MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

DCA 7-3

DIRETRIZ DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2022

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

TECNOLOGIA DA INFORMAÇÃO

DCA 7-3

DIRETRIZ DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2022

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

PORTARIA DECEA Nº 142/SNOT, DE 16 DE ABRIL DE 2022.

Aprova a reedição da Diretriz que dispõe sobre a Gestão de Riscos de Segurança da Informação do Departamento de Controle do Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, de conformidade com o previsto no art. 19, inciso I, Anexo I, da Estrutura Regimental do Comando da Aeronáutica, aprovada pelo Decreto nº 6.834, de 30 de abril de 2009, de acordo com o art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 2.030/GC3, de 22 de novembro de 2019, resolve:

Art. 1º Aprovar a reedição da DCA 7-3 "Diretriz de Gestão de Riscos de Segurança da Informação do Departamento de Controle do Espaço Aéreo", que com esta baixa.

Art. 2º Revogar a Portaria DECEA nº67/DGCEA, de 25 de maio de 2012, publicada no Boletim do Comando da Aeronáutica nº 115, de 18 de junho de 2012.

Art. 2º Esta Portaria entra em vigor em 2 de maio de 2022.

(a)Ten Brig Ar JOÃO TADEU FIORENTINI
Diretor-Geral do DECEA

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Apresentar e estabelecer princípios, diretrizes e responsabilidades relacionados à Gestão de Riscos de Segurança 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 da Informação segundo a metodologia preconizada pela Norma ABNT NBR ISO/IEC 27005 – Gestão de Riscos de Segurança da Informação, de 2019, associando, dessa forma, o processo de Gestão de Riscos à tomada de decisões 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 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 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 (MCA 7-1, de 30 de março de 2012).

2 FUNDAMENTOS

a) PCA 7-11 “Plano Diretor de Segurança da Informação do Departamento de Controle do Espaço Aéreo”, de 2010;

b) Instrução Normativa GSI/PR nº 1, de 2020;

c) Instrução Normativa GSI/PR nº 3, de 2021;

d) ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação, de 2013;

e) ABNT NBR ISO/IEC 27005 – Gestão de Riscos de Segurança da Informação, de 2019; e

f) ABNT ISO/IEC GUIA 73 – Gestão de Riscos – Vocabulário, de 2009.

3 ÂMBITO E GRAU DE SIGILO

3.1 Esta Diretriz de Gestão de Riscos de Segurança 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.

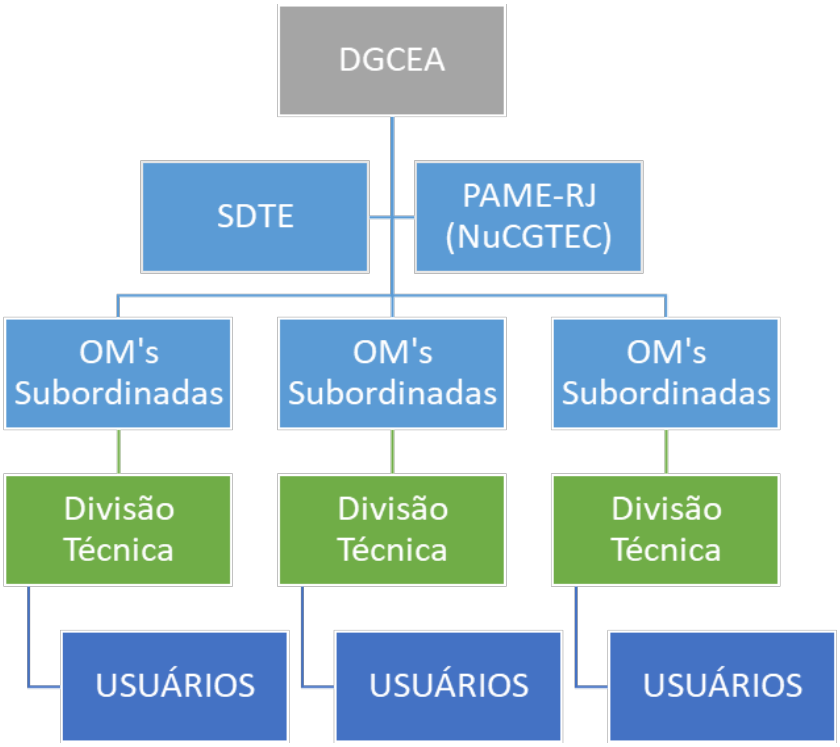
3.2 Este documento é classificado como ostensivo.

4 RESPONSABILIDADES

A Gestão da Segurança da Informação está estruturada de forma sistêmica, sendo o Órgão Central representado pelo Subdepartamento Técnico (SDTE), diretamente subordinado ao Diretor-Geral do DECEA, e os elos sistêmicos representados pelas Divisões Técnicas existentes em cada Regional. A figura a seguir representa essa estrutura sistêmica.

DECEA

GESTÃO DE RISCOS



4.1 DGCEA – DIREÇÃO-GERAL DO DECEA

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

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

4.2 SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA

4.2.1 Revisar, divulgar e fazer cumprir esta Diretriz no âmbito do DECEA e de suas Organizações Subordinadas.

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

4.2.3 Estabelecer e manter atualizadas normativas gerenciais e técnicas e outros documentos afins relativos à Gestão de Riscos de Segurança 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 da Informação.

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

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

4.3.1 Garantir o cumprimento desta Diretriz, 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 da Informação nas diversas Organizações Militares.

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.

4.3.4 Ao PAME-RJ (NuCGTEC – Núcleo do Centro de Gerenciamento Técnico) caberá o monitoramento da infraestrutura sujeita a vulnerabilidades, a coordenação junto às OM subordinadas da avaliação e aceitação dos riscos e a gerência geral do serviço.

4.4 DT – DIVISÕES TÉCNICAS (ORGANIZAÇÕES SUBORDINADAS AO DECEA)

4.4.1 Implantar as diretrizes de Gestão de Riscos de Segurança da Informação indicadas pelo SDTE.

4.4.2 Manter atualizado o inventário de ativos de informação sob sua responsabilidade, em coordenação com o PAME-RJ (NuCGTEC).

4.4.3 Realizar a análise e avaliação de riscos sob os ativos de informação de sua administração e informar ao PAME-RJ (NuCGTEC).

4.4.4 Realizar o tratamento dos riscos sob a sua responsabilidade, em coordenação com o PAME-RJ (NuCGTEC).

4.4.5 Contribuir para o processo de melhoria contínua da Gestão de Riscos de Segurança 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 ao SDTE situações que comprometam a Gestão de Riscos de Segurança da Informação.

4.4.8 Encaminhar ao SDTE os relatórios relativos à Gestão de Riscos de Segurança da Informação, elaborados de acordo com as ferramentas de gestão de riscos disponíveis e em coordenação com o PAME-RJ (NuCGTEC).

4.5 USUÁRIOS DAS INFORMAÇÕES

4.5.1 Cumprir a Diretriz de Gestão de Riscos de Segurança 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 de suas Organizações Subordinadas.

5 DIRETRIZES DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

5.1 As diretrizes de Gestão de Riscos de Segurança da Informação estão em conformidade com a ABNT NBR ISO/IEC 27001:2013 e a ABNT NBR ISO/IEC 27005:2019.

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

5.3 Neste capítulo estão descritas as diretrizes da Gestão de Riscos de Segurança 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 de suas Organizações Subordinadas.

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

5.3.2 O processo de identificação e avaliação dos Riscos de Segurança da Informação deve guardar conformidade com o processo de gerenciamento de risco da Segurança Operacional, assim como a priorização dos riscos de SI deve priorizar os riscos com maior impacto operacional.

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

5.3.4 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.

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

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

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

5.3.8 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.

5.3.9 A adoção de uma linguagem padrão de Gestão de Riscos de Segurança da Informação é essencial ao processo, uma vez que possibilita melhor entendimento entre as partes e um processo livre de interferências.

5.3.10 A utilização de um modelo (ABNT NBR ISO/IEC 27005:2019) baseado em padrões e metodologias formalizados, reconhecidos internacionalmente, é capaz de se adequar às diretrizes, iniciativas e estrutura organizacional do DECEA, além de atender às exigências dos órgãos reguladores e fiscalizadores da administração pública federal.

5.3.11 As responsabilidades dos usuários perante a Gestão de Riscos de Segurança da Informação estão descritas nesta Diretriz.

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

5.3.13 O DECEA será responsável pela coordenação e integração, junto às OM da FAB, do serviço de proteção de perímetro das redes da FAB, em coordenação estreita com o COMGAP (DTI).

5.3.14 A Gestão de Riscos de Segurança da Informação envolve todas as práticas e processos organizacionais do DECEA e de 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.

5.3.15 Em conformidade com a ABNT NBR ISO/IEC 27005:2019, a Gestão de Riscos de Segurança da Informação deve contemplar as seguintes atividades:

a) 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;

b) 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;

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

d) 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;

e) 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; e

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

6 DIVULGAÇÃO

Esta Diretriz 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 Diretriz de Gestão de Riscos de Segurança 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 Diretriz de Gestão de Riscos de Segurança da Informação deverá estar em conformidade com as Diretrizes da DTI – Órgão Central do Sistema de Tecnologia da Informação 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 Diretriz, 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.