MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-26

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2024

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

TECNOLOGIA DA INFORMAÇÃO

ICA 7-26

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2024

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

PORTARIA DECEA Nº 1.323/SNOT, DE 13 DE MAIO DE 2024.
Protocolo COMAER nº 67600.010350/2024-71

Aprova a reedição da Instrução acerca do Processo de Gestão de Riscos de Segurança e Tecnologia da Informação do Departamento de Controle do Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso da atribuição que lhe confere o art. 4º da Portaria nº 651/GC3, de 11 de dezembro de 2023, e considerando o que consta do Processo nº 67600.026477/2023-21, procedente do DECEA, resolve:

Art. 1º Aprovar a reedição da ICA 7-26 "Processo de Gestão de Riscos de Segurança e Tecnologia da Informação do Departamento de Controle do Espaço Aéreo", que com esta baixa.

Art. 2º Revogar a Portaria DECEA nº 59/DGCEA, de 24 de maio de 2013 publicada no Boletim do Comando da Aeronáutica nº 120, de 26 de junho de 2013.

Art. 3º Esta Instrução entra em vigor em 3 de junho de 2024.

(a)Ten Brig Ar ALCIDES TEIXEIRA BARBACOVI
Diretor-Geral do DECEA

(Publicado no BCA nº , de de de 2024.)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar o Processo de Gestão de Riscos de Segurança e Tecnologia da Informação para o Departamento de Controle do Espaço Aéreo (DECEA) e suas Organizações Militares Subordinadas, bem como descrever os procedimentos correlatos ao referido Processo.

1.2 ÂMBITO E GRAU DE SIGILO

Esta Instrução se aplica ao DECEA e a todas as suas Organizações Militares Subordinadas, sendo considerado ostensivo o seu grau de sigilo.

1.3 ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

DCA – Diretriz do Comando da Aeronáutica

DECEA – Departamento de Controle do Espaço Aéreo

DTI – Diretoria de Tecnologia da Informação da Aeronáutica

GRSTI – Gestão de Riscos de Segurança da Informação

MCA – Manual do Comando da Aeronáutica

OM – Organização Militar

SDTE – Subdepartamento Técnico do DECEA

SSSI – Seção de Segurança de Sistemas da Informação

1.4 DEFINIÇÕES

Os conceitos e definições estão listados no Glossário de Segurança da Informação do DECEA (MCA 7-1) e no Glossário de Segurança da Informação (Portaria GSI/PR nº93, de 18 de outubro de 2021).

Para efeito desta Instrução, entende-se por:

1.4.1 ATIVO DE INFORMAÇÃO

Todo elemento que compõe os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada e os equipamentos em que ela é manuseada, transportada e descartada. O termo “ativo” possui essa denominação por ser considerado um elemento de valor para um indivíduo ou Organização e que, por esse motivo, necessita de proteção adequada.

1.4.2 ACEITAÇÃO DO RISCO

É a decisão de conviver com as consequências, caso um cenário de risco se materialize.

1.4.3 AMEAÇAS

Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas na confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização.

1.4.4 ANÁLISE DO RISCO

Constitui-se no uso sistemático de informações para identificar fontes de risco e estimar seu valor.

1.4.5 APETITE AO RISCO

Nível de risco que uma organização está disposta a aceitar.

1.4.6 AUDITORIA BASEADA EM RISCO

Auditoria planejada com base em uma avaliação de análise de riscos.

1.4.7 AVALIAÇÃO DE RISCO

Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

1.4.8 CONTROLE

Medida que mantém e/ou modifica o risco.

1.4.9 EVITAR O RISCO

Forma de tratamento de risco, na qual a alta administração decide não realizar a atividade, não se envolver ou não agir, a fim de se retirar de uma situação de risco. Pode também ser definida como a eliminação da causa raiz do risco, implementando ações para levar a probabilidade do risco a zero.

1.4.10 GESTÃO DE RISCOS

Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

1.4.11 IMPACTO DO RISCO

Reflete a severidade dos efeitos da ocorrência do risco nos objetivos da Organização, do Projeto ou da Atividade.

1.4.12 ÍNDICE DO RISCO

Classificação da magnitude do nível de risco em faixas (ou intervalos), exemplo, para 25 níveis de risco distintos, podem-se criar cinco índices de risco: o primeiro, para níveis 1 a 2; o segundo, para os níveis de 3 a 5; o terceiro, para os níveis de 6 a 10; o quarto, para os níveis de 12 a 16; e o quinto, para os níveis de 20 a 25.

1.4.13 MATRIZ DE RISCO

Ferramenta utilizada para avaliar os processos que envolvam riscos na organização, permitindo um enquadramento dos riscos dentro dos parâmetros estabelecidos.

1.4.14 NÍVEL DE RISCO

Magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências (severidade) e de suas probabilidades. Exemplo: Se as probabilidades dos riscos tiverem cinco níveis e a severidade quatro níveis, a combinação resulta em 20 níveis de risco possíveis.

1.4.15 PARTES INTERESSADAS

Também denominado de *stakeholders*, em inglês, são as pessoas e as organizações que podem ser afetadas por um projeto ou empresa, de forma direta ou indireta, positiva ou negativamente. Os *stakeholders* fazem parte da base da gestão de comunicação e são importantes para o planejamento e execução de um projeto. As principais partes interessadas de um projeto são os clientes, usuários, fornecedores, empresas, governo, gerente de projetos, patrocinador, investidor, sócio, colaborador, órgãos regulamentadores e outros.

1.4.16 PROBABILIDADE DE OCORRÊNCIA DO RISCO

É a chance de ocorrência de um evento que pode afetar o alcance dos objetivos organizacionais.

1.4.17 PROPRIETÁRIO DE ATIVO DE INFORMAÇÃO

Refere-se à parte interessada da unidade da Organização Militar, pessoa legalmente instituída por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

1.4.18 PROPRIETÁRIO DO RISCO

Pessoa ou entidade com a responsabilidade e a autoridade de gerenciar o risco, sendo que cada risco identificado deverá ser associado a um proprietário (ref. DCA 16-2/2017).

1.4.19 RISCO

Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, de integridade e de disponibilidade nos ativos de informação, causando, possivelmente, impactos ao negócio.

1.4.20 RISCO INERENTE

Risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

1.4.21 RISCO RESIDUAL

Risco a que a Organização, o projeto ou a atividade estão expostos, após a implementação de ações gerenciais para o tratamento do risco.

2 RESPONSABILIDADES

2.1 SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA

2.1.1 Normatizar e divulgar o processo no âmbito do DECEA.

2.1.2 Gerenciar e garantir a execução do processo de gestão de riscos no âmbito do DECEA.

2.1.3 Definir o contexto da gestão de riscos.

2.1.4 Comunicar riscos às partes interessadas.

2.1.5 Definir e coletar indicadores para a medição do nível de maturidade do processo de gestão de riscos.

2.1.6 Identificar oportunidades de melhorias no processo.

2.2 AUTORIDADE COMPETENTE DA OM – CHEFES DOS SUBDEPARTAMENTOS DO DECEA, CHEFES, DIRETORES E COMANDANTES DAS ORGANIZAÇÕES SUBORDINADAS AO DECEA

2.2.1 Garantir o cumprimento da Diretriz de Gestão de Riscos de Segurança e Tecnologia da Informação do DECEA (DCA 7-3), bem como os procedimentos a ela relacionados, por parte dos usuários sob sua responsabilidade.

2.2.2 Designar e instituir o Comitê de Segurança da Informação ou estrutura equivalente com a composição dos representantes de cada área/setor.

2.2.3 Orientar e supervisionar o Comitê.

2.2.4 Aprovar o Plano de Tratamento de Riscos.

2.2.5 Dar parecer e aprovar o adiamento de tratamento dos riscos definidos como nível "Médio".

2.2.6 Aprovar um intervalo de tempo para a resposta ao tratamento dos riscos definidos como nível "Alto".

2.3 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

2.3.1 Indicar os responsáveis pela execução das atividades de análise, avaliação e tratamento dos riscos no âmbito da OM.

2.3.2 Promover a integração dos responsáveis no Processo de Gestão de Riscos.

2.3.3 Monitorar o Processo de Gestão de Riscos.

2.3.4 Propor reuniões para tratar de assuntos pertinentes do Processo de Gestão de Riscos da OM.

2.3.5 Encaminhar as decisões deliberadas em reuniões à Autoridade Competente da OM.

2.3.6 Encaminhar os registros do processo de gestão de riscos ao SDTE.

2.3.7 Propor à Autoridade Competente da OM um intervalo de tempo para a resposta ao tratamento dos riscos definidos como nível “Alto”.

2.3.8 Informar imediatamente à Autoridade Competente da OM os riscos definidos como “Muito Alto”.

2.3.9 Receber, formalmente ou informalmente, de todos os participantes do Processo de Gestão de Riscos as sugestões de melhoria de contínua.

2.3.10 Apoiar o SDTE na definição do contexto da análise de riscos.

2.3.11 Avaliar o Plano de Tratamento de Riscos e encaminhar a Autoridade Competente da OM para aprovação.

2.3.12 Decidir e aprovar sobre a aceitação de riscos.

2.4 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO

2.4.1 Propor ao Comitê de Segurança da Informação sugestões e melhorias na definição do contexto da análise de riscos.

2.4.2 Coordenar e acompanhar a execução do processo de gestão de riscos no âmbito da OM.

2.4.3 Identificar e estimar os riscos acompanhado do proprietário do ativo de informação.

2.4.4 Avaliar os riscos acompanhado do proprietário do ativo de informação.

2.4.5 Elaborar o Plano de Tratamento de Riscos e comunicar os riscos ao proprietário de ativos de informação.

2.4.6 Monitorar os riscos aceitos.

2.4.7 Apresentar os registros do processo de gestão de riscos ao Comitê de Segurança da Informação.

2.5 PROPRIETÁRIO DE ATIVO DE INFORMAÇÃO

2.5.1 Implementar medidas ou controles para diminuição dos riscos dentro do prazo definido no Plano de Tratamento de Riscos.

2.5.2 Acompanhar a análise e avaliação dos riscos.

2.5.3 Revisar os resultados dos riscos analisados e avaliados.

2.5.4 Apoiar na comunicação de riscos às partes interessadas.

2.5.5 Propor novos controles no tratamento dos riscos identificados.

2.5.6 Aceitar os riscos.

3 MAPA DE GERENCIAMENTO DE RISCOS

3.1 INTRODUÇÃO

3.1.1 O Mapa de Gerenciamento de Riscos é uma atividade que deve conter a identificação e a análise dos principais riscos, que consiste a combinação da probabilidade e das consequências, a natureza do risco e a determinação do nível do risco, para que se possa orientar as Organizações nas ações e soluções para alcançar os resultados pretendidos.

3.1.2 O Gerenciamento de Riscos irá auxiliar as Organizações no estabelecimento de estratégias e tomadas de decisões fundamentadas para alcançar seus objetivos com ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos.

3.1.3 Primeiramente, as Organizações devem identificar e constituir uma listagem de eventos que possam ter múltiplas causas e levar a múltiplas consequências para que se possa avaliar e determinar seus riscos com o propósito de apoiar nas decisões e ações mais bem informadas.

3.1.4 Cada risco identificado significa a ocorrência de um evento que possa causar impacto no cumprimento de seus objetivos. A definição de risco pode ser resumida como a combinação de probabilidade e consequência.

3.1.5 A probabilidade é uma estimativa de ocorrência do evento, enquanto a consequência é o dano causado pelo evento em caso de perda da confidencialidade, integridade e disponibilidade.

3.1.6 O nível de risco é o resultado da multiplicação da probabilidade e consequência. Se a probabilidade do risco tiver cinco níveis e a consequência cinco níveis, a combinação resultará em 25 níveis de riscos possíveis.

3.1.7 As Organizações sempre devem proceder à atualização contínua do Mapa de Gerenciamento de Riscos, procedendo à reavaliação dos riscos identificados nas fases anteriores com a atualização de suas respectivas ações de tratamento, e à identificação, análise, avaliação e tratamento de novos riscos.

3.1.8 A etapa do tratamento de riscos de segurança da informação deve ser resultante da etapa de identificação, análise e avaliação dos riscos de segurança da informação.

3.2 ETAPA DEFINIÇÃO DO CONTEXTO

3.2.1 O contexto é o ambiente no qual a Organização busca atingir os seus objetivos e um dos primeiros passos para atingir estes objetivos é o estabelecimento do contexto, que identifica os fatores do ambiente, interno e externo, no qual a Organização persegue para alcançar seus objetivos.

3.2.2 Uma das ferramentas utilizadas para realizar a análise de fatores de ambiente é a matriz SWOT, que verifica o ambiente interno da Organização em relação aos pontos fortes (*Strengths*) e fracos (*Weaknesses*); e seu ambiente externo em relação às oportunidades (*Opportunities*) e ameaças (*Threats*).

3.2.3 Deve ser realizada a análise das partes interessadas e seus interesses, com uso de ferramentas tais como a análise das partes interessadas (*Stakeholders*), matriz de RACI (Responsável, Autoridade, Consultado e Informado).

3.2.4 Cada Organização pode adotar um conjunto de critérios considerados os mais importantes para analisar e avaliar os níveis de risco, tais como, escalas de probabilidade; escalas de consequências ou impactos; como será determinado se o nível de risco é tolerável ou aceitável e se novas ações de tratamento são necessárias, bem como as diretrizes de aceitação de riscos, a priorização e o tratamento de riscos.

3.2.5 Os Critérios de Avaliação de Riscos que são usados na fase de avaliação para estabelecer as prioridades para o tratamento de riscos devem ser descritos de forma concisa no contexto, sendo que a **probabilidade** é a estimativa de ocorrência de um evento e a **consequência** o nível do impacto para a Organização. A proposta da metodologia é que cada fator tenha uma escala numérica e pode ser interpretado como, por exemplo, 1- Muito Baixo, 2- Baixo, 3- Médio, 4- Alto e 5- Muito Alto.

3.2.6 Os ativos quanto à sua relevância também são considerados Critérios de Avaliação de Riscos que podem ser classificados em Confidencialidade (C), Integridade (I) e Disponibilidade (D) conforme ilustrado na tabela 1.

Relevância	Valor	Descrição
Muito Baixa	1	Critério de segurança da informação do ativo é desprezível
Baixa	2	Critério de segurança da informação do ativo é pouco importante
Média	3	Critério de segurança da informação do ativo é importante
Alta	4	Critério de segurança da informação do ativo é muito importante
Muito Alta	5	Critério de segurança da informação do ativo é fundamental

Tabela 1 – Avaliação dos ativos de informação

3.2.7 A escala de probabilidade proposta para o processo de gestão de riscos pode ser feita com 5 níveis. A tabela 2 descreve cada nível de probabilidade.

Nível de Probabilidade	Descrição	Frequência	Fator
Muito Baixo	Improvável. Evento extraordinário	Até 10%	1
Baixo	Raro. Evento casual	11% a 30%	2
Médio	Possível. Evento esperado	31% a 50%	3
Alto	Provável. Evento usual	51% a 90%	4
Muito alto	Praticamente Certo. Evento repetitivo	Maior que 90%	5

Tabela 2 – Descrição probabilidades de ocorrências

3.2.8 A seguir, apresentaremos 2 (duas) metodologias para definir o nível do risco. A primeira será pela fórmula **Valor de Risco = (C+I+D) x P;** a segunda pela Matriz Riscos, que é o resultado da combinação de **probabilidade e consequência** ou **probabilidade e impacto**.

3.2.9 A primeira metodologia para definir o Valor do Risco é calculado pela soma dos valores de Confidencialidade (1 a 5), Integridade (1 a 5) e Disponibilidade (1 a 5), que representam as consequências (estimativa do dano por perda de confidencialidade, integridade e disponibilidade), multiplicado pela Probabilidade de ocorrência da ameaça (1 a 5). A fórmula conhecida é **Valor de Risco = (C+I+D) x P**. Desta forma, o Nível do Risco vai variar de acordo com o Valor de Risco (3 a 75), que serão tratados como: "Muito Baixo", "Baixo", "Médio", "Alto" e "Muito Alto". A tabela 3 ilustra o Nível do Risco e o Valor de Risco para Critérios de Aceitação dos Riscos.

Nível do Risco	Valor do Risco
Muito Baixo	3 a 8
Baixo	9 a 16
Médio	18 a 35
Alto	36 a 56
Muito alto	60 a 75

Tabela 3 – Descrição nível de risco e valor de risco

3.2.10 A segunda metodologia para definir o Nível de Risco é por meio da **Matriz de Probabilidade x Consequência**, também conhecida como **Matriz de Risco** ou **Mapa de Calor**. A exibição do risco será pela combinação de probabilidade e consequência.

3.2.11 Outras metodologias podem ser definidas na Etapa Definição do Contexto, desde que encaminhadas para aprovação do SDTE.

3.2.12 A estimativa de risco na Etapa de Análise de Riscos pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas.

3.2.13 O Método Qualitativo define o impacto, a probabilidade e o nível de risco por qualificadores como, por exemplo, "Muito Alto", "Alto", "Médio", "Baixo", e "Muito Baixo", com base na percepção das pessoas.

3.2.14 O Método Semiquantitativo usa uma escala de valores previamente convencionados para mensurar a consequência e a probabilidade, os quais são combinados, por meio de uma fórmula, para produzir o nível de risco, como por exemplo, **(C+I+D) x P** ou **P x I (Probabilidade x Impacto** ou **Probabilidade x Consequência)** e que se baseia na opinião de especialistas.

3.2.15 O Método Quantitativo estima valores para as consequências e suas probabilidades na maioria dos casos a partir de dados históricos de incidentes e calculam o nível de risco a partir de unidades específicas definidas no desenvolvimento do contexto.

3.2.16 A seguir, apresentaremos uma Matriz de Risco que apresenta a valoração pelo Método Semiquantitativo, pois apresenta uma escala de valores de probabilidade e consequência de 1 a 5 e o resultado da combinação destes para calcular o nível do risco.

3.2.17 Primeiramente, devemos escolher um fator ou peso para a escala de consequências conforme ilustrado na tabela 4.

Nível do Impacto	Descrição	Fator / Peso
Muito Baixo	Mínimo impacto nos objetivos	1
Baixo	Pequeno impacto nos objetivos	2
Médio	Moderado impacto nos objetivos	3
Alto	Significativo impacto nos objetivos	4
Muito alto	Catastrófico impacto nos objetivos	5

Tabela 4 – Escala de consequências

3.2.18 Na sequência, calcula-se o Nível do Risco pela multiplicação dos fatores probabilidades e consequências (P x I), que vai variar de 1 a 25. A Organização pode utilizar a tabela 1 – Descrição probabilidades de ocorrências para efetuar a fórmula na Matriz de Probabilidade x Consequência.

PROBABILIDADE X CONSEQUÊNCIA		CONSEQUÊNCIA				
		1 Muito Baixo	2 Baixo	3 Médio	4 Alto	5 Muito alto
PROBABILIDADE	Muito Alto 5	5	10	15	20	25
	Alto 4	4	8	12	16	20
	Médio 3	3	6	9	12	15
	Baixo 2	2	4	6	8	10
	Muito Baixo 1	1	2	3	4	5

Tabela 5 – Matriz de Probabilidade x Consequência

3.2.19 Ao utilizar a Matriz de Riscos, o usuário deve primeiro definir a consequência que mais se adapta a situação e depois definir a probabilidade que mais se identifica com a consequência que ocorrerá (ABNT NBR IEC 31010:2021).

3.2.20 É importante que a Organização possua uma equipe de pessoas com entendimento dos riscos que estão sendo classificados e dos dados que estão disponíveis para ajudar no julgamento das consequências e probabilidades (ABNT NBR IEC 31010:2021).

3.2.21 Os riscos com consequências potencialmente altas são frequentemente mais preocupantes para uma tomada de decisão mesmo que a sua probabilidade seja baixa. Entretanto um risco frequente com um impacto baixo pode ter consequências cumulativas grandes ou de longo prazo (ABNT NBR IEC 31010:2021).

3.2.22 Uma vez que todos os riscos são identificados e devidamente documentados no Mapa de Riscos, uma minuciosa análise deve ser feita para cada um deles utilizando-se a escala de probabilidades e consequências conforme a tabela 5.

3.2.23 Nesta etapa, é realizada a análise do risco inerente sem considerar os controles já existentes, ou seja, sem nenhum tipo de mitigação por qualquer tipo de controle.

3.2.24 É importante ressaltar que a Matriz de Riscos poderá ser visualizada de duas formas, ou seja, com os índices de risco inerentes e residuais.

3.2.25 Os Critérios de Avaliação de Riscos devem ser desenvolvidos para que se possa especificar as prioridades dos riscos para tratamento.

3.2.26 Os Critérios para Avaliação de Riscos são usados na fase de Avaliação dos Riscos – Item 5 do ANEXO B – Registro GRSTI02 – Análise e Avaliação de Riscos, que compreende a ordenação dos riscos quanto à prioridade para tratamento.

3.2.27 A seguir, podemos desenvolver um exemplo de Critérios de Avaliação de Riscos utilizando a metodologia Matriz de Risco conforme a tabela 6.

Riscos	Valor da Consequência	Valor da Probabilidade	Índice do Risco	Prioridade
Risco A	1	3	3	5
Risco B	5	4	20	2
Risco C	3	2	6	4
Risco D	5	5	25	1
Risco E	4	3	12	3

Tabela 6 – Prioridade dos Riscos

3.2.28 O exemplo da tabela acima exibe os riscos e suas prioridades. Como podemos observar, os riscos foram ordenados do mais alto para o mais baixo conforme a sequência a seguir: 1º Risco D; 2º Risco B, 3º Risco E, 4º Risco C; e 5º Risco A.

3.2.29 Após a definição do Índice do Risco na Matriz de Probabilidade x Consequência ou pelo conhecimento do Valor do Risco por meio da metodologia **(C+I+P) x P**, os Critérios de Aceitação de Riscos podem ser conhecidos conforme a tabela 7.

Nível do Risco	Valor do Risco (C+I+P) X P	Índice do Risco (P X I)	Descrição
Muito Baixo	3 a 8	1, 2	Aceitável e sem impactos para o contexto, mas devendo registrar o evento.
Baixo	9 a 16	3, 4, 5	Aceitável e sem impactos consideráveis, mas altera o contexto e deve registrar o evento.
Médio	18 a 35	6, 8, 9, 10	Pode ser aceitável após revisão dos responsáveis pela atividade.
Alto	36 a 56	12, 15, 16	Inaceitável, devendo informar ao Comitê de Segurança da Informação e ao responsável pela área/setor do risco.
Muito Alto	60 a 75	20, 25	Absolutamente inaceitável, devendo informar à Autoridade Competente da OM, ao Comitê de Segurança da Informação e ao responsável pela área/setor do risco.

Tabela 7 – Critérios de Aceitação de Riscos

3.2.30 Deve-se também documentar as partes interessadas que são afetadas pela gestão de riscos.

3.2.31 Cada ativo identificado deve possuir um responsável ou proprietário, sendo este a principal fonte de informações do ativo.

3.2.32 O responsável pelo ativo deve ser a pessoa mais indicada para determinar o valor do ativo para a Organização;

3.2.33 O mapeamento dos ativos de informação define informações relevantes de critérios de segurança, como a confidencialidade, integridade e disponibilidade, e constante no documento do Anexo A – GRSTI01 – Definição do Contexto da Gestão de Ativos, como uma avaliação dos ativos de informação.

3.2.34 A classificação dos ativos pode ser definida quanto aos seguintes tipos (Anexo A - GRSTI01 – Definição do Contexto da Gestão de Ativos):

a) Ativos da informação;

b) Ativos de tecnologia;

c) Ativos físicos;

d) Pessoas;

e) Processos; e

f) Ativos intangíveis.

3.3 ETAPA ANÁLISE DE RISCOS

3.3.1 A Análise de Risco é o processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos. Seus processos são compostos de Identificação do Risco e de Estimativa do Risco.

3.3.2 A Identificação do Risco é o processo de busca, reconhecimento e descrição dos riscos, tendo por base o contexto estabelecido e devendo se apoiar na comunicação e consulta com as partes interessadas internas e externas.

3.3.3 A Identificação do Risco pode basear-se em dados históricos, análises teóricas, opiniões de pessoas informadas, analistas e especialistas.

3.3.4 As atividades que compõe a identificação de riscos são compreendidas em cinco fatores para serem analisadas individualmente:

a) Identificação de ativos;

b) Identificação de ameaças e fontes;

c) Identificação de controles de segurança;

d) Identificação de vulnerabilidades; e

e) Identificação de consequências.

3.3.5 Os fatores que afetam a probabilidade e as consequências também é parte da análise de riscos, incluindo a apreciação das causas, as fontes e as consequências positivas ou negativas do risco.

3.3.6 A identificação dos ativos compreende o mapeamento dos ativos de informação quanto ao nome, tipo, relevância, localização e responsáveis (Anexo A - GRSTI01 – Definição do Contexto da Gestão de Ativos).

3.3.7 A identificação das ameaças e fontes é uma etapa que lista os eventos possíveis que se constituem em ameaças aos ativos das possíveis fontes causadoras. A ameaça pode ser definida como um agente ou condição que exercita ameaças. O Anexo C da ABNT NBR IEC 27005: 2019 apresenta um catálogo de ameaças típicas, classificadas quanto ao tipo e à origem.

3.3.8 A identificação de controles de segurança existentes e planejados são realizados possivelmente antes da identificação de vulnerabilidades, mas após a identificação de ameaças. Ao se detectar os controles atualmente existentes e planejados na Organização, pode-se encontrar uma série de vulnerabilidades potenciais devido à ausência de controles, bem como cada controle pode corresponder à redução de uma vulnerabilidade.

3.3.9 A identificação das vulnerabilidades tem como objetivo verificar as possíveis ameaças associadas. As vulnerabilidades têm origem no ambiente interno dos ativos e são utilizados métodos, técnicas e ferramentas específicas, tais como: ferramenta automatizada de análise de vulnerabilidades, teste e avaliação de segurança baseado na elaboração e execução de scripts, teste de penetração, revisão de códigos etc. O Anexo D da ABNT NBR IEC 27005: 2019 apresenta um catálogo de vulnerabilidades e suas ameaças associadas.

3.3.10 A identificação de consequências está relacionada a perda de segurança de um ativo decorrente de um evento de segurança. A ocorrência deste evento é resultante da combinação entre ameaça e vulnerabilidade.

3.3.11 A Estimativa do Risco é a última etapa da fase de análise do risco, que tem como objetivo atribuir valores para as probabilidades e consequências de cada risco por meio de abordagens qualitativas, semiquantitativa e quantitativas, ou combinação destas.

3.3.12 Uma vez que todos os riscos identificados forem devidamente documentados, as escalas de probabilidade e consequência podem ser utilizadas e serem multiplicados para obtermos o Índice do Risco conforme demonstrada na Tabela 5 – Matriz de Probabilidade x Consequência ou por meio da metodologia exibida na Tabela 3 – Descrição nível de risco e valor de risco.

3.3.13 Após todos os riscos serem analisados e seus valores ou índices de risco, inerentes e residuais, forem apurados, teremos um universo de riscos variando entre índice de 1 a 25 (Matriz de Riscos) ou valores de 3 a 75 ((C+I+D) x P). Neste momento, a Organização deve estabelecer os Critérios de Aceitação de Riscos conforme a Tabela 7 para dar início a análise de riscos.

3.3.14 Ao calcular do Valor do Risco ou Índice do Risco se obtém o Nível do Risco correspondente.

3.3.15 O Nível do Risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, ou seja, do impacto nos objetivos, que podem ser tratados como: “Muito Baixo”, “Baixo”, “Médio”, “Alto” e “Muito Alto”.

3.3.16 Após a implementação de controles de mitigação, a eficácia desses controles deve ser verificada e, consequentemente, uma nova análise dos critérios de probabilidade e consequência deve ser realizada. Esta nova medida de índice de risco é denominada Índice de Risco Residual.

3.3.17 O risco residual é aquele que ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos, incluindo controles existentes e outras ações.

3.3.18 Esta nova análise do risco residual pode ser realizada por meio da Matriz de Probabilidade x Consequência conforme a Tabela 5 – Matriz de Probabilidade x Consequência ou por meio de outra atividade de controle que possa estimar o risco que ainda permanece, como a exibida na Tabela 3 – Descrição nível de risco e valor de risco.

3.3.19 Ambos os níveis de risco, inerente e residual, devem ser devidamente documentados nesta etapa com o objetivo de avaliar e verificar se os resultados esperados com as ações de controles internos existentes estão sendo alcançados.

3.4 ETAPA AVALIAÇÃO DE RISCOS

3.4.1 A Avaliação de Riscos tem como objetivo auxiliar na tomada de decisões, com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento.

3.4.2 Os critérios de avaliação de riscos e os critérios de aceitação de riscos definidos na etapa Definição do Contexto devem ser considerados na avaliação de risco

3.4.3 Devem também ser observados os aspectos legais, normativos e contratuais em relação aos riscos estimados.

3.4.4 Após o conhecimento e compreensão do nível do risco obtido na etapa de Análise de Riscos, a Organização deve tomar decisões acerca dos riscos analisados e determinar se o risco precisa de tratamento e prioridade para isso; se uma determinada atividade deve ser realizada ou descontinuada; se os controles de segurança internos devem ser implementados ou, se já existirem, se devem ser modificados, mantidos ou eliminados.

3.4.5 Se os riscos não tiverem uma avaliação satisfatória, devem retornar à etapa de Definição do Contexto, para mudanças e nova análise e avaliação. Caso os riscos tenham uma avaliação satisfatória, devem passar à etapa de Tratamento de Riscos (Figura 1).

3.4.6 A Organização deve documentar uma lista dos riscos que requerem tratamento, com suas respectivas classificações e prioridades.

3.4.7 As avaliações de riscos devem ser realizadas trimestralmente e sempre que houver uma alteração nos sistemas ou quando uma nova ameaça for identificada.

3.5 ETAPA TRATAMENTO DE RISCOS

3.5.1 O Tratamento de Riscos visa auxiliar na elaboração de um Plano de Tratamento ou na implementação de novos controles ou modificação dos existentes.

3.5.2 As opções de resposta ao risco incluem evitar, reduzir (mitigar), transferir (compartilhar) e aceitar (tolerar) o risco.

3.5.3 Evitar o risco é a decisão de não iniciar ou de descontinuar uma atividade ou processo, ou ainda desfazer-se do objeto que dá origem ao risco.

3.5.4 Reduzir ou mitigar o risco consiste em adotar medidas para reduzir a probabilidade ou a consequência dos riscos ou até mesmo ambos.

3.5.5 Compartilhar ou transferir o risco é o caso especial de se mitigar a consequência ou probabilidade de ocorrência do risco por meio da transferência ou compartilhamento de uma parte do risco.

3.5.6 Aceitar ou tolerar o risco é não tomar, deliberadamente, nenhuma medida para alterar a probabilidade ou a consequência do risco. Ocorre quando o risco está dentro do nível de tolerância da organização, ou seja, quando o risco é considerado baixo ou muito baixo.

3.5.7 Deve ser estabelecido na etapa de Definição de Contexto o Critério para Tratamento de Riscos com o objetivo de auxiliar na elaboração do Plano de Tratamento de Riscos.

3.5.8 Um exemplo de Critério de Tratamento de Riscos é exibido na tabela 8.

Nível do Risco	Critério Adotado	Diretriz para a Resposta
Muito Baixo	Monitoramento contínuo e tratamento sob demanda	Não se faz necessário adotar medidas especiais de tratamento, exceto manter os controles existentes.
Baixo	Tratamento posterior e monitoramento constante	Explorar as oportunidades, se determinado pela Autoridade Competente.
Médio	Tratamento mediante aprovação	Admite-se o adiamento do tratamento somente com o parecer e aprovação da Autoridade Competente
Alto	Tratamento imediato	Um intervalo de tempo para a resposta ao tratamento é definido pela Autoridade Competente.
Muito Alto	Tratamento imediato	Uma resposta ao risco deve ser imediata

Tabela 8 – Critérios para Tratamento de Riscos

3.5.9 Novos controles de segurança podem ser implementados para fornecer um ou mais tipos de proteção para reduzir os riscos, tais como: correção, prevenção, eliminação, redução de impacto, detecção, recuperação, monitoramento e conscientização.

3.5.10 Durante a seleção dos controles de segurança, é imprescindível que a Organização avalie o custo da aquisição, implementação, administração, operação, monitoramento e manutenção dos controles em relação ao valor dos ativos que estão sendo protegidos.

3.5.11 Os eventos que possuem riscos de grandes consequências negativas e baixa probabilidade de impacto podem levar à falsa impressão de que o nível do risco poderia ser tolerado após a implantação de controles preventivos. Entretanto, se a Organização assumir que o evento de risco pode se concretizar algum dia, deve-se avaliar a necessidade de um controle reativo específico, como um **Plano de Continuidade do Negócio**.

3.5.12 Os eventos mencionados no item anterior são tratados geralmente em casos catastróficos, como incêndios, inundações, terremotos, epidemias etc.

3.5.13 O Plano de Tratamentos dos Riscos deve ser realizado pelos Responsáveis do Ativo, executores das atividades destinadas a implementação de controles e que tenha relação direta com os eventos que geraram os riscos, enquanto os Responsáveis pela Segurança da Informação devem coordenar, monitorar, realizar análise crítica, definir um tratamento e comunicar as partes interessadas.

3.5.14 Os Responsáveis pela Segurança da Informação sempre devem avaliar a melhor opção de tratamento e enviar estas informações aos Responsáveis do Ativo pela execução das atividades relacionadas com o risco envolvido, bem como devem acompanhar todas as ações até a conclusão da implementação das medidas de tratamento dos riscos.

3.5.15 Após a resposta ou combinação desta no tratamento de risco, deve ser feita uma análise dos riscos residuais existentes para verificar se estão dentro dos limites estabelecidos pela gestão.

3.5.16 Se os riscos residuais não estiverem dentro dos limites estabelecidos, deve ser definida a implementação de tratamento adicional e, posteriormente, a avaliação da eficácia desse tratamento.

3.6 ETAPA ACEITAÇÃO DOS RISCOS

3.6.1 Esta fase da gestão de riscos define o registro formal da decisão pelo aceite dos riscos residuais existentes na Organização.

3.6.2 Se os riscos forem identificados e analisados como baixo e muito baixo, estes deverão ser formalmente registrados e definidos como aceitáveis e não terão tratamento de riscos.

3.6.3 A Autoridade Competente, o Comitê de Segurança da Informação, mais os Responsáveis pelo Tratamento dos Riscos são os responsáveis pela aprovação dos riscos aceitáveis.

3.6.4 Os riscos considerados aceitáveis devem ser registrados e aprovados juntamente com os riscos residuais que após o tratamento foram definidos como aceitáveis.

3.7 ETAPA COMUNICAÇÃO DOS RISCOS

3.7.1 A comunicação dos riscos é um conjunto de atividades continuamente executadas que tem como objetivo compartilhar informações entre os tomadores de decisões e outras partes interessadas na Organização.

3.7.2 Como as percepções e o consenso sobre o risco variam de pessoa para pessoa, o compartilhamento de informações é imprescindível entre os tomadores de decisão e outras partes interessadas.

3.7.3 É obrigatório identificar, documentar e considerar de forma clara e objetiva as percepções e trocas de informações das pessoas acerca do risco envolvido.

3.7.4 Cada Organização deve estabelecer um canal de comunicação sobre riscos, principalmente para situações de crises e emergência.

3.8 ETAPA MONITORAMENTO DOS RISCOS

3.8.1 É uma etapa essencial da gestão de riscos que tem por finalidade detectar quaisquer mudanças no contexto externo e interno, atualizar o mapa de riscos da organização e aprimorar o processo de gestão de riscos da organização.

3.8.2 É imprescindível que os riscos e seus fatores, como valores dos ativos, consequências, vulnerabilidades e probabilidades, sejam monitorados e analisados criticamente e

continuamente a fim de se identificar o mais rápido possível quaisquer eventuais mudanças no contexto da Organização.

3.8.3 A Organização deve ter em mente que os riscos são dinâmicos e que, portanto, as ameaças, vulnerabilidades, probabilidades ou consequências podem mudar sem qualquer indicação.

3.8.4 É imprescindível a adoção de indicadores de risco para representar, de forma padronizada e consistente, os resultados obtidos pelo processo, com o objetivo de viabilizar o monitoramento do desempenho das práticas de gestão de riscos por meio da coleta, análise e divulgação das informações aos envolvidos no processo, bem como facilitar a tomada de decisão a nível estratégico.

3.9 ETAPA MELHORIA CONTÍNUA

3.9.1 Esta etapa visa verificar se novas ocorrências surgiram no processo de gestão de riscos. A Organização deve observar se os critérios de riscos foram modificados; se o contexto interno e externo sofreu alteração; ou se novos indicadores para o processo de gestão de riscos poderão ser criados; e se foram identificados novos pontos de medição como melhoria.

3.9.2 Compete ao Subdepartamento Técnico do DECEA identificar as oportunidades de melhoria contínua no processo.

3.9.3 Sempre deve ser feito um acompanhamento de todas as atividades com o objetivo de buscar novas oportunidades de melhoria.

3.9.4 A Organização deve encorajar todos os participantes do processo de gestão de riscos a encaminharem formalmente ou informalmente sugestões de melhoria contínua ao Comitê de Segurança da Informação.

4 PROCESSO DE GESTÃO DE RISCOS

4.1 GESTÃO DE RISCOS

4.1.1 De acordo com o item 3.2 da DCA 14-8 - Política de Segurança da Informação do Comando da Aeronáutica, esta norma de segurança da informação visa a identificação, a análise e a avaliação das vulnerabilidades com objetivo de se mitigar tais fragilidades, buscando o aprimoramento dos mecanismos de tratamento de riscos de segurança da informação. Assim, o DECEA e OM subordinadas devem se estruturar para promover atividades de gestão de riscos de segurança da informação, com vistas ao levantamento do impacto e probabilidades de ocorrência dos referidos riscos nos ativos de informação, bem como identificar as ameaças associadas às vulnerabilidades destes ativos e medir os níveis de risco para selecionar os controles necessários ao seu tratamento.

4.1.2 O processo de gestão de riscos permite identificar os riscos que podem causar impacto negativo nas atividades operacionais e administrativas do DECEA e em suas Organizações Militares subordinadas.

4.2 VISÃO GERAL DO PROCESSO DE GESTÃO DE RISCOS

4.2.1 Segue abaixo o fluxograma da Gestão de Riscos de acordo com a Norma ABNT ISO/IEC 27005:2008.

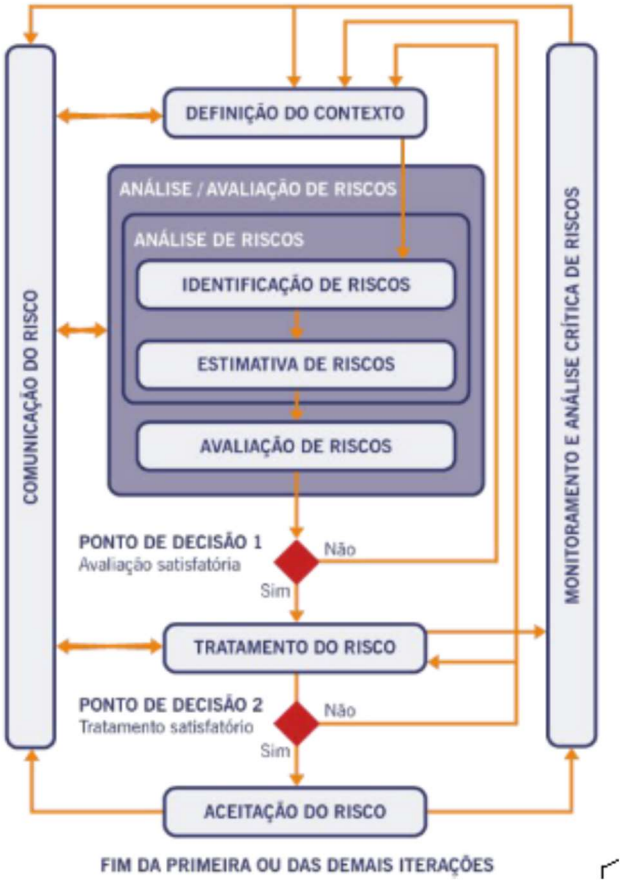

Figura 1 - Fonte ABNT ISO/IEC 27005:2008

4.2.2 De modo geral, processo é um conjunto sequencial de ações ou atividades particulares com a finalidade de alcançar um determinado objetivo. Pode ser composto de uma ou mais entradas, que são processadas, retornando uma ou mais saídas.

4.2.3 Para a presente normatização, o processo será dividido em subprocessos, que por sua vez poderão também ser subdivididos em outros subprocessos denominados etapas ou fases.

4.2.4 No caso do processo de gestão de risco em tela, ele é composto por 6 (seis) subprocessos a seguir descritos: definição de contexto, análise e avaliação de risco, tratamento de risco, aceitação de riscos, comunicação de risco e monitoração e análise crítica, conforme ilustrado na figura 2.

4.2.5 Com a aprovação do SDTE, todos os formulários descritos nesta Instrução poderão ser reproduzidos e automatizados em ferramentas de software apropriadas.

Figura 2 - Visão Geral do Processo de Gestão de Riscos

4.3 SUBPROCESSO “DEFINIR CONTEXTO”

4.3.1 Contexto é um conjunto de circunstâncias que se relacionam de alguma forma com um determinado acontecimento. É a situação geral ou o ambiente a que está sendo referido um determinado assunto, neste caso a análise e avaliação de riscos. Denomina-se contextualização a atividade de mapear todo o ambiente que envolve o evento sob análise.

4.3.2 Este subprocesso é composto de 3 (três) etapas, a saber: identificar as informações sobre o contexto interno e externo, definir os critérios da gestão de risco e, por último, mapear os ativos de informação, conforme ilustrado na figura 3.

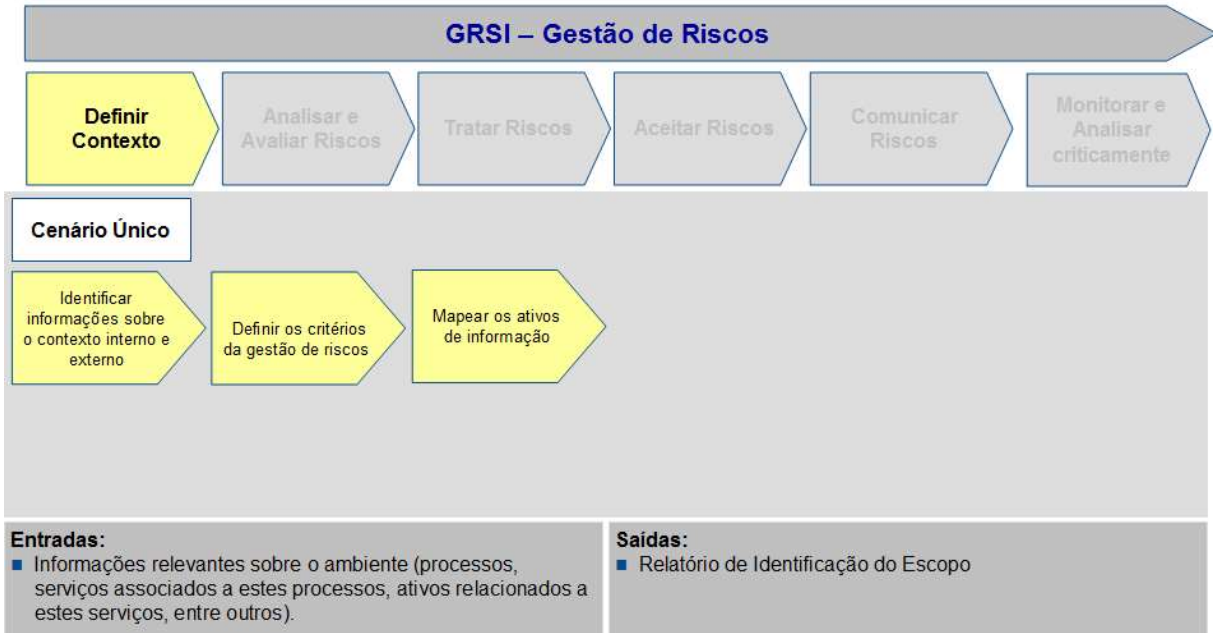

Figura 3 - Subprocesso "Definir Contexto"

4.3.3 Nas atividades que envolvem a gestão de riscos de segurança da informação, a definição do contexto é a parte inicial e tem como objetivo permitir o conhecimento do ambiente da organização.

4.3.4 Contextualização é a atividade de mapeamento de todo o ambiente que envolve o evento em análise.

4.3.5 Além de identificar o contexto interno e externo da organização, os critérios da gestão de riscos deverão ser identificados e os ativos de informação mapeados.

4.3.6 Para identificar as informações sobre o Contexto Interno e Externo, deverá ser realizada uma análise no ambiente da Organização pela equipe de analistas, identificando os elementos que caracterizam a Organização e que contribuem para o seu desenvolvimento. Essas informações deverão ser transcritas no documento GRSTI01 – Definição do Contexto da Gestão de Riscos, conforme modelo apresentado no Anexo A.

4.3.7 No que tange à etapa de definição de critérios da Gestão de Riscos, é importante ressaltar que os critérios fazem parte do método da gestão de riscos e são a forma e o valor (pesos) com que os riscos e impactos serão valorados. Os critérios definidos também deverão ser documentados no documento GRSTI01 – Definição do Contexto da Gestão de Riscos.

4.3.8 Quanto à etapa de identificação dos ativos, deve ser feita em um nível de detalhamento que permita o fornecimento de informações adequadas e suficientes para a análise e avaliação de riscos. Devem ser listados os ativos considerados sensíveis para a Organização e, também, uma lista de componentes organizacionais que este ativo suporta. O mapeamento dos ativos de informação deverá ser documentado no documento GRSTI01 – Definição do Contexto da Gestão de Riscos.

4.3.9 As informações necessárias em relação à identificação dos ativos são: nome do ativo, tipo do ativo (tecnologia, pessoa, ambiente e processo) e importância do ativo quanto ao grau de "Relevância" em cada um dos critérios de segurança da informação: Confidencialidade

(representado por “C”), Integridade (representado por “I”) e Disponibilidade (representado por “D”) e os responsáveis.

4.4 SUBPROCESSO “ANALISAR E AVALIAR RISCOS”

4.4.1 Este subprocesso visa produzir os dados que auxiliarão na decisão sobre quais riscos serão tratados e quais formas de tratamento serão empregadas. Também se subdivide em três etapas, a saber: identificação, estimação e avaliação dos riscos, conforme ilustrado na figura 4. O produto de saída do subprocesso é o Relatório de Análise e Avaliação de Risco.

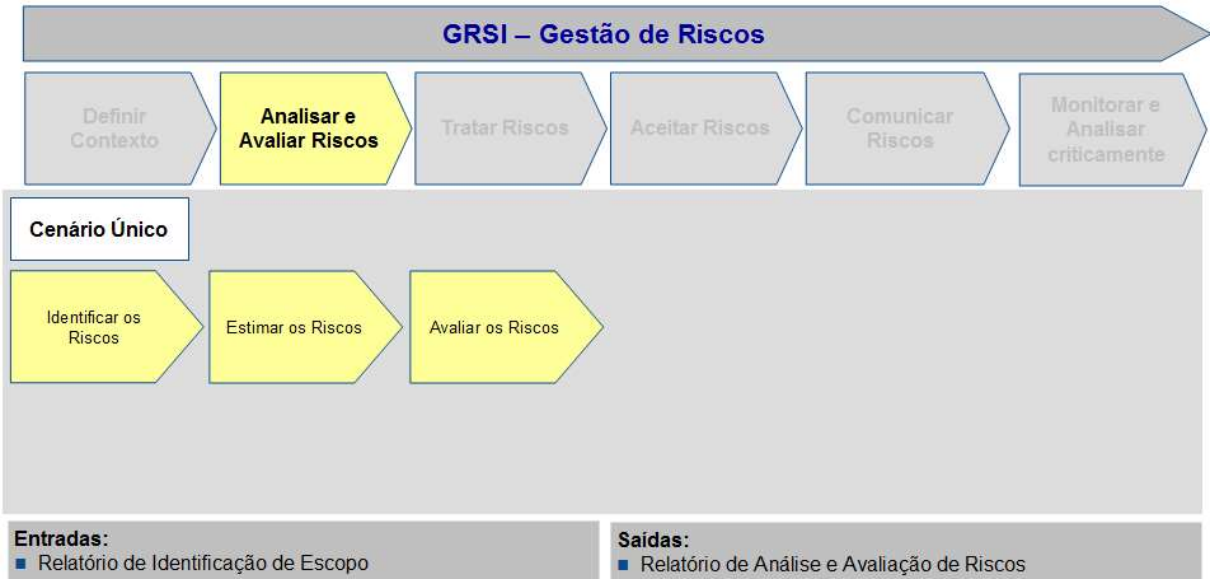

Figura 4 - Subprocesso para Analisar e Avaliar Riscos

4.4.2 Após o subprocesso de definição de contexto, o subprocesso subsequente é o de análise/avaliação de riscos, que valora ativos, ameaças e vulnerabilidades, sendo composto pelas seguintes etapas:

- Identificação de riscos – determina os eventos que podem causar perdas potenciais;
- Estimativa de riscos – determina a probabilidade de ocorrência e os impactos desses eventos; e
- Avaliação de risco – ordena os riscos de acordo com os critérios de avaliação estabelecidos na definição do contexto.

4.4.3 Na etapa de identificação de riscos é necessário levantar as seguintes informações, a saber: as ameaças e suas fontes, os controles de segurança da informação implantados e os planejados, as vulnerabilidades em cada ativo de informação que possam ser exploradas por ameaças relacionadas ao escopo e, por último, as consequências ou prejuízos para a Organização, advindas de um cenário de incidentes, resultado da exploração da vulnerabilidade existente.

4.4.4 As informações obtidas e relacionadas no item anterior devem ser inseridas no documento GRSTI02 – Análise e Avaliação de Riscos, conforme padronizado no Anexo B.

4.4.5 Após a realização da etapa de identificação de riscos, é necessário atribuir valores para os ativos, probabilidades e consequências. Assim, será possível listar os riscos em ordem de

prioridade, para tratá-los de acordo com sua urgência ou criticidade. Esses valores seguem os mesmos critérios definidos na fase de definição do contexto. Essas informações deverão ser transcritas no documento GRSTI02 – Análise e Avaliação de Riscos.

4.4.6 A etapa de avaliação de riscos tem por objetivo comparar os níveis de riscos identificados na fase anterior com os critérios de avaliação e aceitação de riscos e obter uma lista de riscos ordenados por prioridade. Essas informações também deverão ser transcritas no documento GRSTI02 – Análise e Avaliação de Riscos.

4.5 SUBPROCESSO "TRATAR RISCOS"

4.5.1 Este subprocesso visa relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos na definição de escopo, detalhados na figura 5.

4.5.2 O subprocesso "Tratar Risco" faz uso em uma das suas etapas do Processo de Gestão de Mudanças, que será objetivo de normatização específica a ser elaborada pelo Subdepartamento Técnico do DECEA.

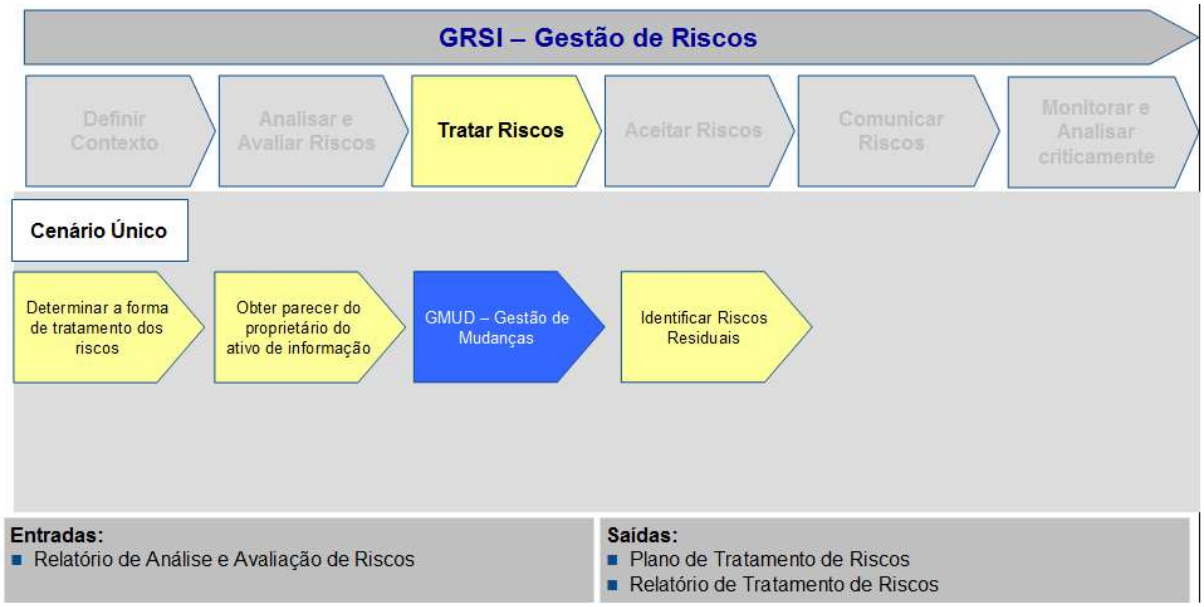

Figura 5 - Subprocesso para Tratar Riscos

4.5.3 Em relação ao subprocesso "Determinar a forma de tratamento de risco", para cada risco identificado deverá ser informada a ação de tratamento. Adicionalmente essas informações deverão ser transcritas no documento GRSTI03 – Plano de Tratamento de Riscos, conforme padrão estabelecido no Anexo C.

4.5.4 O subprocesso de tratamento de risco é realizado após os subprocessos de definição do contexto e análise/avaliação de riscos. Ao final desses subprocessos, a equipe ou setor responsável deverá fazer uma análise crítica dos resultados a fim de verificar a situação dos trabalhos desenvolvidos. Caso essa análise se mostre insatisfatória, deve-se retornar ao início do processo, para ajustes.

4.5.5 Deverão ser determinadas as ações para tratamento de cada risco identificado.

4.5.6 O proprietário pelo ativo de informação deverá emitir parecer sobre os riscos identificados nos ativos sob sua responsabilidade. Este poderá concordar ou não em relação aos riscos identificados. Após emissão de parecer, os riscos considerados aplicáveis deverão ser inseridos no documento GRSTI03 – Plano de Tratamento de Riscos, e os controles de segurança da informação necessários para tratar os riscos deverão ser implementados de acordo com o processo de Gestão de Mudanças dependendo da ação de tratamento escolhida.

4.5.7 Posteriormente ao tratamento, deverá ser feita uma análise para identificar os riscos residuais eventualmente ainda existentes a fim de identificar se deverão ou não ser gerenciados. Essas informações deverão ser transcritas no documento GRSTI03 – Plano de Tratamento de Riscos, que se encontra disponível no Anexo C.

4.5.8 Uma vez definido o Plano de Tratamento de Risco, é necessário identificar os riscos residuais após implementação de controles para evitar, transferir ou mitigar riscos, ou seja, após a implementação de um determinado controle, é possível que ele não seja suficiente para mitigar totalmente um risco. A diferença, isto é, a possibilidade restante da ocorrência do risco, após a implantação do controle para mitigá-lo caracteriza o risco residual.

4.5.9 As informações acerca dos riscos residuais deverão ser inseridas no documento GRSTI03 – Plano de Tratamento de Riscos.

4.6 SUBPROCESSO “ACEITAR RISCOS”

4.6.1 Neste subprocesso, o objetivo é verificar se os resultados obtidos do subprocesso tratamento de risco podem ser aceitos ou se devem ser submetidos a uma reavaliação. O referido subprocesso se encontra ilustrado na figura 6. O produto final desejado é o termo de Aceitação dos Riscos.

Figura 6 - Subprocesso para Aceitar Riscos

4.6.2 Após a definição do Plano de Tratamento, tem início o subprocesso de aceitação do risco, que trata da aprovação formal do Plano de Tratamento pela direção da Organização Militar.

4.6.3 Os riscos aceitos deverão ser formalmente registrados, justificando aqueles que não satisfizeram os critérios definidos. Essas informações deverão ser transcritas no documento GRSTI04 – Termo de Aceite dos Riscos, cujo modelo se encontra no Anexo D.

4.7 SUBPROCESSO "COMUNICAR OS RISCOS"

4.7.1 A gestão de riscos pode ter diversas partes interessadas. Essas partes devem ser identificadas e seus papéis e responsabilidades delimitados. Os riscos serão comunicados para os seus respectivos responsáveis. Assim, o subprocesso de comunicação de riscos se encarrega de proporcionar essa comunicação, sendo composta de duas etapas: a primeira relativa à identificação das partes interessadas e a outra efetivamente associada à comunicação, ambas ilustradas na figura 7.

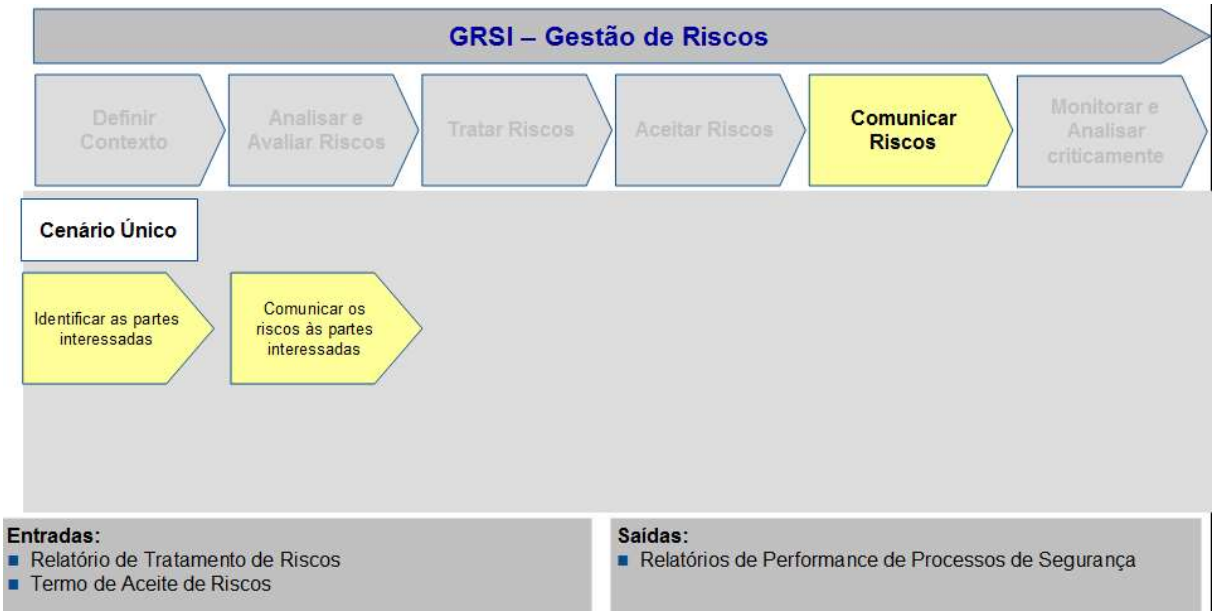

Figura 7 - Subprocesso "Comunicar os Riscos"

4.7.2 A comunicação do risco é uma troca interativa, documentada formalmente, contínua e intencional de informações, conhecimentos e percepções sobre como os riscos devem ser gerenciados.

4.7.3 A comunicação é realizada entre a equipe envolvida e partes interessadas nas decisões do processo de análise de riscos.

4.7.4 As partes interessadas deverão ser identificadas e documentadas no documento GRSTI01 – Definição do Contexto da Gestão de Riscos.

4.7.5 No que tange à comunicação dos riscos às partes interessadas, esta etapa deverá abordar com o máximo de detalhes os riscos encontrados, informando:

- A existência da ameaça, vulnerabilidade e risco;
- A natureza e forma de ação;

- A estimativa de probabilidade;
- Sua severidade e consequências possíveis; e
- Tratamento e aceitação de riscos.

4.8 SUBPROCESSO "MONITORAR E ANALISAR CRITICAMENTE"

4.8.1 Intrínseco a todo processo, a retroalimentação é necessária para corrigir e aperfeiçoar o próprio processo. Assim, este subprocesso permite detectar possíveis falhas nos resultados, monitorar os riscos, os controles de segurança da informação e verificar a eficácia do processo de Gestão de Riscos. Subdivide-se em três etapas, conforme ilustrado na figura 8.

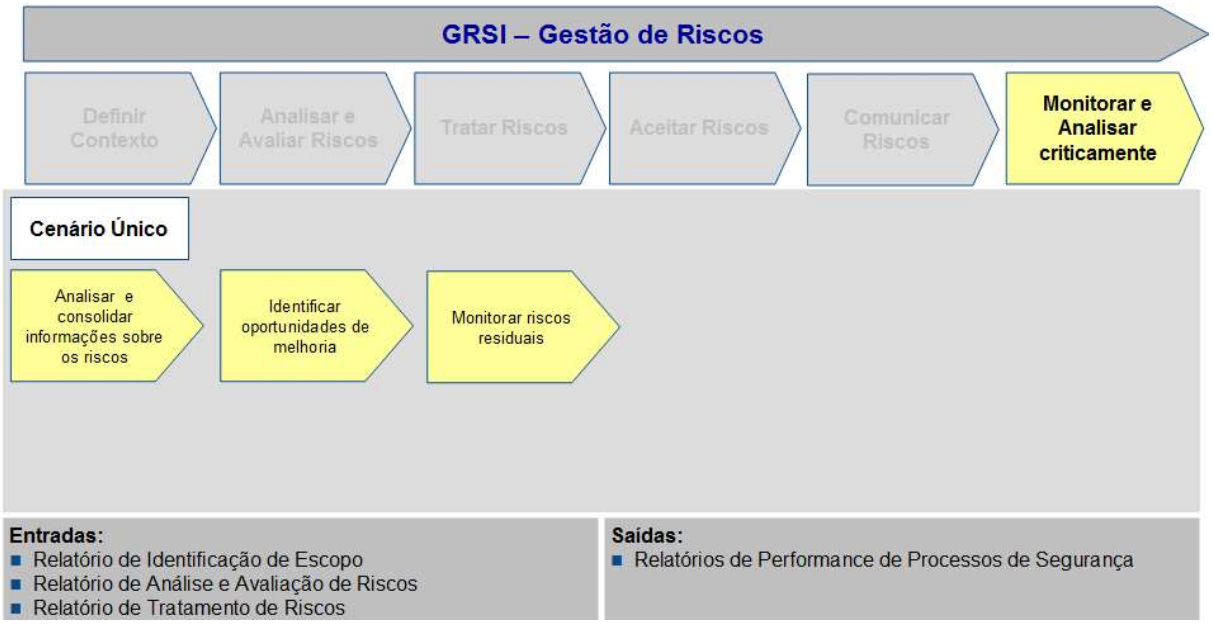

Figura 8 - Subprocesso para Monitorar e Analisar Criticamente

4.8.2 Após o tratamento e aceitação dos riscos, é necessário consolidar informações sobre o processo e identificar oportunidades de melhoria.

4.8.3 Na etapa de "Analisar e Consolidar Informações sobre os Riscos," deve-se identificar e quantificar os indicadores do processo no documento GRSTI06 – Identificação, Quantificação e Análise dos Indicadores do Processo, conforme detalhado no Anexo F.

4.8.4 Quanto à etapa "Identificar Oportunidades de Melhoria", deve-se analisar as informações consolidadas do processo, através dos seus indicadores, e identificar oportunidades de melhoria. Essas informações deverão ser também inseridas no documento GRSTI06 – Identificação, Quantificação e Análise dos Indicadores do Processo.

4.8.5 Por fim, no que tange à etapa "Monitorar Riscos Residuais", os riscos residuais e seus fatores deverão ser monitorados. Quaisquer alterações de valores em relação a estes riscos deverão ser identificadas e registradas no documento GRSTI05 – Monitoramento dos Riscos Residuais, utilizando o modelo contido no Anexo E.

4.9 CONTROLE E MATURIDADE DO PROCESSO

4.9.1 MEDIÇÃO DO NÍVEL DE MATURIDADE ATUAL DO PROCESSO

4.9.1.1 A maturidade deste processo é medida através da seguinte escala:

0 – Não Existente: A gestão de riscos como parte de decisões sobre o negócio não ocorre. A organização não considera os impactos no negócio associados à gestão de riscos e a incertezas de projetos de desenvolvimento. A gestão de riscos não tem sido identificada como relevante para a aquisição de soluções de Tecnologia da Informação e para a entrega dos serviços de TI.

1 – Inicial/*Ad Hoc*: Os riscos de Tecnologia da Informação são levados em consideração de maneira *Ad Hoc*. As vulnerabilidades técnicas relacionadas à TI, como segurança, disponibilidade e integridade, são eventualmente consideradas. Existe uma compreensão emergente de que a gestão de riscos é importante e precisa ser considerada.

2 – Repetível e Intuitivo: Uma abordagem de avaliação sobre a gestão de riscos imatura e em desenvolvimento existe e está implantada. A gestão de riscos é normalmente de alto nível e é tipicamente aplicada apenas a projetos importantes ou em resposta a problemas. Os processos de tratamentos dos riscos estão começando a ser implementados.

3 – Processo Definido: A gestão de riscos segue um processo definido e documentado. O treinamento em análise de riscos está disponível para todo o pessoal. As decisões para acompanhar o processo de gestão de riscos e receber treinamento são deixadas a critério individual. A metodologia de aplicação para a avaliação de riscos é convincente e bem estruturada, garantindo que os principais riscos para o negócio sejam identificados. Um processo para mitigar os riscos é normalmente instituído.

4 – Gerenciado e Mensurável: A gestão de riscos é um processo padrão. As exceções ao processo são relatadas. Os riscos são avaliados em nível termos de projeto individual e também regularmente a respeito da operação de Tecnologia da Informação como um todo. Existe a capacidade de monitorar a posição dos riscos associados às vulnerabilidades e tomar decisões informadas referentes à exposição que se deseja assumir. Todos os riscos identificados têm um proprietário nomeado. Além disso, um banco de dados de gerenciamento de riscos é estabelecido e parte dos processos de gestão de riscos começa a ser automatizado.

5 – Otimizado: A gestão de riscos já se desenvolveu a um estágio onde um processo estruturado é executado e bem gerenciado. Boas práticas são aplicadas através de toda a Organização. A captura, a análise e o relatório de dados da gestão de riscos são altamente automatizados.

4.9.1.2 A tabela abaixo apresenta as metas para a evolução dos níveis de maturidade:

Nível de Maturidade	Metas
2 – Repetível e Intuitivo	• Possuir uma normativa interna do DECEA para gestão de riscos de segurança da informação • Obter aprovação da Política de Gestão de Riscos • Iniciar a implantação e testes do processo em pelo menos 50% das Organizações Subordinadas ao DECEA
3 – Processo Definido	• Implantar o processo em todas as Organizações Subordinadas ao DECEA • Capacitar todos os chefes das seções de segurança da informação
4 – Gerenciado e Mensurável	• Criar um painel para acompanhamento, através de indicadores gerenciais do processo, a fim de garantir a tomada de decisão pela Direção do DECEA
5 – Otimizado	• Realizar uma reunião semestral de análise crítica para melhoria contínua do processo • Possuir sistema informatizado para emissão de relatórios automatizados

4.9.1.3 Cada Organização deverá elaborar e encaminhar ao Subdepartamento Técnico do DECEA um Relatório de Evolução dos Níveis de Maturidade, que deverá ser atualizado anualmente e sempre houver alteração no nível de maturidade.

4.9.1.4 O Relatório de Evolução dos Níveis de Maturidade deverá conter, no mínimo:

a) O nível de maturidade e a meta atual;

b) As mudanças e justificativas em relação ao nível de maturidade; e

c) O prazo de evolução dos níveis de maturidade;

4.9.2 ACOMPANHAMENTO DO PROCESSO POR INDICADORES

O acompanhamento do processo será feito por intermédio dos indicadores e métricas listadas na Tabela abaixo, contudo as metas ainda serão definidas posteriormente pelo SDTE.

Objetivos do Processo	Indicadores do Processo
• Determinar e reduzir a ocorrência e o impacto de riscos. • Determinar planos de ação com custos eficientes para tratar os riscos identificados.	• Percentual de riscos identificados que tenham sido avaliados como Muito Alto; • Quantidade de novos riscos identificados (comparado com o exercício anterior); • Quantidade de incidentes significativos causados por riscos não identificados no processo; e • Quantidade de análise de riscos realizada.

4.9.3 FATORES CRÍTICOS DE SUCESSO

São os seguintes os fatores críticos de sucesso para o alcançar os objetivos e metas definidos para o processo, bem como nortear as avaliações dos resultados alcançados:

a) garantir apoio da Direção do DECEA através da divulgação da Política de Gestão de Riscos de Segurança e Tecnologia da Informação do DECEA (DCA 7-3);

b) garantir cumprimento das responsabilidades atribuídas no processo;

c) gerenciamento de riscos integrado aos processos de negócio;

d) garantir cumprimento dos procedimentos relacionados ao processo;

e) acompanhamento da situação do processo e apresentação de relatórios detalhados; e

f) garantir comunicação eficiente e eficaz do processo a todas as partes interessadas e envolvidas no processo.

5 DISPOSIÇÕES FINAIS

5.1 O Processo e procedimentos de Segurança da Informação apresentados neste documento são de caráter geral e devem ser revisados periodicamente a cada trinta e seis meses, ou quando fato relevante demandar atualização extemporânea.

5.2 Esta Instrução de Comando da Aeronáutica deverá estar em conformidade com as Diretrizes da DTI – Órgão Central do Sistema de Tecnologia da Aeronáutica –, e será revisada e atualizada sempre que forem atualizadas ou aprovadas Normas relativas ao assunto pela Diretoria de Tecnologia da Informação do Comando da Aeronáutica.

5.3 Casos não previstos nesta Instrução deverão ser levados à apreciação do Exmo. Sr. Diretor-Geral do DECEA.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISSO Guia 73, **Gestão de Riscos: Vocabulário: Recomendação para uso em normas**. Rio de Janeiro, RJ, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27001. **Tecnologia da informação: Técnicas de segurança: Sistemas de Gestão de Segurança da Informação: Requisitos**. Rio de Janeiro, RJ, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27002. **Tecnologia da Informação: Técnicas de segurança: Código de práticas para a gestão da segurança da informação**. Rio de Janeiro, RJ, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27005. **Tecnologia da informação: Técnicas de segurança: Gestão de riscos de segurança da informação**. Rio de Janeiro, RJ, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 31000. **Gestão de riscos-Diretrizes**. Rio de Janeiro, RJ, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 31010. **Gestão de riscos-Técnicas para o processo de avaliação de riscos**. Rio de Janeiro, RJ, 2021.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 1.274 /SNOT, de 1° de março de 2024. Aprova a reedição da "Diretriz do Comando da Aeronáutica que dispõe sobre a Segurança da Informação do Departamento de Controle do Espaço Aéreo" = **DCA 7-2**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2024, n. 53, 18 mar. 2024.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 142/SNOT, de 16 de abril de 2022. Aprova a reedição da "Diretriz que dispõe sobre a de Gestão de Riscos de Segurança e Tecnologia da Informação do DECEA" = **DCA 7-3**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n.83, 05 maio 2022.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 745 /DGCEA, de 14 de fevereiro de 2023. Aprova a reedição do "Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo" = **MCA 7-1**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 39, 01 mar. 2023.

BRASIL Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria GABAER n° 273/GC3, de 18 de abril de 2022. Aprova a Diretriz que estabelece a "Política de Segurança da Informação do Comando da Aeronáutica" = **DCA 14-8**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 74, 18 abr. 2022.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº 8/3SC2, de 14 de abril de 2003. "Aprova a Reedição do Manual de Abreviaturas, Siglas e Símbolos da Aeronáutica" = **MCA 10-3**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2003, n. 74, 22 abr. 2003.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº 2/3SC2, de 30 de janeiro de 2001. "Aprova a reedição do Manual que dispõe sobre padronização

do uso de termos, palavras, vocábulos e expressões de uso corrente no âmbito do Comando da Aeronáutica" = **MCA 10-4**. Boletim Externo Ostensivo, Rio de Janeiro, RJ, 2001.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 248, 27 dez. 2018 - Seção 1.

BRASIL. Instrução Normativa CGU nº 1, de 10 de maio de 2016 - Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 89, 11 maio 2016 - Seção 1.

BRASIL. Instrução Normativa SGD/ME nº 1, de 04 de abril de 2019 – Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 66, 05 abr. 2019 – Seção 1.

BRASIL. Instrução Normativa GSI nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 101, 28 maio 2020 – Seção 1.

BRASIL. Instrução Normativa GSI nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 101, 31 maio 2021 - Seção 1.

BRASIL. Portaria GSI_PR Nº 93, de 18 de outubro de 2021. Glossário de Segurança Institucional da Presidência da República. Glossário de Segurança da Informação. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 197, 19 out. 2021, Seção 1.

Anexo A - Registro GRSTI01 – Definição do Contexto da Gestão de Riscos

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GRSTI01 – 001			OM <inserir a sigla da OM ou do Destacamento>
ASSUNTO	Definição do Contexto da Gestão de Riscos			

1 Definição do contexto interno e externo

[Ao analisar o ambiente da organização, a equipe de analistas deve identificar os elementos que caracterizam a organização e contribuem para o seu desenvolvimento]

2 Definição dos critérios da gestão de riscos

[Os critérios fazem parte do método da gestão de riscos e são a forma e o valor (pesos) com que os riscos e impactos serão valorados]

3 Documentar as partes interessadas

[As partes interessadas são entidades que são afetadas ou afetam a gestão de riscos]

4 Mapeamento dos ativos de informação

Nome	Tipo	Relevância			Localização		Responsáveis	
		C	I	D	Física	Lógica	Proprietário	Custodiante

Aprovado por:	[Comitê de Segurança da Informação ou estrutura equivalente]
Comentários:	

Anexo B - Registro GRSTI02 – Análise e Avaliação de Riscos

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GRSTI02 – 001			OM <inserir a sigla da OM ou do Destacamento>
ASSUNTO	Análise e Avaliação de Riscos			

1 Identificação das ameaças e fontes

[Identificar as ameaças e suas fontes de acordo com o contexto definido para a gestão de riscos]

2 Identificação dos controles de segurança

[Identificar os controles de segurança da informação implementados e planejados]

3 Identificação dos Riscos

Ativo	Ameaça	Vulnerabilidade	Consequências

4 Estimativa dos Riscos

Ativo	Risco	Estimativa		Valor ou Índice do Risco	Nível
		(C+I+D) ou I	P		

5 Avaliação dos Riscos

[Comparar os níveis de riscos identificados com os critérios de avaliação e aceitação de riscos e obter uma lista de riscos ordenados por prioridade]

Aprovado por:	[Comitê de Segurança da Informação ou estrutura equivalente]
Comentários:	

Anexo C - Registro GRSTI03 – Plano de Tratamento dos Riscos

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GRSTI03 – 001			OM <inserir a sigla da OM ou do Destacamento>
ASSUNTO	Plano de Tratamento dos Riscos			

1 Matriz de tratamento dos riscos

Ativo	Risco	Ação de Tratamento	Prazo	Riscos Residuais	Parecer do Proprietário do Ativo

Aprovado por:	[Autoridade Competente da OM]
Comentários:	

Anexo D - Registro GRSTI04 – Termo de Aceite dos Riscos

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GRSTI04 – 001			OM <inserir a sigla da OM ou do Destacamento>
ASSUNTO	Termo de Aceite dos Riscos			

1 Registro de Aceitação dos Riscos

Ativo	*Risco*	*Justificativa*

Aprovado por:	[Comitê de Segurança da Informação ou estrutura equivalente]
Comentários:	

Anexo E - Registro GRSTI05 – Monitoramento dos Riscos Residuais

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GRSTI05 – 001			OM <inserir a sigla da OM ou do Destacamento>
ASSUNTO	Monitoramento dos Riscos Residuais			

1	**Registro de Alteração de Risco Residual**

Risco:

Ativo:

Valor Alterado:

Detalhes sobre o Novo Risco:

Detalhes da Ação sobre o Novo Risco:

Data da Identificação:

Aprovado por:	[Comitê de Segurança da Informação ou estrutura equivalente]
Comentários:	

Anexo F - Registro GRSTI06 – Identificação, Quantificação e Análise dos Indicadores do Processo

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GRSTI06 – 001			OM <inserir a sigla da OM ou do Destacamento>
ASSUNTO	Identificação, Quantificação e Análise dos Indicadores do Processo			

1	**MEDIÇÃO DOS INDICADORES**	
Indicador	**Quantitativo**	**Observações**
Percentual de riscos identificados que tenham sido avaliados como “Muito Alto”.		
Quantidade de novos riscos identificados (comparado com o exercício anterior).		
Quantidade de incidentes significativos causados por riscos não identificados no processo.		
Quantidade de análise de riscos realizada.		

2	**ANÁLISE DOS INDICADORES**

3	**AÇÕES DE MELHORIA CONTÍNUA**

Aprovado por:	[Comitê de Segurança da Informação ou estrutura equivalente]
Comentários:	