

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



TECNOLOGIA DA INFORMAÇÃO

DCA 7-3

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

2012

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



TECNOLOGIA DA INFORMAÇÃO

DCA 7-3

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

2012



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

PORTARIA DECEA Nº 67/DGCEA, DE 25 DE MAIO DE 2012.

Aprova a edição da Diretriz que disciplina a Política 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 confere 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. 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 da DCA 7-3 “Política de Gestão de Riscos de Segurança e Tecnologia da Informação do Departamento de Controle do Espaço Aéreo”, que com esta baixa.

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

(a) Ten Brig Ar MARCO AURÉLIO GONÇALVES MENDES
Diretor-Geral do DECEA

(Publicado no BCA nº 115, de 18 de junho de 2012.)

SUMÁRIO

1	DISPOSIÇÕES PRELIMINARES	7
1.1	<u>FINALIDADE</u>	7
1.2	<u>OBJETIVO</u>	7
1.3	<u>CONCEITUAÇÃO</u>	7
2	FUNDAMENTOS	8
3	ÂMBITO E GRAU DE SIGILO	9
4	RESPONSABILIDADES	10
4.1	<u>DGCEA – DIREÇÃO-GERAL DO DECEA</u>	10
4.2	<u>ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO</u>	10
4.3	<u>CHEFES DOS SUBDEPARTAMENTOS, CHEFES, DIRETORES E COMANDANTES DAS ORGANIZAÇÕES SUBORDINADAS AO DECEA</u>	11
4.4	<u>SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO (ORGANIZAÇÕES SUBORDINADAS AO DECEA)</u>	11
4.5	<u>USUÁRIOS DAS INFORMAÇÕES</u>	12
5	DIRETRIZES DA POLÍTICA DE GESTÃO DE RISCOS DE SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO	13
6	DIVULGAÇÃO	15
7	PROCESSO DE ATUALIZAÇÃO	16
7.1	<u>REVISÃO E ATUALIZAÇÃO</u>	16
8	PENALIDADES	17
9	DISPOSIÇÕES FINAIS	18

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Apresentar e estabelecer princípios, diretrizes e responsabilidades relacionados à Gestão de Riscos de Segurança e Tecnologia da Informação para o Departamento de Controle do Espaço Aéreo (DECEA) e suas Organizações Subordinadas.

1.2 OBJETIVO

1.2.1 Orientar o planejamento, a execução e a manutenção do processo de Gestão de Riscos de Segurança e Tecnologia da Informação segundo a metodologia preconizada pela Norma ABNT NBR ISO/IEC 27005 – Gestão de Riscos de Segurança e Tecnologia da Informação, de 2008, associando, dessa forma, o processo de Gestão de Riscos à tomada de decisões estratégicas da Organização, em conformidade com as boas práticas recomendadas pelos órgãos de controle da Administração Pública Federal.

1.2.2 Definir responsabilidades para a Gestão de Riscos de Segurança e Tecnologia da Informação, bem como para a atualização da documentação pertinente.

1.2.3 Fomentar, ao longo de toda a cadeia hierárquica, a obtenção de atitude favorável no tocante à Gestão de Riscos de Segurança e Tecnologia da Informação, bem como incrementar a conscientização a respeito da importância do assunto.

1.3 CONCEITUAÇÃO

Os conceitos dos termos e expressões utilizados neste documento constam do Glossário da Aeronáutica (MCA 10-4, de 30 de janeiro de 2001), do Manual de Abreviaturas, Siglas e Símbolos da Aeronáutica (MCA 10-3, de 22 de abril de 2003) e do Glossário de Segurança da Informação do DECEA de 2012 (MCA 7-1, de 30 de março de 2012).

2 FUNDAMENTOS

- a) DCA 14-8 Política de Segurança da Informação do Comando da Aeronáutica, de 2006;
- b) DCA 14-7 Política do Comando da Aeronáutica para a Tecnologia da Informação, de 2004;
- c) PCA 7-11 Plano Diretor de Segurança da Informação do Departamento de Controle do Espaço Aéreo, de 2010;
- d) ICA 7-19 Preceitos de Segurança da Informação do Departamento de Controle do Espaço Aéreo, de 2012;
- e) Instrução Normativa GSI/PR nº 1, de 2008;
- f) Norma Complementar 03/IN01/DSIC/GSIPR, de 30 de junho de 2009;
- g) ABNT NBR ISO/IEC 27001 Sistema de Gestão de Segurança da Informação, de 2006;
- h) ABNT NBR ISO/IEC 27005 Gestão de Riscos de Segurança e Tecnologia da Informação, de 2008; e
- i) ABNT ISO/IEC GUIA 73: Gestão de Riscos – Vocabulário, de 2009.

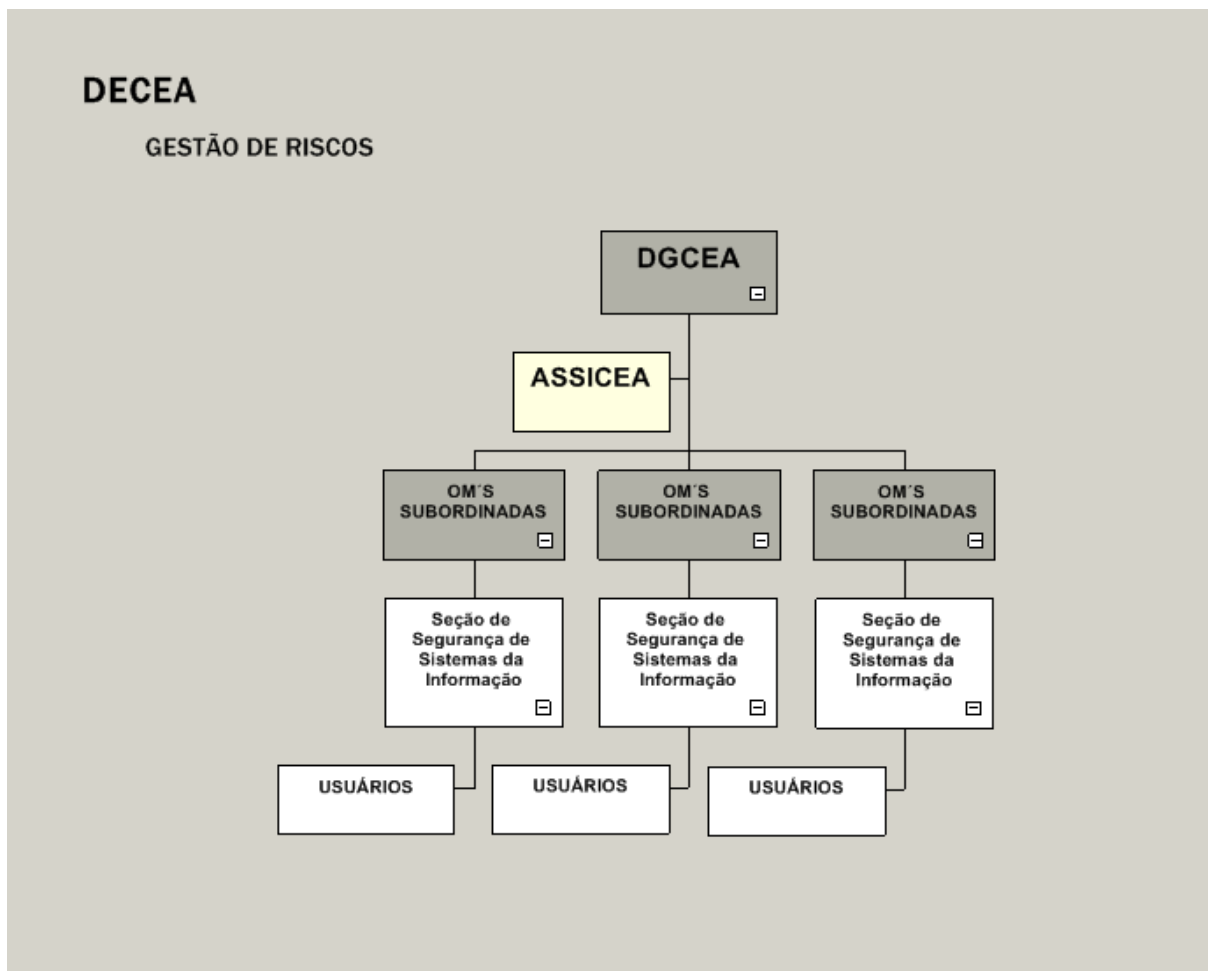
3 ÂMBITO E GRAU DE SIGILO

3.1 Esta Política de Gestão de Riscos de Segurança e Tecnologia da Informação se aplica às atividades de todos os servidores civis ou militares, prestadores de serviços e fornecedores que venham a desempenhar atividades no âmbito do DECEA e das suas Organizações Subordinadas.

3.2 Este documento é classificado como Ostensivo.

4 RESPONSABILIDADES

A gestão da Segurança da Informação está estruturada de forma sistêmica, sendo o Órgão Central representado pela Assessoria de Segurança de Sistemas da Informação do Controle do Espaço Aéreo (ASSICEA), diretamente subordinada ao Diretor-Geral do DECEA, e os elos sistêmicos representados pelas Seções de Segurança de Sistemas da Informação existentes em cada Regional. A figura a seguir representa esta estrutura sistêmica:



4.1 DGCEA – DIREÇÃO-GERAL DO DECEA

4.1.1 Prover orientação e apoio para o cumprimento da Política de Gestão de Riscos de Segurança e Tecnologia da Informação do DECEA.

4.1.2 Deliberar quanto a decisões relacionadas à Gestão de Riscos de Segurança e Tecnologia da Informação, incluindo sanções na ocorrência de violação desta Política.

4.2 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

4.2.1 Revisar, divulgar e fazer cumprir esta Política no âmbito do DECEA e Organizações Subordinadas.

4.2.2 Coordenar, orientar, avaliar e implantar as atividades e projetos relativos à Gestão de Riscos de Segurança e Tecnologia da Informação no DECEA, promovendo ações de interesse deste Departamento, programas educacionais e de conscientização.

4.2.3 Estabelecer e manter atualizadas normativas gerenciais e técnicas e outros documentos afins relativos à Gestão de Risco de Segurança e Tecnologia da Informação no DECEA, em articulação com as partes interessadas.

4.2.4 Auxiliar na aquisição de ferramentas informatizadas que viabilizem a Gestão de Riscos de Segurança e Tecnologia da Informação.

4.2.5 Realizar auditorias periódicas para avaliar os níveis de conformidade desta Política e dos demais documentos normativos de Gestão de Riscos da Segurança e Tecnologia da Informação no âmbito do DECEA e Organizações Subordinadas.

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

4.3.1 Garantir o cumprimento desta Política, bem como os procedimentos a ela relacionados, por parte dos usuários sob sua responsabilidade.

4.3.2 Prover infraestrutura necessária para implantar a Gestão de Riscos de Segurança e Tecnologia da Informação em sua Organização Militar.

4.3.3 Aplicar ações corretivas e disciplinares nos casos de quebra da segurança da informação ocasionadas por riscos não identificados ou riscos que não foram tratados por usuários sob sua responsabilidade.

4.4 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO (Organizações Subordinadas ao DECEA)

4.4.1 Implantar as diretrizes de Gestão de Riscos de Segurança e Tecnologia da Informação indicadas pela ASSICEA.

4.4.2 Manter atualizado o inventário de ativos de informação sob sua responsabilidade.

4.4.3 Realizar a análise e avaliação de riscos sob os ativos de informação de sua administração.

4.4.4 Realizar o tratamento dos riscos sob a sua responsabilidade.

4.4.5 Contribuir para o processo de melhoria contínua da Gestão de Riscos de Segurança e Tecnologia da Informação monitorando e realizando a análise crítica.

4.4.6 Comunicar os riscos às partes interessadas que estejam sob a sua responsabilidade.

4.4.7 Reportar à ASSICEA situações que comprometam a Gestão de Riscos de Segurança e Tecnologia da Informação.

4.4.8 Encaminhar à ASSICEA os relatórios relativos à Gestão de Riscos de Segurança e Tecnologia da Informação.

4.5 USUÁRIOS DAS INFORMAÇÕES

4.5.1 Cumprir a Política de Gestão de Riscos de Segurança e Tecnologia da Informação do DECEA e suas normativas gerenciais e técnicas.

4.5.2 Reportar ao chefe imediato situações de riscos que comprometam a segurança das informações do DECEA e Organizações Subordinadas.

5 DIRETRIZES DA POLÍTICA DE GESTÃO DE RISCOS DE SEGURANÇA E TECNOLOGIA DA INFORMAÇÃO

5.1 As diretrizes descritas nesta Política estão em conformidade com a ABNT NBR ISO/IEC 27005:2008.

5.2 O processo de Gestão de Riscos de Tecnologia e Segurança da Informação deve ser contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação – (SGSI).

5.3 O processo de Gestão de Riscos de Tecnologia e Segurança da Informação deve estar alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na ABNT NBR ISO/IEC 27001:2006.

5.4 Neste capítulo estão descritas as diretrizes da Gestão de Riscos de Segurança e Tecnologia da Informação, que são as declarações de alto nível sobre como esse processo será utilizado nas atividades de trabalho do Departamento de Controle do Espaço Aéreo e suas Organizações Subordinadas.

5.4.1 Todos os riscos de segurança da informação devem ser identificados e tratados.

5.4.2 Todos os usuários são responsáveis pela identificação de riscos e devem prestar contas por gerenciar os riscos de suas atividades.

5.4.3 O DECEA irá difundir um sistema de cultura de risco, no qual procedimentos e sistemas de controle serão disseminados em todas as áreas administrativas e operacionais, com total comprometimento do Alto-Comando do DECEA.

5.4.4 Um sistema amplo de divulgação deve permear todo o DECEA e suas Organizações Subordinadas de forma clara e objetiva.

5.4.5 Uma análise bem estruturada que avalie, identifique e reconheça o comprometimento de todos os usuários com o gerenciamento de riscos de segurança e tecnologia da informação é fundamental para o sucesso dessa iniciativa.

5.4.6 As decisões estratégicas de segurança da informação serão baseadas nos níveis de exposição aos riscos.

5.4.7 A adoção das boas práticas de Governança de Segurança da Informação é uma forma sistemática, estruturada e oportuna de mitigar os riscos de má gestão das informações com o objetivo de alcançar e manter a transparência, a qualidade e a segurança das informações do DECEA.

5.4.8 A adoção de uma linguagem padrão de Gestão de Riscos de Segurança e Tecnologia da Informação é essencial ao processo, possibilitando melhor entendimento entre as partes e um processo livre de interferências.

5.4.9 A utilização de um modelo (ABNT NBR ISO/IEC 27005:2008) baseado em padrões e metodologias formalizados, reconhecidos internacionalmente, é capaz de se adequar às estratégias, iniciativas e estrutura organizacional do DECEA, além de atender às exigências dos órgãos reguladores e fiscalizadores da administração pública federal.

5.4.10 As responsabilidades dos usuários perante a Gestão de Riscos de Segurança e Tecnologia da Informação estão descritas nesta Política.

5.4.11 Uma infraestrutura comum de tecnologia da informação, processos e pessoas será implementada para a Gestão de Riscos de Segurança e Tecnologia da Informação, estabelecendo mecanismos de forma clara e objetiva.

5.4.12 A Gestão de Riscos de Segurança e Tecnologia da Informação envolve todas as práticas e processos organizacionais do DECEA e suas Organizações Subordinadas, de forma a garantir a identificação de eventos de riscos inerentes a todas as áreas de atividades e suporte em suas Organizações.

5.4.13 Em conformidade com a ICA 7-19 “Preceitos de Segurança da Informação do Controle do Espaço Aéreo”, a Gestão de Riscos de Segurança e Tecnologia da Informação deve contemplar as seguintes atividades:

5.4.13.1 Definição do contexto: definir o contexto interno e externo, os critérios utilizados para análise, avaliação, tratamento e aceitação dos riscos e o mapeamento dos ativos de informação do escopo definido.

5.4.13.2 Análise e avaliação de riscos: produzir dados que irão auxiliar na decisão sobre quais riscos serão tratados e as formas de tratamento com melhor eficiência de custos.

5.4.13.3 Tratamento dos riscos: relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos na definição de escopo.

5.4.13.4 Aceitação dos riscos: verificar os resultados do processo executado de gestão de riscos considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.

5.4.13.5 Monitoramento e análise crítica de riscos: detectar as possíveis falhas nos resultados, monitorar os riscos, os controles de segurança da informação e verificar a eficácia do processo de Gestão de Riscos.

5.4.13.6 Comunicação dos riscos: a gestão de riscos pode ter diversas partes interessadas. Estas partes devem ser identificadas e seus papéis e responsabilidades, delimitados. Os riscos devem ser comunicados aos seus respectivos responsáveis.

6 DIVULGAÇÃO

Esta Política e suas atualizações deverão ser divulgadas a todos os servidores militares e civis, terceiros e fornecedores que habitualmente trabalham no Departamento de Controle do Espaço Aéreo e suas Organizações Subordinadas.

7 PROCESSO DE ATUALIZAÇÃO

7.1 REVISÃO E ATUALIZAÇÃO

7.1.1 A Política de Gestão de Riscos de Segurança e Tecnologia da Informação deve ser revisada e atualizada periodicamente, sempre que forem observadas novas ameaças e vulnerabilidades, mudanças organizacionais e necessidades de atendimento a requisitos legais e regulatórios.

7.1.2 Esta Política de Gestão de Riscos de Segurança e Tecnologia da Informação 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.

8 PENALIDADES

Nos casos em que houver violação desta Política, sanções poderão ser adotadas pelos respectivos Diretores, Chefes ou Comandantes de Organizações Militares.

9 DISPOSIÇÕES FINAIS

Os casos não previstos nesta Diretriz serão submetidos à apreciação do Diretor-Geral do Departamento de Controle do Espaço Aéreo.