MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

PROTEÇÃO AO VOO

MCA 63-14

MANUAL DE GERENCIAMENTO DO RISCO À SEGURANÇA OPERACIONAL NO SISCEAB

2012

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

PROTEÇÃO AO VOO

MCA 63-14

MANUAL DE GERENCIAMENTO DO RISCO À SEGURANÇA OPERACIONAL NO SISCEAB

2012

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

PORTARIA DECEA Nº 45/DGCEA, DE 30 DE MARÇO 2012.

Aprova a edição do Manual do Comando da Aeronáutica, que trata de Gerenciamento do Risco à Segurança Operacional no SISCEAB.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere o art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 369/GC3, de 9 de junho de 2010, resolve:

Art. 1º Aprovar a edição do MCA 63-14 "Manual de Gerenciamento do Risco à Segurança Operacional no SISCEAB", que com esta baixa.

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

(a) Ten Brig Ar RAMON BORGES CARDOSO
Diretor-Geral do DECEA

(Publicado no BCA nº 093, de 15 de maio de 2012)

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

PORTARIA Nº 186/DGCEA, DE 18 DE NOVEMBRO DE 2013.

Aprova a 1ª Modificação do MCA 63-14, que dispõe sobre o "Manual de Gerenciamento do Risco à Segurança Operacional (GRSO) no SISCEAB".

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere o artigo 195, inciso IV, do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1.049/GC3, de 11 de novembro de 2009, e o artigo 10, inciso IV do Regulamento do DECEA, aprovado pela Portaria nº 1.668/GC3, de 16 de setembro de 2013, resolve:

Art. 1º Aprovar a 1ª Modificação do MCA 63-14 "Manual de Gerenciamento do Risco à Segurança Operacional (GRSO) no SISCEAB", que com esta baixa.

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

(a) Ten Brig Ar RAFAEL RODRIGUES FILHO
Diretor-Geral do DECEA

(Publicado no BCA nº 230, de 02 de dezembro de 2013)

Proteção ao Voo

MANUAL DE GERENCIAMENTO DO RISCO À SEGURANÇA OPERACIONAL (GRSO) NO SISCEAB

O MCA 63-14, aprovada pela Portaria Nº 45/DGCEA, de 30 de março de 2012, é assim modificado:

1 SUBSTITUIÇÃO DE PÁGINAS

RETIRE	ANO	COLOQUE	ANO
9	2012	9	2012
10	2012	10	2012
12	2012	12	2012
15	2012	15	2012
26	2012	26	2012
27	2012	27	2012
66	2012	65	2012
68	2012	68	2012

2 CORREÇÃO

PÁGINA	ITEM	ALÍNEA
9	1.2 (Alteração)	
10	2.1 (Alteração)	
12	2.2.7 (Alteração)	
15	3.1.4 (Alteração)	
15	3.1.2.1 (Alteração)	
26	3.7.2 (Alteração)	
26	3.7.2.1 (Alteração)	
26	3.7.2.2 (Alteração)	
26	3.7.2.2 (Alteração)	(d) (Alteração)
26	3.7.2.3 (Alteração)	
26	3.7.2.5 (Alteração)	
26	3.7.2.6 (Alteração e renumeração para 3.7.2.5.1)	
26	3.7.2.5.1	(a) (Exclusão)
26	3.7.2.5.1	(b) (Renumeração para "a")
26	3.7.2.5.1	(c) (Exclusão)
26	3.7.2.5.1	(d) (Alteração e renumeração para "b")
26	3.7.2.5.1	(e) (Alteração e renumeração para "c")
27	3.7.2.7 (Alteração e renumeração para 3.7.2.6)	
66	Anexo A (Alteração)	
68	*N* (Alteração)	

3 ARQUIVO

Depois de efetuar as substituições, arquive esta folha após a página de rosto da publicação original.

4 APROVAÇÃO

Portaria Nº 186/DGCEA, de 18 de novembro de 2013.

SUMÁRIO

PREFÁCIO

A Organização de Aviação Civil Internacional (OACI) estabeleceu em diversos Anexos à Convenção de Aviação Civil Internacional (CACI) a necessidade da implementação de Sistemas de Gerenciamento da Segurança Operacional (SGSO), com o objetivo de aperfeiçoar os processos necessários à elevação do nível da segurança operacional mundial.

Uma das principais ferramentas do SGSO é o Gerenciamento do Risco à Segurança Operacional (GRSO), que identifica os perigos e avalia os riscos, de modo a concentrar as atividades de segurança operacional na eliminação ou mitigação dos riscos avaliados.

O Gerenciamento de Risco será empregado nas mudanças a serem estabelecidas no SISCEAB e nas operações correntes dos Provedores dos Serviços de Navegação Aérea (PSNA).

A metodologia aplicada no gerenciamento do risco evidencia os tipos de mudanças e os riscos correntes que devem ser considerados para a avaliação da segurança operacional e o detalhamento do processo determina quando uma mudança necessita de uma análise completa.

Dessa forma, é publicado este Manual com a finalidade de detalhar os procedimentos em conformidade com os requisitos estabelecidos para a realização do Gerenciamento do Risco nas atividades do SISCEAB e atender às orientações da Diretriz para a Implementação de Sistemas de Gerenciamento da Segurança Operacional no SISCEAB (DCA 63-3) e da Instrução Normativa que trata do Gerenciamento do Risco à Segurança Operacional (ICA 63-26).

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

O presente Manual tem por finalidade descrever o processo, a metodologia e os procedimentos a serem utilizados no Gerenciamento do Risco à Segurança Operacional aplicado às atividades do SISCEAB.

1.2 OBJETIVO

O Gerenciamento do Risco à Segurança Operacional tem como objetivo identificar os perigos, analisar, classificar e eliminar (ou mitigar) os riscos, de forma a garantir os Níveis Aceitáveis de Desempenho da Segurança Operacional (NADSO) na prestação dos Serviços de Navegação Aérea (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

1.3 ÂMBITO

Este Manual aplica-se a todas as Organizações, Unidades e PSNA pertencentes ao SISCEAB.

2 SIGLAS E CONCEITUAÇÕES

2.1 SIGLAS

ACC	Centro de Controle de Área
AIS	Serviço de Informações Aeronáuticas
ANS	Serviços de Navegação Aérea
ALARP	*As Low as Reasonably Practicable*
ATC	Controle de Tráfego Aéreo
ATCO	Controlador de Tráfego Aéreo
ATM	Gerenciamento do Tráfego Aéreo
ASEGCEA	Assessoria de Segurança Operacional do Controle do Espaço Aéreo
CNS	Comunicação, Navegação e Vigilância
CTG	Cartografia Aeronáutica
DECEA	Departamento do Controle do Espaço Aéreo
DGRSO	Documento de Gerenciamento do Risco à Segurança Operacional
GRSO	Gerenciamento do Risco à Segurança Operacional
IHM	Interface Homem-Máquina
IFR	Regra de Voo por Instrumentos
MET	Meteorologia Aeronáutica
NADSO	Nível Aceitável de Desempenho da Segurança Operacional (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013
NOSS	Normal Operation Safety Survey (Pesquisa da Segurança Operacional durante as Operações de Rotina)
SNA	Provedor de Serviço de Navegação Aérea
RCSV	Relatórios Confidenciais de Segurança de Voo
REGRSO	Registro de Redução do Escopo do Gerenciamento do Risco à Segurança Operacional (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013
RELPREV	Relatório de Prevenção de Acidentes Aeronáuticos
RICEA	Relatórios de Investigação do Controle do Espaço Aéreo
SAR	Busca e Salvamento
SEGCEA	Subsistema de Segurança Operacional do SISCEAB
SGSO	Sistema de Gerenciamento da Segurança Operacional
SIPAER	Sistema de Investigação e Prevenção de Acidentes Aeronáuticos
SISCEAB	Sistema de Controle do Espaço Aéreo Brasileiro
VFR	Regras de Voo Visual

2.2 CONCEITUAÇÕES

2.2.1 ACIDENTE AERONÁUTICO

Toda ocorrência relacionada com a operação de uma aeronave, havida entre o momento em que uma pessoa nela embarca com a intenção de realizar um voo até o momento em que todas as pessoas tenham dela desembarcado e durante o qual pelo menos uma das situações abaixo ocorra:

a) uma pessoa sofra lesão grave ou morra como resultado de estar,
- na aeronave;
- em contato direto com qualquer parte da aeronave, incluindo aquelas que dela tenham se desprendido; ou
- submetido à exposição direto do sopro de hélice, rotor ou escapamento de jato, ou às suas conseqüências;

NOTA: Exceção é feita quando as lesões resultarem de causas naturais, forem auto ou por terceiros infligidas, ou forem causadas a pessoas que embarcaram clandestinamente e se acomodaram em área que não as destinadas aos passageiros ou aos tripulantes.

b) a aeronave sofra dano ou falha estrutural que,
- afete adversamente a resistência estrutural, o seu desempenho ou as suas características de voo; e
- normalmente, se exija a realização de grande reparo ou a substituição do componente afetado;

NOTA: Exceção é feita para falha ou danos limitados ao motor, suas carenagens ou seus acessórios, ou para danos limitados a hélices, pontas de asas, antenas, pneus, freios, carenagens do trem ou amassamentos leves e perfurações no revestimento da aeronave.

c) a aeronave seja considerada desaparecida ou o local onde se encontrar for, absolutamente, inacessível.

2.2.2 ALARP

A sigla ALARP é usada para descrever um risco à segurança operacional que foi reduzido a um nível tão baixo quanto razoavelmente praticável.

Para determinar o que é "razoavelmente praticável" no contexto do gerenciamento do risco à segurança operacional, devem ser considerados tanto a viabilidade técnica de reduzir ainda mais o risco, quanto os custos que esta redução acarreta. Isso deve incluir uma análise de custo-benefício, mostrando que quando o risco em um sistema é ALARP, significa que qualquer redução do risco torna-se impraticável, considerando-se os altos custos que isto acarreta. Convém, no entanto, ter em mente que, quando uma organização "aceita" um risco, isso não significa que o risco foi eliminado. Alguns níveis residuais de risco para a segurança continuam a existir, no entanto, a organização aceita que este nível de risco residual é suficientemente baixo e é compensado pelos benefícios auferidos.

2.2.3 ASSESSORIA DE SEGURANÇA OPERACIONAL DO CONTROLE DO ESPAÇO AÉREO – ASEGCEA

Órgão Central do SEGCEA, ligado diretamente ao Diretor-Geral do DECEA, que tem por atribuição o trato de assuntos relacionados ao gerenciamento da segurança operacional, à investigação, análise e prevenção de acidentes, de incidentes aeronáuticos e de incidentes de tráfego aéreo no âmbito do SISCEAB, bem como a coordenação dos procedimentos de interação com o SIPAER.

2.2.4 ERRO OPERACIONAL

São aqueles que surgem da interação do homem com a tecnologia, onde a fonte do erro está na incompatibilidade da interface homem-máquina.

2.2.5 INCIDENTE AERONÁUTICO

Toda ocorrência associada à operação de uma aeronave, havendo intenção de voo, que não chegue a se caracterizar como um acidente aeronáutico ou uma ocorrência de solo, mas que afete ou que possa afetar a segurança da operação.

2.2.6 MITIGAÇÃO DO RISCO

É o conjunto de medidas que visam à eliminação dos perigos ou à redução da probabilidade e/ou da severidade dos riscos associados.

2.2.7 NÍVEL ACEITÁVEL DE DESEMPENHO DA SEGURANÇA OPERACIONAL - NADSO

Conceito adotado para expressar os níveis de desempenho da segurança operacional aceitos pelo DECEA, considerando o gerenciamento dos riscos existentes na operação (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

2.2.8 PERIGO

Qualquer condição, potencial ou real, que possa causar dano físico, doença ou morte a pessoas, dano ou perda de um sistema, equipamento ou propriedade ou dano ao meio ambiente. Um perigo é uma condição que se constitui num pré-requisito para a ocorrência de um acidente ou incidente.

2.2.9 PROBABILIDADE DO RISCO

Possibilidade de uma situação de perigo à segurança operacional ocorrer, classificada em níveis de probabilidade para análise e gerenciamento do risco.

2.2.10 PROVEDOR DE SERVIÇO DE NAVEGAÇÃO AÉREA – PSNA

Organização/Unidade/Órgão provedor de um, ou mais, dos serviços prestados pelo SISCEAB, observando as disposições normativas do DECEA. Por convenção, no Brasil, tal serviço é conhecido como "Controle do Espaço Aéreo", abrangendo as áreas de Gerenciamento de Tráfego Aéreo (ATM), de Informações Aeronáuticas (AIS); de Comunicações, Navegação e Vigilância (CNS); de Meteorologia Aeronáutica (MET); de Cartografia (CTG); e de Busca e Salvamento (SAR).

2.2.11 RISCO

Possibilidade de perda ou dano, medida em termos de severidade e probabilidade. A possibilidade de um evento ocorrer e suas consequências se efetivamente ocorrer.

2.2.12 RISCO CORRENTE

É o risco baseado em dados reais, considerando-se o momento atual de uma atividade ou operação. Ao determinar-se o risco atual, os controles validados e os verificados podem ser usados na avaliação do risco.

2.2.13 RISCO INICIAL

É o risco baseado em dados de projeto, considerando-se somente os controles verificados e suposições documentadas para um determinado cenário. É o risco deduzido no estágio preliminar ou fase inicial de uma mudança proposta, programa ou avaliação.

2.2.14 RISCO RESIDUAL

É o risco que permanece depois que todas as técnicas de controle tenham sido esgotadas, as medidas mitigadoras implementadas e depois que todos os controles tenham sido verificados.

2.2.15 RISCO RESIDUAL PREVISTO

É o risco resultante depois de completada a análise de segurança e verificados todos os requisitos de segurança. O Risco Residual Previsto está baseado na suposição de que todos os requisitos de segurança foram validados e verificados.

2.2.16 SEGURANÇA OPERACIONAL

É o estado no qual o risco de lesões às pessoas, danos às propriedades ou ao meio ambiente são reduzidos e mantidos em (ou abaixo de) um nível aceitável, mediante um processo contínuo de identificação de perigos e gerenciamento de riscos.

2.2.17 SERVIÇOS DE NAVEGAÇÃO AÉREA (ANS)

Conjunto de serviços prestados pelo SISCEAB, observando as disposições normativas do DECEA, órgão central e regulador do sistema.

Por convenção, no Brasil, tal conjunto de serviços é denominado “Controle do Espaço Aéreo”, abrangendo outros serviços, como o de tráfego aéreo; de informação aeronáutica; de comunicações, navegação e vigilância; de meteorologia aeronáutica; de cartografia aeronáutica e de busca e salvamento.

2.2.18 SEVERIDADE DO RISCO

As consequências possíveis de uma situação de perigo à Segurança Operacional, tomando como referência a pior condição previsível.

2.2.19 SISTEMA DE CONTROLE DO ESPAÇO AÉREO BRASILEIRO – SISCEAB

Sistema que tem por finalidade prover os meios necessários para o gerenciamento e o controle do espaço aéreo e o serviço de navegação aérea, de modo seguro e eficiente, conforme estabelecido nas normas nacionais e nos acordos e tratados internacionais de que o Brasil seja parte. As atividades desenvolvidas no âmbito do SISCEAB são aquelas realizadas em prol do gerenciamento e do controle do espaço aéreo, de forma integrada, civil e militar, com vistas à vigilância, à segurança e à defesa do espaço aéreo sob a jurisdição do Estado Brasileiro.

2.2.20 SISTEMA DE GERENCIAMENTO DA SEGURANÇA OPERACIONAL – SGSO

Sistema que apresenta os objetivos, políticas, responsabilidades e estruturas organizacionais necessárias ao funcionamento do Gerenciamento da Segurança Operacional, de acordo com metas de desempenho aceitas pelo DECEA, contendo os procedimentos para o Gerenciamento do Risco.

2.2.21 SISTEMA DE INVESTIGAÇÃO E PREVENÇÃO DE ACIDENTES AERONÁUTICOS – SIPAER

O Sistema que tem finalidade de planejar, orientar, coordenar, controlar e executar as atividades de investigação e prevenção de acidentes aeronáuticos no Brasil.

2.2.22 SISTEMAS DE TOLERÂNCIA OU DE RESISTÊNCIA AO ERRO HUMANO

São sistemas projetados e implementados de forma que, na medida do possível, o erro humano e a falha no equipamento não resultem em um incidente ou acidente. Um sistema tolerante ou resistente ao erro inclui mecanismos que irão reconhecer uma falha ou erro do operador, a fim de que a ação corretiva seja tomada antes que a sequência de eventos que levem ao acidente seja desencadeada.

2.2.23 SUBSISTEMA DE SEGURANÇA OPERACIONAL DO SISCEAB – SEGCEA

Subsistema que tem por finalidade o gerenciamento das atividades de prevenção de acidentes, de incidentes aeronáuticos e de incidentes de tráfego aéreo, incluindo as relativas ao Gerenciamento da Segurança Operacional, bem como das atividades de investigação de incidentes de tráfego aéreo.

3 GERENCIAMENTO DO RISCO À SEGURANÇA OPERACIONAL (GRSO)

3.1 VISÃO GERAL DO GERENCIAMENTO DO RISCO

3.1.1 A MUDANÇA E A SEGURANÇA OPERACIONAL

3.1.1.1 A implementação de uma mudança que afete as atividades dos Serviços de Navegação Aérea (ANS) pode gerar riscos à segurança operacional, pois as mudanças fazem interface com os procedimentos, sistemas e ambientes operacionais existentes.

3.1.1.2 Uma mudança no ANS é qualquer modificação que afete suas atividades. Tais mudanças podem ocorrer na infraestrutura aeroportuária, na operação de aeronaves, no Controle do Espaço Aéreo, abrangendo as áreas de Gerenciamento de Tráfego Aéreo (ATM), de Informações Aeronáuticas (AIS), de Comunicações, Navegação e Vigilância (CNS), de Meteorologia Aeronáutica (MET), de Cartografia Aeronáutica (CTG) e de Busca e Salvamento (SAR).

3.1.1.3 Devem ser consideradas, também, as mudanças nos sistemas de apoio, nas tecnologias, nas regras, normas e procedimentos operacionais, nas políticas e no pessoal que implementa, dá suporte ou opera os elementos do sistema. O GRSO fornece uma estrutura para garantir que uma vez que uma mudança seja implementada, a mesma continue a ser monitorada durante todo o seu ciclo de vida útil.

3.1.1.4 Uma mudança significativa no ANS, que afete a segurança operacional, somente deverá ser implementada depois que uma avaliação da segurança operacional tenha demonstrado que o Nível Aceitável de Desempenho da Segurança Operacional (NADSO) está assegurado (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

3.1.2 O RISCO CORRENTE E A SEGURANÇA OPERACIONAL

3.1.2.1 Os perigos e os riscos são componentes inerentes aos sistemas complexos. Dessa forma, os riscos correntes, presentes nas operações rotineiras no ANS, devem ser analisados e mitigados e/ou eliminados, de forma a garantir o NADSO. Esses perigos podem ser identificados a qualquer momento, por pessoa direta ou indiretamente envolvida na provisão do ANS, por meio da aplicação das diversas ferramentas de segurança operacional (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

3.1.3 O GERENCIAMENTO DO RISCO

3.1.3.1 O Gerenciamento do Risco à Segurança Operacional é um elemento fundamental do SGSO e consiste em uma abordagem formalizada e pró-ativa ao sistema de segurança operacional, aplicada ao risco corrente e a todas as mudanças que afetam a segurança operacional.

3.1.3.2 Consiste, ainda, em uma abordagem analítica, sistemática, explícita e pormenorizada para o gerenciamento de segurança operacional em todos os níveis e durante todo o âmbito de uma operação ou da vida útil de um sistema. O Gerenciamento do Risco exige disciplina, abrangência e profundidade na avaliação e no gerenciamento da segurança operacional.

3.1.3.3 Os PSNA devem utilizar o GRSO para manter e aperfeiçoar a segurança no ANS, identificando os perigos, avaliando, classificando e mitigando os riscos à segurança operacional.

3.1.3.4 Três importantes termos devem ser necessariamente considerados ao se efetuar mudanças que resultem em perigo potencial no ANS e o gerenciamento de seus riscos:

a) Sistema: Um conjunto integrado constituído por partes, combinadas em um ambiente operacional ou de apoio, para alcançar um objetivo definido. Essas partes incluem recursos humanos, equipamentos, informações, procedimentos, facilidades e outros serviços de apoio;

b) Perigo: Qualquer condição real ou potencial que possa causar lesão, doença ou morte às pessoas, prejuízo ou perda de um sistema, equipamento ou propriedade; ou dano ao meio ambiente. Um perigo é uma condição potencial e constitui-se em um pré-requisito para a ocorrência de um acidente ou incidente; e

c) Risco: É a composição da severidade e da probabilidade previsíveis, relativas ao efeito potencial de um perigo, considerando o pior cenário possível de ocorrer.

3.2 SISTEMA TOLERANTE AO ERRO

3.2.1 Diante da complexa interação entre os fatores humanos, materiais e ambientais que interagem em uma operação, a eliminação completa do risco é uma meta inalcançável. Mesmo em organizações com os melhores programas de treinamento e uma cultura de segurança positiva, os operadores possivelmente cometerão erros; mesmo os equipamentos resultantes dos melhores projetos e mantidos de forma adequada poderão, ocasionalmente, falhar.

3.2.2 Os desenvolvedores de sistemas levam tais fatores em conta e trabalham para projetar e implementar sistemas nos quais um erro humano ou uma falha no equipamento não resultem em acidente. Esses sistemas são tolerantes ao erro. Portanto, um sistema tolerante ao erro é definido como aquele projetado e implementado de forma que, na medida do possível, o erro humano e a falha no equipamento não resultem em um incidente ou acidente.

3.2.3 Um sistema tolerante ao erro inclui mecanismos que irão reconhecer uma falha ou erro, a fim de que a ação corretiva seja tomada antes que a sequência de eventos que levem ao acidente seja desencadeada. A necessidade de uma série de defesas, e não um único nível defensivo, surge da possibilidade de que as defesas nem sempre operam como foram projetadas. Essa filosofia de projeto é denominada “defesas em profundidade”, ou seja, defesas redundantes.

3.2.4 Falhas nas barreiras de defesa de um sistema operacional podem criar lacunas que permitam que essas defesas sejam violadas. Como a situação operacional ou o estado de manutenção dos equipamentos/sistemas mudam, essas lacunas podem ocorrer como resultado de:

a) deficiências inéditas ou preexistentes nas defesas;

b) indisponibilidade temporária de alguns elementos do sistema, como, por exemplo, resultado da ação de manutenção;

c) falha de equipamentos, sistemas e software; e

d) erro humano ou violação.

3.2.5 Os atributos de um projeto de sistema tolerante ao erro incluem:

a) tornar os erros aparentes (sistemas de evidência de erro);

b) reter o erro para não permitir que afete o sistema (sistemas de captura de erro);

c) detectar erros e fornecer sistemas de alerta e de aviso (sistemas de alerta de erro); e

d) assegurar que existe um caminho de recuperação (sistemas de recuperação do erro).

3.2.6 Para que um acidente ocorra, em um sistema bem projetado, as falhas devem acontecer em todas as barreiras defensivas do sistema em um determinado momento; quando na verdade tais defesas deveriam ter sido capazes de detectar e/ou impedir previamente o erro ou a falha. A ilustração de como um perigo pode passar por todas as camadas defensivas é mostrada na Figura 1.

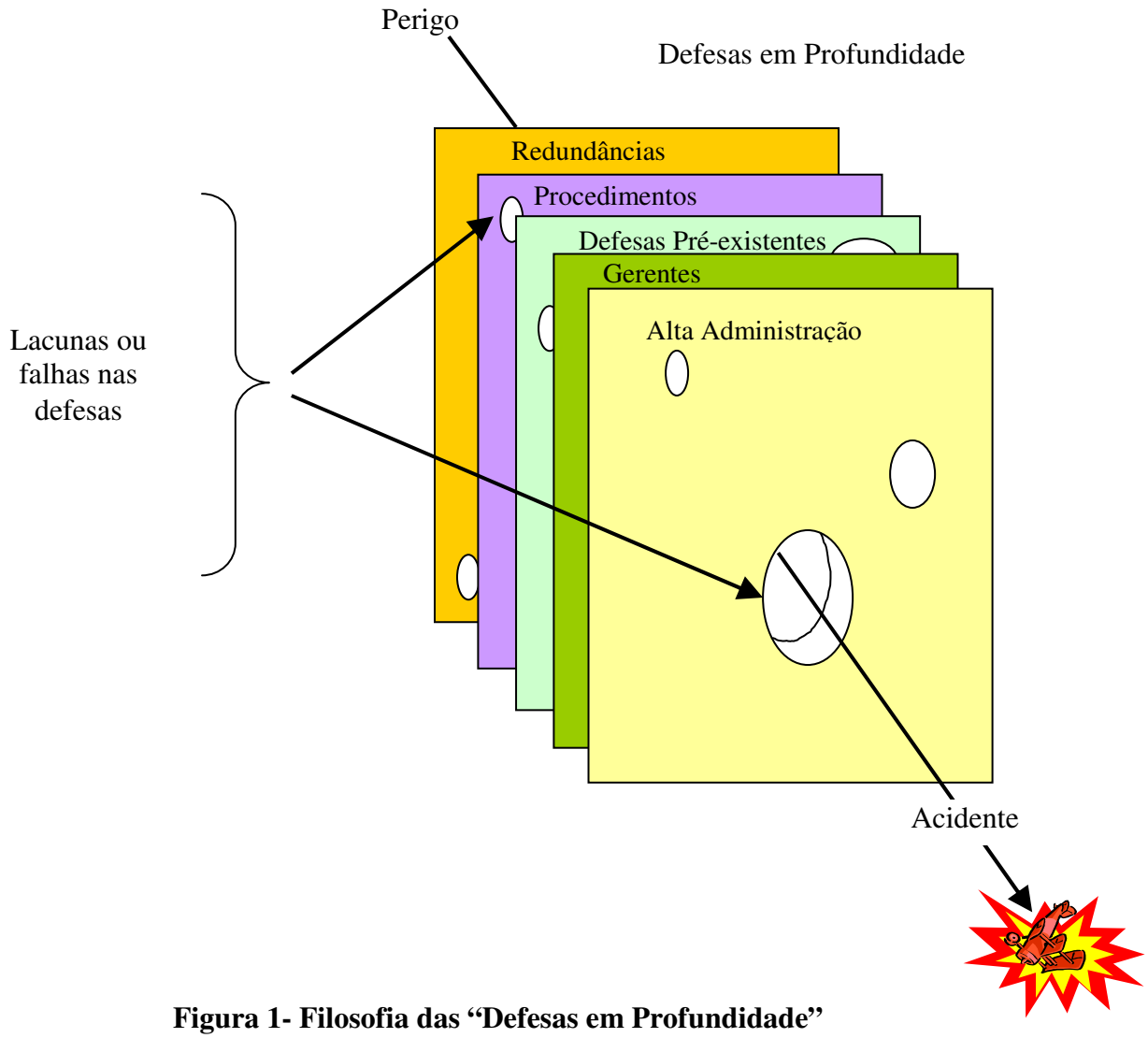


Figura 1- Filosofia das "Defesas em Profundidade"

3.2.7 As lacunas nas defesas do sistema mostradas na Figura 1 não são necessariamente estáticas. Lacunas "abrem" e "fecham" enquanto as situações operacionais, ambientes ou estados de manutenção dos equipamentos mudam.

3.2.8 Uma lacuna pode algumas vezes ser o resultado de um lapso momentâneo por parte de um operador, enquanto outras lacunas podem ser consequência de falhas latentes da organização.

3.2.9 Uma falha latente é aquela que não é revelada na hora em que ocorre, permanecendo no sistema até que uma outra falha ou um erro humano a revele.

3.2.10 IDENTIFICAÇÃO DE FALHAS

3.2.10.1 A análise acurada de um sistema e o monitoramento de dados operacionais permitem identificar sequências de falhas e erros (isolados ou combinados) que poderiam conduzir a um incidente ou acidente antes que ele ocorra. No entanto, se ocorrer um acidente/incidente, a mesma abordagem poderá ser utilizada. A identificação das falhas ativas e latentes, reveladas por esse tipo de análise, permite que se tome ação corretiva para reforçar as defesas do sistema.

3.2.11 ELIMINAÇÃO DAS FALHAS

3.2.11.1 Equipamentos

a) implementação de redundâncias,

- redundância completa fornecendo o mesmo nível de funcionalidade quando estiver operando em um sistema alternativo; e
- redundância parcial resultando em alguma redução na funcionalidade (por exemplo: cópia local de dados essenciais a partir de uma base de dados da rede centralizada);

b) verificação independentemente de projeto e premissas;

c) desenvolvimento de sistemas projetados para assegurar que uma funcionalidade crítica será mantida em modo degradado, mesmo que os elementos individuais venham a falhar;

d) adoção de políticas e procedimentos relacionados à manutenção para não resultar em perda de alguma funcionalidade no sistema ativo ou perda da redundância;

e) implementação de auxílios automatizados ou processos de diagnóstico projetados para detectar falhas no sistema ou processamento de erros e relatar essas falhas de maneira apropriada; e

f) realização de manutenção programada.

3.2.12 PROCEDIMENTOS OPERACIONAIS

a) utilização da fraseologia e dos procedimentos padrões;

b) adoção do cotejamento das autorizações e instruções;

c) emprego do *Checklist* em ações rotineiras;

d) aplicação de treinamento continuado;

e) análises de procedimentos operacionais; e

f) estabelecimento de políticas de notificação de ocorrências.

3.2.12.1 Fatores Organizacionais

a) comprometimento da alta gerência com a segurança operacional;

b) desenvolvimento de uma cultura de segurança operacional positiva;

c) clareza na Política de Segurança Operacional,

- garantindo o compromisso da administração em atingir as metas de desempenho da segurança operacional;
- assegurando os recursos necessários para o gerenciamento eficaz da segurança;
- mantendo a segurança operacional como sua mais alta prioridade; e
- estabelecendo uma política sobre responsabilidades e obrigações pela segurança operacional em todos os seus níveis hierárquicos;

d) supervisão e controle para assegurar que as normas e os procedimentos operacionais estão sendo adequadamente cumpridos,

- não tolerância a violações ou a atalhos deliberados;

e) controle adequado sobre as atividades dos recursos humanos e empresas contratadas ou terceirizadas.

NOTA: Os exemplos de defesas típicas, anteriormente citados, usadas de forma combinada para eliminar falhas, são ilustrativos e não uma lista completa de soluções.

3.3 EFEITOS DO *HARDWARE* E DO *SOFTWARE* NA SEGURANÇA OPERACIONAL

3.3.1 Desenvolvedores de sistemas geralmente projetam os componentes de *hardware* e *software* para atingir os níveis especificados de confiança, de manutenção e de disponibilidade. As técnicas para estimar o desempenho do sistema, considerando esses parâmetros, estão bem estabelecidas. Quando necessário, podem ser desenvolvidas redundâncias para disponibilizar alternativas no caso de falha em um ou mais elementos desses sistemas.

3.3.2 Diversidade física é outro método utilizado para aumentar a disponibilidade de serviços no caso de falhas. Diversidade física envolve separar funções redundantes a fim de que um ponto único de falha não venha a corromper ambos os trajetos, tornando o serviço indisponível. Um exemplo da diversidade física é a exigência de disponibilizar energia comercial nos órgãos ATC por dois caminhos diferentes. No caso de um incêndio ou outro problema em um caminho, o caminho alternativo continuaria fornecendo energia, o que aumenta a disponibilidade do serviço.

3.3.3 Quando um sistema inclui *software* e/ou *hardware*, devem ser feitas análises de segurança visando identificar possíveis erros de projeto e os perigos que eles podem criar. Essas análises de segurança devem constituir parte integrante do projeto e são importantes para detectar e eliminar erros de projeto.

3.4 EFEITOS DO ELEMENTO HUMANO NA SEGURANÇA OPERACIONAL

3.4.1 Os Fatores Humanos devem ser compreendidos como um esforço multidisciplinar para gerar e reunir informações sobre as capacidades e limitações humanas em prol do desempenho eficaz e seguro e aplicar tais informações:

a) ao desenvolvimento de sistemas e equipamentos;

b) a auxílios à navegação aérea;

c) a procedimentos operacionais;

d) à definição de funções e tarefas;

e) a ambientes de trabalho;

f) ao treinamento e capacitação; e

g) ao gerenciamento de recursos humanos.

3.4.2 A aplicação desses conhecimentos na atividade de Gerenciamento do Risco estará em grande parte voltada para área que envolve a integração do ser humano com o suporte tecnológico, tendo em vista a natureza altamente tecnológica das atividades de navegação aérea.

3.4.3 No entanto, é fundamental que se perceba que todos os sistemas, equipamentos, procedimentos operacionais, normas, etc. presentes no ANS existem para dar suporte ao ser humano no desempenho de suas tarefas.

3.4.4 Reconhecer o papel central que os seres humanos têm na prestação dos serviços de tráfego aéreo deve levar os desenvolvedores dos sistemas e/ou os gerentes ATM a desenvolver uma abordagem de projetos que seja centrada no elemento humano. Ou seja, adotar o conceito de que ao se desenvolver um sistema ou estabelecer um novo procedimento operacional devem ser consideradas, principalmente, as capacidades e limitações dos seres humanos, sendo crítico para a segurança a adoção de medidas e ferramentas que não levem esses parâmetros em consideração.

3.4.5 É necessário que os desenvolvedores dos sistemas e gerentes ATM façam uma análise cuidadosa e completa a respeito do impacto dos sistemas/procedimentos sobre o desempenho humano. Devem se preocupar em potencializar as capacidades humanas e compensar suas limitações. Uma dessas limitações é a variabilidade do desempenho humano, tanto no que diz respeito às variações no mesmo indivíduo em momentos distintos quanto ao que diz respeito às diferenças entre os indivíduos. Máquinas e sistemas são construídos para funcionar dentro de tolerâncias específicas, a fim de que máquinas idênticas tenham características idênticas ou semelhantes. Diferentemente, o desempenho dos seres humanos varia devido às diferenças determinadas pela genética e pelo ambiente.

3.4.6 Os projetistas devem levar em consideração essas diferenças ao projetarem produtos, instrumentos, máquinas e sistemas, ajustando-os ao usuário. As capacidades e os atributos humanos são diferentes em áreas como:

a) modalidades dos sentidos humanos (ex.: visão, audição e tato);

b) funcionamento cognitivo;

c) tempo de reação;

d) tamanho e forma física; e

e) resistência fisiológica.

3.4.7 O erro humano tem sido fator contribuinte em mais de 85% dos incidentes de tráfego aéreo. As pessoas cometem erros com o potencial de gerar riscos. Acidentes e incidentes resultam frequentemente de uma sequência de erros interdependentes. Por essa razão, os desenvolvedores de sistemas devem preocupar-se em projetar sistemas de segurança que:

a) eliminem tantos erros quanto possível;

b) minimizem as consequências dos erros que não possam ser eliminados; ou

c) diminuam o impacto negativo de qualquer erro potencial humano remanescente.

3.4.8 Inúmeros fatores internos e externos podem causar impacto no desempenho humano. São fatores a fadiga e doenças, bem como os próprios estressores do ambiente de trabalho (aspectos da ergonomia física e cognitiva e interrupção nas tarefas). A princípio, um sistema deve ser projetado para resistir ao erro humano (sistema de resistência ao erro) ou, no mínimo, para ser tolerante ao mesmo (sistema de tolerância ao erro).

3.4.9 A análise dos aspectos relacionados aos fatores humanos no Gerenciamento do Risco deverá levar em conta o desempenho humano em interação com todas as interfaces existentes durante a prestação dos serviços de tráfego aéreo. Ou seja, os aspectos que podem interferir na interação do elemento humano com o(s):

a) outros seres humanos,

b) sistemas e equipamentos;

c) ambiente de trabalho; e

d) sistema de apoio.

3.4.10 Ao examinar os eventos adversos atribuídos ao erro humano, em geral são negligenciados aspectos como os elementos de interface homem-máquina (IHM), ferramentas operacionais, treinamentos, manuais ou documentação e carga de trabalho. A análise da confiabilidade humana e a aplicação do conhecimento sobre o desempenho humano devem ser uma parte integral do SGSO e, por consequência, do Gerenciamento do Risco.

3.4.11 Fatores Humanos aplicam conhecimento de como os seres humanos funcionam em termos de percepção, cognição e biomecânica, na concepção de projetos, de ferramentas, de produtos e de sistemas que favoreçam o desempenho da capacidade humana, protegendo sua saúde e proporcionando segurança no trabalho.

3.4.12 Ao realizarem o Gerenciamento do Risco, os especialistas deverão identificar os perigos e riscos consequentes relacionados, verificando se os requisitos relativos aos fatores humanos, partindo da ótica acima descrita, foram considerados.

3.5 PLANEJAMENTO DO GERENCIAMENTO DO RISCO

3.5.1 A realização do GRSO requer a elaboração de um planejamento que contemple todas as fases do Gerenciamento do Risco e deve levar em consideração a abrangência e a

profundidade da análise de segurança, bem como a coordenação com as outras organizações que possam ser afetadas pela mudança ou pela operação corrente.

3.5.2 O dimensionamento do esforço despendido no GRSO deve levar em consideração a natureza, a complexidade, o impacto e as consequências da mudança ou do risco corrente. Para tanto, é fundamental que a análise da segurança seja compatível com o âmbito e a complexidade da mudança ou do risco em tela.

3.5.3 É importante que a equipe GRSO reconheça que itens que aparentemente não causariam impacto na segurança podem, potencialmente, provocar impacto no sistema que está sendo analisado. Por exemplo, o ar-condicionado inicialmente parece não provocar impacto no sistema que está sendo analisado; entretanto, quando um sistema depende do ar-condicionado para evitar o superaquecimento ou a falha, o ar-condicionado (ou a falta dele) poderia afetar a segurança daquele sistema e em consequência a segurança do ANS.

3.6 EQUIPES DO GERENCIAMENTO DO RISCO

3.6.1 A implementação de uma mudança envolve profissionais de várias áreas de atuação, tornando-se necessário o estabelecimento de uma equipe multidisciplinar para efetuar o gerenciamento dos riscos associados a tal mudança.

3.6.2 Uma Equipe de Gerenciamento do Risco deve ser composta pelos representantes das várias organizações e das áreas envolvidas na mudança ou na operação corrente. Devem ser considerados os profissionais com as capacitações pertinentes às áreas envolvidas nas mudanças propostas e capazes de contribuir nas etapas de Descrição do Sistema, Identificação de Perigos, Avaliação e Classificação dos Riscos, Estabelecimento das Medidas Mitigadoras, Classificação dos Riscos Residuais, estabelecimento de novas medidas mitigadoras para o Risco Residual, se for o caso, e, finalmente, estabelecimento de um planejamento para a implementação das medidas mitigadoras.

3.6.3 Para a definição das áreas envolvidas na mudança e dos profissionais que devem fazer parte dessa equipe deve-se considerar a amplitude definida pela Descrição do Sistema, o qual limitará a abrangência das áreas envolvidas. Cabe observar que a Descrição do Sistema deve ser ampla o suficiente para garantir que os perigos significativos sejam considerados.

3.6.4 Embora a dimensão do grupo varie de acordo com as características e a complexidade de cada mudança proposta, a composição da Equipe de Gerenciamento do Risco deve considerar a participação dos seguintes especialistas (relação não exaustiva):

a) pessoal diretamente responsável pelo projeto/concepção/desenvolvimento da mudança proposta;

b) profissional especializado, com conhecimento e experiência no sistema atual e na mudança proposta;

c) especialista em SGSO para orientar a aplicação da metodologia do GRSO;

d) especialista em Fatores Humanos;

e) especialista em Sistemas/Automação/*Software*, para fornecer informações sobre o desempenho dos equipamentos e sistemas; e

f) profissionais de segurança operacional, qualificados na coleta e análise de dados de perigo e erro e que utilizem ferramentas e técnicas especializadas para tal (ex.: pesquisa em operações, dados, fatores humanos etc.).

3.6.5 RESPONSABILIDADES DO COORDENADOR DA EQUIPE DE GRSO

3.6.5.1 Toda equipe de GRSO deve possuir um coordenador responsável por conduzir a equipe por todas as fases do processo de Gerenciamento do Risco. O coordenador deve ser um profissional especialista em segurança operacional, que detenha os conhecimentos específicos do processo de gerenciamento do risco.

3.6.5.2 O coordenador é responsável por obter as informações relevantes para a mudança ou a avaliação do risco corrente, as quais devem esclarecer as seguintes questões:

a) o estado ou a condição atual do sistema;

b) a mudança proposta;

c) o objetivo da mudança; e

d) o(s) estado(s) do sistema em que a mudança será conduzida.

3.6.5.3 O coordenador também é responsável pelo estabelecimento dos limites da análise de segurança e das condições que podem influenciar a análise para a mudança ou a avaliação do risco corrente.

3.6.5.4 A abrangência da análise do GRSO varia conforme a organização, o proponente da mudança e/ou o tipo de mudança. Em alguns casos, as equipes de GRSO farão análises de âmbito internacional, nacional, regional ou local.

3.6.5.5 O coordenador deve garantir que:

a) os membros da equipe sejam selecionados adequadamente com base nos critérios anteriormente estabelecidos;

b) os membros tenham um entendimento comum dos princípios do SGSO e GRSO;

c) o material necessário para a primeira reunião seja coletado, incluindo,

- listas de perigos preliminares de mudanças semelhantes;
- coleta e análise dos dados apropriados à mudança ou à operação corrente para auxiliar na identificação dos perigos e na avaliação dos riscos; e
- tabela de severidade e probabilidade e matriz de risco;

d) os membros do grupo estejam familiarizados com a dinâmica da reunião da equipe GRSO;

e) seja indicado um coordenador auxiliar que trabalhará depois com o coordenador e o proponente da mudança para ajudar na confecção do DGRSO;

f) que os componentes da equipe tenham conhecimento do processo, metas, objetivo e cronograma de atividades do GRSO; e

g) que as atribuições de cada membro da equipe GRSO sejam claramente definidas.

3.6.5.6 Na reunião inicial, o coordenador deverá orientar os membros da equipe, considerando os seguintes aspectos:

a) resumo das metas e do objetivo da equipe;

b) resumo das fases do processo do GRSO;

c) estabelecimento das regras básicas para a equipe;

d) apresentação da mudança proposta ou do risco corrente; e

e) outras informações julgadas pertinentes.

3.6.5.7 O coordenador deve enfatizar que o gerenciamento do risco é essencialmente um trabalho de equipe. Portanto, a integração dos profissionais com conhecimento e experiência variada permitirá uma abordagem multidisciplinar mais abrangente e equilibrada do que uma avaliação individual.

3.7 ANÁLISE DE SEGURANÇA PRELIMINAR

3.7.1 NÍVEIS EXIGIDOS DE ANÁLISE DE SEGURANÇA

A Figura 2 descreve o processo para determinar que tipo de análise de segurança é necessária segundo o GRSO.

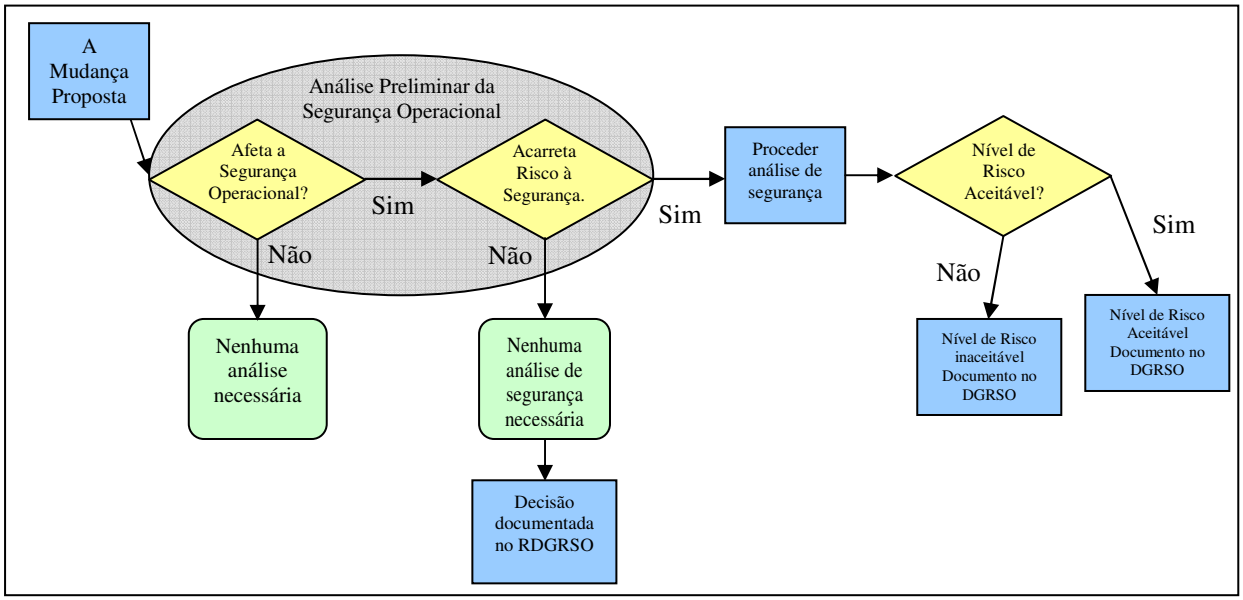


Figura 2- Processo de Decisão do GRSO

3.7.1.1 Ao propor uma mudança para o ANS, deve ser realizada uma análise de segurança preliminar. Se a mudança não afetar o ANS, não haverá necessidade de realizar uma análise de segurança adicional. Se a mudança afetar o ANS, deve-se analisar se a mudança tem potencial para introduzir riscos à segurança no ANS.

3.7.1.2 Adicionalmente à análise preliminar, acima citada, para subsidiar a decisão pela aplicação do GRSO, deve-se analisar se as respostas às perguntas abaixo indicam a presença de risco à segurança operacional:

a) a modificação pretendida acarreta risco em potencial para a segurança operacional?;

b) a modificação pretendida afeta a interação entre pilotos e controladores?;

c) a modificação pretendida afeta os processos e/ou procedimentos operacionais existentes?;

d) a modificação pretendida acarreta alteração nas operações de serviços de tráfego aéreo e sistemas de manutenção?; e

e) a modificação pretendida impõe a necessidade de qualificação dos recursos humanos?.

3.7.1.3 Quando uma mudança não causar risco à segurança no ANS, não haverá necessidade de conduzir análises de risco adicionais, no entanto, o proponente da mudança deve documentar esse fato, juntamente com a justificativa para a decisão de encerrar o processo de GRSO na análise preliminar, documentando tal análise no Registro de Decisão de Gerenciamento do Risco à Segurança Operacional (RDGRSO), conforme o subitem 3.7.2, a seguir.

3.7.1.4 A Figura 3 apresenta vários exemplos de mudança no ANS.

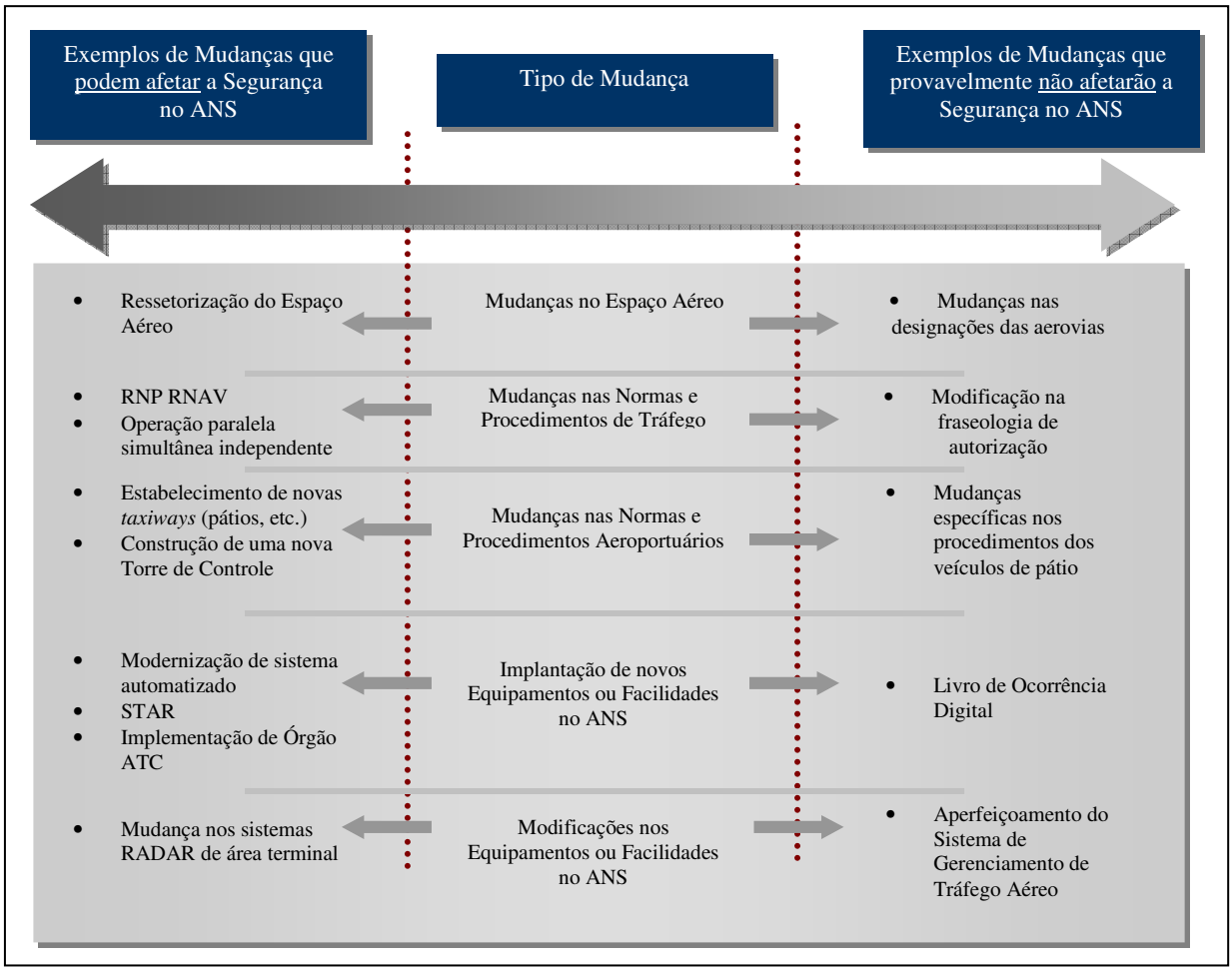


Figura 3- Esquema de Exemplos de Mudanças no ANS

3.7.2 REGISTRO DE REDUÇÃO DO ESCOPPO DO GERENCIAMENTO DO RISCO À SEGURANÇA OPERACIONAL - REGRSO

3.7.2.1 Nos primeiros estágios da análise preliminar, pode ficar claro que determinada mudança não vai causar riscos à segurança no ANS ou os riscos aceitáveis, por se tratar de baixo risco . Nesse caso, não há necessidade de dar prosseguimento ao Gerenciamento do Risco; porém tal decisão deverá ser documentada por meio da elaboração de um REGRSO, que tem por objetivo registrar todas as mudanças propostas para o ANS que não causam riscos à segurança operacional ou os riscos são aceitáveis (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

3.7.2.2 O REGRSO será elaborado conforme explicitado no Anexo A e deverá incluir os seguintes itens (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013:

a) uma descrição da mudança proposta;

b) a documentação utilizada na análise de segurança preliminar;

c) a justificativa de que a mudança não está sujeita às condições de avaliações de GRSO adicionais; e

d) a descrição de todos os aspectos que expliquem por que a mudança não acarreta riscos à segurança no ANS ou os riscos são aceitáveis (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

3.7.2.3 Um REGRSO deve conter, pelo menos, duas assinaturas, sendo uma do proponente da mudança e outra do profissional responsável pela realização da análise preliminar (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

3.7.2.4 O profissional responsável pela Avaliação Preliminar deverá ser capacitado em Gerenciamento do Risco à Segurança Operacional.

3.7.2.5 Aprovação do REGRSO (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013

3.7.2.5.1 A aprovação do REGRSO depende da abrangência da mudança e, dessa maneira, segundo o caso, a aprovação pode ser feita pelas seguintes autoridades:

a) pelo Comandante (ou Chefe) da Organização Regional, quando a abrangência da mudança proposta se encontrar, exclusivamente, na Organização Regional;

b) pelo Gerente Regional de Navegação Aérea da INFRAERO ou pelo ocupante do posto de mais alto grau hierárquico das demais empresas prestadoras de Serviços de Navegação Aérea, quando a abrangência da mudança proposta se encontrar na INFRAERO ou em outra empresa prestadora dos Serviços de Navegação Aérea; e (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013

c) pelos Comandantes (ou Chefe) das Organizações Regionais envolvidas, pelo Gerente Regional de Navegação Aérea da INFRAERO ou pelo ocupante do posto de mais alto grau hierárquico, de outra empresa, quando a abrangência da mudança proposta se encontrar em uma ou mais Organização Regional e, ainda, em um PSNA da INFRAERO ou em PSNA de outras empresas prestadoras dos Serviços de Navegação Aérea (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

3.7.2.6 Toda documentação do GRSO, incluindo REGRSO, deverá ser mantida em arquivo durante todo o ciclo de vida de determinado sistema ou mudança (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

4 QUANDO UMA ANÁLISE DE SEGURANÇA É NECESSÁRIA

4.1 FASES DA ANÁLISE DE SEGURANÇA DO GRSO

4.1.1 Em conformidade com as diretrizes da OACI e melhores práticas do SGSO, as fases do GRSO apresentadas na Figura 4 são igualmente aplicáveis a qualquer GRSO relativo às áreas de operação, manutenção, procedimentos ou desenvolvimento de um novo sistema. A Figura 5 mostra como as cinco fases da análise de segurança GRSO são realizadas. Concluir, sistematicamente, cada uma dessas fases leva a uma análise de segurança operacional completa e consistente.

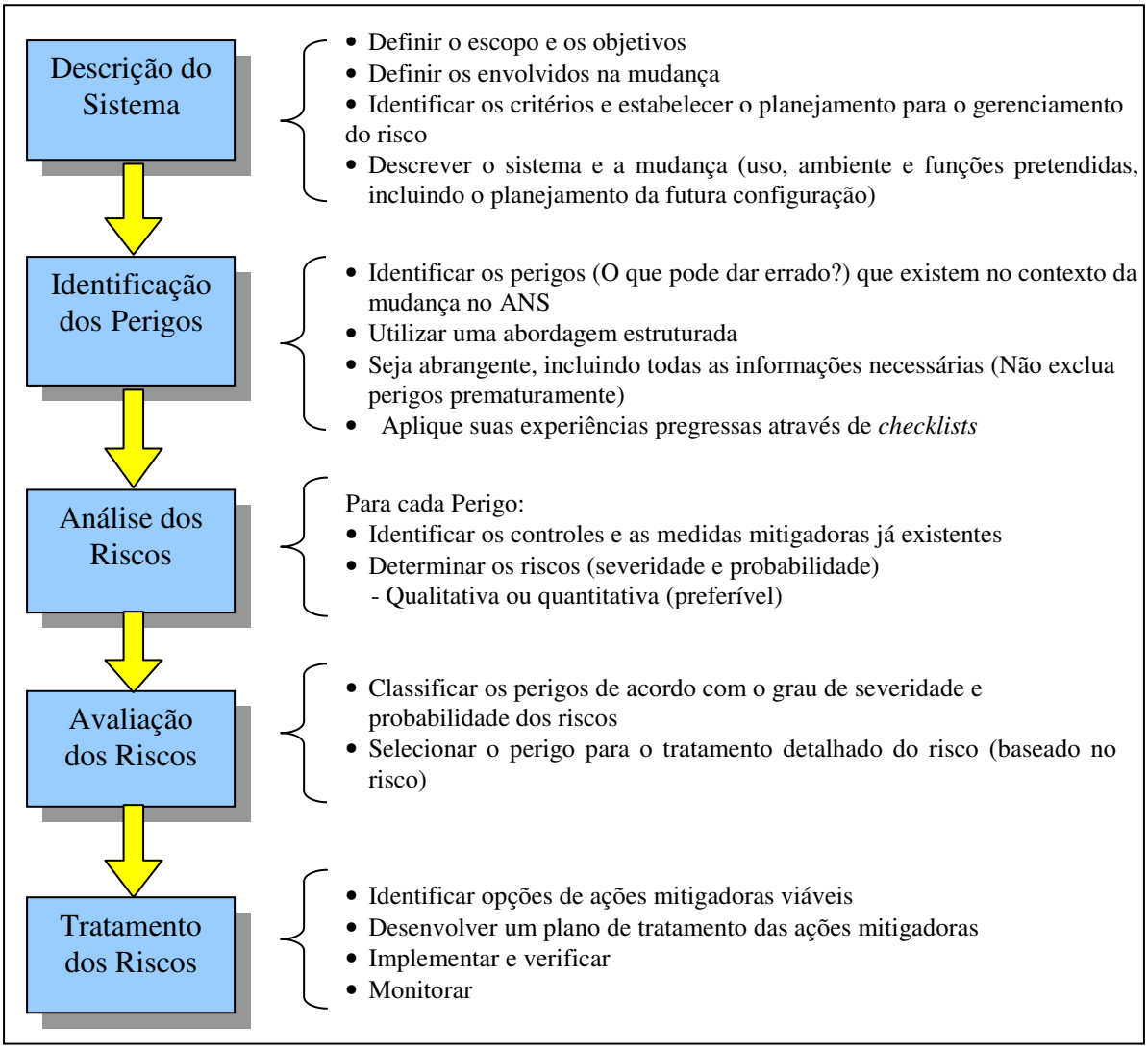
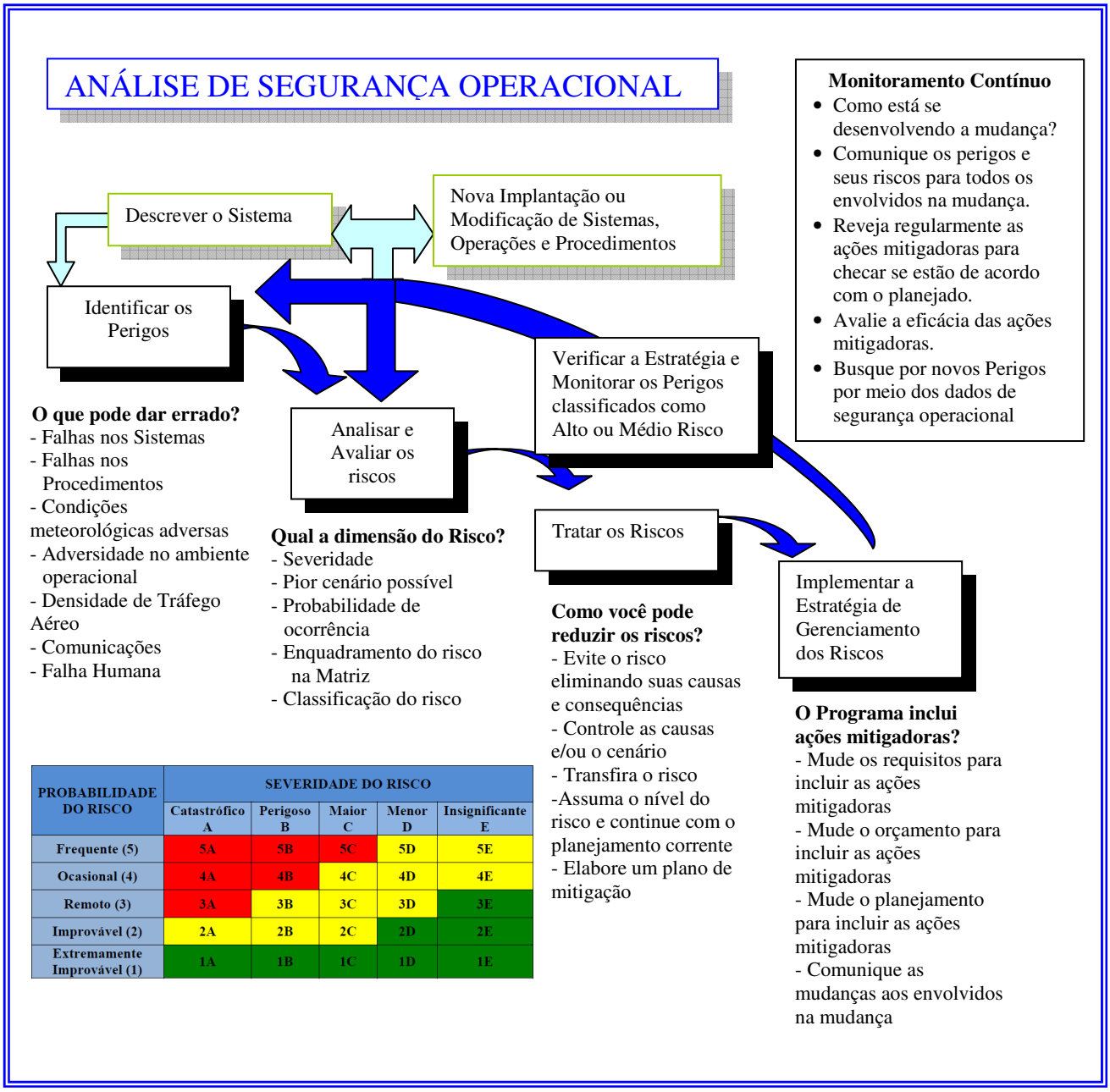


Figura 4- Fases do Gerenciamento de Risco à Segurança Operacional



PROBABILIDADE DO RISCO	SEVERIDADE DO RISCO				
	Catastrófico A	Perigoso B	Maior C	Menor D	Insignificante E
Frequente (5)	5A	5B	5C	5D	5E
Ocasional (4)	4A	4B	4C	4D	4E
Remoto (3)	3A	3B	3C	3D	3E
Improvável (2)	2A	2B	2C	2D	2E
Extremamente Improvável (1)	1A	1B	1C	1D	1E

Figura 5- Como realizar com sucesso uma Análise de Segurança

4.1.2 As etapas de segurança constituem um ciclo fechado, o que significa que quem está encarregado do GRSO repete um ou mais passos até que o risco à segurança para cada perigo seja aceitável. Independentemente da fase da operação, essas etapas auxiliam os especialistas de GRSO a identificar e gerenciar o risco à segurança associado com as atividades do ANS.

5 FASE 1: DESCRIÇÃO DO SISTEMA

5.1 CONSIDERAÇÕES SOBRE A DESCRIÇÃO DO SISTEMA

5.1.1 Uma descrição do sistema completa e minuciosa constitui a base essencial para realizar uma análise de segurança aprofundada. A descrição do sistema oferece informações que servem de base para identificar todos os perigos e riscos associados.

5.1.2 É fundamental que os membros de uma equipe GRSO:

a) definam e documentem a abrangência e os objetivos da mudança ou do sistema propostos;

b) descrevam e estruturem o sistema e a operação em detalhes suficientes para que a análise de segurança passe para a segunda fase - identificação dos perigos. A modelagem pode incluir a criação de um fluxograma funcional para ajudar a descrever o sistema e criar uma interface com os usuários, com outros sistemas e subsistemas; e

c) estejam cientes de que o sistema é sempre um subsistema de um sistema maior. Por exemplo, mesmo se a análise incorporar todos os serviços fornecidos dentro de um ACC, o sistema pode ser considerado um subconjunto de uma organização maior do espaço aéreo.

5.2 EFEITOS POTENCIAIS SOBRE O SISTEMA OU NAS INTERFACES COM OUTROS SISTEMAS

5.2.1 Esta fase considera todos os fatores críticos. A descrição resultante define a abrangência do Gerenciamento do Risco. As descrições do sistema precisam apresentar duas características essenciais – correção e integridade.

a) **Correção,** em uma descrição, significa que ela reflete com precisão o sistema sem ambiguidades ou erros; e

b) **Integridade** significa que nada foi omitido e que todo o conteúdo é essencial e apropriado em relação ao nível de detalhe.

5.2.2 Uma descrição do sistema ou da mudança pode ser um relatório completo ou um parágrafo. O tamanho não é importante, desde que a descrição inclua todos os elementos essenciais. É vital que a descrição do sistema ou da mudança proposta esteja correta e completa. Se a descrição estiver vaga demais, incompleta ou pouco clara, deverá ser esclarecida antes da continuação da análise de segurança. Para auxiliar na descrição, as seguintes perguntas podem ser consideradas:

a) qual é o objetivo do sistema ou da mudança?;

b) como o sistema ou a mudança será usado?;

c) quais são as funções do sistema ou da mudança?;

d) quais são os limites e as interfaces externas do sistema ou da mudança?;

e) qual é o ambiente em que o sistema ou a mudança vai operar?;

f) qual é a interconectividade e/ou quais são as interdependências entre os sistemas?; e

g) como a mudança vai afetar os usuários do sistema?

5.2.3 Seguem exemplos de dados que devem ser considerados ao conduzir a análise de segurança para descrever o sistema:

a) média de aproximações anuais em cada pista;

b) horas que o aeroporto operou nos mínimos meteorológicos ou abaixo deles;

c) tipo de operações do aeroporto;

d) aeronaves controladas no solo, no circuito de tráfego, nas aproximações e nas saídas (IFR e VFR) e nas transições;

e) horas em que o aeroporto opera como VFR e IFR e a relação entre eles;

f) disponibilidade e confiabilidade de *hardware e software*;

g) erros e/ou violações na operação das aeronaves;

h) erros e/ou violações no ATC;

i) erros e/ou violações de pedestres e/ou veículos; e

j) dados de acidentes e incidentes.

5.3 METODOLOGIA PARA A DESCRIÇÃO DO SISTEMA

5.3.1 A Equipe de GRSO pode utilizar vários métodos para fazer uma descrição do sistema. O Modelo da Figura 6 apresenta um método útil para coletar as informações necessárias para descrever o sistema.

5.3.2 Quando observamos um sistema como usuário, normalmente, só identificamos aqueles elementos que nos afetam ou nos interessam. Numa observação um pouco mais abrangente, conseguimos até identificar um sistema com maior amplitude, mas nos escapam os subsistemas e os demais componentes necessários para fazer com que o sistema, como um todo, cumpra a sua missão e funcione adequadamente para o que foi projetado.

5.3.3 Para que possamos visualizar todas as possíveis fontes de perigo, é necessário que se identifique todos os subsistemas e componentes de um sistema ou mudança, identificando suas funções e contribuições para o sistema como um todo. Somente dessa maneira, analisando do macro para o micro, conseguiremos decompor o sistema, o que nos permitirá identificar cada um dos elementos que fazem parte do sistema/mudança ou são afetados por eles. Esses elementos nos auxiliarão nas próximas fases do gerenciamento do risco.

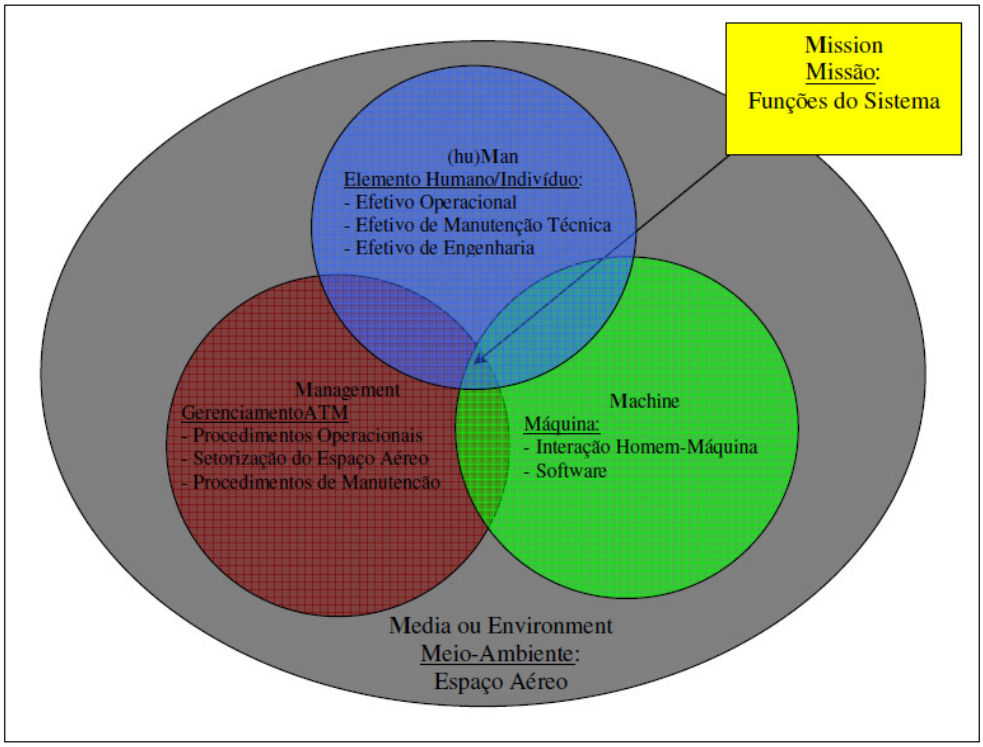


Figura 6- Modelo 5M

5.3.4 O modelo da figura 6 mostra os cinco elementos integrados presentes em qualquer sistema:

a) Missão – as funções que o sistema precisa para funcionar;

b) Elemento Humano – os recursos humanos necessários para a operação e manutenção;

c) Máquina – o equipamento usado no sistema, incluindo *hardware, firmware, software*, IHM e aviônica;

d) Decisões Gerenciais – os procedimentos e políticas que estabelecem a utilização, modos e limite de operação do sistema; e

e) Meio Ambiente – o ambiente de trabalho (técnico, operacional e físico) em que o sistema é operado e mantido.

5.4 DELIMITAÇÃO DO SISTEMA

5.4.1 A definição dos limites envolve restringir a análise da mudança ou do sistema aos elementos que afetam ou interagem entre si para realizar a função central. O nível de detalhamento na descrição varia, em geral, de forma proporcional à amplitude da mudança.

5.4.2 A descrição do sistema tem amplitude e profundidade. A amplitude está relacionada aos limites do sistema e a profundidade refere-se ao nível de detalhamento na descrição. Uma descrição detalhada do sistema e dos elementos que dele fazem parte pode evidenciar fontes potenciais de perigos associados com a mudança proposta.

5.5 AMPLITUDE E PROFUNDIDADE DA ANÁLISE

5.5.1 A amplitude e a profundidade necessárias para uma análise do GRSO variam com diversos fatores. Alguns destes fatores, usados para determinar a amplitude e a profundidade da análise, são:

a) **Tamanho e complexidade da mudança considerada** – Uma mudança maior e mais complexa pode exigir uma análise maior e mais complexa;

b) **Amplitude de determinada mudança** – O escopo do GRSO deve aumentar caso a mudança envolva mais de uma organização; e

c) **Tipo de mudança** – Mudanças nos procedimentos ou equipamentos tendem a exigir mais análise do que uma mudança na frequência de VHF.

5.5.2 A abrangência da análise permite tomar uma decisão fundamentada sobre se a proposta de mudança é aceitável da perspectiva da segurança operacional. Se houver dúvida quanto a incluir ou não um elemento específico na análise, é preferível incluí-lo.

5.5.3 Para auxiliar na determinação da abrangência de um sistema/mudança, pode-se considerar as seguintes diretrizes:

a) entendimento suficiente dos limites do sistema para abarcar possíveis impactos causados pelo sistema, incluindo interfaces com sistemas semelhantes, sistemas mais amplos do qual este é um componente, usuários e pessoal de manutenção;

b) elementos do sistema (missão, máquina, elemento humano, ações gerenciais e meio ambiente); e

c) limitação do sistema aos elementos que afetam ou interagem entre si para realizar a missão ou a função.

5.5.4 No mínimo, a análise de segurança deverá detalhar o sistema e seus perigos para que se compreendam claramente os riscos à segurança associados. As diretrizes que ajudam a determinar a profundidade a ser considerada em um sistema/mudança, incluem:

a) funções mais complexas e/ou maior quantidade de funções aumentarão o número de perigos e causas relacionadas;

b) análises complexas e detalhadas explorarão vários níveis de causas de perigos, às vezes em várias análises de segurança;

c) os perigos que podem ter associados algum risco inicial alto ou médio devem ser analisados cuidadosamente para determinar suas causas e probabilidades de ocorrências; e

d) a análise deve ser conduzida em um nível no qual o risco possa ser medido ou avaliado.

6 FASE 2: IDENTIFICAÇÃO DOS PERIGOS

6.1 CONSIDERAÇÕES SOBRE IDENTIFICAÇÃO DOS PERIGOS

6.1.1 Após a descrição precisa do sistema e da conclusão do planejamento, a equipe de gerenciamento de riscos poderá iniciar as sessões de identificação dos perigos. Um **perigo** é definido como qualquer condição real ou potencial que pode resultar em lesão, doença ou morte; danos ou perdas de determinado sistema, equipamento ou propriedade, ou danos ao meio ambiente.

6.1.2 A descrição abrangente do sistema e dos elementos que o compõem constituem fontes potenciais de identificação de perigos latentes na operação corrente ou de perigos potenciais que estejam associados a uma mudança. Deve ser considerado que o nível de detalhamento exigido no processo de identificação de perigos depende da complexidade do sistema e da mudança pretendida.

6.1.3 Durante a fase de identificação de perigos, a equipe de gerenciamento de riscos identifica e documenta potenciais problemas de segurança, suas possíveis causas, controles e consequências correspondentes.

6.1.4 Deve ser considerado, nos casos de gerenciamento do risco em PSNA prestador dos Serviços de Tráfego Aéreo, que a identificação dos perigos deverá ter como foco principal as condições reais ou potenciais que resultam em perdas ou danos para o ATC, concentradas, basicamente, em três requisitos principais:

a) Separação de Aeronaves;

b) Capacidade de Controle; e

c) Carga de Trabalho.

6.2 POTENCIAIS FONTES DE PERIGO

6.2.1 Para um gerenciamento de risco confiável a identificação dos perigos deve ser baseada em informações detalhadas sobre o projeto das mudanças propostas, em pesquisas da segurança operacional e, ainda, em observações e entrevistas. Devem ser consideradas todas as informações obtidas e assegurado que sejam verdadeiras.

6.2.2 Os dados relevantes devem ser coletados, classificados e ordenados para que os métodos analíticos apropriados sejam, então, selecionados e aplicados. Portanto, o tempo despendido na coleta de dados para a identificação dos perigos deve ser suficiente para assegurar a objetividade, evitando-se conclusões intuitivas que não sejam consistentes para um bom gerenciamento de risco.

6.2.3 Uma descrição abrangente do sistema e dos elementos que o compõem constitui fontes de identificação de perigos potenciais associados à mudança pretendida. O nível de detalhamento exigido no processo de identificação de perigos depende da complexidade da mudança. Quanto mais abrangente a identificação dos perigos, mais rigorosa será a análise dos riscos associados.

6.2.4 Dependendo da complexidade e da dimensão do sistema que está sendo analisado, a fase de identificação de perigos deve considerar todas as potenciais fontes de perigo, julgadas importantes, dentre as quais se destacam as seguintes:

a) fatores de projeto, incluindo os sistemas implantados (*hardware* e *software*);

b) procedimentos e práticas operacionais, incluindo sua documentação e listas de verificação, bem como sua validação sob as condições operacionais;

c) comunicações, inclusive o meio, a terminologia e a linguagem;

d) fatores humanos, como as políticas da organização para treinamento e habilitação;

e) fatores organizacionais, como a compatibilidade das metas de desempenho, a alocação de recursos, pressões operacionais e a cultura corporativa de segurança;

f) fatores do ambiente de trabalho, como barulho, temperatura, iluminação e a disponibilidade de equipamentos;

g) fatores de supervisão, incluindo a aplicabilidade e o cumprimento de normas; e

h) defesas, incluindo a existência de sistemas adequados de defesa e advertência, a tolerância do equipamento a erros e o grau em que o equipamento é protegido contra falhas.

6.3 MEIOS DE IDENTIFICAÇÃO DE PERIGOS

6.3.1 A possibilidade da existência de perigos potenciais na provisão dos serviços de navegação aérea requer a aplicação de metodologias proativas e reativas para a identificação desses perigos e, além disso, devem ser considerados os meios formais para a sua identificação, tais como:

a) pesquisa da segurança operacional durante as operações de rotina (NOSS);

b) pesquisas do fator humano;

c) notificações de ocorrências de trafego aéreo;

d) gráficos de disponibilidade da infraestrutura de navegação aérea;

e) cálculos de confiabilidade dos sistemas implantados *(hardware e software*);

f) inspeções técnicas e operacionais;

g) vistorias de segurança operacional do SEGCEA;

h) inspeções de segurança operacional;

i) relatórios de prevenção de acidentes aeronáuticos (RELPREV);

j) relatórios confidenciais de segurança de voo (RCSV); e

k) relatórios de investigação do controle do espaço aéreo (RICEA).

6.3.2 A equipe de gerenciamento de riscos deve definir as fontes de dados e as medidas necessárias para identificar os perigos e, ainda:

a) detectar os perigos que são mais frequentes do que o esperado; e

b) as estratégias de mitigação de riscos, adotadas anteriormente, que foram menos eficazes do que a expectativa.

6.4 ANÁLISE DA SEGURANÇA PARA IDENTIFICAÇÃO DE PERIGOS

6.4.1 A análise da segurança operacional para identificação de perigos se baseia em informações concretas, em pesquisas da segurança operacional e, ainda, em observações e entrevistas. Os dados relevantes devem ser coletados, classificados e ordenados para que os métodos analíticos apropriados sejam, então, selecionados e aplicados:

a) análise estatística – a estatística desempenha um papel importante na análise da segurança operacional, ajudando a quantificar situações e fornecendo, dessa forma, compreensão através de números;

b) análise das tendências – as tendências dos dados estatísticos sobre segurança operacional permitem gerar estimativas sobre eventos futuros, que podem ser indícios de perigos potenciais. Os métodos estatísticos são usados para se avaliar a importância das tendências observadas e permitir o estabelecimento dos limites do desempenho aceitável, com o qual se deve comparar o desempenho atual;

c) comparação situacional – poderão existir dados insuficientes para se comparar as circunstâncias de um evento de segurança operacional com a situação rotineira do PSNA. Para que a falta de dados confiáveis não comprometa a utilidade da análise da segurança, deve ser obtida uma amostra da experiência em outros PSNA sob condições operacionais similares;

d) simulação ATC – testes em simuladores ATC podem evidenciar perigos potenciais de segurança operacional. Portanto, para a validação de novos procedimentos e para a verificação de indícios de falhas de procedimentos em uso, a simulação das condições operacionais deve ser empregada; e

e) comitê de especialistas – devido à natureza variada de fatores contribuintes, que podem afetar a segurança operacional e as diferentes perspectivas possíveis na avaliação de uma determinada condição insegura, deve ser formado um comitê de especialistas para avaliar a possível existência de um perigo.

6.5 FERRAMENTAS PARA IDENTIFICAÇÃO DE PERIGOS

6.5.1 O gerenciamento da segurança operacional requer uma resposta continuada de seu desempenho. Por meio dessa resposta, o desempenho do sistema poderá ser avaliado e as mudanças necessárias efetuadas. Embora os interessados no processo de segurança de uma organização façam avaliações regulares, suas perspectivas individuais sobre "o que é seguro" variam consideravelmente.

6.5.2 Quando uma organização adiciona defesas contra perigos potenciais, pode-se considerar um aprimoramento da segurança operacional. No entanto, ainda podem faltar informações para uma tomada de decisão eficaz, sendo necessárias ferramentas adicionais para se medir o desempenho da segurança de uma forma sistemática e convincente. Dessa forma, para atender a essa premissa, devem ser efetuadas pesquisas para a identificação dos perigos latentes, conforme explicitado a seguir:

a) Pesquisas do Fator Humano (PPFH); e

b) Pesquisa da Segurança durante as Operações de Rotina (NOSS).

6.5.3 PESQUISAS DO FATOR HUMANO PARA IDENTIFICAÇÃO DE PERIGOS (PPFH)

6.5.3.1 O entendimento dos perigos sistêmicos e dos riscos intrínsecos relacionados às atividades cotidianas permite que se minimizem os erros operacionais, que são aqueles que surgem da interação do homem com a tecnologia, onde a fonte do erro está na incompatibilidade da interface homem-máquina. Portanto, a pesquisa da influência do desempenho humano na operação é uma forma de examinar sistematicamente a segurança operacional dos serviços prestados.

6.5.3.2 Para poder identificar os perigos latentes nessa área, as pesquisas devem ser realizadas sob a influência dos princípios dos fatores humanos (fatores individuais, psicossociais e organizacionais) mediante a observação contínua do ambiente operacional, de entrevistas e avaliações efetuadas por profissionais de psicologia, diretamente com os profissionais da área operacional. Essas pesquisas são independentes das inspeções de rotina e oferecem importantes diagnósticos sobre a rotina operacional, constituindo um mecanismo para se obter informações significativas sobre muitos aspectos dos PSNA, tais como:

a) IHM nos órgãos operacionais;

b) Observação da disposição dos postos de trabalho para o desempenho das tarefas de trafego aéreo;

c) Qualidade do relacionamento inter e intra-grupo;

d) Organização do trabalho (gerenciamento adequado da equipe, compreensão adequada das funções operacionais, divisão de tarefas, supervisão, etc.);

e) Qualificação adequada nas funções exercidas;

f) Qualidade da comunicação estabelecida;

g) Condições ambientais (iluminação, temperatura, ventilação, ruído, etc.);

h) Identificação de divergências e conflitos; e

i) Cultura de segurança operacional.

6.5.3.3 As pesquisas sobre segurança são feitas através de listas de verificação, questionários e entrevistas informais confidenciais, pois a confidencialidade garante a obtenção de informações que não seriam obtidas de outra forma.

6.5.3.4 Vale ressaltar que as pesquisas estruturadas e gerenciadas podem levantar dados específicos para a avaliação do desempenho da segurança operacional. No entanto, a validade de todas as informações obtidas nas pesquisas precisa ser verificada antes que as medidas corretivas sejam tomadas. Da mesma forma que nos sistemas de notificação voluntária de ocorrências, as pesquisas são subjetivas, refletindo percepções individuais.

6.5.4 PESQUISA DA SEGURANÇA DURANTE AS OPERAÇÕES DE ROTINA (NOSS)

6.5.4.1 Normalmente o monitoramento da segurança operacional depende da identificação dos perigos potenciais e reais, feita pelos próprios operadores. Quando a prática insegura é

incorporada à rotina da operação, é pouco provável que estes operadores a reconheçam como insegura e venham a apresentar reportes por meio do sistema de notificação de ocorrências.

6.5.4.2 O NOSS é um método de coleta de dados de segurança durante a operação de rotina nos órgãos ATC. É realizado, por meio de um ATCO treinado para observar a prática no ambiente operacional, sem interferir, por um período que pode variar de 1 a 2 meses, durante 1 hora diária. Após cada sessão o observador escreve um relatório onde identifica as ameaças, falhas e estados indesejáveis mais frequentes e como foram gerenciados durante o turno.

6.5.4.3 Essas informações irão auxiliar a organização a identificar os pontos que realmente precisam de incremento na segurança. Podem ser usadas na expansão de estratégias e programas de segurança mais efetivos e determinar onde os esforços de segurança operacional efetivamente devem ser aplicados.

6.5.4.4 Além disso, a aplicação da metodologia NOSS representa uma ferramenta preventiva adicional, sem depender dos operadores envolvidos na rotina diária e deve ser empregada nos serviços de tráfego aéreo para a coleta de dados de segurança operacional que poderão indicar a necessidade de estabelecer o gerenciamento do risco.

6.5.4.5 Os controladores de tráfego aéreo, normalmente, são responsáveis por gerenciar as ameaças, os riscos e estados indesejáveis com os quais eles se deparam todos os dias, no curso normal das operações. As suas intervenções em tempo hábil preservam as margens desejáveis de segurança. Entender a maneira e o nível de eficiência com que os controladores lidam com uma situação em andamento, é vital para o desenvolvimento das contramedidas necessárias para preservar as defesas do ATS. Assim sendo, um dos objetivos do NOSS é a identificação das ameaças advindas do erro humano, já que as estratégias de gerenciamento de riscos são mais bem direcionadas contra ameaças sistêmicas do que contra erros individuais.

6.6 REGISTRO DOS PERIGOS

6.6.1 Durante o processo de identificação dos perigos, a equipe de gerenciamento de risco deve registrar os perigos que podem advir com a implementação de uma mudança, na Tabela Síntese de Registro dos Perigos (Tabela 10).

6.6.2 Dessa forma, os perigos identificados devem ser associados às suas possíveis causas, às condições em que os perigos podem ocorrer (cenário) e às consequências correspondentes.

6.6.3 Portanto, a equipe de gerenciamento de risco deve, para cada perigo identificado, considerar:

a) suas possíveis causas;

b) os cenários de sua ocorrência;

c) os controles e requisitos aplicáveis; e

d) suas consequências correspondentes.

6.6.4 Esses perigos, basicamente, se enquadram em quatro categorias que devem ser documentadas em processos específicos para garantir a propriedade, a documentação e o monitoramento, conforme especificado abaixo:

a) perigos preexistentes que não estão no escopo da mudança;

b) perigos preexistentes que estão no escopo da mudança;

c) perigos que estão no escopo e são causados pela mudança; e

d) perigos que não estão no escopo, mas são causados pela mudança.

6.6.5 Pode haver casos em que a equipe de gerenciamento de risco identifique perigos preexistentes de médio ou alto risco que, independente da mudança, estão presentes na rotina operacional do PSNA. Nesses casos, ações corretivas são necessárias para mitigar o risco do perigo identificado, independentemente da conclusão do gerenciamento do risco.

6.6.6 Se a equipe de gerenciamento de risco encontrar uma medida mitigadora que reduza o risco a um nível aceitável, ou pelo menos tolerável, deverá encaminhar a proposta de medida ao gerente da segurança operacional do PSNA.

6.7 CAUSAS DOS PERIGOS

6.7.1 Causas são eventos que podem ocorrer de forma independente ou combinada e que resultam em um perigo ou falha.

6.7.2 O primeiro passo para o entendimento da avaliação dos riscos é a compreensão de que para cada perigo identificado haverá uma ou várias causas que provocará um ou mais efeitos relacionados. Para a ocorrência de um resultado indesejável de segurança operacional (efeito) existe um conjunto de fatores (causas) que contribuíram para esse resultado.

6.7.3 Para a determinação das causas, devem ser consideradas todas as situações reais ou potenciais que podem levar ao perigo, dentre as quais, destacam-se:

a) IHM inadequada;

b) erro humano;

c) erro operacional;

d) procedimentos e práticas operacionais inadequadas;

e) projetos ou concepções operacionais inadequadas;

f) implementação de *hardwares* e/ou *softwares* falhos;

g) infraestrutura inadequada de navegação aérea; e

h) normalização do desvio.

6.8 CENÁRIO DOS PERIGOS

6.8.1 O cenário é caracterizado pelas condições em que os perigos podem ocorrer, considerando a interação das variáveis operacionais, humanas e de infraestrutura que existem em um sistema. O cenário pode evidenciar a presença do perigo e/ou agravar suas conseqüências. Pode ser descrito, por exemplo, pela comparação dos termos abaixo, ou pela combinação deles:

a) Operacional – devem ser confrontadas situações de operação radar com operação não-radar, sistema automatizado com sistema manual, operação

VFR com operação IFR, espaços aéreos condicionados ativados com não ativados etc;

b) Condicional – devem ser confrontadas as condições meteorológicas desfavoráveis que requeiram desvios de rota com condições favoráveis, VMC com IMC, pico de tráfego com pouco movimento de tráfego etc; e

c) Físico – devem ser confrontadas as condições de variações ambientais, fonte de energia primária com fonte secundária, pistas abertas com pistas fechadas, pistas secas com pistas contaminadas etc.

6.8.2 Qualquer perigo identificado pode ter um nível de risco diferente em cenários distintos e deve considerar todas as possibilidades, da menos para a mais provável, permitindo condições de "pior caso". É importante identificar todos os cenários para determinar as piores consequências possíveis e formas de mitigação. A equipe de gerenciamento de risco deverá garantir que os riscos a serem incluídos na análise final sejam "verossímeis" considerando todos os controles aplicáveis existentes. As seguintes definições podem ser usadas como guia para tomar essas decisões:

a) Pior – condições mais desfavoráveis esperadas (por exemplo, pico de tráfego associado a condições meteorológicas desfavoráveis que requeiram desvios de rota); e

b) Verossímil – condição em que é razoável esperar que determinado cenário venha a ocorrer durante o ciclo operacional da mudança.

6.8.3 O objetivo de identificar os perigos em cenários desfavoráveis, porém verossímeis, é definir elementos adequados de mitigação para todos os riscos associados com cada perigo. Embora o pior resultado verossímil possa ter o maior risco, a probabilidade do pior resultado verossímil em geral é muito baixa. Entretanto, um resultado menos severo poderá ocorrer com mais frequência e resultar em maior risco do que o de pior efeito. As mitigações para os dois resultados podem ser diferentes e ambas devem ser consideradas. Portanto, a equipe de gerenciamento de risco deve considerar todos os cenários verossímeis possíveis para a avaliação dos riscos com o objetivo de desenvolver medidas de mitigação eficazes para cada resultado específico.

6.8.4 Em síntese, a descrição adequada de um cenário permite melhor evidenciar um perigo e contribui para melhor avaliação das respectivas consequências.

6.9 CONTROLES EXISTENTES

6.9.1 O controle é uma exigência de segurança já existente, que deve ser considerado para prevenir a ocorrência do perigo ou atenuar as suas conseqüências. Deve ser avaliado cada perigo e o cenário no qual ele existe potencialmente, de forma a determinar quais controles são aplicados.

6.9.2 São considerados controles os requisitos estabelecidos para balizar a operação e as ações relativas a uma mudança proposta, tais como:

a) requisitos estabelecidos para os projetos;

b) normas para a capacitação dos recursos humanos;

c) requisitos dos equipamentos (*hardware* e *software*);

d) manuais de operações;

e) modelos operacionais; e

f) normas e os procedimentos aplicáveis.

6.9.3 A equipe de gerenciamento do risco deve avaliar cada perigo e o cenário no qual o perigo existe em potencial para determinar os controles que previnem ou reduzem a sua ocorrência ou, até mesmo, podem mitigar suas consequências. Um controle só pode ser considerado se tiver sido validado e verificado mediante uma evidência objetiva.

6.9.4 Devem ser considerados três tipos de controles:

a) Validados – são controles e requisitos inequívocos, corretos, completos e verificáveis;

b) Verificados – são controles e requisitos determinados objetivamente para estar de acordo com a solução do projeto; e

c) Recomendados – são controles com potencial para atenuar um perigo ou risco, mas ainda não fazem parte do sistema ou de seus requisitos.

6.9.5 A equipe de gerenciamento de risco precisa documentar os controles existentes porque a compreensão sobre os controles facilitará, na fase de avaliação dos riscos, o estabelecimento de probabilidades e de severidades verossímeis. Vale salientar que ao identificar os controles existentes, a equipe de gerenciamento do risco aprova os controles específicos para a mudança, para o perigo e para o cenário.

6.10 CONSEQUÊNCIAS DO PERIGO

6.10.1 A consequência é uma descrição do dano ou do efeito potencial do perigo, caso ele ocorra em um cenário definido. Deve ser considerado pela equipe de gerenciamento de riscos que cada perigo pode ser representado por uma ou várias causas, tendo o potencial de provocar também uma ou mais consequências (incidentes ou eventos) para cada um dos cenários analisados.

6.10.2 Deve ser considerado, ainda, que as consequências dos perigos nos PSNA prestadores dos Serviços de Tráfego Aéreo estão concentradas, basicamente, em três requisitos:

a) Separação de Aeronaves – desde redução da separação com um erro operacional de severidade baixa até colisão de aeronaves;

b) Capacidade de Controle – desde redução leve até perda total da capacidade ATC; e

c) Carga de Trabalho – desde aumento leve até aumento significativo da carga de trabalho ATC.

6.10.3 Para cada perigo e sua consequência associada, a equipe de gerenciamento de risco efetuará uma avaliação de riscos baseada na severidade das consequências e na probabilidade de sua ocorrência.

6.11 TABELA DE REGISTRO DE PERIGOS

6.11.1 A tabela de registro de perigos apresentada a seguir, constitui uma abordagem estruturada na qual as causas dos perigos identificados estão diretamente relacionadas às possíveis consequências e permite condensar os dados básicos relativos a um perigo identificado em um único documento.

Tabela 1 – Registro de Perigos

NÚMERO DO PERIGO	**PREEXISTENTE** □ **NOVO PERIGO** □	**NO ESCOPO DA MUDANÇA SIM** □ **NÃO** □	**CAUSADO PELA MUDANÇA SIM** □ **NÃO** □
DESCRIÇÃO DO PERIGO			
CAUSAS			
CENÁRIO			
CONTROLES			
CONSEQUÊNCIA			

7 FASE 3: AVALIAÇÃO DOS RISCOS

7.1 CONSIDERAÇÕES SOBRE AVALIAÇÃO DOS RISCOS

7.1.1 A combinação da severidade com a probabilidade do efeito potencial de um perigo ocorrer, no pior cenário verossímil possível, caracteriza o risco. Desse modo, o risco é definido como a possibilidade de perda ou dano, medida em termos de severidade e probabilidade.

7.1.2 Para a avaliação de riscos a equipe de gerenciamento pode utilizar métodos quantitativos ou qualitativos e deve ser considerado, dependendo da aplicação e do rigor usado para analisar e caracterizar o risco, que modos diferentes de falhas podem provocar impacto de maneira singular, tanto na severidade como na probabilidade.

7.1.3 Deve ser considerada a possibilidade de um evento ocorrer e as suas consequências, se efetivamente ocorrer, levando em consideração os parâmetros de Severidade e Probabilidade.

7.2 SEVERIDADE DOS RISCOS

7.2.1 A severidade dos riscos é caracterizada pelas consequências possíveis de uma situação de perigo à segurança operacional, tomando como referência a pior condição previsível.

7.2.2 A determinação da severidade deve ser efetuada considerando o pior resultado possível, ou seja, a equipe de gerenciamento de risco para estabelecer a severidade deve examinar todos os efeitos e considerar o pior, porém, verossímil.

7.2.3 Entretanto, é preciso levar em consideração que, embora o pior resultado possa ter o maior risco, a probabilidade da ocorrência do pior resultado verossímil em geral é muito baixa.

7.2.4 Em contrapartida, um resultado menos severo pode ocorrer mais frequentemente e resultar em um risco maior do que a pior consequência. Por essa razão, a equipe de gerenciamento de risco deve considerar os resultados possíveis, a fim de identificar o maior risco.

7.2.5 DETERMINAÇÃO DA SEVERIDADE

7.2.5.1 A Severidade está baseada nas consequências possíveis de uma situação de perigo à segurança operacional. Para sua determinação nos Serviços de Tráfego Aéreo deve ser utilizada a tabela abaixo:

Tabela 2 – Severidade do Risco

SEVERIDADE DO EVENTO NOS SERVIÇOS DE TRÁFEGO AÉREO		
DEFINIÇÃO	**SIGNIFICADO**	**VALOR**
Catastrófica	Colisão com outra aeronave, obstáculos ou terreno.	**A**
Perigosa	Redução da separação com um erro operacional de severidade alta ou uma perda total da capacidade ATC.	**B**
Maior	Redução da separação com um erro operacional de severidade baixa ou moderada ou redução significativa em capacidade ATC.	**C**
Menor	Redução leve da capacidade ATC, ou aumento significativo da carga de trabalho ATC.	**D**
Insignificante	Aumento leve na carga de trabalho ATC	**E**

7.2.5.2 Para a aplicação da tabela a equipe de gerenciamento de risco deve considerar os incidentes de tráfego aéreo classificados como Risco Crítico com erro operacional de severidade alta (Perigosa – B) e aqueles classificados como Risco Potencial como erro operacional de severidade moderada (Maior – C).

7.3 PROBABILIDADE DOS RISCOS

7.3.1 A combinação da severidade previsível com a probabilidade do efeito potencial de um perigo define o risco. Nesse contexto, considera-se que a probabilidade é caracterizada pela frequência que se pode esperar o dano resultante acontecer, na pior severidade previsível. Determinada a severidade da ocorrência, será avaliada a probabilidade de o evento ocorrer.

7.3.2 A equipe de gerenciamento de risco deve efetuar a determinação de uma probabilidade que seja compatível com a severidade escolhida e considerar que o uso de dados quantitativos é preferível, pois tende a ser mais objetivo. Porém, quando dados quantitativos não estiverem disponíveis, é aceitável o emprego de dados qualitativos.

7.3.3 No entanto, sempre que for possível estabelecer a probabilidade pelo método qualitativo e quantitativo, deverá ser considerado o resultado de maior probabilidade de ocorrência do evento, cujo resultado é mais crítico para a segurança operacional.

7.3.4 Os termos quantitativos são estabelecidos pela ocorrência do evento por determinada quantidade de movimento que se baseiam em informações concretas e em pesquisas da segurança operacional. A equipe de gerenciamento de risco deve considerar que dados relevantes devem ser coletados por meio de:

a) Análise estatística – quantifica situações através de números;

b) Análise das tendências – gera estimativas sobre eventos futuros;

c) Comparação situacional – obtém uma amostra da experiência em outros PSNA sob condições operacionais similares; e

d) Simulação ATC – evidencia perigos potenciais de segurança operacional.

7.3.5 Os termos qualitativos são estabelecidos pela ocorrência do evento em determinado espaço de tempo e são considerados os dados subjetivos expressos como medida de qualidade.

7.3.6 DETERMINAÇÃO DA PROBABILIDADE

7.3.6.1 A Probabilidade é a mensuração, em termos qualitativos ou quantitativos, da possibilidade de uma situação de perigo ocorrer. Para a avaliação da probabilidade de um evento nos Serviços de Navegação Aérea a equipe de gerenciamento de risco deve utilizar o quadro a seguir:

Tabela 3 – Probabilidade dos Perigos

Frequência	PROBABILIDADE DO EVENTO NO SISTEMA ATC			Valor
	Qualitativo		Quantitativo	
	AUXÍLIOS	ATC	ATC	
Frequente	Esperado acontecer mais de uma vez por semana.	Esperado acontecer uma vez a cada período de 2 dias.	$P \geq 10^{-3}$	**5**
Ocasional	Esperado acontecer, aproximadamente, uma vez todos os meses.	Esperado acontecer várias vezes por mês.	$10^{-3} > P \geq 10^{-5}$	**4**
Remoto	Esperado acontecer, aproximadamente, uma vez todos os anos.	Esperado acontecer uma vez em poucos meses.	$10^{-5} > P \geq 10^{-7}$	**3**
Improvável	Esperado acontecer, aproximadamente, uma vez entre 10 e 100 anos.	Esperado acontecer uma vez a cada 3 anos.	$10^{-7} > P \geq 10^{-9}$	**2**
Extremamente Improvável	Esperado acontecer menos que uma vez em 100 anos.	Esperado acontecer menos que uma vez a cada 30 anos.	$P < 10^{-9}$	**1**

P = Probabilidade de ocorrência do evento por movimentos.

8 FASE 4: CLASSIFICAÇÃO DOS RISCOS

8.1 MATRIZ DE AVALIAÇÃO DE RISCO

8.1.1 Após a avaliação dos riscos quanto à severidade e à probabilidade, deve-se proceder à classificação dos riscos, utilizando-se uma Matriz de Avaliação de Riscos.

8.1.2 Uma vez avaliado o risco, será necessária uma análise para avaliar o potencial de prejuízo ou dano. Nessa avaliação, serão observados os seguintes aspectos:

a) a severidade das potenciais consequências adversas do evento perigoso; e

b) a probabilidade da ocorrência do evento perigoso.

8.1.3 A avaliação dos riscos envolve o exame da probabilidade e da severidade das consequências adversas. Em outras palavras, o potencial de prejuízo é determinado. Na realização de avaliações de riscos, é importante distinguir entre perigos (o potencial de causar prejuízo) e risco (a probabilidade de que o prejuízo aconteça). A matriz de avaliação de riscos é uma ferramenta útil para se dar prioridade aos perigos que requeiram maior atenção.

8.1.4 Na Matriz de Avaliação de Riscos, as fileiras refletem as categorias de severidade previamente introduzidas, e as colunas, as categorias de probabilidade previamente introduzidas gerando um índice alfanumérico, conforme tabela a seguir:

Tabela 4 – Matriz de Avaliação de Riscos

PROBABILIDADE DO RISCO	SEVERIDADE DO RISCO				
	Catastrófico A	Perigoso B	Maior C	Menor D	Insignificante E
Frequente (5)	5A	5B	5C	5D	5E
Ocasional (4)	4A	4B	4C	4D	4E
Remoto (3)	3A	3B	3C	3D	3E
Improvável (2)	2A	2B	2C	2D	2E
Extremamente Improvável (1)	1A	1B	1C	1D	1E

8.2 ACEITABILIDADE DOS RISCOS

8.2.1 Depois de identificados os índices dos riscos, os mesmos devem ser classificados quanto à aceitabilidade, conforme a tabela abaixo:

Tabela 5 – Classificação do Risco

Nível do Risco	Índice de Avaliação do Risco
ALTO RISCO	**5A, 5B, 5C, 4A, 4B, 3A**
MÉDIO RISCO	**5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C**
BAIXO RISCO	**3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E**

8.2.2 Os riscos são classificados, quanto à aceitabilidade, em:

a) ALTO RISCO – Risco inaceitável: nos casos de Risco Inicial, significa que as mudanças não devem ser implementadas até que os riscos associados aos perigos sejam mitigados e reduzidos a Médio ou Baixo. Nos casos de Risco Corrente, as operações/atividades nas condições atuais devem cessar até que o risco seja reduzido, pelo menos, para um nível tolerável. Neste caso, a mitigação e a supervisão dos riscos (Residuais) serão necessárias;

b) MÉDIO RISCO – Risco tolerável: significa que o risco (Inicial ou Corrente) deve ser mitigado a um nível tão baixo quanto praticável (ALARP). Em tais condições, a mudança pode ser implementada ou as operações podem ser mantidas, desde que haja a Supervisão do Desempenho da Segurança Operacional e o monitoramento dos riscos correntes; e

c) BAIXO RISCO – Risco aceitável sem restrição ou limitação: significa que não precisa ser tomada nenhuma medida e que os riscos assumidos (Inicial ou Corrente) compensam os benefícios auferidos. Os perigos não precisam ser gerenciados ativamente, porém precisam ser documentados. No entanto, se a organização entender que uma mitigação representa baixo custo ou pequeno esforço, o risco poderá ser mitigado.

8.2.3 Deve ser considerado pela equipe de gerenciamento de risco que, independentemente da classificação de risco, se a causa de um perigo for falha de um ponto único ou de causa comum, o risco deve ser classificado como Alto Risco. No caso de risco inicial, o projeto deve adotar medidas para a mitigação dessas condições e, no caso de risco corrente, as operações devem cessar até que o risco seja reduzido, pelo menos, para um nível tolerável. Em ambos os casos, a mitigação e o monitoramento dos riscos residuais serão necessários.

8.2.4 As falhas de um ponto único e as falhas de causa comum são definidas, conforme explicitado abaixo:

a) falha de um ponto único – é definida como uma falha de um item que resultará na falha do sistema e não será compensada quanto à redundância ou a um procedimento operacional alternativo. Um exemplo de falha de um ponto único é um sistema com *hardware* redundante, no qual as partes do *hardware* dependem de única fonte de energia. Nesse caso, se a fonte falhar, o sistema falhará; e

b) falha de causa comum é definida como uma simples falha que resulta na falha correspondente dos componentes múltiplos. Um exemplo de falha de causa comum é a implementação de um novo *software* (ainda não continuamente testado na operação) em toda a rede de computadores que

dá suporte ao ATC. Apesar da redundância de *hardware*, todos estarão suscetíveis aos mesmos problemas do *software* comum.

8.3 TIPIFICAÇÃO DE RISCOS

8.3.1 Depois da classificação dos riscos, quanto à aceitabilidade, devem ser considerados os tipos de risco, conforme as definições abaixo:

a) Risco Corrente – risco baseado em dados reais, considerando-se o momento atual de uma atividade ou operação. Ao determinar-se o risco corrente, os controles validados e os verificados podem ser usados na avaliação do risco;

b) Risco Inicial – risco baseado em dados de projeto, considerando-se somente os controles verificados e suposições documentadas para um determinado cenário. É o risco deduzido no estágio preliminar ou fase inicial de uma mudança proposta, programa ou avaliação;

c) Risco Residual – risco que permanece depois que todas as técnicas de controle tenham sido esgotadas, as medidas mitigadoras implementadas e depois que todos os controles tenham sido verificados; e

d) Risco Residual Previsto – risco resultante depois de completada a análise de segurança e verificados todos os requisitos de segurança. O Risco Residual Previsto está baseado na suposição de que todos os requisitos de segurança foram validados e verificados.

8.4 TABELA DE AVALIAÇÃO DE RISCOS

8.4.1 A tabela de avaliação de riscos apresentada a seguir, constitui uma continuação da tabela de registro de perigos, apresentada no subitem 6.11, visando manter os dados básicos relativos a um perigo identificado e a avaliação de riscos em um único documento.

Tabela 6 – Avaliação dos Riscos

ANÁLISE DE RISCO	**INICIAL □ CORRENTE □**	**FALHA DE PONTO ÚNICO SIM □ NÃO □**	**FALHA DE CAUSA COMUM SIM □ NÃO □**
SEVERIDADE DO RISCO			
PROBABILIDADE DO RISCO			
CLASSIFICAÇÃO DO RISCO			

9 FASE 5: MITIGAÇÃO DOS RISCOS

9.1 CONSIDERAÇÕES SOBRE MITIGAÇÃO DOS RISCOS

9.1.1 Mitigação de riscos é um conjunto de medidas que visa à eliminação dos perigos ou à redução da probabilidade e/ou da severidade dos riscos associados. Dessa forma, a fim de minimizar os impactos à segurança operacional, sempre que os riscos não puderem ser eliminados devem ser mitigados.

9.1.2 Na avaliação das opções para mitigar os riscos, deve-se considerar, antes de tomar uma decisão, o esforço para a implementação e a eficácia das medidas mitigadoras para que se possa adotar a solução adequada, considerando-se os seguintes aspectos:

a) a análise da defesa;

b) a estratégia para mitigação de riscos; e

c) as opções de mitigação de riscos.

9.2 ANÁLISE DA DEFESA

9.2.1 O nível de risco mais baixo praticável deve ser buscado para todas as operações, a fim de manter um equilíbrio entre o tempo despendido, os custos e as dificuldades em aplicar as medidas eliminadoras ou mitigadoras.

9.2.2 Quando o risco for considerado “Alto Risco” ou “Médio Risco”, devem ser adotadas medidas mitigadoras para reduzir a severidade das possíveis consequências, para reduzir a probabilidade da sua ocorrência e para reduzir a exposição a esse risco.

9.2.3 Neste contexto, as defesas disponíveis para proteger pessoas, bens e/ou meio ambiente podem ser categorizadas em dois tipos, a saber:

a) Defesas físicas – incluem equipamentos e objetos que desestimulam ou evitam uma ação indevida, diminuindo a probabilidade de eventos indesejáveis e podem, também, atenuar as consequências desses eventos; e

b) Defesas operacionais – incluem procedimentos e práticas que podem atenuar tanto a severidade das consequências quanto a probabilidade de ocorrência dos eventos indesejáveis.

9.3 ESTRATÉGIAS PARA MITIGAÇÃO DE RISCOS

9.3.1 Para estabelecer a estratégia de mitigação de risco devem ser adotadas as medidas, isoladas ou combinadas, explicitadas a seguir:

a) Prevenção da exposição – a operação perigosa é evitada quando o risco excede os benefícios;

b) Redução do prejuízo – a operação é efetuada, mas são implementadas ações para reduzir a probabilidade dos eventos perigosos ou a magnitude das consequências; e

c) Segregação da exposição – a operação é efetuada, mas são implementadas ações para isolar os efeitos e reduzir a severidade do risco.

9.4 PROPOSTAS PARA MITIGAÇÃO DE RISCOS

9.4.1 Na avaliação das alternativas para mitigação dos riscos, deve ser considerado que nem todas as opções têm o mesmo potencial para reduzir riscos. Assim, antes de decidir pela adoção de qualquer uma delas, devem ser adotadas aquelas que apresentarem a melhor eficácia. É importante que toda a variedade de medidas de controle seja considerada e que as combinações de medidas também o sejam, para se encontrar a melhor solução.

9.4.2 Cada opção proposta de mitigação de riscos deverá ser examinada sob as seguintes perspectivas:

a) Eficácia – avaliação da medida quanto à possível eliminação ou redução dos riscos identificados e até que ponto as alternativas atenuam os riscos. A eficácia pode ser,

- nível um (ações técnicas) – medida de segurança que elimina o risco;
- nível dois (ações de controle) – medida de segurança que aceita o risco, mas ajusta o sistema - para atenuá-lo, reduzindo-o a um nível administrável; e
- nível três (ações pessoais) – medida de segurança que aceita que o perigo não pode ser eliminado (Nível Um) nem controlado (Nível Dois), de modo que o pessoal deve ser treinado para lidar com ele;

b) Custo/Benefício – análise dos benefícios esperados da opção, dos custos da medida e se os potenciais ganhos serão proporcionais ao impacto da mudança exigida;

c) Praticabilidade – verificação se a medida é apropriada em termos de tecnologia, recursos financeiros, operacionalidade, normas e procedimentos aplicáveis;

d) Desafio – avaliação da medida de mitigação de riscos, quanto ao exame crítico de todos os grupos interessados;

e) Aceitação – verificação da adesão à medida ou da resistência que se pode esperar dos interessados;

f) Viabilidade – verificação, quando implementada, se a medida poderá ser cumprida;

g) Duração – análise da medida, quanto aos benefícios que ela trará no curto, no médio e no longo prazo;

h) Riscos residuais – verificação dos possíveis riscos residuais que a medida de mitigação de riscos acarretará, relacionados ao perigo original; e

i) Novos perigos - avaliação dos possíveis novos problemas, que a medida mitigadora poderá acarretar.

9.5 TABELA DE MEDIDAS MITIGADORAS

9.5.1 A tabela de medidas mitigadoras apresentada a seguir constitui uma continuação da tabela de avaliação de riscos apresentada em 8.4, para que os dados relativos à avaliação de riscos constituam um único documento.

Tabela 7 – Medidas Mitigadoras

MEDIDAS MITIGADORAS	AS MEDIDAS SÃO VIÁVEIS? SIM □ NÃO □	HAVERÁ RISCO RESIDUAL? SIM □ NÃO □	CAUSAM NOVO PERIGO? SIM □ NÃO □
DESCRIÇÃO DAS MEDIDAS			

9.6 AVALIAÇÃO DOS RISCOS RESIDUAIS

9.6.1 A equipe de gerenciamento de risco deve proceder a uma avaliação do risco residual empregando a mesma metodologia que foi usada na análise dos riscos inicial e/ou corrente e considerar, ainda, as seguintes situações:

a) provavelmente não ocorra – são ocorrências isoladas e riscos em que o índice de exposição é muito baixo ou o tamanho da amostra é pequeno. A complexidade das circunstâncias necessárias para criar uma situação de incidente pode ser tal que é improvável que a cadeia de eventos venha a acontecer;

b) pode ocorrer – são perigos com uma probabilidade razoável de que pode haver deficiências no desempenho humano nas mesmas condições de trabalho em outros PSNA, ou que as mesmas falhas de infraestrutura existam em outras partes do sistema; e

c) provavelmente ocorrerá – são ocorrências que refletem um possível padrão de falhas materiais e humanas que ainda não foram eliminadas. Dado o tipo ou a manutenção do equipamento, é provável que, sob condição de operação contínua, haverá uma falha. Do mesmo modo, pode-se esperar, com alguma certeza, que as pessoas que operam sob condições de trabalho semelhantes têm a probabilidade de cometer os mesmos erros ou estarem sujeitos ao mesmo resultado indesejável de desempenho.

9.6.2 Se na classificação do risco residual for obtido um resultado de alto risco, devem ser implementadas novas medidas mitigadoras apropriadas até ser obtida a redução do risco a um nível que seja aceitável ou, pelo menos, tolerável para implementação da mudança.

9.6.3 Mesmo quando for classificado como baixo risco, se qualquer medida mitigadora puder reduzir ainda mais o risco residual, a equipe de gerenciamento de risco deverá:

a) propor a implementação dessas medidas, se factíveis;

b) considerar a viabilidade técnica de redução do risco mais adiante; e

c) avaliar todos os casos individualmente.

9.6.4 Se o risco não puder ser reduzido a um nível pelo menos tolerável, após a tentativa das possíveis medidas de mitigação, a mudança não satisfaz os requisitos de segurança e não poderá ser implementada.

9.6.5 Nesse caso, o proponente da mudança terá que revisar os objetivos originais ou abandonar a mudança proposta.

9.7 TABELA DE AVALIAÇÃO DE RISCOS RESIDUAIS

9.7.1 A tabela de avaliação de riscos residuais apresentada a seguir constitui uma continuação da tabela de medidas mitigadoras apresentada no subitem 9.5.

Tabela 8 – Avaliação dos Riscos Residuais

RISCO RESIDUAL	**PREVISTO** **SIM □ NÃO □**	**TOLERÁVEL** **SIM □ NÃO □**	**REQUER MEDIDAS MITIGADORAS** **SIM □ NÃO □**
SEVERIDADE DO RISCO RESIDUAL			
PROBABILIDADE DO RISCO RESIDUAL			
CLASSIFICAÇÃO DO RISCO RESIDUAL			

Tabela 9 – Tabela Consolidada de Registro de Perigos

NÚMERO DO PERIGO	**PREEXISTENTE □ NOVO PERIGO □**	**NO ESCOPO DA MUDANÇA? SIM □ NÃO □**	**CAUSADO PELA MUDANÇA? SIM □ NÃO □**
DESCRIÇÃO DO PERIGO			
CAUSAS			
CENÁRIO			
CONTROLES			
CONSEQUÊNCIA			
ANÁLISE DE RISCO	**INICIAL □ CORRENTE □**	**FALHA DE PONTO ÚNICO? SIM □ NÃO □**	**FALHA DE CAUSA COMUM? SIM □ NÃO □**
SEVERIDADE DO RISCO			
PROBABILIDADE DO RISCO			
CLASSIFICAÇÃO DO RISCO			
MEDIDAS MITIGADORAS	**SÃO VIÁVEIS? SIM □ NÃO □**	**HAVERÁ RISCO RESIDUAL? SIM □ NÃO □**	**CAUSAM NOVO PERIGO? SIM □ NÃO □**
DESCRIÇÃO DAS MEDIDAS			
RISCO RESIDUAL	**PREVISTO? SIM □ NÃO □**	**TOLERÁVEL? SIM □ NÃO □**	**REQUER MEDIDAS MITIGADORAS? SIM □ NÃO □**
SEVERIDADE DO RISCO RESIDUAL			
PROBABILIDADE DO RISCO RESIDUAL			
CLASSIFICAÇÃO DO RISCO RESIDUAL			

Tabela 10 – Tabela Síntese de Registro dos Perigos

Perigo nº	**Descrição do Perigo:**							
Causas	Cenário	Controle/ Requisitos Existentes	Consequências Possíveis	Severidade	Probabilidade	Risco Inicial	Medidas Mitigadoras	Risco Residual Previsto
1) ... 2) ... 3)	1) ... 2) ... 3)	1) ... 2) ... 3)					1) ... 2) ... 3)	

9.8 AVALIAÇÃO DOS RISCOS PARA OS NOVOS PERIGOS

9.8.1 Deve ser dada preferência àquelas medidas mitigadoras que eliminam completamente o risco. Entretanto, tais soluções não podem ser adotadas em todas as situações em razão da natureza dos problemas e da limitação de recursos tecnológicos, financeiros, operacionais e humanos. Nesses casos são implementadas medidas que reduzem o risco a um nível aceitável, ou pelo menos tolerável, para a implementação da mudança proposta.

9.8.2 No entanto, deve ser considerada a possibilidade de uma medida mitigadora, implementada para eliminar ou atenuar um risco, acarretar novo perigo que não tenha sido identificado anteriormente.

9.8.3 Quando a implementação de uma medida mitigadora causar um novo perigo, este deverá ser submetido a todos os procedimentos de avaliação de risco e, consequentemente, tal medida mitigadora somente deverá ser validada se a avaliação concluir por risco aceitável, ou pelo menos tolerável e, ainda, que os benefícios compensem os custos de sua implementação e/ou seja obtida uma vantagem significativa em termos da segurança operacional.

10 MONITORAMENTO DAS MEDIDAS MITIGADORAS

10.1 CONSIDERAÇÕES SOBRE O MONITORAMENTO DAS MEDIDAS MITIGADORAS

10.1.1 Gerenciar um risco é um processo dinâmico no qual os perigos e as informações dos riscos associados devem ser monitorados e atualizados através do ciclo de evolução da mudança. Portanto, gerenciar um risco inclui o monitoramento do *status* da implementação das medidas mitigadoras.

10.1.2 Dessa forma, a Organização responsável pela execução de uma medida mitigadora deve desenvolver o respectivo plano para a sua efetiva implementação, e o PSNA, objeto da mudança, deve estabelecer uma forma de monitoramento dessa implementação.

Tabela 11 – Planejamento para a Implementação das Medidas Mitigadoras

Número do Perigo	Descrição da Medida Mitigadora	Organização Responsável	Cargo ou Função do Responsável	Status	Prazo de Conclusão
1					
2					
...					
n					

11 SUPERVISÃO DO DESEMPENHO DA SEGURANÇA OPERACIONAL

11.1 CONSIDERAÇÕES SOBRE A SUPERVISÃO DA SEGURANÇA OPERACIONAL

11.1.1 A supervisão da segurança operacional deve ser incluída na estratégia para validação da mudança e para identificar condições insatisfatórias que surgiram durante o desenvolvimento do projeto, ou da execução da mudança, com vistas à manutenção da segurança operacional.

11.1.2 O gerenciamento da segurança operacional requer uma resposta continuada de seu desempenho, e por meio dessa resposta o desempenho do sistema poderá ser avaliado e as mudanças necessárias efetuadas. Embora os interessados no processo de segurança de uma organização façam avaliações regulares, suas perspectivas individuais sobre "o que é seguro" variam consideravelmente.

11.1.3 Quando uma organização adiciona defesas contra perigos potenciais, pode-se considerar um aprimoramento da segurança operacional. No entanto, ainda podem faltar informações para uma tomada de decisão eficaz, sendo necessárias ferramentas adicionais para se medir o desempenho da segurança de forma sistemática e convincente, tais como:

a) Monitoramento da segurança operacional; e

b) Controle dos riscos residuais.

11.2 MONITORAMENTO DA SEGURANÇA OPERACIONAL

11.2.1 Os resultados obtidos inicialmente no gerenciamento de risco poderão requerer atualizações ou mudanças a partir do desenvolvimento do projeto e da implementação da mudança, em razão da possibilidade de modificações ou ajustes de algumas decisões.

11.2.2 Dessa forma, o monitoramento da segurança operacional deverá rastrear os perigos identificados, indicando se as medidas mitigadoras implementadas foram suficientemente eficazes conforme o esperado originalmente ou, ainda, se existe algum tipo de perigo a ser identificado, o que poderá requerer uma nova avaliação de riscos e a implementação de novas medidas mitigadoras.

11.3 MÉTODOS DE MONITORAMENTO DA SEGURANÇA OPERACIONAL

11.3.1 Uma das bases do gerenciamento eficaz da segurança operacional é um sistema formal para sua supervisão e envolve o monitoramento regular, quando não for contínuo, de todos os aspectos das operações de um PSNA. O monitoramento da segurança demonstra a conformidade com as regras, normas e procedimentos. No entanto, seu valor vai mais além ao proporcionar a validação da eficácia das medidas tomadas e a avaliação permanente do desempenho da segurança.

11.3.2 A frequência do monitoramento da segurança dependerá do impacto e/ou da complexidade da mudança, bem como da profundidade e extensão da análise original. Para o monitoramento adequado da segurança operacional nos PSNA deve ser empregada a combinação dos seguintes métodos:

a) observação das atividades da rotina operacional;

b) avaliação das áreas críticas de segurança operacional;

c) entrevista sobre segurança operacional, tanto de um ponto de vista geral quanto sobre a mudança implementada;

d) acompanhamento sistemático de todos os reportes de problemas de segurança operacional;

e) execução de análises do desempenho da segurança operacional;

f) manutenção de um programa regular de vistorias de segurança operacional; e

g) divulgação dos resultados da segurança operacional a todos os agentes operacionais envolvidos.

11.3.3 O monitoramento da segurança operacional deve ser efetuado em todos os ciclos de evolução da mudança, ou até que seja atenuado o risco e verificada a eficácia das medidas de mitigação. Após a conclusão da mudança, o monitoramento da segurança operacional deve se tornar um procedimento na rotina operacional do PSNA.

11.4 CONTROLE DOS RISCOS RESIDUAIS

11.4.1 O monitoramento do status da implementação das medidas mitigadoras deve ser considerado como uma ferramenta para a atualização da classificação dos riscos residuais e o controle desses riscos deve ser efetuado para todos os ciclos de evolução das medidas mitigadoras, ou até que seja atenuado o risco para um nível aceitável ou, pelo menos, tolerável e verificada a eficácia da mitigação do risco.

11.4.2 Em cada ciclo de evolução das medidas de mitigação, as atenuações devem ser verificadas e, em função do andamento da implementação dessas medidas, deve ser realizada uma classificação do risco residual considerando o status das medidas mitigadoras.

11.4.3 Em alguns casos, é possível que a implementação parcial das medidas de mitigação já atinja um risco residual que pode ser classificado como baixo risco. Excepcionalmente, nesses casos, será permitido prosseguir no desenvolvimento do projeto e na execução da mudança proposta antes da conclusão da implementação de todas as medidas mitigadoras.

11.4.4 Por outro lado, podem existir casos que, mesmo após a conclusão das medidas de mitigação, o risco residual obtido, diferentemente do esperado, seja classificado como alto ou médio risco. Nessa situação, além da reavaliação da efetividade das medidas mitigadoras adotadas, o PSNA deve adotar os seguintes procedimentos:

a) no caso de alto risco, apesar da conclusão da implementação das medidas mitigadoras, a mudança não deve ser executada até que sejam desenvolvidas e aplicadas novas medidas capazes de reduzir o risco residual para um nível aceitável ou, pelo menos, tolerável; e

b) no caso de médio risco, quando era esperado baixo risco, devem ser adotadas novas medidas mitigadoras, até a obtenção do menor risco praticável.

11.4.5 Portanto, a implementação das medidas mitigadoras, isoladamente, não é condição suficientemente válida para o desenvolvimento do projeto e a execução da mudança. Somente a obtenção de um risco residual aceitável ou, pelo menos, tolerável é condição válida para a execução da mudança.

Tabela 12 – Tabela de Monitoramento dos Riscos Residuais

Número do perigo	**Descrição do Perigo:**			
Descrição das medidas mitigadoras	**Classificação do Risco Residual**	**Status da Medida Mitigadora**	**Classificação do Risco Residual em função do Status**	**Data da Classificação**

12 ACEITAÇÃO DOS RISCOS

12.1 CRITÉRIOS PARA ACEITAÇÃO DO RISCO

12.1.1 Aceitação dos riscos é a certificação pelas autoridades apropriadas, de que elas compreendem os riscos associados às mudanças propostas ou a uma operação/atividade em andamento, bem como estão convictas de que as medidas mitigadoras são viáveis e serão implementadas e, portanto, tais riscos podem ser aceitos e as mudanças podem ser implementadas.

12.1.2 A aceitação dos riscos à segurança operacional é um pré-requisito para a implementação de uma mudança proposta e deve estar baseada no risco residual previsto. Nenhuma mudança proposta, onde tenha sido aplicado o gerenciamento do risco, deve ser implementada sem que os riscos associados sejam aceitos pela autoridade apropriada.

12.1.3 A aceitação dos riscos à segurança operacional deve ser formalizada por meio das assinaturas das autoridades que detenham a responsabilidade pela mudança, pelo controle da implementação das medidas mitigadoras e pela supervisão da segurança operacional. Tais assinaturas deverão constar do Documento de Gerenciamento do Risco à Segurança Operacional (DGRSO).

12.1.4 A definição da autoridade para a aceitação do risco à segurança operacional depende da abrangência da mudança, da classificação do risco e do planejamento para implementação das medidas mitigadoras utilizadas para controlar os riscos. Somente as autoridades responsáveis pela implementação da mudança e que, efetivamente, estejam capacitadas e detenham a condição funcional apropriada para gerenciar os riscos, devem ser indicadas para a aceitação dos riscos à segurança operacional.

13 DOCUMENTO DE GERENCIAMENTO DO RISCO À SEGURANÇA OPERACIONAL

13.1 CONSIDERAÇÕES SOBRE O DGRSO

13.1.1 O Documento de Gerenciamento do Risco à Segurança Operacional (DGRSO) deve descrever completamente a análise da segurança para uma mudança proposta e documentar as evidências para verificar se a mudança proposta é aceitável sob o ponto de vista da Segurança Operacional. O DGRSO também deve contribuir para a decisão de implementar uma mudança sob uma perspectiva programática ou de gerenciamento.

13.1.2 Portanto, todas as fases do processo de Gerenciamento do Risco devem ser descritas, documentadas e consubstanciadas por meio do Documento de Gerenciamento do Risco à Segurança Operacional.

13.2 CONTEÚDO DO DGRSO

13.2.1 O DGRSO deve prover detalhes suficientes sobre uma mudança proposta para um sistema atual ou para a introdução de um sistema totalmente novo para prover os Serviços de Navegação Aérea. Deve ser uma fonte única que permita entender a mudança, os riscos associados e as providências mitigadoras tomadas (ou propostas) para reduzir os riscos iniciais, residuais ou subsequentes para um nível aceitável ou, pelo menos, tolerável.

13.2.2 O documento deve conter detalhes suficientes sobre o sistema atual, os objetivos da mudança e o sistema proposto, de modo a permitir a compreensão dos processos adotados para identificar os perigos, classificar os riscos associados e desenvolver as medidas mitigadoras correspondentes.

13.2.3 O planejamento para a execução da Supervisão do Desempenho da Segurança Operacional também deve ser descrito no DGRSO, de forma a garantir a monitoração da eficácia das medidas mitigadoras.

13.2.4 Dessa forma, o Documento de Gerenciamento do Risco à Segurança Operacional deverá conter, no mínimo, os itens descritos a seguir:

a) Descrição da mudança ou do sistema a ser introduzido,

- descrição do sistema atual;
- objetivos da mudança;
- descrição da mudança ou do sistema a ser introduzido;
- interface pertinente e sistemas de apoio requeridos;
- impacto da mudança ou do sistema a ser introduzido; e
- planejamento do gerenciamento do risco;

b) Identificação de perigos e fatores causais,

- descrição da metodologia e ferramentas usadas;
- descrição dos perigos identificados e suas causas;
- cenários e/ou circunstâncias onde eles existirem;
- controles existentes afetados pelo sistema a ser introduzido e/ou mudança proposta; e
- descrição dos efeitos do perigo potencial;

c) Avaliação e mitigação dos riscos associados,

- avaliação dos riscos associados em termos de severidade e probabilidade;
- classificação dos riscos iniciais;
- medidas mitigadoras requeridas;
- avaliação dos riscos residuais;
- monitoramento das medidas de mitigação; e
- estratégia para controle dos riscos residuais;

d) Estratégia para validação e verificação da mudança ou do sistema a ser introduzido,

- metodologia para obtenção de dados para o monitoramento da segurança operacional; e
- metodologia para análise da segurança operacional;

e) Tabela de Síntese de Registro dos Perigos (tabela 10);

f) Tabela de Planejamento para a Implementação das Medidas Mitigadoras (tabela 11);

g) Aceitação dos Riscos,

- avaliação dos riscos residuais previstos; e
- aceitação de cada risco pela autoridade aeronáutica competente;

h) Aprovação do DGRSO pela autoridade competente.

13.3 BENEFÍCIOS DO DGRSO

13.3.1 A organização responsável pela implementação da mudança deve manter toda a documentação relativa ao processo de Gerenciamento do Risco, inclusive o DGRSO, durante todo o ciclo de vida do sistema ou da mudança, pois esse documento fornece uma sequência padronizada para o desenvolvimento do gerenciamento de risco e, ainda:

a) reduz omissões e inconsistências na preparação e condução da análise da segurança operacional;

b) facilita o desenvolvimento da documentação das ações subsequentes;

c) compartilha os dados de risco com os envolvidos com a segurança operacional;

d) fortalece as habilidades do gerenciamento do risco;

e) encoraja uma cultura de segurança operacional positiva;

f) assegura que os dados de segurança operacional sejam monitorados para reduzir riscos;

g) garante que os processos do gerenciamento do risco sejam monitorados;

h) estabelece a compatibilidade entre autoridade e responsabilidade;

i) permite a rastreabilidade do processo; e

j) reduz o reestudo de propostas de mudança similares.

13.3.2 O DGRSO deve ser mantido em arquivo mesmo se não for aprovado ou se a mudança não for implementada, pois os PSNA podem usar essa informação na avaliação de propostas similares de mudança ou como subsídios para os DGRSO de outras propostas de mudança.

13.4 APROVAÇÃO DO DGRSO

13.4.1 A Aprovação do DGRSO é a certificação de que a documentação foi desenvolvida corretamente, de que todos os perigos significativos foram identificados, todos os riscos foram nominados, analisados e avaliados adequadamente, de que as medidas mitigadoras propostas são eficazes, verificáveis e controláveis e que foi elaborado um planejamento apropriado para a implementação destas medidas.

13.5 EMENDAS AO DGRSO

13.5.1 O resultado da análise da segurança é uma parte da informação básica do sistema. O PSNA, objeto da mudança, pode precisar atualizar ou mudar um DGRSO enquanto um projeto ainda está em desenvolvimento. A monitoração da segurança pode indicar que os controles e as medidas de mitigação são menos eficazes do que o originalmente esperado ou que existem perigos adicionais que possam requerer mitigações adicionais. Desse modo, qualquer mudança que possa afetar os perigos supostos ou identificados no DGRSO, ou os riscos avaliados, necessita de uma emenda ao DGRSO.

13.5.2 Além disso, o DGRSO deve incluir um cronograma de avaliação da segurança operacional, a fim de se verificar os resultados das análises prévias e atualizar o documento. Quando for importante para a operacionalidade do sistema ou da mudança, a periodicidade dessas avaliações de segurança pode variar dependendo do tipo, do impacto potencial da segurança e/ou da complexidade da mudança, bem como da profundidade e abrangência da análise original.

14 DISPOSIÇÕES FINAIS

14.1 RECURSOS NECESSÁRIOS

14.1.1 Sem prejuízo do preconizado na legislação vigente, a execução das ações estabelecidas neste Manual será custeada com os recursos próprios de cada Organização.

14.2 CASOS NÃO PREVISTOS

14.2.1 Os casos não previstos neste MCA serão apreciados pelo Diretor-Geral do DECEA, por meio da Assessoria de Segurança Operacional do Espaço Aéreo (ASEGCEA).

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Diretriz para Implementação de Sistemas de Gerenciamento da Segurança Operacional (SGSO) no SISCEAB*: **DCA 63-3**. Rio de Janeiro-RJ, 2011.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Plano de Implementação de Sistemas de Gerenciamento da Segurança Operacional (SGSO) nas Organizações Subordinadas ao DECEA*: **PCA 63-2**. Rio de Janeiro-RJ, 2011.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Gerenciamento do Risco à Segurança Operacional (GRSO) no SISCEAB*: **ICA 63-26**. Rio de Janeiro-RJ, 2010.

ICAO. DOC 9859 *Manual de Gerenciamento da Segurança Operacional (OACI)* - 2ª Edição – 2009

FAA. *Safety Management System Manual – Air Traffic Organization – FAA*, Versão 2.1, Maio de 2008.

Anexo A– Registro de Redução do Escopo do Gerenciamento do Risco à Segurança Operacional (REGRSO)

ORGANIZAÇÃO REGIONAL OU EMPRESA DO PSNA
ÓRGÃO LOCAL DO PSNA
NOME DO PSNA

REGISTRO DE REDUÇÃO DO ESCOPO DO GERENCIAMENTO DO RISCO À SEGURANÇA OPERACIONAL - REGRSO Portaria nº 186/DGCEA, de 18 de novembro de 2013

Designador do PSNA:

Elaborado por:

Assunto: mudança proposta

---

1) Descrição da Mudança: resumo sobre a mudança, incluindo o objetivo e as razões específicas pelas quais as mudanças foram propostas.

2) Justificativa de que a Mudança não está sujeita às condições de GRSO: razões pelas quais não será necessária a realização do Gerenciamento do Risco e descrição dos aspectos que expliquem que a mudança não acarretará riscos à segurança no ANS ou que os riscos são aceitáveis (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

3) Documentação utilizada na Análise de Segurança Preliminar: citar e anexar a documentação utilizada na Análise de Segurança Preliminar.

4) Assinaturas:

Nós, abaixo assinados, asseguramos que a mudança acima descrita NÃO acarreta riscos à segurança no ANS (ou implicará em RISCOS ACEITÁVEIS) (NR) – Portaria nº 186/DGCEA, de 18 de novembro de 2013.

Proponente da mudança:

_____	(a)_____	_____
Organização	Nome e Cargo ou Função	Data

Responsável pela análise preliminar:

_____	(a)_____	_____
Organização	Nome e Cargo ou Função	Data

Aprovado por:

_____	(a)_____	_____
Organização	Nome e Cargo ou Função	Data

ÍNDICE