MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

GOVERNANÇA

PCA 16-17

PLANO DE GERENCIAMENTO DE RISCOS E DA INTEGRIDADE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

2023

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

GOVERNANÇA

PCA 16-17

PLANO DE GERENCIAMENTO DE RISCOS E DA INTEGRIDADE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

2023

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

PORTARIA CIAER Nº 31/CHF-CIAER, DE 15 DE FEVEREIRO DE 2023.
Protocolo COMAER Nº 67002.000701/2023-02

Aprova a edição da PCA 16-17 "Plano de Gerenciamento de Riscos e da Integridade do Centro de Inteligência da Aeronáutica".

O **CHEFE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA**, tendo em vista o disposto na alínea 'b' do item 5.6 da DCA 16-2, aprovada pela Portaria nº 59/7SC, de 5 de novembro de 2018, resolve:

Art. 1º Aprovar a edição da PCA 16-17 "Plano de Gerenciamento de Riscos e da Integridade do Centro de Inteligência da Aeronáutica".

Art. 2º Esta Portaria entrará em vigor na data de sua publicação.

Art. 3º Revoga-se a Portaria CIAER nº 5, de 1º de junho de 2021, publicada no BCA nº 144, de 22 de junho de 2021.

Brig Ar RODRIGO GIBIN DUARTE
Chefe do CIAER

(Publicada no BCA nº , de de de 2023)

SUMÁRIO

PREFÁCIO

Uma cultura de gestão de riscos é fundamental para a obtenção dos resultados planejados por uma Organização.

Conforme menciona o "Referencial Básico de Gestão de Riscos" do TCU, a mitigação de riscos remonta à antiga Babilônia. Mas foi no presente século que a abordagem sobre a gestão de riscos se desenvolveu amplamente.

Em 2002, um ano após o colapso da empresa Enron, decorrente de ocultação e manipulação de dados contábeis e falhas em auditorias, os Estados Unidos aprovaram a chamada Lei Sarbanes-Oxley. Por meio dela buscaram mitigar riscos, evitar a ocorrência de fraudes, proteger investidores e assegurar que as empresas que participam do mercado acionário norte-americano possuam estruturas e mecanismos adequados de governança.

No ano de 2004 o *Committee of Sponsoring Organizations* (***COSO***) publicou o *Enterprise Risk Management – Integrated Framework*, conhecido como COSO-ERM. Esta estrutura foi projetada com o objetivo de orientar as organizações no estabelecimento de um processo de gestão de riscos corporativos e na aplicação de boas práticas sobre o tema.

Em 2009 foi publicada a norma técnica ISO 31000 *Risk Management – Principles and Guidelines*, que provê princípios e boas práticas para um processo de gestão de riscos corporativos, aplicável a organizações de qualquer setor, atividade e tamanho (ABNT, 2009).

No âmbito da Administração Pública Federal, o Ministério do Planejamento, Desenvolvimento e Gestão (MP) e a Controladoria-Geral da União (CGU) expediram a Instrução Normativa Conjunta nº 1, de 10 de maio de 2016, dispondo sobre controles internos, gestão de riscos e governança. Posteriormente foi editado o Decreto nº 9.203, de 22 de novembro de 2017, dispondo sobre a política de governança e abordando, dentre outros temas, a gestão de riscos.

Sendo assim, em consonância com o arcabouço normativo que rege o assunto, particularmente com as diretrizes gerais do Comando da Aeronáutica, o CIAER deve identificar, dentre os processos que permeiam suas atividades, quais as situações que geram riscos que podem impactar no alcance de seus objetivos.

Os riscos variam conforme a organização, pois são peculiares às suas práticas internas e à área em que atua.

Com base na sua identificação e análise, deve-se desenvolver e aplicar políticas e procedimentos voltados à sua prevenção e detecção, a fim de remediar a ocorrência de riscos que possam ameaçar seus objetivos, incluindo aqueles relacionados a fraudes e à corrupção. Essas políticas devem ser coordenadas entre si, bem como ser de fácil compreensão e aplicação na rotina de trabalho dos servidores.

O instrumento que formaliza o processo de gerenciamento de riscos corporativos é a Política de Gestão de Riscos – PGR, que, segundo a ISO 31000/2009, é a "declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos".

Nesse entendimento, essa Política de Gestão de Riscos, por meio do presente Plano de Gerenciamento de Riscos, tem como objetivo aplicar, no âmbito do CIAER, o gerenciamento de riscos diante da visão de portfólio de riscos a que a entidade está exposta, de modo

a identificar eventos em potencial, quer sejam ameaças ou oportunidades, cuja ocorrência poderá afetar os objetivos estabelecidos, traçando respostas que auxiliem em tomadas de decisões mais efetivas.

Este Plano de Gerenciamento de Riscos vincula-se ao Macroprocesso Inteligência do Plano Estratégico Militar da Aeronáutica e segue as orientações contidas na Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016; na DCA 16-2/2018, "Gestão de Riscos no Comando da Aeronáutica", que regula a gestão de riscos no âmbito da Força e cria o Comitê Diretivo de Gestão de Riscos – COMGER; na estrutura COSO ERM (Committee of Sponsoring Organizations Enterprise Risk Management)[1]– Gerenciamento de Riscos Corporativos; e na Cartilha de Metodologia de Gestão de Riscos 2018 do Ministério da Transparência e Controladoria Geral da União.

Ademais, descreve também os papéis e as responsabilidades de todos os envolvidos no plano para assegurar o efetivo funcionamento do processo de Gerenciamento de Riscos, no âmbito do CIAER. Assim, a publicação em apreço intenta propiciar ao seu efetivo orientação segura para a condução do aludido processo de modo a assegurar, com razoável probabilidade, o alcance dos objetivos do CIAER.

[1] Projetado para criar uma "consciência sobre riscos e controles" por toda a empresa e tornar-se um modelo comum para a discussão e avaliação de riscos organizacionais, o Enterprise Risk Management Framework (ERM), criado pelo COSO, é um processo executado pela Diretoria Executiva, gerência e outras pessoas e aplicado na determinação de estratégias por toda a empresa. Disponível em: <http://www.caposoftware.com/sgir-gestao-de-riscos-corporativos/coso-erm-enterprise-risk-management-framework/>. Acesso em: 09/10/2019.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

A presente publicação tem por finalidade estabelecer os princípios e as diretrizes gerais para o gerenciamento de riscos e da integridade em várias áreas e níveis de responsabilidade do CIAER.

1.2 CONCEITUAÇÕES

A terminologia utilizada baseou-se nas seguintes normas:

a) ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes que revisam a norma ABNT NBR ISO 31000:2009;

b) ABNT NBR ISO/IEC 31010:2012 – Técnicas para o Processo de Avaliação de Riscos; e

c) ABNT ISO/TR 31004:2015 – Gestão de Riscos – Guia para implementação da ABNT NBR ISO 31000:2009.

1.2.1 ANÁLISE DOS RISCOS

Processo pelo qual se busca compreender a natureza do risco e determinar o nível do mesmo. A análise dos riscos envolve a definição das probabilidades de ocorrência de cada evento de risco e seus impactos sobre os objetivos da organização. A probabilidade de ocorrência de um evento de risco está associada às causas geradoras do evento. Os impactos sobre a organização estão associados às consequências do evento de risco. Na fase de análise deverão ser identificados, também, os controles existentes para modificar os riscos.

1.2.2 APETITE A RISCO

Nível de risco que uma organização está disposta a aceitar. Conhecê-lo tem a ver com a percepção dos riscos que uma organização pode assumir. A sua definição deverá ser feita mediante declaração escrita de sua chefia. Este documento deverá orientar o comportamento da empresa e as suas decisões estratégicas.

Assim, a tomada de decisão deverá estar alinhada com o limite adequado de risco suportável de modo que se preserve a probabilidade razoável de atingirem-se os objetivos estabelecidos.

1.2.3 CATEGORIAS DO RISCO

a) **Estratégico** trata-se de eventos que podem impactar na missão, nas metas ou nos objetivos estratégicos da unidade/órgão;

b) **Operacional** trata-se de eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e a eficiência dos processos organizacionais; e

c) **Integridade** trata-se de eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos.

1.2.4 COMITÊ DIRETIVO DE GESTÃO DE RISCOS (COMGER)

O COMGER é o órgão de mais alto nível de assessoria do Comandante da Aeronáutica, do Chefe do Estado-Maior e do Alto-Comando, podendo ser convocado por iniciativa de qualquer uma dessas instâncias da alta administração da FAB. Tem por objetivo auxiliar na identificação, comunicação, análise, avaliação, tratamento e monitoramento dos riscos. É composto pelos seguintes membros: Presidente (Vice-Chefe do Estado-Maior da Aeronáutica); Vice-Presidente (Chefe do EGE do EMAER); membros permanentes (Chefe do Estado-Maior do COMPREP, Chefe do Estado-Maior Conjunto do COMAE, Chefe do Estado-Maior do COMGAP, Chefe do Estado-Maior do COMGEP, Vice-Diretor do DECEA, Vice-Diretor do DCTA e Vice-Secretário de Economia, Finanças e Administração da Aeronáutica) e membro assessor (Chefe do Centro de Controle Interno da Aeronáutica).

1.2.5 CRITÉRIOS DE RISCOS

Os critérios de Gestão de Riscos estabelecem as bases para a avaliação dos riscos. Devem definir como serão mensuradas as probabilidades, os impactos dos eventos de risco, as naturezas das causas e consequências, bem como sua mensuração.

1.2.6 ESTRATÉGIA DE CONTENÇÃO

Linha de ação a ser adotada para reduzir a probabilidade de ocorrência de um evento de risco ou atenuar o seu impacto.

1.2.7 EFEITO

Um desvio em relação ao esperado (positivo ou negativo).

1.2.8 EVENTO

Ocorrência ou mudança, em um conjunto específico de circunstâncias, que pode consistir em uma ou mais ocorrências e ter várias causas, decorrentes de um incidente ou um acidente.

1.2.9 GERENCIAMENTO DE RISCOS

É um processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações para fornecer razoável certeza quanto ao alcance dos objetivos de uma organização.

1.2.10 GESTÃO DE RISCO

Processo aplicado no desenvolvimento de estratégias, formuladas pra identificar em toda organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco da organização.

1.2.11 GESTOR DE RISCO

Agente responsável pelo gerenciamento de determinado risco. Ele deve possuir competência suficiente para orientar e acompanhar as ações de mapeamento, de avaliação e de mitigação do risco. São responsabilidades do gestor de risco:

a) assegurar que o risco seja gerenciado de acordo com o Plano de Gestão de Riscos da organização;

b) monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com o apetite a riscos da organização; e

c) garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da organização.

1.2.12 IDENTIFICAÇÃO DOS RISCOS

Processo de busca, reconhecimento e descrição dos riscos. A identificação dos riscos envolve a identificação das fontes de risco, das áreas impactadas, dos eventos de risco, bem como suas causas e consequências. A identificação dos riscos deve ser a mais ampla possível, visto que aqueles não identificados não são tratados nem acompanhados.

1.2.13 IMPACTO DO RISCO

Reflete a severidade dos efeitos da ocorrência do risco nos objetivos do projeto ou da atividade.

1.2.14 ÍNDICE DE RISCO

Classificação da magnitude do nível de risco em faixas (ou intervalos). Exemplo: os riscos podem ser classificados em baixo, médio, alto e extremo, dependendo da faixa de nível de risco.

1.2.15 MATRIZ DE RISCO

Instrumento gráfico em que são listados os riscos, organizados de acordo com o seu impacto e probabilidade.

1.2.16 MENSURAÇÃO DO RISCO

Significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência.

1.2.17 NÍVEL DE DECISÃO

Refere-se à autoridade competente para assumir os variados níveis de risco.

1.2.18 NÍVEL DE RISCO

Magnitude de um risco ou combinação de riscos expressa em termos da combinação das consequências e de suas probabilidades.

1.2.19 PARTE INTERESSADA

Pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por um evento.

1.2.20 PLANO DE AÇÃO

Documento desenvolvido com o intuito de orientar, facilitar e organizar as ações necessárias às respostas de controle dos riscos e que estabelece o que fazer, quando fazer, quem são os responsáveis e como esses implementarão os controles ou ações propostas para os riscos definidos.

1.2.21 PLANO DE GERENCIAMENTO DE RISCOS

Documento derivado da Política de Gestão de Riscos que especifica os riscos identificados, planos de resposta ao risco (para cada risco identificado), legenda da terminologia adotada, além de outras informações julgadas relevantes.

1.2.22 PLANO DE RESPOSTA AO RISCO

Documento do Gestor de Riscos que descreve as ações de contenção de efeitos potenciais dos riscos identificados, constando: identificação do risco, causas que podem levar à ocorrência do risco, consequências da ocorrência do risco, estratégia de contingência, limite para disparar a estratégia de contingência, ações para contenção do risco, acompanhamento das ações de contenção do risco e seus efeitos, objetivos do projeto afetados e custos, se o risco ocorrer.

1.2.23 PROBABILIDADE DE OCORRÊNCIA DO RISCO

É a chance de ocorrência de uma falha que pode conduzir a um determinado acidente. Essa falha pode ser de um equipamento ou componente, de uma falha humana ou de fatores externos.

1.2.24 PROPRIETÁRIO DO RISCO

Pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco. OBS: Cada risco identificado deverá ser associado a um proprietário.

1.2.25 PROGRAMA DE TRABALHO ANUAL (PTA)

É o documento que tem por finalidade orientar, de forma integrada e articulada com o Plano Setorial do CIAER, as ações a serem desenvolvidas por este Centro.

1.2.26 REGISTRO DE RISCOS

Documento que registra a lista com a descrição dos riscos identificados e analisados.

1.2.27 RISCO

Possibilidade de ocorrência de um evento que venha a ter efeito no cumprimento dos objetivos, sendo medido em termos de impacto e de probabilidade.

1.2.28 RISCOS PRIORITÁRIOS

Grupo de riscos cuja gestão deve ser priorizada e os seus indicadores devem ser monitorados regularmente e com a máxima atenção, devido ao impacto potencialmente elevado para o negócio.

1.3 ÂMBITO

Este Plano é de observância obrigatória e aplica-se ao Centro de Inteligência da Aeronáutica.

2 METODOLOGIA

2.1 FUNDAMENTOS

O Plano em tela foi elaborado a partir da análise e do estudo da Política de Gestão de Riscos do COMAER (DCA 16-2, de 2018), do material disponibilizado pelo Ministério da Defesa, do Manual de Elaboração de Relatórios do Controle Interno emitido pela CGU, bem como diversos regulamentos expedidos pelas Organizações Militares pertencentes ao COMAER.

2.2 FERRAMENTAS DE APOIO

Por intermédio do curso EAD oferecido pelo então Ministério do Planejamento, Desenvolvimento e Gestão, foi aproveitado o documento intitulado "Planilha Documentadora", a qual, após seu preenchimento, apresenta a síntese de Mapa de Riscos como resultado, tendo sido adaptada à realidade do CIAER.

2.3 ADAPTAÇÕES

As referidas adaptações foram realizadas na planilha denominada "Impacto – Fatores de Análise", que indicam a mensuração do evento de risco a ser considerado.

2.4 BASE DOS EVENTOS

Os eventos de risco foram identificados com base em dados históricos, experiências, retroalimentação de partes interessadas, observações, previsões e opiniões de especialistas do CIAER.

2.5 PROPOSTA

Feita a análise e a revisão dos eventos identificados pela Assessoria de Governança (ASGOV), foram extraídas as melhores informações, a fim de compor o Plano de Ação do CIAER, os quais seguem anexos.

2.6 RESPONSÁVEIS PELO PLANO DE RISCO

A planilha abaixo aponta os responsáveis pelo risco de cada Assessoria/Divisão do CIAER.

Quadro 1 – Responsáveis pelo risco

ASSESSORIA/DIVISÃO	RESPONSÁVEL
DIC	Chefe da DIC
DAI	Chefe da DAI
DCI	Chefe da DCI

Fonte: CIAER.

2.6.1 DIRETRIZES E PROCESSO DE GESTÃO DE RISCO

As diretrizes apresentadas neste Plano definem e caracterizam as macro-etapas do processo de gestão integrada de riscos neste Centro de Inteligência. Servem de base para o desenvolvimento e a implementação do Plano de Gestão de Riscos, levando em consideração o planejamento estratégico, em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes adotados pelo CIAER, sendo compreendido pelas seguintes atividades:

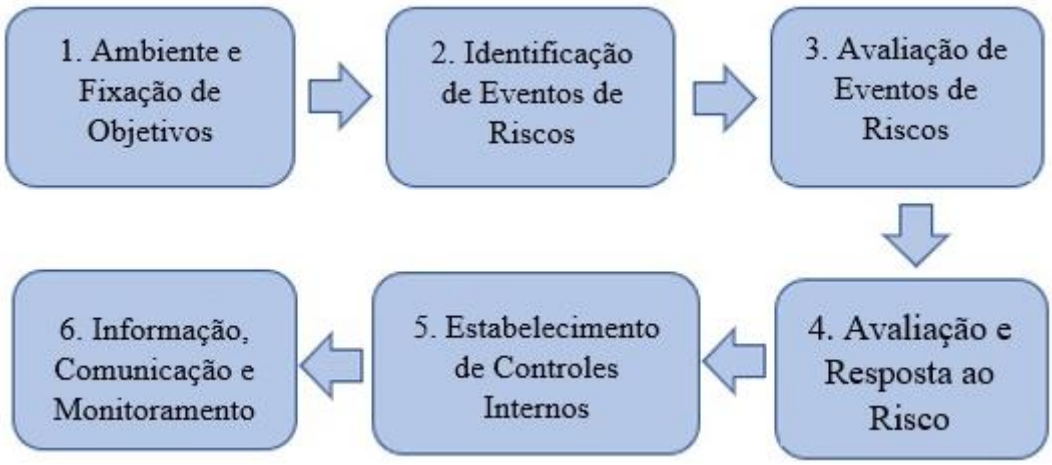

Figura 1: Atividades
Fonte: DCA 16-2/22.

2.7 AMBIENTE E FIXAÇÃO DE OBJETIVOS

O Chefe do CIAER organizou o ambiente interno da Organização para implementação do gerenciamento de riscos. A preparação do ambiente visou colher dados e informações a fim de identificar os eventos de riscos e escolher as ações mais adequadas para assegurar o alcance das metas.

2.7.1 TÉCNICA DE LEVANTAMENTO

Por meio da técnica denominada *brainstorming*[2] foi possível realizar um levantamento a respeito do ambiente interno e da fixação de objetivos, contribuindo para identificar a existência de aspectos relacionados à integridade e demais riscos, conforme modelo abaixo:

2 O brainstorming é uma dinâmica de grupo que é usada em várias empresas como uma técnica para resolver problemas específicos, para desenvolver novas ideias ou projetos, para juntar informação e para estimular o pensamento criativo. < https://www.significados.com.br/brainstorming/>. Acesso em: 09/10/2019

Órgão / Unidade/ Divisão		
A- Informações sobre o Ambiente Interno - existência de:	**Sim**	**Não**
Código de Ética / Normas de Conduta	( )	( )
Estrutura Organizacional	( )	( )
Política de Recursos Humanos (compromisso com a competência e desenvolvimento)	( )	( )
Atribuição de Alçadas e Responsabilidades	( )	( )
Normas Internas	( )	( )
B- Informações sobre a Fixação de Objetivos - existência de:	**Sim**	**Não**
Missão	( )	( )
Visão	( )	( )
Objetivos	( )	( )
Este formulário tem a finalidade de avaliar aspectos dos dois primeiros componentes do COSO GRC (Ambiente Interno e Fixação de Objetivos) e contribui para identificar também a existência de aspectos relacionados à integridade.		
Informações sobre a meta do PTA decorrente do PLANSET		
Meta		
Tarefa		
Objetivo da meta		
Leis e Regulamentos:		
Sistemas:		

Figura 2: Modelo de formulário utilizado para o *brainstorming*.
Fonte: Divisões do CIAER 2022.

2.7.2 AMBIENTE INTERNO

Cabe destacar que o ambiente interno, segundo o COSO ERM (COSO 2017), compreende o tom de uma organização e fornece a base para a identificação dos riscos, bem como a sua filosofia de gerenciamento, além do apetite a risco, da integridade e dos valores éticos, do ambiente em que estes estão.

Formulário de Levantamento de Informações sobre Ambiente e sobre a Fixação de Objetivos		
Órgão / Unidade	COMAER	
ODSA	CIAER	
Informações sobre o Ambiente Interno - existência de:	**Sim**	**Não**
Código de Ética / Normas de Conduta	(X)	( )
Estrutura Organizacional	(X)	( )
Política de Recursos Humanos (compromisso com a competência e desenvolvimento)	(X)	( )
Atribuição de Alçadas e Responsabilidades	(X)	( )
Normas Internas	(X)	( )
Informações sobre a Fixação de Objetivos - existência de:	**Sim**	**Não**
Missão	(X)	( )
Visão	(X)	( )
Objetivos	(X)	( )
Este formulário tem a finalidade de avaliar aspectos dos dois primeiros componentes do COSO GRC (Ambiente Interno e Fixação de Objetivos) e contribui para identificar também a existencia de aspectos relacionados à integridade.		
Informações sobre o Macroprocesso/Processo		
Macroprocesso:	Inteligência	
Processos:	Produção e Proteção do Conhecimento	
Objetivo do Macroprocesso / Processo:	Fornecer subsídios úteis e oportunos	
Leis e Regulamentos:	Normas e Diretrizes do COMAER e do CIAER	
Sistemas:	SINTAER, SISBIN, SINDE	

Figura 3: Formulário de Levantamento de Informações sobre Ambiente e sobre a Fixação de Objetivos.

2.8 ANÁLISE SWOT

Em seguida foi realizada análise SWOT[3], com foco nos processos de produção e proteção do conhecimento, visando obter informações para apoiar a identificação de eventos de riscos, bem como escolher as ações mais adequadas para assegurar o alcance dos objetivos do CIAER.

2.8.1 OBTENÇÃO DE INFORMAÇÕES

As informações obtidas sobre o ambiente interno e externo, em conjunto com as informações do processo, contribuem para as demais etapas do processo de gerenciamento de riscos. A imagem abaixo sintetiza a aplicação da análise SWOT:

Figura 4: Modelo de formulário para *brainstorming*.
Fonte: PCA 11-344/19.

2.8.2 PROCEDIMENTO

Conforme mencionado, a análise SWOT foi aplicada mediante questionário entregue aos Chefes de Divisão, cujas respostas não estão inseridas no formulário abaixo por tratar-se de informações sensíveis e/ou classificadas como sendo de acesso restrito.

C- Análise do Ambiente Interno	
Forças (Pontos Fortes)	1. 2. 3. 4. 5.
Fraquezas (Pontos Fracos)	1. 2. 3. 4. 5.
Análise do Ambiente Externo	
Oportunidades (Pontos Fortes)	1. 2. 3. 4. 5.
Ameaças (Pontos Fracos)	1. 2. 3. 4. 5.

Figura 5: Modelo de formulário utilizado para o *brainstorming*.

3 A análise SWOT é um importante instrumento utilizado para planejamento estratégico que consiste em recolher dados importantes que caracterizam o ambiente interno (forças e fraquezas) e externo (oportunidades e ameaças da Instituição).

2.8.3 RESULTADO

Desse modo, foi possível obter informações para apoiar a identificação de potenciais eventos de riscos, bem como escolher as ações mais adequadas para assegurar a razoável probabilidade de alcance dos objetivos do CIAER.

2.9 IDENTIFICAÇÃO DE EVENTOS DE RISCO

A identificação de riscos deve reconhecer e descrever os riscos aos quais a organização está exposta. Nesta etapa devem ser definidos eventos, fontes, impactos e responsáveis por cada risco (Anexo A).

2.9.1 PARTICIPAÇÃO DOS ENVOLVIDOS

A identificação dos riscos foi realizada com a participação de todos os envolvidos nas atividades do CIAER, em seus diferentes níveis.

2.9.2 MENSURAÇÃO DOS RISCOS

Nessa etapa foram mensuradas as causas, os efeitos e as consequências dos eventos de risco, considerando o resultado da análise do Ambiente Interno e da Fixação de Objetivos da primeira etapa.

2.10 AVALIÇÃO DE EVENTOS DE RISCOS

Após a identificação dos riscos, foram realizadas análises qualitativas e quantitativas, visando à definição dos atributos de impacto e de vulnerabilidade, utilizadas na priorização dos riscos a serem tratados. Esta etapa incluiu o levantamento e a análise dos controles já existentes, apurando, assim, os riscos residuais (Anexo B).

Subprocesso / Atividade	Identificação de Eventos de Riscos				
	Eventos de Risco	Causas	Efeitos / Consequências	Categoria do Risco	Natureza do Risco orçamentário ou financeiro?
Proteção do Conhecimento/ Segurança nas comunicações.	Comprometimento de informações sigilosas.	1.Ataque de hackers. 2.Interceptação das comunicações sigilosas. 3.Vazamento não intencional ou intencional de informações sigilosas.	1.Impacto na operação do COMAER. 2.Impacto na proteção de conhecimentos sigilosos.	Estratégico	Não
Produção do Conhecimento/ Sistema de obtenção e exploração de dados de forma automática e integrada.	Degradação da capacidade de operação do sistema.	1.Insuficiência de pessoal capacitado para operar os sistemas. 2.Insuficiência na manutenção de sistemas e meios de TI.	1.Redução da capacidade de obtenção de dados no ambiente cibernético 2.Redução da quantidade de dados obtidos no ambiente cibernético. 3.Impacto nos processos de produção e proteção de conhecimento.	Operacional	Não
Proteção do Conhecimento/ Credenciamento de segurança.	Ingresso de pessoas com antecedentes de corrupção e fraude.	Insuficiência de controles, ferramentas e recursos de TI com capacidade detectiva de elementos de integridade indesejada.	Utilização de informações privilegiadas que possam alimentar esquemas de corrupção e fraude.	Integridade	Não
Produção do Conhecimento/ Avaliação, Análise, Integração e Interpretação dos dados e/ou informações disponíveis.	Assessoramento de Inteligência equivocado e/ou sem perfeita concordância com os fatos e/ou com as situações pela mera ilusão da verdade.	Insuficiência de controles no ciclo de Produção de Conhecimento, visando a proceder a uma avaliação, análise, integração e interpretação precisa dos dados e/ou informações disponíveis.	1.Impacto na operação do COMAER. 2.Impacto na produção de conhecimentos pela utilização de dados e/ou informações cujos conteúdos são duvidosos ou não são verdadeiros.	Estratégico	Não

Figura 6: Identificação de eventos de riscos.
Fonte: CIAER

2.11 CONTROLES INTERNOS

Nesta fase foram realizadas a identificação e a avaliação dos controles existentes com objetivo de analisar as possíveis medidas de mitigação previamente aplicadas aos eventos identificados. Essas medidas serviram de base para a primeira avaliação da probabilidade e do impacto dos eventos considerados e da primeira evolução do nível de risco (NR) ou grau de risco. A figura a seguir apresenta um exemplo de planilha para a execução dessa atividade:

Avaliação do Riscos		
Identificação dos Controles Existentes		
Descrição do Controle Atual	**Avaliação quanto ao Desenho do Controle**	**Avaliação quanto a Operação do Controle**
O CIAER possui uma série de instruções que reúnem medidas de segurança, recomendações e determinações que devem ser observadas para garantir condições mínimas de segurança dos ativos que deseja proteger.	(5) Há procedimentos de controles adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.
O CIAER promove a capacitação de militares por meio do Programa de Atividades de Ensino do CIAER. Quanto à manutenção dos sistemas de TI, o CIAER possui painel digital de controle on-line do funcionamento dos sistemas e dos meios.	(4) Há procedimentos de controles adequados (suficientes), mas não estão formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.
O CIAER realiza processo seletivo e de acompanhamento de conduta dos integrantes do Centro por meio de normativos que regulam o processo.	(5) Há procedimentos de controles adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.
"Check points" existentes nas fases do ciclo de Produção do Conhecimento, realizados pelos Chefes das Divisões Operacionais, até a avaliação final pelo Chefe do CIAER	(5) Há procedimentos de controle adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.

Figura 7: Identificação de controles existentes.
Fonte: CIAER.

2.12 APETITE AO RISCO

O apetite ao risco definido pelo Chefe do CIAER é **MODERADO**. Na hipótese de níveis de risco acima do apetite ao risco escolhido, serão estabelecidos outros mecanismos de controle de modo a diminuir a probabilidade e/ou impacto até que se alcance o nível de risco compatível com o apetite ao risco determinado.

2.13 PREENCHIMENTO AUTOMÁTICO DA PLANILHA

Ao se preencher a Matriz de Risco, presente nas abas “Cálculo do risco inerente” e “Cálculo do risco residual”, com os valores de probabilidade e de impacto de cada evento de risco, o nível de risco fica automaticamente definido e preenchido no campo correspondente por meio de fórmula da planilha (Anexo C e D).

Avaliação do Riscos					
Identificação dos Controles Existentes			**Risco Residual**		
Descrição do Controle Atual	**Avaliação quanto ao Desenho do Controle**	**Avaliação quanto à Operação do Controle**	**P**	**I**	**NR**
O CIAER possui uma série de instruções que reúnem medidas de segurança, recomendações e determinações que devem ser observadas para garantir condições mínimas de segurança dos ativos que deseja proteger.	(5) Há procedimentos de controles adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.	2	3	Risco Moderado
O CIAER promove a capacitação de militares por meio do Programa de Atividades de Ensino do CIAER. Quanto à manutenção dos sistemas de TI, o CIAER possui painel digital de controle on-line do funcionamento dos sistemas e dos meios.	(4) Há procedimentos de controles adequados (suficientes), mas não estão formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.	2	3	Risco Moderado
O CIAER realiza processo seletivo e de acompanhamento de conduta dos integrantes do Centro por meio de normativos que regulam o processo.	(5) Há procedimentos de controles adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.	1	3	Risco Pequeno
"Check points" existentes nas fases do ciclo de Produção do Conhecimento, realizados pelos Chefes das Divisões Operacionais, até a avaliação final pelo Chefe do CIAER	(5) Há procedimentos de controle adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.	2	3	Risco Moderado

Figura 8: Controles existentes e os riscos.
Fonte: CIAER

2.14 RESPOSTA AO RISCO

Posteriormente à avaliação dos riscos relevantes, a organização determinou as respostas a serem adotadas. As respostas possíveis são: mitigar, aceitar, transferir ou evitar os riscos (Anexo E).

Figura 9: Respostas aos riscos.

Fonte: DCA 16-2/22.

2.14.1 APETITE E RESPOSTA AO RISCO

A escolha fundamentalmente do grau de apetite ao risco do CIAER foi homologada pelo Chefe no presente Plano de Gerenciamento de Riscos do Centro. Neste documento decidiu-se **MITIGAR**, conforme o nível do risco sob análise. Desse modo, embora o risco residual apresentar NR dentro do apetite ao risco estabelecido, a estratégia adotada como resposta ao risco gerou ações propostas no Plano de Ação (Anexo F).

2.14.2 MEDIDAS DE CONTROLE

No caso de o NR encontrar-se fora do apetite ao risco estabelecido, poderiam ser adotadas medidas de controle aptas a minimizar a probabilidade e/ou o impacto até que o NR estivesse dentro do apetite ao risco. Importante ressaltar que a análise custo-benefício deverá sempre ser considerada ao se definir mecanismos de controle para a mitigação dos eventos de risco. Essa reflexão visa evitar a adoção de controles que possam se revelar mais custosos do que as consequências da materialização do risco.

2.14.3 NÍVEIS DE RISCO

Os valores utilizados para a definição dos níveis de riscos foram definidos conforme figura a seguir:

Quadro 2 – Escala de nível de risco

Níveis	**Pontuação**
RC – Risco crítico	13 a 25
RA – Risco Alto	7 a 12
RM – Risco Moderado	4 a 6
RP – Risco Pequeno	1 a 3

Fonte: Estudo da ASGOV para elaboração do Plano de Gerenciamento de Riscos e da Integridade do CIAER/2022.

2.14.4 PLANO DE AÇÃO

Previamente à implementação das medidas de controle definidas, fez-se necessária a implementação de um Plano de Ação. Na elaboração desse plano foi adotada a metodologia "5W2H"[4], a qual permitiu obter as informações mínimas necessárias a serem inseridas no planejamento. A "Planilha Documentadora" tem uma aba denominada "Plano de Ação", a qual foi preenchida com essas informações (Anexo F).

[4] O nome desta ferramenta foi assim estabelecido por juntar as primeiras letras dos nomes (em inglês) das diretrizes utilizadas neste processo. As palavras são: *what*: o que será feito (etapas); *why*: por que será feito (justificativa); *where*: onde será feito (local); *when*: quando será feito (tempo); *who:* por quem será feito (responsabilidade); *how*: como será feito (método); *how much*: quanto custará fazer (custo).

2.15 INFORMAÇÃO, COMUNICAÇÃO E MONITORAMENTO

Em todas as etapas do processo de gestão integrada de riscos, a comunicação atingiu todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança exigidas.

2.15.1 MONITORAMENTO DOS RISCOS

No processo de monitoramento, acompanha-se a implantação e a manutenção do plano de ação, onde é verificado o alcance das metas estabelecidas, por meio de atividades gerenciais contínuas e/ou avaliações independentes.

Todos os riscos identificados serão monitorados por intermédio da ferramenta GPAer[5], que apresenta suporte para a gestão de risco e por intermédio de controles internos realizados pelos Chefes de Divisão em assuntos/matérias classificados como sendo de acesso restrito.

[5] É a ferramenta tecnológica desenvolvida para suportar as atividades previstas no SPGIA. O Sistema de Gestão Estratégica da Aeronáutica (GPAer) foi desenvolvido a partir do programa GPWeb, um software atualmente consolidado no mercado nacional. O sistema é uma poderosa ferramenta de planejamento e gestão estratégica, que permite, adicionalmente, o gerenciamento de projetos e portfólios de projetos seguindo conceitos internacionalmente padronizados.

3 DISPOSIÇÕES GERAIS

3.1 OBSERVAÇÃO DE OUTRAS NORMAS

O presente documento foi considerado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes adotados pelo CIAER.

3.1.1 DESDOBRAMENTO NORMATIVO

Este Plano poderá ser desdobrado em outros atos normativos, em alinhamento às diretrizes e princípios estabelecidos, os quais serão divulgados em todo o Centro.

3.2 COMPARAÇÃO DE RISCOS ENTRE CICLOS

De forma geral, nos ciclos seguintes do processo de gerenciamento de risco do processo organizacional, o CIAER considerou o nível de risco inerente calculado no 1º ciclo e reavaliou os controles para o cálculo do risco residual. A comparação entre os níveis de riscos residuais de diferentes ciclos objetivou identificar se os controles definidos nos Planos de Tratamento estão sendo eficazes para tratar os riscos.

3.3 PROCESSO DINÂMICO E ALTERAÇÕES

Considerando a dinâmica do processo, os anexos deste Plano podem sofrer alterações caso um novo risco seja identificado.

3.3.1 TRATAMENTO DOS RISCOS

Os riscos deverão ser tratados no nível de decisão no qual foram classificados. Caso o nível de decisão no qual o risco foi classificado seja acima da esfera da própria OM, ele deverá ser encaminhado à autoridade competente, seguindo a cadeia de comando.

4 DISPOSIÇÕES FINAIS

4.1 VIGÊNCIA

O presente Plano entrará em vigor a partir da data de publicação de sua Portaria de Aprovação.

4.2 ATUALIZAÇÃO

A atualização deste Plano é da responsabilidade da Assessoria de Governança do CIAER (ASGOV), em coordenação com os demais setores.

4.3 SITUAÇÕES NÃO PREVISTAS

Os casos não previstos neste documento serão levados à apreciação do Chefe do CIAER.

REFERÊNCIAS

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Gestão de Riscos no Comando da Aeronáutica: **DCA 16-2**. Aprovada pela Portaria nº 28/EGE1, de 31 de agosto de 2022. Brasília, 2022.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Gerenciamento de Riscos Corporativos –** Integrado com Estratégia e Performance: Sumário Executivo. Jun. 2017, 10 p. Título original: Enterprise Risk Management – Integrating with Strategy and Performance.

ROCHA, Hugo. **5W2H: o que significa, para que serve, como fazer e exemplos**. [S.l.], 06 fev. 2018: não paginado.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. Secretaria de Economia, Finanças e Administração da Aeronáutica. Gestão de Riscos da Secretaria de Economia, Finanças e Administração da Aeronáutica: **PCA 11-344**. Aprovada pela Portaria nº 8/AJUR, de 28 de janeiro de 2019. Boletim do Comando da Aeronáutica 202, Rio de Janeiro, RJ, 5 fev. 2019. Quarta Parte, Seção I, fl. 13058. Brasília, 2018. 43 p.

Anexo A – Identificação de eventos de risco

Identificação de Eventos de Riscos									
Subprocesso / Atividade	Eventos de Risco	Causas	Efeitos / Consequências	Categoria do Risco	Natureza do Risco orçamentário ou financeiro?	Risco Inerente			
						P	I	NR	
Proteção do Conhecimento/ Segurança nas comunicações.	Comprometimento de informações sigilosas.	1.Ataque de hackers. 2.Interceptação das comunicações sigilosas. 3.Vazamento não intencional ou intencional de informações sigilosas.	1.Impacto na operação do COMAER. 2.Impacto na proteção de conhecimentos sigilosos.	Estratégico	Não	2	3	Risco Moderado	
Produção do Conhecimento/ Sistema de obtenção e exploração de dados de forma automática e integrada.	Degradação da capacidade de operação do sistema.	1.Insuficiência de pessoal capacitado para operar os sistemas. 2.Insuficiência na manutenção de sistemas e meios de TI.	1.Redução da capacidade de obtenção de dados no ambiente cibernético. 2.Redução da quantidade de dados obtidos no ambiente cibernético. 3.Impacto nos processos de produção e proteção de conhecimento.	Operacional	Não	2	3	Risco Moderado	
Proteção do Conhecimento/ Credenciamento de segurança.	Ingresso de pessoas com antecedentes de corrupção e fraude.	Insuficiência de controles, ferramentas e recursos de TI com capacidade detectiva de elementos de integridade indesejada.	Utilização de informações privilegiadas que possam alimentar esquemas de corrupção e fraude.	Integridade	Não	1	3	Risco Pequeno	
Produção do Conhecimento/ Avaliação, Análise, Integração e Interpretação dos dados e/ou informações disponíveis.	Assessoramento de Inteligência equivocado e/ou sem perfeita concordância com os fatos e/ou com as situações pela mera ilusão da verdade.	Insuficiência de controles no ciclo de Produção de Conhecimento visando a proceder a uma avaliação, análise, integração e interpretação precisa dos dados e/ou informações disponíveis.	1.Impacto na operação do COMAER. 2.Impacto na produção de conhecimentos pela utlização de dados e/ou informações cujos conteúdos são duvidosos ou não são verdadeiros.	Estratégico	Não	2	3	Risco Moderado	

Anexo B – Avaliação dos riscos

Avaliação do Riscos						
Identificação dos Controles Existentes			Risco Residual		
Descrição do Controle Atual	Avaliação quanto ao Desenho do Controle	Avaliação quanto à Operação do Controle	P	I	NR
O CIAER possui uma série de instruções que reúnem medidas de segurança, recomendações e determinações que devem ser observadas para garantir condições mínimas de segurança dos ativos que deseja proteger.	(5) Há procedimentos de controles adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.	2	3	Risco Moderado
O CIAER promove a capacitação de militares por meio do Programa de Atividades de Ensino do CIAER. Quanto à manutenção dos sistemas de TI, o CIAER possui painel digital de controle on-line do funcionamento dos sistemas e dos meios.	(4) Há procedimentos de controles adequados (suficientes), mas não estão formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.	2	3	Risco Moderado
O CIAER realiza processo seletivo e de acompanhamento de conduta dos integrantes do Centro por meio de normativos que regulam o processo.	(5) Há procedimentos de controles adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.	1	3	Risco Pequeno
"Check points" existentes nas fases do ciclo de Produção do Conhecimento, realizados pelos Chefes das Divisões Operacionais, até a avaliação final pelo Chefe do CIAER	(5) Há procedimentos de controle adequados (suficientes) e formalizados.	(5) Procedimentos de controle são executados e com evidência de sua realização.	2	3	Risco Moderado

Anexo C - Cálculo de Risco Inerente

Macroprocesso / Processo	**Eventos de Riscos**
	Pesos
Proteção do Conhecimento/ Segurança nas comunicações.	Comprometimento de informações sigilosas.
Produção do Conhecimento/ Sistema de obtenção e exploração de dados de forma automárica e integrada.	Degradação da capacidade de operação do sistema.
Proteção do Conhecimento/ Credenciamento de segurança.	Ingresso de pessoas com antecedentes de corrupção e fraude.
Produção do Conhecimento/ Avaliação, análise, integração e interpretação dos dados e/ou informações disponíveis.	Assessoramento de Inteligência equivocado e/ou sem perfeita concordância com os fatos e/ou com as situações pela mera ilusão da verdade.

Probabilidade - Frequência Observada/Esperada						
Frequência Prevista	**Aspectos Avaliativos**					**Peso**
	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento **pode** ocorrer em algum momento	Evento **deve** ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias	
	< 10%	**>=10% <= 30%**	**>=30% <= 50%**	**>=50% <= 90%**	**>90%**	
	1 Muito baixa	**2 Baixa**	**3 Média**	**4 Alta**	**5 Muito Alta**	
2			Baixa			**2**
2			Baixa			**2**
1			Muito baixa			**1**
2			Baixa			**2**

Anexo C - continuação

Impacto - Fatores de Análise						
Aspectos Avaliativos						Peso
Estratégico-Operacional					Econômico-Financeiro	
Esforço de Gestão	Regulação	Reputação	Negócios/Serviços à Sociedade	Intervenção Hierárquica	Valor Orçamentário	
15%	17%	12%	18%	13%	25%	100%
Pesos Atribuídos ao Impacto (Análise Hierárquica de Processo - AHP)						
4	0	3	3	4	0	3
4	0	2	3	3	0	3
4	0	3	2	3	0	3
4	0	3	2	3	0	3

Matriz de Riscos							
IMPACTO	Catastrófico	5	5	10	15	20	25
	Grande	4	4	8	12	16	20
	Moderado	3	3	6	9	12	15
	Pequeno	2	2	4	6	8	10
	Insignificante	1	1	2	3	4	5
			1	2	3	4	5
			Muito Baixa	Baixa	Média	Alta	Muito Alta
			< 10%	>=10% <= 30%	>=30% <= 50%	>=50% <= 90%	>90%
			PROBABILIDADE				

Matriz de Risco:
-Impacto
-Probabilidade
-Nível de risco

Escala de Nível de Risco	
Níveis	Pontuação
RC - Risco Crítico	13 a 25
RA - Risco Alto	7 a 12
RM - Risco Moderado	4 a 6
RP - Risco Pequeno	1 a 3

Probabilidade					
Aspectos Avaliativos	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento **pode** ocorrer em algum momento	Evento **deve** ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias
Frequência Observada/Esperada	Muito baixa (< 10%)	Baixa (>=10% <= 30%)	Média (>30% <= 50%)	Alta (>50% <= 90%)	Muito alta (>90%)
Peso	1	2	3	4	5

Anexo D - Cálculo de Risco Residual

Macroprocesso / Processo	Eventos de Riscos
	Pesos
Proteção do Conhecimento/ Segurança nas comunicações.	Compromentimento de informações sigilosas.
Produção do Conhecimento/ Sistema de obtenção e exploração de dados de forma automárica e integrada.	Degradação da capacidade de operação do sistema.
Proteção do Conhecimento/ Credenciamento de segurança.	Ingresso de pessoas com antecedentes de corrupção e fraude.
Produção do Conhecimento/ Avaliação, análise, integração e interpretação dos dados e/ou informações disponíveis.	Assessoramento de Inteligência equivocado e/ou sem perfeita concordância com os fatos e/ou com as situações pela mera ilusão da verdade.

Probabilidade - Frequência Observada/Esperada						
Frequência Previstas	Aspectos Avaliativos					Peso
	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento **pode** ocorrer em algum momento	Evento **deve** ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias	
	< 10%	>=10% <= 30%	>=30% <= 50%	>=50% <= 90%	>90%	
	1 Muito baixa	2 Baixa	3 Média	4 Alta	5 Muito alta	
2	Baixa					2
2	Baixa					2
1	Muito baixa					1
1	Muito baixa					2

Anexo D - continuação

Impacto - Fatores de Análise							Nível de Risco	
Aspectos Avaliativos						Peso		
Estratégico-Operacional					Econômico-Financeiro			
Esforço de Gestão	Regulação	Reputação	Negócios/Serviços à Sociedade	Intervenção Hierárquica	Valor Orçamentário		Probabilidade x Impacto	Descrição
15%	17%	12%	18%	13%	25%	100%		
Pesos Atribuídos ao Impacto (Análise Hierárquica de Processo - AHP)								
4	0	3	3	4	0	3	6	Risco Moderado
4	0	2	3	3	0	3	6	Risco Moderado
5	0	3	2	3	0	3	3	Risco Pequeno
4	0	3	2	3	0	3	6	Risco Moderado

Matriz de Riscos							
IMPACTO	Catastrófico	5	5	10	15	20	25
	Grande	4	4	8	12	16	20
	Moderado	3	3	6	9	12	15
	Pequeno	2	2	4	6	8	10
	Insignificante	1	1	2	3	4	5
			1	2	3	4	5
			Muito Baixa	Baixa	Média	Alta	Muito Alta
			< 10%	>=10% <= 30%	>=30% <= 50%	>=50% <= 90%	>90%
			PROBABILIDADE				

Matriz de Risco:
-Impacto
-Probabilidade
-Nível de risco

Escala de Nível de Risco	
Níveis	Pontuação
RC - Risco Crítico	13 a 25
RA - Risco Alto	7 a 12
RM - Risco Moderado	4 a 6

Anexo E – Respostas aos riscos

Resposta a Risco					
Possíveis Respostas	**Controles Propostos / Ações Propostas**				
	Tipo	**Descrição**	**Data do Início**	**Data da Conclusão**	**Status**
Mitigar	Preventivo	Revisão de instruções e atos normativos do CIAER.	1/1/2023	23/12/2024	Em andamento
Mitigar	Preventivo	Realização dos cursos de capacitação previstos no CIAER quanto à gestão de pessoas. Quanto à manutenção de recursos de TI, deve-se manter os painéis e ferramentas de controles existentes.	1/1/2023	23/12/2024	Em andamento
Aceitar	Preventivo	Revisão da metodologia de ingresso de pessoas no CIAER e dos normativos do CIAER relacionados à integridade.	1/1/2023	23/12/2024	Em andamento
Mitigar	Preventivo	Revisão periódica das fases do ciclo da Produção do Conhecimento e dos respectivos "check points".	1/1/2023	23/12/2024	Em andamento

Macroprocesso / Processo	Controle Proposto / Ação Proposta								
	Descrição	Tipo	Objetivo	Área Responsável pela Implementação	Responsável Implementação	Como será implementado	Data do Início	Data da Conclusão	Status
Proteção do Conhecimento/ Segurança nas comunicações.	Revisão de instruções e atos normativos do CIAER.	Preventivo	Melhorar Controle Existente	Divisões do CIAER envolvidas	Grupo de trabalho de revisão de atos normativos e Divisões envolvidas	Por meio da publicação das instruções e atos normativos do CIAER atualizados.	1/1/2023	23/12/2024	Em andamento
Produção do Conhecimento/ Sistema de obtenção e exploração de dados de forma automática e integrada.	Realização dos cursos de capacitação previstos no CIAER quanto à gestão de pessoas. Quanto à manutenção de recursos de TI, deve-se manter os painéis e ferramentas de controles existentes.	Preventivo	Melhorar Controle Existente	Divisões do CIAER envolvidas	Chefes das Divisões envolvidas	Por meio da conclusão dos cursos de capacitação e formação de alunos	1/1/2023	23/12/2024	Em andamento
Proteção do Conhecimento/ Credenciamento de segurança.	Revisão da metodologia de ingresso de pessoas no CIAER e dos normativos do CIAER relacionados à integridade.	Preventivo	Melhorar Controle Existente	Divisões do CIAER envolvidas	Chefes das Divisões envolvidas	Por meio da publicação das instruções e atos normativos do CIAER atualizados.	1/1/2023	23/12/2024	Em andamento
Produção do Conhecimento/ Avaliação, Análise, Integração e Interpretação dos dados e/ou informações disponíveis.	Revisão periódica das fases do ciclo da Produção do Conhecimento e dos respectivos *"check points"*.	Preventivo	Melhorar Controle Existente	Divisões envolvidas, Vice-Chefe e Chefe do CIAER	Chefes das Divisões envolvidas	Por meio da publicação das instruções e atos normativos do CIAER atualizados.	1/1/2023	23/12/2024	Em andamento

[6] As instruções e atos normativos são classificados como sendo material de acesso restrito e encontram-se sob guarda dos respectivos Chefes de Divisão.