MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-26

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

2013

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

TECNOLOGIA DA INFORMAÇÃO

ICA 7-26

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

2013

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

PORTARIA DECEA Nº 59/DGCEA, DE 24 DE MAIO DE 2013.

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

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe conferem o art. 195, inciso IV, do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1049/GC3, de 11 de novembro de 2009, e o art. 11, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 369/GC3, de 9 de junho de 2010, resolve:

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

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

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

(Publicado no BCA nº 120, de 26 de junho de 2013.)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

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

1.2 ÂMBITO E GRAU DE SIGILO

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

1.3 ABREVIATURAS

SDTE – Subdepartamento Técnico do DECEA

DECEA – Departamento de Controle do Espaço Aéreo

GRSTI – Gestão de Riscos de Segurança da Informação

OM – Organização Militar

SSSI – Seção de Segurança de Sistemas da Informação

SI – Segurança da Informação

1.4 DEFINIÇÕES

Os conceitos e definições estão listados no Glossário de Segurança da Informação do DECEA (MCA 7-1).

Para efeito desta Instrução, entende-se por:

1.4.1 ATIVO DE INFORMAÇÃO

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

1.4.2 GESTÃO DE RISCOS

Conjunto de atividades coordenadas para identificar e controlar os riscos existentes em uma organização.

2 RESPONSABILIDADES

2.1 SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA

2.1.1 Normatizar e divulgar o processo no âmbito do DECEA.

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

2.1.3 Definir o contexto da gestão de riscos.

2.1.4 Comunicar riscos às partes interessadas.

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

2.1.6 Identificar oportunidades de melhorias no processo.

2.2 CHEFES DOS SUBDEPARTAMENTOS DO DECEA, CHEFES, DIRETORES E COMANDANTES DAS ORGANIZAÇÕES SUBORDINADAS AO DECEA

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

2.2.2 Decidir sobre a aceitação de riscos.

2.3 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO

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

2.3.2 Identificar os riscos.

2.3.3 Analisar e avaliar os riscos.

2.3.4 Comunicar os riscos ao proprietário de ativos de informação.

2.3.5 Tratar os riscos mediante autorização do proprietário de ativos de informação.

2.3.6 Monitorar os riscos aceitos.

2.3.7 Apresentar registros do processo de gestão de riscos ao SDTE.

2.4 PROPRIETÁRIO DOS ATIVOS DE INFORMAÇÃO

2.4.1 Revisar os resultados dos riscos identificados.

2.4.2 Apoiar na comunicação de riscos às partes interessadas.

2.4.3 Apoiar no tratamento dos riscos identificados.

2.4.4 Aceitar os riscos.

3 PROCESSO DE GESTÃO DE RISCOS

3.1 GESTÃO DE RISCOS

3.1.1 De acordo com o item 4.1.4, letra "g", nº 12, do Plano Diretor de Segurança da Informação do Departamento de Controle do Espaço Aéreo (PCA 7-11), está prevista a estruturação e a definição da respectiva metodologia para tratar a gestão de riscos de segurança da informação com o objetivo de desenvolver procedimentos de análise e avaliação de riscos, de atender aos requisitos legais, regulatórios e de segurança da informação e de desenvolver critérios para o tratamento e aceitação de riscos. Assim, o DECEA e OM subordinadas devem se estruturar para promover atividades de gestão de riscos de segurança da informação, com vistas ao levantamento do impacto e probabilidades de ocorrência dos referidos riscos nos ativos de informação, bem como, identificar ameaças associadas às vulnerabilidades destes ativos, medir os níveis de risco para selecionar os controles necessários ao seu tratamento.

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

3.2 VISÃO GERAL DO PROCESSO DE GESTÃO DE RISCOS

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

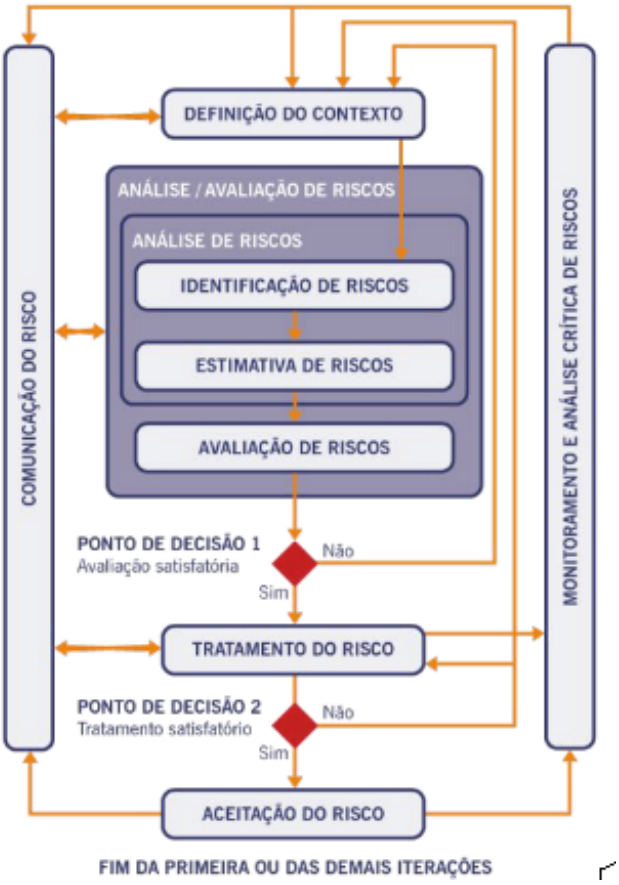

Figura 1 - Fonte ABNT ISO/IEC 27005:2008

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

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

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

Figura 2 - Visão Geral do Processo de Gestão de Riscos

3.3 SUBPROCESSO "DEFINIR CONTEXTO"

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

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

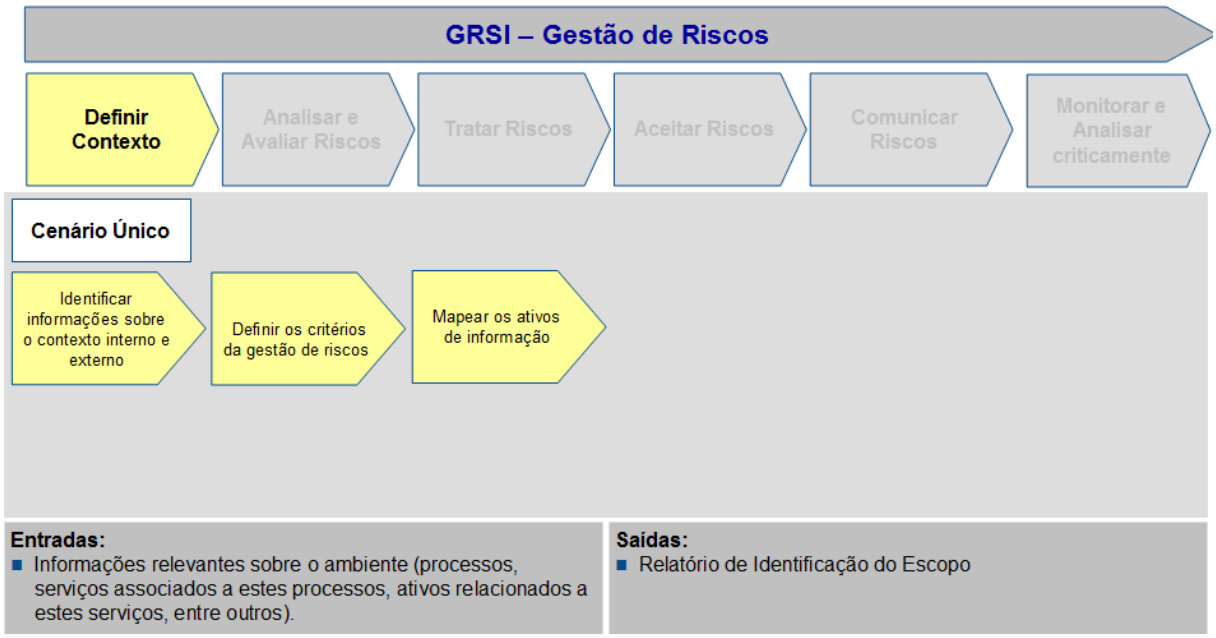

Figura 3 - Subprocesso "Definir Contexto"

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

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

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

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

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

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

3.3.9 As informações necessárias em relação à identificação dos ativos são: nome do ativo, tipo do ativo (tecnologia, pessoa, ambiente e processo) e importância do ativo quanto ao grau de "Relevância" em cada um dos critérios de segurança da informação: Confidencialidade (representado por "C"), Integridade (representado por "I") e Disponibilidade (representado por "D") e os responsáveis.

3.4 SUBPROCESSO "ANALISAR E AVALIAR RISCOS"

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

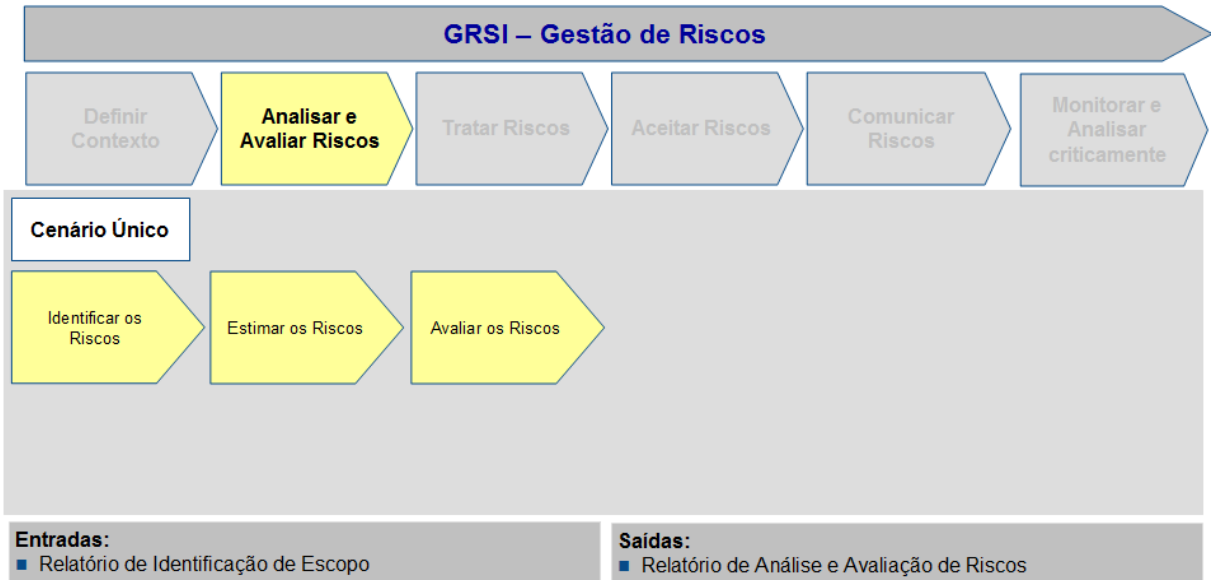

Figura 4 - Subprocesso para Analisar e Avaliar Riscos

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

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

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

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

3.4.5 Após a realização da etapa de identificação de riscos, é necessário atribuir valores para os ativos, vulnerabilidades e consequências. Assim, será possível listar os riscos em ordem de prioridade, para tratá-los de acordo com sua urgência ou criticidade. Esses valores seguem os mesmos critérios definidos na fase de definição do contexto. Essas informações deverão ser transcritas no documento GRSTI02 – Análise e Avaliação de Riscos.

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

3.5 SUBPROCESSO "TRATAR RISCOS"

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

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

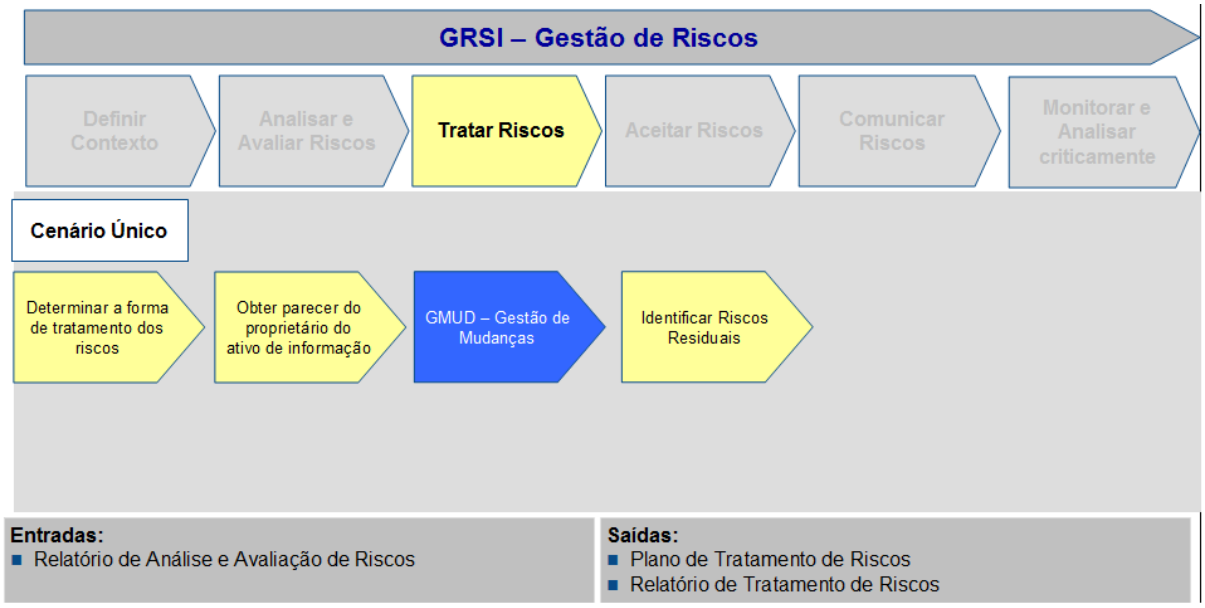

Figura 5 - Subprocesso para Tratar Riscos

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

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

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

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

3.5.7 Posteriormente ao tratamento, deverá ser feita uma análise para identificar os riscos residuais eventualmente ainda existentes a fim de identificar se deverão ou não ser

gerenciados. Essas informações deverão ser transcritas no documento GRSTI03 – Plano de Tratamento de Riscos, que se encontra disponível no Anexo C.

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

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

3.6 SUBPROCESSO "ACEITAR RISCOS"

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

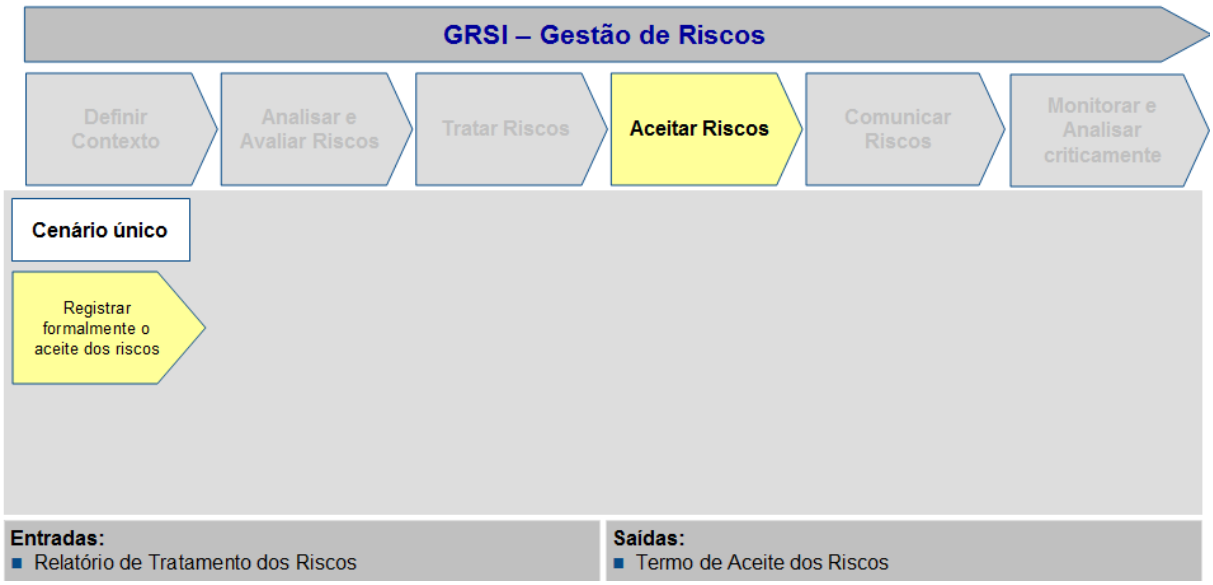

Figura 6 - Subprocesso para Aceitar Riscos

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

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

3.7 SUBPROCESSO "COMUNICAR OS RISCOS"

3.7.1 A gestão de riscos pode ter diversas partes interessadas. Essas partes devem ser identificadas e seus papéis e responsabilidades delimitados. Os riscos serão comunicados para

os seus respectivos responsáveis. Assim, o subprocesso de comunicação de riscos se encarrega de proporcionar essa comunicação, sendo composta de duas etapas: a primeira relativa à identificação das partes interessadas e a outra efetivamente associada à comunicação, ambas ilustradas na figura 7.

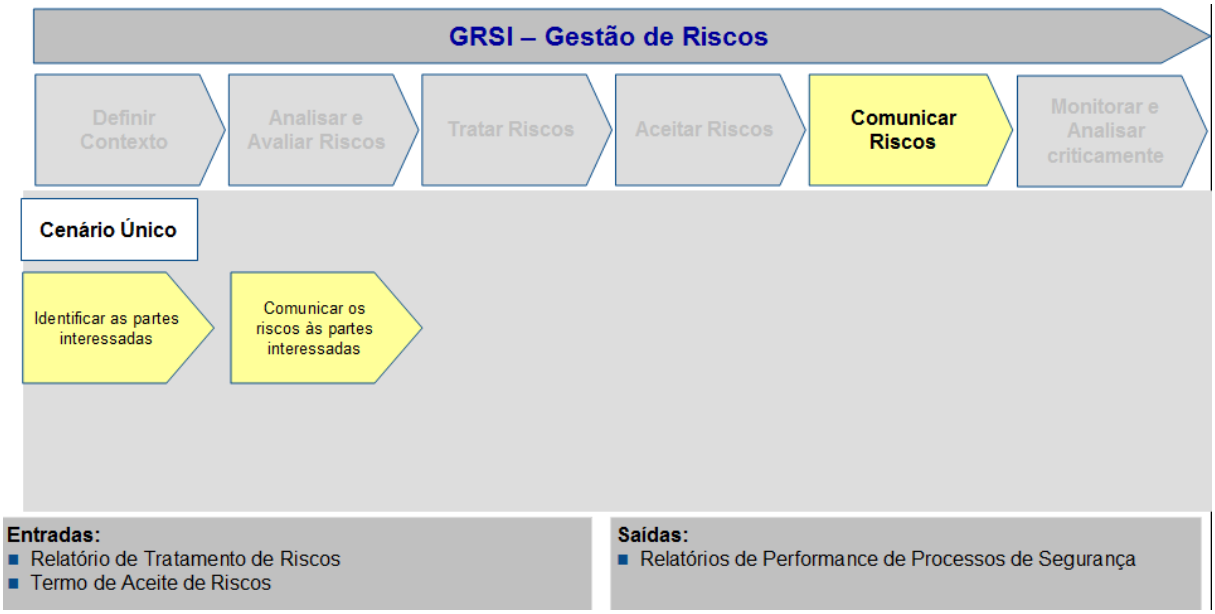

Figura 7 - Subprocesso "Comunicar os Riscos"

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

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

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

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

- A existência da ameaça, vulnerabilidade e risco;
- A natureza e forma de ação;
- A estimativa de probabilidade;
- Sua severidade e consequências possíveis; e
- Tratamento e aceitação de riscos.

3.8 SUBPROCESSO "MONITORAR E ANALISAR CRITICAMENTE"

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

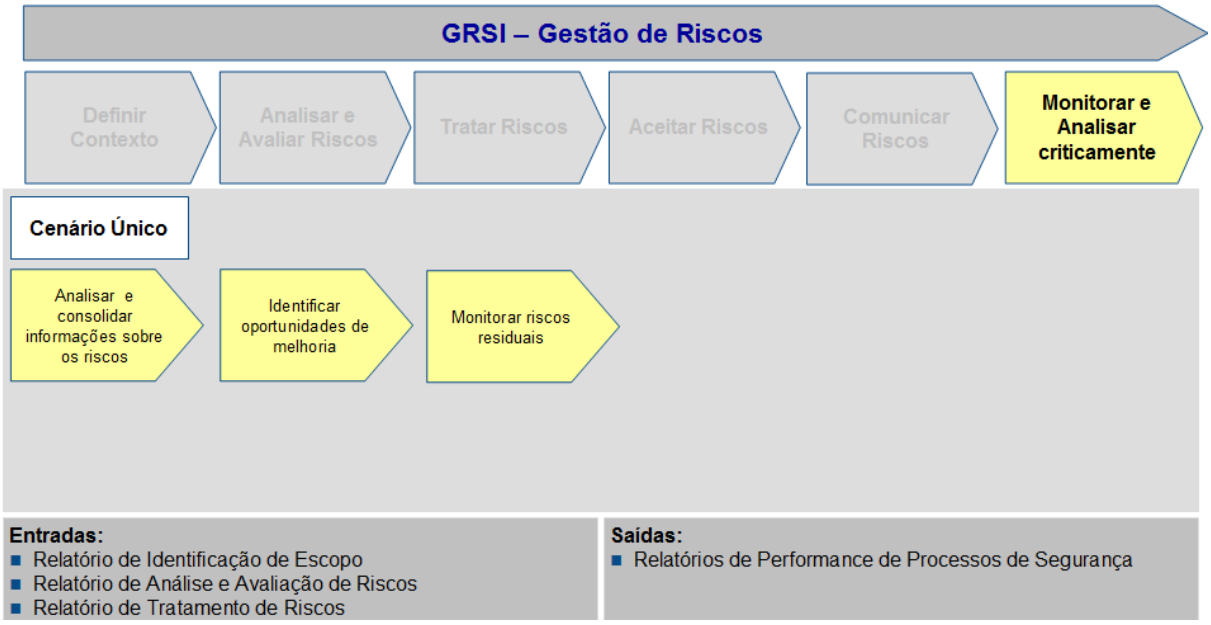

Figura 8 - Subprocesso para Monitorar e Analisar Criticamente

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

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

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

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

3.9 CONTROLE E MATURIDADE DO PROCESSO

3.9.1 MEDIÇÃO DO NÍVEL DE MATURIDADE ATUAL DO PROCESSO

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

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

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

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

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

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

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

3.9.1.2 A tabela abaixo apresenta as metas para a evolução dos níveis de maturidade e seus respectivos prazos:

Nível de Maturidade	Metas	Prazos
2 – Repetível e Intuitivo	• Possuir uma normativa interna do DECEA para gestão de riscos de segurança da informação • Obter aprovação da Política de Gestão de Riscos • Iniciar a implantação e testes do processo em pelo menos 50% das Organizações Subordinadas ao DECEA	• Até dezembro de 2013
3 – Processo Definido	• Implantar o processo em todas as Organizações Subordinadas ao DECEA • Capacitar todos os chefes das seções de segurança da informação	• Até julho de 2014
4 – Gerenciado e Mensurável	• Criar um painel para acompanhamento, através de indicadores gerenciais do processo, a fim de garantir a tomada de decisão pela Direção do DECEA	• Até dezembro de 2014
5 – Otimizado	• Realizar uma reunião semestral de análise crítica para melhoria contínua do processo • Possuir sistema informatizado para emissão de relatórios automatizados	• Até dezembro de 2015

3.9.2 ACOMPANHAMENTO DO PROCESSO POR INDICADORES

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

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

3.9.3 FATORES CRÍTICOS DE SUCESSO

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

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

b) garantir cumprimento das responsabilidades atribuídas no processo;

c) gerenciamento de riscos integrado aos processos de negócio;

d) garantir cumprimento dos procedimentos relacionados ao processo;

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

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

4 DISPOSIÇÕES FINAIS

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

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

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

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27005. *Tecnologia da informação: Técnicas de segurança: Gestão de riscos de segurança da informação*. Rio de Janeiro, RJ, 2008.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo*: **MCA 7-1**. Rio de Janeiro, RJ, 2012.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Plano Diretor de Segurança da Informação do DECEA*: **PCA 7-11**, Rio de Janeiro, RJ, 2010.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Política de Gestão de Riscos de Segurança e Tecnologia da Informação do DECEA*: **DCA 7-3**. Rio de Janeiro, RJ, 2012.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Política de Segurança da Informação do DECEA*: **DCA 7-2**. Rio de Janeiro, RJ, 2010.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Preceitos de Segurança da Informação do DECEA*: **ICA 7-19**, Rio de Janeiro, RJ, 2012.

BRASIL. Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1).

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

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

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

1 Definição do contexto interno e externo

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

2 Definição dos critérios da gestão de riscos

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

3 Documentar as partes interessadas

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

4 Mapeamento dos ativos de informação

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

Anexo B - Registro GRSTI02 – Análise e Avaliação de Riscos

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

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

1 Identificação das ameaças e fontes

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

2 Identificação dos controles de segurança

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

3 Identificação dos Riscos

Ativo	Ameaça	Vulnerabilidade	Consequências

4 Estimativa dos Riscos

Ativo	Risco	Estimativa				Valor Risco	Nível
		C	I	D	P		

5 Avaliação dos Riscos

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

Anexo C - Registro GRSTI03 – Plano de Tratamento dos Riscos

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

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

1 Matriz de tratamento dos riscos

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

Anexo D - Registro GRSTI04 – Termo de Aceite dos Riscos

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

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

1 Registro de Aceitação dos Riscos

Ativo	*Risco*	*Justificativa*

Aprovado por:	
Comentários:	

Anexo E - Registro GRSTI05 – Monitoramento dos Riscos Residuais

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

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

1 Registro de Alteração de Risco Residual

Risco:

Ativo:

Valor Alterado:

Detalhes sobre o Novo Risco:

Detalhes da Ação sobre o Novo Risco:

Data da Identificação:

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

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

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

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

2	**ANÁLISE DOS INDICADORES**

3	**AÇÕES DE MELHORIA CONTÍNUA**