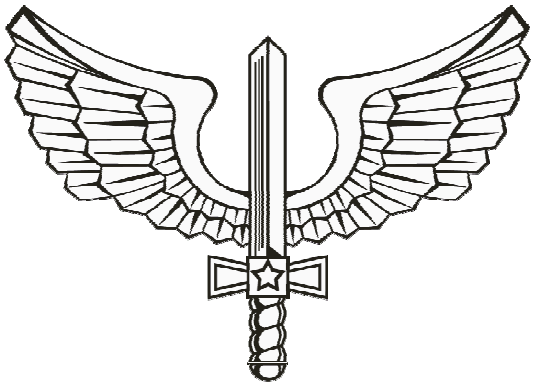
MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA



TECNOLOGIA DA INFORMAÇÃO

DCA 7-2

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2010

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

TECNOLOGIA DA INFORMAÇÃO

DCA 7-2

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2010

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

PORTARIA DECEA Nº 147/DGCEA, DE 19 DE NOVEMBRO DE 2010.

Aprova a edição da Diretriz do Comando da Aeronáutica que disciplina a Política de Segurança 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 7-2 "Política de Segurança 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 RAMON BORGES CARDOSO
Diretor-Geral do DECEA

(Publicado no BCA nº 219, de 26 de novembro de 2010.)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Apresentar a Política de Segurança da Informação para o Departamento de Controle do Espaço Aéreo e Organizações Subordinadas.

1.2 OBJETIVO

1.2.1 Orientar o planejamento e a execução das ações relacionadas à Segurança da Informação.

1.2.2 Definir responsabilidades para o planejamento, execução, manutenção e controle das atividades relativas à 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 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).

1.3.1 PROPRIETÁRIO DAS INFORMAÇÕES

É o responsável pela autorização de acesso às informações, considerando as normas vigentes no DECEA.

1.3.2 CUSTODIANTE

Usuário responsável pela guarda adequada da informação, que cuida do ativo onde está armazenada a informação no dia-a-dia.

1.3.3 USUÁRIO DAS INFORMAÇÕES

Entende-se como usuário das informações, qualquer indivíduo com acesso às informações originadas no DECEA e em suas Organizações Subordinadas.

2 FUNDAMENTOS

a) DCA 351-1 Política da Aeronáutica para o Controle do Espaço Aéreo, de 2010;

b) DCA 14-8 Política de Segurança da Informação do Comando da Aeronáutica, de 2006;

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

d) DCA 21-2 Diretriz para a Implantação do Centro de Gerenciamento Técnico do SISCEAB, de 2009;

e) DECRETO Nº 3505, DE 13 DE JUNHO DE 2000. Institui a Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal;

f) Instrução Normativa GSI/PR nº 1, de 2008; 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; e

h) ABNT NBR ISO/IEC 27002 Código de Prática para a Gestão da Segurança da Informação, de 2005.

3 ÂMBITO E GRAU DE SIGILO

3.1 Esta Política 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

4.1 DGCEA – DIREÇÃO-GERAL DO DECEA

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

4.1.2 Deliberar quanto a decisões relacionadas à segurança 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 segurança 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 segurança da informação no DECEA, em articulação com as partes interessadas.

4.2.4 Auxiliar na aquisição de ferramentas informatizadas que viabilizem a gestão da segurança da informação.

4.2.5 Realizar a gestão de incidentes de segurança da informação no âmbito do DECEA.

4.2.6 Realizar a gestão de riscos de segurança da informação no âmbito do DECEA.

4.2.7 Realizar a gestão da continuidade das operações afetas à segurança da informação no âmbito do DECEA.

4.2.8 Realizar auditorias periódicas para avaliar os níveis de conformidade desta Política e dos Processos de Gestão da Segurança da Informação no âmbito do DECEA e Organizações Subordinadas.

4.2.9 Acompanhar estudos de implantação de novas tecnologias e projetos, quanto a possíveis impactos para a segurança da informação.

4.2.10 Acompanhar todas as mudanças no ambiente organizacional do DECEA, quanto a possíveis impactos para a segurança da informação.

4.2.11 Prover normativas para os ambientes, equipamentos, processos de informação, pessoas, sistemas e redes de comunicação do DECEA.

4.2.12 Reportar às partes interessadas situações que comprometam a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

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

4.3.1 Implantar as medidas de segurança da informação indicadas pela ASSICEA.

4.3.2 Realizar testes periódicos para avaliar a eficiência e eficácia da segurança da informação no âmbito de sua Organização Militar e Organizações Subordinadas.

4.3.3 Administrar a infraestrutura tecnológica de segurança da informação de forma a garantir o nível de serviços necessários para preservar a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

4.3.4 Realizar análise de riscos nos ativos de informação.

4.3.5 Realizar o tratamento de incidentes de segurança da informação.

4.3.6 Estabelecer procedimentos afetos à segurança da informação.

4.3.7 Reportar à ASSICEA situações que comprometam a segurança das informações.

4.4 SINT - SEÇÃO DE INTELIGÊNCIA

4.4.1 Prover medidas para classificar as informações circulantes no DECEA.

4.4.2 Especificar os sistemas criptográficos a serem utilizados como medidas de controle de segurança da informação.

4.4.3 Apurar incidentes de segurança da informação com o assessoramento da ASSICEA.

4.5 AJUR – ASSESSORIA JURÍDICA

4.5.1 Participar do processo de revisão desta Política quanto aos requisitos legais e regulatórios.

4.5.2 Assessorar o DGCEA na aplicação de sanções legais em caso de incidentes de segurança da informação no âmbito do DECEA.

4.6 ASCOM – ASSESSORIA DE COMUNICAÇÃO

4.6.1 Prover serviços de comunicação social sobre o tema segurança da informação no âmbito do DECEA.

4.7 APLOG – ASSESSORIA DE PLANEJAMENTO, ORÇAMENTO E GESTÃO

4.7.1 Propor ao DGCEA, com o assessoramento da ASSICEA, orçamento exclusivo para a segurança da informação.

4.8 SDTE – SUBDEPARTAMENTO TÉCNICO

4.8.1 Normatizar e emitir Diretrizes para os sistemas e para seus respectivos suportes logísticos afetos à segurança da informação, com o assessoramento da ASSICEA.

4.8.2 Fiscalizar e supervisionar os requisitos de segurança da informação para os sistemas e para seus respectivos suportes logísticos, com o assessoramento da ASSICEA.

4.8.3 Controlar, supervisionar e fiscalizar todos os investimentos em infraestrutura de segurança da informação no âmbito do DECEA e de suas Organizações Subordinadas.

4.9 SDOP – SUBDEPARTAMENTO DE OPERAÇÕES

4.9.1 Assegurar, com o assessoramento da ASSICEA, a integridade e a disponibilidade das informações necessárias às atividades operacionais do DECEA, por meio da proteção adequada dos recursos tecnológicos e da implantação de Planos de Continuidade que visem à continuidade das operações.

4.10 SDAD – SUBDEPARTAMENTO DE ADMINISTRAÇÃO

4.10.1 Garantir o entendimento das responsabilidades inerentes a esta Política, mediante assinatura do Termo de Responsabilidade de Segurança da Informação por funcionários (servidores militares e civis), terceiros e fornecedores.

4.10.2 Normatizar a aplicação de processo disciplinar nos casos de incidentes de segurança da informação no DECEA e Organizações Subordinadas.

4.10.3 Informar, em tempo hábil, à ASSICEA todos os desligamentos, afastamentos e mudanças de funções no DECEA.

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

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

4.11.2 Aplicar ações corretivas e disciplinares nos casos de quebra da segurança da informação por usuários sob sua responsabilidade.

4.11.3 Determinar o responsável por informar as movimentações de usuários terceiros sob responsabilidade do Comandante, Chefe ou Diretor aos proprietários de informações e custodiantes.

4.11.4 Reportar aos proprietários de informações situações que comprometam a segurança das informações.

4.11.5 Definir os proprietários das informações sob sua responsabilidade.

4.12 PROPRIETÁRIO DAS INFORMAÇÕES

4.12.1 Identificar e classificar as informações sob sua responsabilidade.

4.12.2 Definir as necessidades de segurança para as informações sob sua responsabilidade, explicitando as limitações de acesso e as condições de disponibilidade.

4.12.3 Definir o custodiante das informações sob sua responsabilidade.

4.12.4 Autorizar o custodiante a conceder as autorizações de acesso às informações sob sua responsabilidade, promovendo revisões periódicas das autorizações concedidas.

4.13 CUSTODIANTES

4.13.1 Garantir a disponibilidade, integridade e a confidencialidade das informações e dos recursos de informação sob sua custódia, conforme as condições estabelecidas pelo proprietário das informações.

4.13.2 Comunicar aos proprietários de informações e usuários, restrições e recursos de controle da sua instalação.

4.13.3 Prover salvaguardas físicas e procedimentos para recuperação de informações e recursos críticos sob sua responsabilidade.

4.13.4 Reportar ao proprietário da informação situações que comprometam a segurança das informações sob sua custódia.

4.14 USUÁRIOS DAS INFORMAÇÕES

4.14.1 Cumprir a Política de Segurança da Informação do DECEA e suas normativas gerenciais e técnicas.

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

5 PRINCÍPIOS

5.1 Neste capítulo estão descritos os princípios de segurança da informação, que são as declarações de alto nível sobre como a segurança da informação é utilizada nos processos de trabalho do DECEA e Organizações Subordinadas.

5.2 As informações do DECEA devem ser utilizadas de modo ético e seguro, em benefício exclusivo dos interesses deste Departamento.

5.3 A segurança da informação é de responsabilidade de todos, sendo norteada pelos seguintes princípios:

5.3.1 Confidencialidade: o meio utilizado para tratar a informação terá proteção adequada para permitir que apenas as pessoas autorizadas tenham acesso às informações necessárias.

5.3.2 Integridade: serão implantados mecanismos para garantir que a informação não seja modificada ou destruída de maneira não autorizada ou acidental.

5.3.3 Disponibilidade: as informações e as atividades críticas do DECEA manterão alto nível de disponibilidade.

5.3.4 Autenticidade: a validade referente às informações transmitidas e à identidade do seu remetente será verificada por meio de mecanismos que permitirão ao destinatário comprovar a origem e a autoria da mensagem.

5.3.5 Legalidade: toda informação produzida no DECEA deve respeitar a legislação vigente. O uso da tecnologia da informação e dos controles de segurança da informação devem estar de acordo com as leis vigentes.

5.3.6 Uso adequado: os usuários devem fazer uso dos ativos de informação providos pelo DECEA exclusivamente para o desempenho das atividades de interesse deste Departamento.

5.3.7 Integração: os ativos de informação terão gestão centralizada que garanta a plena integração de equipamentos, aplicações e dados para garantir a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações destes ativos.

5.3.8 Controle: o DECEA se reserva o direito de monitorar a utilização dos ativos de informação disponibilizados neste Departamento e em suas Organizações Subordinadas.

5.3.9 Custos: o DECEA deve priorizar o investimento em soluções tecnológicas de segurança da informação mediante o uso de software livre em detrimento de aquisições de software proprietário.

6 DIRETRIZES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

6.1 A informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado.

6.2 A segurança da informação no DECEA deve compreender um conjunto de Objetivos, Diretrizes, Normas e Procedimentos, de modo a gerenciar a segurança da informação neste Departamento e nas suas Organizações Subordinadas, visando garantir a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade da informação em todo o seu ciclo de vida.

6.3 O DECEA deve estruturar-se para a gestão de toda a documentação normativa relacionada à Segurança da Informação a ser elaborada ou revisada em seu âmbito. Estas documentações devem estar em consonância com esta Política e demais requisitos legais afetos ao tema.

6.4 Toda informação produzida e/ou manipulada no DECEA, pelo efetivo ou por partes externas, deve ser identificada, inventariada e submetida a procedimentos de segurança que minimizem o risco de a mesma ser violada ou perdida.

6.5 Além disso, deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para o DECEA, de modo a ser adequadamente protegida quanto ao seu acesso e uso. Para aquelas com classificação sigilosa serão necessárias medidas especiais de tratamento.

6.6 O DECEA deve assegurar que os servidores militares e civis, terceiros e fornecedores entendam suas responsabilidades e trabalhem em conformidade com os seus papéis, bem como deve assegurar o desenvolvimento de procedimentos de segurança da informação para garantir a redução do risco de roubo, de fraude ou de mau uso de recursos de informação.

6.7 O tema Segurança da Informação deve ser proposto pelo DECEA nas escolas e nos cursos de formação e de aperfeiçoamento da Força Aérea Brasileira, de forma a possibilitar uma crescente conscientização e o desenvolvimento de atitudes favoráveis à proteção das informações julgadas relevantes para este Departamento.

6.8 O DECEA deve promover, periodicamente, em todas as Organizações Subordinadas, campanhas de conscientização do público interno, baseadas no teor desta Política e nos demais documentos normativos decorrentes sobre Segurança da Informação que estiverem em vigor, visando apoiar o cumprimento da Política de Segurança da Informação durante a execução das atividades diárias, bem como reduzir o risco de erro humano.

6.9 O DECEA deve estabelecer documentos normativos visando à prevenção de acesso físico não autorizado, de interferências nas instalações e nas informações, de danos, furto ou comprometimento de ativos e interrupção de atividades operacionais ou administrativas.

6.10 O DECEA deve estabelecer normas para o uso de todo e qualquer tipo de serviço e de tecnologias de rede, tanto no contexto de redes locais como de redes de longa distância, capazes de monitorar e registrar os eventos relativos ao funcionamento dos demais serviços.

6.11 Com vistas ao fiel cumprimento das Diretrizes traçadas por esta Política, devem ser estabelecidos procedimentos de manutenção dos serviços, dos mecanismos de defesa contra

ataques, procedimentos periódicos para aferir a efetividade de proteções adotadas e de mecanismos de controle de acessos lógicos.

6.12 A adoção de qualquer solução ou serviço tecnológico, nacional ou estrangeiro, para atender a requisitos relativos à tecnologia e à segurança da informação, no âmbito do DECEA, deve ser precedida de estudos sobre a sua pertinência, abrangência, confiabilidade, permanência, manutenção, suporte e treinamento.

6.13 O DECEA deve buscar o desenvolvimento e a adoção de sistemas criptográficos conforme normas e demais instruções emitidas pelo Sistema de Inteligência do COMAER.

6.14 O DECEA deve estabelecer normas, bem como requisitos operacionais e técnicos de segurança da informação, a serem considerados no gerenciamento do ciclo de vida de sistemas de informação, promovendo a incorporação de funcionalidades que façam uso de certificados digitais, no transporte e no armazenamento de dados e de informações em meio digital, garantindo requisitos de identificação, de autenticação, de controle de acesso e de não repúdio, assim como a integridade de documentos digitais e a confidencialidade nas transações eletrônicas realizadas através de redes, visando minimizar o risco de falhas nos sistemas.

6.15 O DECEA deve desempenhar e manter uma estrutura que promova atividades de gerenciamento de incidentes de segurança da informação em todas as Organizações Subordinadas.

6.16 O DECEA deve estabelecer normas versando sobre medidas de segurança para garantir a continuidade das operações e para salvaguardar informações essenciais à operação do controle e da gestão do Espaço Aéreo.

6.17 O DECEA deve estruturar-se para promover atividades de gestão de riscos de segurança da informação em todas as Organizações Subordinadas, com vistas ao levantamento do impacto e probabilidades de ocorrência dos referidos riscos nos ativos de informação, bem como para identificar ameaças associadas às vulnerabilidades destes ativos, medir os níveis de risco e selecionar os controles necessários ao seu tratamento.

6.18 O DECEA deve estruturar-se para promover auditorias periódicas em todas as Organizações Subordinadas, com o intuito de aferir o nível de segurança da informação, quanto à utilização e ao armazenamento da informação e o controle dos serviços e dos ativos de informação, e ao alinhamento dos processos às normas e instruções voltadas para a Segurança da Informação em vigor no DECEA, a fim de evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

7 DIVULGAÇÃO

Esta Política e suas atualizações deverão ser divulgadas a todos os servidores militares e civis, terceiros e fornecedores que habitualmente trabalham no DECEA e suas Organizações Subordinadas.

8 HIERARQUIA DE DOCUMENTOS DA POLÍTICA

8.1 ORGANIZAÇÃO

8.1.1 A Política de Segurança da Informação está organizada da seguinte forma:

a) Política de Segurança da Informação do DECEA (DCA);
b) Normas de Segurança da Informação (NSI);
c) Procedimentos de Segurança da Informação (PSI);
d) Instruções de Segurança da Informação (ISI); e
e) Registros de Segurança da Informação (RSI).

9 PROCESSO DE ATUALIZAÇÃO

9.1 REVISÃO E ATUALIZAÇÃO

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

9.2 PERIODICIDADE DE REVISÃO

9.2.1 A Política de Segurança da Informação do DECEA (DCA) deve ser revisada, no mínimo, uma vez a cada doze meses.

9.2.2 As Normas de Segurança da Informação (NSI) devem ser revisadas, no mínimo, uma vez a cada doze meses.

9.2.3 Procedimento de Segurança da Informação (PSI) e Instrução de Segurança da Informação (ISI) devem ser revisados, no mínimo, uma vez a cada doze meses.

10 PENALIDADES

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

11 DISPOSIÇÕES FINAIS

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