TCU N° 287, de 12 de abril de 2017. 2017b. Tribunal de Contas da União. Disponível em: <<https://portal.tcu.gov.br/main.jsp?lumPagelId=8A8182A24ED12B19014ED646CE5E1FC0&previewItemId=8A81881F6364D8370163E077B6E26C4D&lumItemId=FF8080816364D7980163E07C355A3C07>>. Acesso em: 03 maio. 2023.

BRASIL. **Política de Gestão de Riscos do Exército Brasileiro (EB10-P-01.004)**. Comando do Exército. 2a Edição. Brasília-DF, 2018a.

BRASIL.. **Programa de Integridade do Exército Brasileiro**. Comando do Exército. 1a Edição. Brasília-DF, 2018b.

BRASIL. **Roteiro de Avaliação de Maturidade da Gestão de Riscos**. Tribunal de Contas da União. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018c. 164 p. Disponível em: <<https://portal.tcu.gov.br/gestao-de-riscos-avaliacao-da-maturidade.htm>>. Acesso em: 08 abr. 2023.

BRASIL. **Portaria Normativa** n° 62/GM-MD, de 29 de julho de 2019. 2019a. Disponível em: <<https://sintse.tse.jus.br/documentos/2019/Jul/31/para-conhecimento-institucional/portaria-normativa-no-62-de-29-de-julho-de-2019-dispoe-sobre-o-projeto-soldado-cidadao-e-o-respectiv>>. Acesso em: 16 mar. 2024

BRASIL. **Regulamento da Diretoria de Civis, Inativos, Pensionistas e Assistência Social (EB10-R-02.020)**. Comando do Exército. 2a Edição. Brasília-DF, 2019b.

BRASIL. **Diretriz Reguladora da Política de Gestão de Riscos do Exército Brasileiro**. Comando do Exército. Brasília-DF, 2019c.

BRASIL. **Manual Técnico da Metodologia de Gestão de Riscos do Exército Brasileiro (EB20-MT-02.001)**. Comando do Exército. 1a Edição. Brasília-DF, 2019d.

BRASIL. **Instrução normativa 84/2020**, de 22 de abril de 2020. Tribunal de Contas da União. Estabelece normas para a tomada e prestação de contas dos administradores e responsáveis da administração pública federal, para fins de julgamento pelo Tribunal de Contas da União, nos termos do art. 7º da Lei 8.443, de 1992, e revoga as Instruções

Normativas TCU 63 e 72, de 1º de setembro de 2010 e de 15 de maio de 2013, respectivamente. 2020a. Disponível em: <<https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-84-de-22-de-abril-de-2020-254756795>>. Acesso em: 14 mar. 2024

_____. BRASIL.. TRIBUNAL DE CONTAS DA UNIÃO. **Referencial básico de governança organizacional para organizações públicas e outros entes jurisdicionados ao TCU**. 3ª edição. 2020b. Tribunal de Contas da União. Disponível em: <<https://portal.tcu.gov.br/imprensa/noticias/tcu-publica-a-3-edicao-do-referencial-basico-de-governanca-organizacional.htm>>. Acesso em: 28 mar. 2024

BRASIL. **Decisão Normativa TCU nº 198/2022**. 2022a. Tribunal de Contas da União. Disponível em: <https://pesquisa.apps.tcu.gov.br/documento/norma/*/COPIATIPONORMA:%28%22Decis%C3%A3o%20Normativa%22%29%20COPIAORIGEM:%28TCU%29%20NUMNORMA:198%20ANONORMA:2022/DATANORMAORDENACAO%20desc/0>. Acesso em: 12 jun. 2024

BRASIL. **Resolução nº 5**, de 28 de maio de 2020. Institui a Política de Gestão de Riscos do Instituto Nacional do Seguro Social - INSS. 2020c. Instituto Nacional de Seguro Social. Disponível em: <<https://in.gov.br/web/dou/-/resolucao-n-5-de-28-de-maio-de-2020-259638760>>. Acesso em: 03 maio. 2023

BRASIL. **Resolução administrativa - ra nº 74**, de 24 de fevereiro de 2022. Dispõe sobre a política de gestão de riscos da Agência Nacional de Saúde Suplementar - ANS. 2022b. Disponível em: <https://bvsmis.saude.gov.br/bvs/saudelegis/ans/2022/res0074_25_02_2022.html>. Acesso em: 03 maio. 2023

BRASILIANO, Antônio Celso Ribeiro. **Gestão e Análise de Riscos Corporativos: Método Brasileiro Avançado**. 2ª ed. São Paulo: Sicurezza Editora, 2012.

CARVALHO, Pedro Filipe M. Lima de. **Enterprise Risk Management e o Custo do Capital Próprio. Uma análise empírica à realidade portuguesa**. 2021. 70 f. Dissertação de Mestrado - Universidade Católica Portuguesa, Porto, Portugal. Disponível em: <<https://repositorio.ucp.pt/handle/10400.14/35197>>. Acesso em: 27 mar. 2024.

CHAVES, Silvana; CAMPELLO, Mauro. **A qualidade e a evolução das normas série ISO 9000**. 2014. Disponível em:

<<https://www.aedb.br/seget/arquivos/artigos16/27224305.pdf>>. Acesso em: 6 abr. 2024.

COSO. **Gerenciamento de Riscos Corporativos - Estrutura Integrada (COSO II)**. 2007. Disponível em: <<https://auditoria.mpu.mp.br/pgmq/COSOIIERMExecutiveSummaryPortuguese.pdf>>. Acesso em: 03 maio 2023.

COSO.. **Controle Interno - Estrutura Integrada (COSO I)**. 2013. Disponível em: <https://auditoria.mpu.mp.br/pgmq/COSOIIICIF_2013_Sumario_Executivo.pdf>. Acesso em: 31 mar. 2023.

COSO.. **Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance**. 2017. Disponível em: <https://repositorio.cgu.gov.br/bitstream/1/74040/1/Coso_portugues_ve rsao_2017.pdf>. Acesso em: 31 mar. 2023.

COSO.. **Compliance Risk Management: Applying The Coso Erm Framework**. 2020. Disponível em: <https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf>. Acesso em: 29 jun. 2024.

DE BRUIN, Tonia et al. **Understanding the Main Phases of Developing a Maturity Assessment Model**. 2005. Disponível em: <https://www.researchgate.net/publication/27482282_Understanding_the_Main_Phases_of_Developing_a_Maturity_Assessment_Model>. Acesso em: 4 abr. 2024.

DIONNE, Georges. **Risk Management: History, Definition and Critique**. 2013. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231635>. Acesso em: 27 mar. 2024.

DUTRA, Haendchen Marcelo; ZANETTE, Maicon Anderson; ALBERTON, Luiz et al. Controles de gestão: uma contribuição ao estudo dos principais modelos. **RACE**, Unoesc, v. 8, n. 1, p. 87-112, jan./jun. 2009. Disponível em: <https://www.researchgate.net/publication/277804886_Controles_de_gestao_uma_contribuicao_ao_estudo_dos_principais_modelos>. Acesso em: 31 mar. 2024.

GATTRINGER, João Luiz; MARINHO, Sidnei Vieira. **O uso do modelo COSO na administração pública: um estudo nos municípios catarinenses**. 2020. Disponível em:

<<https://www.redalyc.org/journal/3071/307163778005/html/>>. Acesso em: 31 mar. 2024.

HILLSON, David. Towards a risk maturity model. **The International Journal of Project and Business Risk Management**. 1997.

IBGC. **Gerenciamento de riscos corporativos: evolução em governança e estratégia**. São Paulo, SP: IBGC, 2017. (Série Cadernos de Governança Corporativa, 19). 64p. Disponível em: <<https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21794>>. Acesso em: 02 ago. 2023

IBGC. **O IBGC**. [s.d.]. <Disponível em: <https://ibgc.org.br/quemsomos>>. Acesso em: 06 abr. 2024

IFAC. International Federation of Accountants. **Good Governance in the Public Sector - Consultation Draft for na International Framework**. 2013. Disponível em: <<http://www.ifac.org/sites/default/files/publications/files/Com-parison-of-Principles.pdf>>. Acesso em: 19 maio. 2024

MAFFI, Daiana. A importância da Metodologia do COSO. RGSN - **Revista Gestão, Sustentabilidade e Negócios**, Porto Alegre, v. 6, n. 2, p. 27-49. 2018. Disponível em: <<https://www.saofranciscodeassis.edu.br/rgsn/arquivos/RGSN12/artigos/A-importancia-da-Metodologia-do-COSO-MAFFI-D.pdf>>. Acesso em: 31 mar. 2024.

NEVES, Glaucio; GUIMARÃES, Aluísio; JÚNIOR, Avilton. **As bases para um novo modelo de administração pública orientada para resultados**: evolução dos paradigmas, novos princípios e dimensões operacionais de funcionamento. Brasília, 2017. Disponível em: <http://consad.org.br/wp-content/uploads/2017/05/Painel-15_01.pdf>. Acesso em: 28 mar. 2024.

NOVAIS, Bruno Fassheber. **Análise da maturidade em gestão de riscos no MP**: proposição e aplicação de um instrumento de avaliação orientado aos processos de TI. Brasília, 2016. 123 p. Disponível em: <<http://icts.unb.br/jspui/handle/10482/22217>>. Acesso em: 04 ago. 2023

PEREIRA, Matheus Rodrigues. **O gerenciamento de riscos empresariais como forma de agregar valor às organizações**. 2014. Disponível em: <<https://pantheon.ufrj.br/bitstream/11422/1666/1/MRPereira.pdf>>. Acesso em: 29 mar. 2024

PINTO, Ysabelle Mariá Aparecida Santos; BARROS, Joseane Cristine Coelho. **Normas ISO, gespública e gestão participativa:** suas práticas e o incremento na qualidade da gestão pública no estado do Rio de Janeiro. 2018. Disponível em: <<https://app.uff.br/riuff;/handle/1/16717?locale-attribute=es>>. Acesso em: 6 abr. 2024

PMI – PROJECT MANAGEMENT INSTITUTE. **A Guide to the Project Management Body of Knowledge** (PMBOK® Guide). 5th ed. [s.l.]: PMI, 2013.

PRZETACZNIK, Sylwia. **The evolution of risk management.** 2022. Disponível em: <<https://scholar.archive.org/work/qdnm7hijyvdxalui4aud5g4r4>>. Acesso em: 27 mar. 2024

SANTOS, T. J.. **Gestão de riscos e a norma ISO 31000:** uma abordagem literária. Management Journal, v.3, n.1, p.1-14, 2021. Disponível em: <<https://www.sapientiae.com.br/index.php/managementjournal/article/view/CBPC2674-6417.2021.001.0001/75>>. Acesso em: 6 abr. 2024

VIANA, Tiago de Alencar. **Maturidade em gestão de riscos nas instituições federais de ensino superior (IFES):** análise do nível de maturidade em gestão de riscos em IFES do nordeste brasileiro. 2021. Disponível em: <https://repositorio.ufrn.br/bitstream/123456789/46556/1/Maturidadegestaoriscos_Viana_2021.pdf>. Acesso em: 31 mar. 2024

VIEIRA, James Batista; BARRETO, Rodrigo T. de Souza. **Governança, gestão de riscos e integridade.** ENAP. 2019. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/4281/1/5_Livro_Governança_Gestão_de_Riscos_e_Integridade.pdf>. Acesso em: 28 mar. 2024

VIEIRA, J. B.; ARAÚJO, A. B. **Risk management in the Brazilian Federal Government: a ministerial analysis. Revista do Serviço Público,** [S. l.], v. 71, n. c, p. 404-437, 2020. Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/4466>. Acesso em: 19 maio. 2024.

WIECZOREK-KOSMALA, Monika. **Risk management practices from risk maturity models perspective.** 2014. Disponível em: <https://www.researchgate.net/publication/262843641_Risk_management_practices_from_risk_maturity_models_perspective>. Acesso em: 6 abr. 2024



ANEXOS

ANEXOS

ANEXOS

ANEXOS A

Questionário de avaliação do nível de maturidade de gestão de riscos

Identificação do respondente

- Proprietário de Riscos e Controles (PRisC)
- Membro da Equipe de Gestão de Riscos e Controles (EGRiC)
- Membro da Assessoria de Gestão de Riscos e Controles (AGRiC)
- Gestor de parcerias

Parte A – Ambiente de Gestão de Riscos

Esta parte do questionário trata de aspectos que compõem o ambiente interno em que se desenvolve a gestão de riscos, em especial os relacionados a liderança, políticas e estratégias, definição de responsabilidades e desenvolvimento de pessoas. Algumas das questões objetivas admitem respostas sim/não; as demais devem ser respondidas com base nesta escala:

1	2	3	4	5
Discordo totalmente	Discordo mais do que concordo	Não discordo Nem concordo	Concordo mais do que discordo	Concordo totalmente

Aspectos Avaliados

1. A alta administração adota medidas suficientes para que a gestão de riscos esteja integrada aos processos de gestão da organização, desde o nível estratégico até o operacional.
2. A alta administração adota medidas que assegurem que os gestores liderem a implementação e o monitoramento das práticas de gestão de riscos.
3. A alta administração considera os riscos-chave que podem comprometer o alcance dos principais objetivos organizacionais e

fornece direção clara para que eles sejam gerenciados.
4. A alta administração estimula gestores e demais servidores a aceitar riscos bem gerenciados visando aproveitar oportunidades e apoiar a inovação.
5. A alta administração promove o aperfeiçoamento da estrutura e do processo de gestão de riscos valendo-se, inclusive, de informações produzidas por auditorias internas e externas.
6. Existe uma política corporativa de gestão de riscos aprovada pela alta administração.
7. Caso exista uma política corporativa de gestão de risco, indicar se ela aborda os seguintes aspectos:
h) Objetivos organizacionais com relação à gestão de riscos.
i) Integração da gestão de riscos a processos e políticas organizacionais.
j) Responsabilidades para gerenciar riscos.
k) Diretrizes sobre como os riscos devem ser identificados, avaliados, tratados e monitorados.
l) Consultas e comunicação com partes interessadas internas e externas sobre assuntos relacionados a risco.
m) Diretrizes para a medição do desempenho da gestão de riscos.
n) Compromisso de analisar criticamente e melhorar a política e a estrutura da gestão de riscos em resposta a um evento ou mudança nas circunstâncias.
8. A política de gestão de riscos é comunicada e está disponível a todos na organização.
9. Existe uma estratégia para assegurar que novas atividades sejam avaliadas quanto a risco e incorporadas ao processo de gestão de riscos.
10. Existe uma estratégia para assegurar compreensão uniforme, na organização, dos conceitos e da terminologia utilizada em questões de risco.
11. Os objetivos estratégicos e as prioridades da organização são claramente comunicados a todos os servidores.
12. Os gestores mantêm suas equipes informadas dos objetivos e das prioridades de suas unidades organizacionais.
13. Os servidores conhecem os principais riscos enfrentados por suas unidades.
14. Os servidores são orientados e estimulados a encaminhar

assuntos relacionados a risco às instâncias decisórias adequadas.
15. Os gestores recebem delegação clara e formal para gerenciar riscos.
16. Os gestores são regularmente capacitados para conduzir a gestão de riscos em suas unidades e orientar suas equipes sobre esse tema.
17. Servidores são formalmente designados para as atividades de identificação, avaliação e tratamento de riscos.
18. Servidores designados para as atividades de identificação, avaliação e tratamento de riscos recebem capacitação suficiente para executá-las.
19. Boas práticas de gestão de riscos desta e de outras organizações são identificadas e compartilhadas internamente.

Parte B – Processos

Esta parte do questionário trata de aspectos relacionados ao processo de gestão de riscos, com destaque para as etapas de identificação, avaliação, tratamento, monitoramento e comunicação de riscos. As questões objetivas devem ser respondidas com base na escala a seguir. Utilizar a opção 1 para indicar que a prática perguntada inexistente na organização; 5 para indicar que ela alcançou elevada maturidade ao ser realizada de forma sistemática e estar incorporada à cultura organizacional; e os pontos 2, 3 e 4 para indicar uma posição intermediária que reflita o estágio de desenvolvimento da prática.

1	2	3	4	5
Prática inexistente na instituição	Prática raramente realizada na instituição	Prática às vezes realizada na instituição	Prática frequentemente realizada na instituição	Prática sistemática plenamente incorporada à cultura

Identificação e Avaliação de Riscos

Aspectos avaliados
1. A organização identifica de forma abrangente os riscos que podem afetar a realização de seus objetivos, bem como suas causas e
2. Servidores de diversas áreas e níveis hierárquicos, conhecedores do negócio da organização, participam da identificação e avaliação de
3. Os riscos identificados são atribuídos a pessoas que têm responsabilidade e autoridade para gerenciá-los.

4. Os riscos identificados são levados à consideração da instância decisória	pertinente
5. Existem instrumentos definidos para documentar as etapas de identificação	e avaliação.
6. Todos os riscos identificados são submetidos ao processo de avaliação de riscos.	
7. São estimadas a probabilidade de ocorrência dos riscos identificados e as consequências, sobre os objetivos organizacionais, da materialização desses riscos.	
8. A avaliação de riscos produz informações qualitativas e quantitativas relevantes para a definição das respostas a riscos.	

Respostas a Riscos

Aspectos avaliados	
9. Existem parâmetros definidos para a escolha das ações de aceitar, transferir, evitar ou mitigar os riscos analisados.	
10. A percepção das partes interessadas é levada em conta na escolha de respostas apropriadas.	
11. A escolha de respostas aos riscos leva em conta a relação custo-benefício das respostas consideradas.	
12. Utilizam-se planos de tratamento de riscos nos quais se especificam as respostas a risco selecionadas, bem como prazos e	
13. Ocorre revisão periódica das respostas a risco visando avaliar se permanecem adequadas.	
14. Medidas de contingência para garantir a continuidade dos serviços prestados são definidas e periodicamente revisadas.	

Monitoramento e Comunicação de Riscos

Aspecto avaliado	
15. A gestão de riscos nesta organização apoia-se em sistema informatizado que permite a visão integrada das etapas de identificação, avaliação, tratamento e monitoramento de riscos.	
16. O controle interno, ou a auditoria interna, contribui ativamente para as atividades de gestão de riscos na organização.	
17. Foram estabelecidas medidas de desempenho que permitem avaliar se as respostas a riscos adotadas foram ou não efetivas.	
18. No monitoramento do processo de gestão de riscos, são evidenciadas as oportunidades de melhoria e as lições aprendidas	

19. Há mecanismos de comunicação que garantam que as partes interessadas sejam comunicadas sobre os riscos-chave a que o negócio está sujeito, as respostas adotadas e a eficácia do processo de gestão de riscos.

Parte C – Parcerias

Esta parte do questionário trata de aspectos relativos a gestão de riscos em parcerias estabelecidas pela organização com entes públicos ou privados. Entende-se por parceria qualquer arranjo estabelecido a fim de possibilitar um relacionamento colaborativo entre as partes visando o alcance de objetivos específicos previamente acordados. Parcerias envolvem riscos e benefícios compartilhados. São exemplos de parceria os arranjos de terceirização ou contratação de serviços relevantes para o negócio e a criação de sociedades de propósito específico.

1. Liste as parcerias existentes entre a DAP e outros órgãos (públicos ou privados) e, para cada uma delas, informe se há atividades conjuntas de gestão de riscos, por meio das seguintes respostas: "sim", "não" ou "em parte".

--

Considerando apenas os tipos de parcerias em que existem atividades conjuntas de gestão de riscos, responder as questões a seguir com base nesta escala:

1	2	3	4	5
Discordo totalmente	Discordo mais do que concordo	Não concordo Nem concordo	Concordo mais do que discordo	Concordo totalmente

Aspectos avaliados
2. Nas parcerias estabelecidas, existe clareza sobre quem é responsável por gerenciar cada risco.
3. Nas parcerias firmadas, está estabelecido em quais condições e para quem cada responsável deve fornecer informações.
4. Os responsáveis pela gestão de riscos no âmbito das parcerias firmadas têm autonomia e recursos para tomar e implementar

decisões relacionadas a risco.
5. Todas as organizações que influenciam o sucesso de projetos, programas ou serviços-chave são identificadas e essas influências consideradas no processo de gestão de riscos.
6. Há informação regular e confiável para monitorar o desempenho da gestão de riscos de todas as organizações parceiras.
7. A organização estrutura com seus parceiros arranjos de contingência (incluindo a priorização de ações de mitigação) para minimizar efeitos adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falha ao entregar o serviço.
8. A transferência de riscos a organizações públicas e privadas é precedida por avaliação da capacidade destas de gerenciá-los.
9. Quando riscos são transferidos a organizações parceiras, mantém-se a capacidade de gerenciar e monitorar desempenho e de adotar tempestivamente medidas em caso de dificuldades.

Parte D – Resultados

Esta parte do questionário trata dos resultados obtidos em decorrência da gestão de riscos existente na organização. Todas as questões objetivas devem ser respondidas com base nesta escala:

1	2	3	4	5
Discordo totalmente	Discordo mais do que concordo	Não concordo Nem concordo	Concordo mais do que discordo	Concordo totalmente

Aspectos Avaliados

1. A organização avalia a eficácia do processo de gestão de riscos.
2. O processo de gestão de riscos contribuiu para a melhoria do processo decisório fornecendo informações sobre riscos e evidências que os suportam.
3. O processo de gestão de riscos contribuiu para uma coordenação clara e efetiva de políticas e ações entre unidades organizacionais.
4. O processo de gestão de riscos contribuiu para uma boa coordenação, compreensão e gerenciamento de riscos com parceiros.

5. Planos e políticas organizacionais têm sido aperfeiçoados com base em avaliações e propostas consistentes de gestão de riscos.
6. O processo de gestão de riscos contribuiu para o aprimoramento da comunicação sobre riscos com as partes interessadas.
7. O processo de gestão de riscos contribuiu para a melhoria do processo decisório na organização.
8. O processo de gestão de riscos tem levado os servidores a se envolverem com avaliação e controle de riscos em suas atividades cotidianas.
9. A gestão de riscos na organização tem contribuído para...
a) ... a realização das objetivos relativos ao gerenciamento de projetos.
b) ... a realização dos objetivos referentes à eficiência das operações.
c) ... a realização dos objetivos referentes à melhoria da governança.
d) ... a realização dos objetivos relativos à reputação da organização.
e) ... a melhoria da qualidade de bens e serviços ofertados.
f) ... assegurar o cumprimento das leis e normas pertinentes.

Anexo b

Perguntas da entrevista

1. Há quanto tempo existe uma gestão de riscos formalizada na DAP?
2. Quais os tipos de riscos que a diretoria gere?
3. Como é realizado o monitoramento dos riscos?
4. Como é realizada a comunicação entre as partes interessadas? Essa comunicação tem se demonstrado eficaz?

5. Existem indicadores para avaliar a gestão de riscos na diretoria?
6. Foi observado que existe uma política, uma diretriz e um manual técnico de gestão de riscos que norteiam todo o exército quanto ao tema. Existe algum documento próprio da DAP tratando sobre gestão de riscos?
7. Como a alta administração (diretor) participa da gestão de riscos?
8. Quais os esforços institucionais empreendidos nos últimos 2 anos e os esforços previstos para os próximos 2 anos para aprimorar a gestão de riscos?
9. Quais as maiores dificuldades enfrentadas pela instituição na gestão de riscos?
10. Existe uma cultura de gestão de riscos na diretoria?



idn

Bo
pro
cit
ref
Nos
são

idp

A ESCOLHA QUE
TRANSFORMA
O SEU CONHECIMENTO