MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-19

PRECEITOS DE SEGURANÇA DA INFORMAÇÃO PARA O DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2012

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

TECNOLOGIA DA INFORMAÇÃO

ICA 7-19

PRECEITOS DE SEGURANÇA DA INFORMAÇÃO PARA O DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2012

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

PORTARIA DECEA Nº 36/DGCEA, DE 16 DE MARÇO DE 2012.

Aprova a edição da Instrução de Preceitos de Segurança da Informação para o Departamento de Controle do Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das suas 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. 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 7-19 "Preceitos de Segurança da Informação para o 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 RAMON BORGES CARDOSO
Diretor-Geral do DECEA

(Publicada no BCA nº 068, de 9 de abril de 2012)

SUMÁRIO

PREFÁCIO

Com a publicação do Plano Diretor de Tecnologia da Informação do DECEA (PCA 7-14) e do Plano Diretor de Segurança da Informação do DECEA (PCA 7-11), torna-se evidente a importância da Segurança da Informação e a sua consideração nos diversos processos e atividades desenvolvidos para se atingir os objetivos e a missão do DECEA. Contudo, devido à sua abrangência, sua especificidade da área, a dimensão do SISCEAB e a quantidade de ativos envolvidos, a aplicação de preceitos de Segurança da Informação pode se tornar dispendiosa e ineficiente caso não seja feita de maneira uniforme e regulamentada.

Desta forma, a presente Instrução visa apresentar Normas para os diversos aspectos da Segurança da Informação e de sua gestão, no âmbito do Sistema de Controle do Espaço Aéreo Brasileiro, contribuindo para a concretização da ação 7 do segundo objetivo da PCA 7-11.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar as Normas de Segurança da Informação que regulamentam e fornecem diretrizes para os diversos aspectos da Segurança da Informação para o DECEA e suas OM subordinadas.

1.2 ÂMBITO E GRAU DE SIGILO

Esta Instrução se aplica ao DECEA e a todas as Organizações Militares subordinadas. Sendo considerado ostensivo o seu grau de sigilo.

1.3 ABREVIATURAS

ASSICEA	–	Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo
DECEA	–	Departamento de Controle do Espaço Aéreo
OM	–	Organização Militar
SDTE	–	Subdepartamento Técnico do DECEA
SGSI	–	Sistema de Gestão de Segurança da Informação
SSSI	–	Seção de Segurança de Sistemas de Informação
STI	–	Seção de Tecnologia da Informação

1.4 PENALIDADES

1.4.1 O Usuário que infringir as normas previstas nesta Instrução do Comando da Aeronáutica estará sujeito a penalidades administrativas, o que não impede e tampouco elide outras penalidades de natureza civil e penal previstas na legislação em vigor e às quais o Usuário tiver dado causa em razão da gravidade do ato praticado.

1.4.2 Compete ao Diretor-Geral do Departamento de Controle do Espaço Aéreo e ao Diretor/Presidente/Chefe/Comandante das Unidades subordinadas ao DECEA, a quem se encontra vinculado o Usuário infrator, ou na qual ele desenvolve sua atividade, fazer aplicar as providências cabíveis quando da ocorrência de infrações a esta Instrução do Comando da Aeronáutica.

2 NORMAS DE SEGURANÇA DA INFORMAÇÃO

2.1 APRESENTAÇÃO

2.1.1 As Normas de Segurança da Informação do DECEA são apresentadas como anexos desta Instrução, sem prejuízo de seus valores como documentos normativos.

2.2 UTILIZAÇÃO

2.2.1 Como precondição para a utilização destas Normas, as OM devem estar estruturadas de acordo com o estabelecido pelo PCA 7-11, ou seja, devem possuir uma Seção de Segurança de Sistemas de Informação (SSSI) responsável pela garantia do cumprimento da Política de Segurança da Informação naquela organização.

2.2.2 As Seções de Tecnologia da Informação de cada OM devem seguir as diretrizes estabelecidas pelas Normas aqui apresentadas e pelas Normas delas derivadas.

2.3 DESCRIÇÃO DOS DOCUMENTOS NORMATIVOS

2.3.1 GESTÃO DE DOCUMENTOS NORMATIVOS DE SEGURANÇA DA INFORMAÇÃO (ANEXO A)

Com esta Norma visa-se garantir a correta divulgação, controle, armazenamento e gerenciamento dos documentos normativos de Segurança da Informação do DECEA.

2.3.2 GESTÃO DE CÓPIAS DE SEGURANÇA DA INFORMAÇÃO (ANEXO B)

Esta Norma estabelece as regras para a gestão de Cópia de Segurança da Informação dos dados custodiados por todas as OM subordinadas ao DECEA. Tem como propósito prover uma base comum para a elaboração de procedimentos e instruções para a realização de cópias de segurança, restauração, armazenamento e transporte de mídias de Cópias de Segurança da Informação.

2.3.3 GESTÃO DE MUDANÇAS (ANEXO C)

Esta Norma visa garantir que mudanças em sistemas operacionais e/ou sistemas e/ou aplicativos sejam planejadas, aprovadas, executadas e registradas, minimizando o risco de impactos de disponibilidade, integridade e confiabilidade.

2.3.4 GESTÃO DE RISCOS DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO (ANEXO D)

Esta Norma tem como objetivo definir as diretrizes para o processo de gestão de riscos de tecnologia e segurança da informação.

2.3.5 CONTROLE DE ACESSO LÓGICO DAS REDES DE TELECOMUNICAÇÕES (ANEXO E)

Esta Norma visa estabelecer as diretrizes para implementação de controles de acesso lógico às redes de telecomunicações gerenciadas pelo DECEA, em conformidade com a ROCA 20-7 (Regulamento do Departamento de Controle do Espaço Aéreo).

2.3.6 AUDITORIA INTERNA DE CONFORMIDADE DE SEGURANÇA DA INFORMAÇÃO (ANEXO F)

Esta Norma tem como objetivo garantir que o Departamento de Controle do Espaço Aéreo e suas unidades subordinadas operem de acordo com as Políticas, Normas, Procedimentos e Instruções de Trabalho determinadas pelo Sistema de Gestão de Segurança da Informação.

2.3.7 GERENCIAMENTO DE CONFIGURAÇÃO (ANEXO G)

Esta Norma tem como objetivo identificar, controlar e auditar os elementos de Tecnologia da Informação e os ativos de informação (por exemplo: *hardware*, *software*, documentação, licenças etc.), mantendo uma base de dados (designada por CMDB – *Configuration Management Data Base*) com o objetivo de fornecer informação segura e atualizada sobre os itens de configuração (IC).

2.3.8 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO (ANEXO H)

Esta Norma tem como objetivo disciplinar a gestão de incidentes de segurança da informação no Departamento de Controle do Espaço Aéreo e suas Organizações Subordinadas.

3 DISPOSIÇÕES FINAIS

3.1 As Normas estabelecidas neste documento são de caráter geral e devem ser revisadas periodicamente a cada vinte e quatro meses.

3.2 Casos omissos deverão ser levados à apreciação do Exmo. Sr. Diretor-Geral do DECEA.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Política do Comando da Aeronáutica para a Tecnologia da Informação*: **DCA 14-7**. Brasília-DF, 2004.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Política de Segurança da Informação do Comando da Aeronáutica*: **DCA 14-8**. Brasília-DF, 2006.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica*: **RCA 205-1**. Brasília-DF, 2006.

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

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Requisitos Básicos das Redes de Comunicações do Comando da Aeronáutica*: **DCA 102-1**. Rio de Janeiro-RJ, 2011.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Diretriz para Implantação do Centro de Gerenciamento Técnico do SISCEAB*: **DCA 21-2**. Rio de Janeiro-RJ, 2009.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Plano Diretor de Tecnologia da Informação do Departamento de Controle do Espaço Aéreo*: **PCA 7-14**. Rio de Janeiro-RJ, 2010.

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

BRASIL. Comando da Aeronáutica. *Regulamento do Departamento de Controle do Espaço Aéreo*: **ROCA 20-7**. Brasília-DF, 2011.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. *Instrução Normativa n° 1*. 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT NBR ISO 19011. *Diretrizes para Auditorias de Sistema de Gestão da Qualidade e/ou Ambiental*. Rio de Janeiro, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT NBR ISO/IEC 27001. *Tecnologia da Informação – Sistemas de gestão de segurança da informação – Requisitos*. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT NBR ISO/IEC 27002**.** *Tecnologia da Informação – Código de Práticas para a Gestão da Segurança da Informação.* Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT NBR ISO/IEC 27005. *Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação*. Requisitos, 2008.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Information technology – Security techniques – Evaluation criteria for IT security*: ISO 15408**.** 2009.

Anexo A - Norma de Gestão de Documentos Normativos de Segurança da Informação

SUMÁRIO

1 OBJETIVO

Garantir a correta divulgação, controle, armazenamento e gerenciamento dos documentos normativos de segurança da informação do Departamento de Controle do Espaço Aéreo e suas Organizações subordinadas.

2 APLICAÇÃO

Esta Norma de Segurança da Informação é de aplicação no Departamento de Controle do Espaço Aéreo e suas Organizações subordinadas.

3 DEFINIÇÕES

Os conceitos e definições estão listados na MCA 7-1 Glossário de Segurança da Informação do DECEA.

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 ASSICEA

Assessoria de Segurança de Sistemas da Informação do Controle do Espaço Aéreo, subordinada diretamente ao Diretor-Geral do DECEA.

3.2 SSSI

Seção de Segurança de Sistemas de Informação subordinada diretamente ao Chefe, Comandante ou Diretor da Organização Militar subordinada ao DECEA.

3.3 SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI)

Sistema que classifica e gerencia os ativos em relação ao risco, também classifica as informações, os objetivos e controles e também o grau de segurança requerido pelo DECEA, de acordo com a Norma ISO/IEC 27001.

3.4 DOCUMENTO NORMATIVO DE SEGURANÇA DA INFORMAÇÃO

Refere-se aos documentos do SGSI. São eles: Política de Segurança da Informação, Normas de Segurança da Informação, Procedimentos de Segurança da Informação e Instruções de Segurança da Informação.

3.5 REGISTRO DE SEGURANÇA DA INFORMAÇÃO

Documento que fornece evidência objetiva de atividades realizadas ou resultados obtidos.

4 RESPONSABILIDADES

4.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

É da competência e responsabilidade da ASSICEA a elaboração das Normas de Segurança da Informação, a revisão de todos os procedimentos de segurança da informação e instrução de segurança da informação relativas à padronização de documentos normativos de segurança da informação do Sistema de Gestão da Segurança da Informação (SGSI).

É de responsabilidade da ASSICEA controlar, gerenciar e armazenar os documento normativos de segurança da informação.

4.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

4.2.1 As Seções de Segurança de Sistemas da Informação (SSSI) das Organizações Militares subordinadas ao DECEA deverão elaborar os procedimentos de segurança da informação e instrução de segurança da informação de acordo com as Normas de Segurança da Informação elaboradas pela ASSICEA.

4.2.2 Posteriormente à elaboração dos procedimentos e instruções, as Organizações Militares subordinadas ao DECEA deverão enviar esses documentos normativos para a revisão da ASSICEA. Após a aprovação da ASSICEA, os documentos normativos deverão ser publicados pelas organizações militares subordinadas ao DECEA.

4.3 ASCOM – ASSESSORIA DE COMUNICAÇÃO SOCIAL

É de responsabilidade da ASCOM divulgar os documentos normativos de segurança da informação utilizando um *software* de gestão de documentos normativos de segurança da informação de acordo com as diretrizes estabelecidas pela ASSICEA.

5 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

A elaboração, revisão e aprovação dos documentos normativos de segurança da informação devem ter controles de segurança, de segregações de funções e controle de acesso.

5.1 ELABORAÇÃO DE DOCUMENTOS NORMATIVOS

A elaboração dos documentos normativos de segurança da informação deve ser realizada pela ASSICEA – Assessoria de Segurança de Sistemas da Informação do Controle

do Espaço Aéreo ou pela SSSI – Seção de Segurança de Sistemas da Informação, presentes nas Organizações Militares subordinadas ao DECEA.

5.2 REVISÃO DE DOCUMENTOS NORMATIVOS

5.2.1 A revisão dos documentos normativos de segurança da informação deverá ser realizada pelo Chefe da ASSICEA e pelo Chefe da SSSI.

5.2.2 Todo procedimento de segurança da informação e instrução de segurança da informação elaborado pela SSSI deve ser encaminhado à ASSICEA para a verificação de qualidade e verificação técnica no documento normativo de segurança da informação.

5.3 APROVAÇÃO DE DOCUMENTOS NORMATIVOS

5.3.1 Os documentos normativos de segurança da informação elaborados pela ASSICEA deverão ser aprovados pelo Diretor-Geral do Departamento de Controle do Espaço Aéreo.

5.3.2 Após a revisão da ASSICEA, os documentos normativos de segurança da informação elaborados pela SSSI serão encaminhados às Organizações Militares Subordinadas ao DECEA e deverão ser aprovados pelos Chefes, Comandantes ou Diretores de cada Organização Militar.

5.4 DIVULGAÇÃO DE DOCUMENTOS NORMATIVOS

5.4.1 A ASSICEA, conjuntamente com a ASCOM, realizará a divulgação dos documentos normativos de segurança da informação após a sua publicação.

5.4.2 Esta divulgação deve estar de acordo com as ações do Plano de Divulgação de Segurança da Informação do DECEA.

5.5 CONTROLE E GERENCIAMENTO DOS DOCUMENTOS NORMATIVOS

As versões dos documentos normativos devem ser controladas pela ASSICEA de forma a implantar controle de versão, controle de numeração e histórico de revisão.

5.6 ARMAZENAMENTO

Os documentos normativos de segurança da informação devem ser armazenados pela ASSICEA de forma a gerar evidências, registros de distribuição e leitura dos documentos.

6 REQUISITOS MÍNIMOS DO SOFTWARE DE GESTÃO DE DOCUMENTOS NORMATIVOS

6.1 Conforme descrito no relatório EPSI_REL_003_ESPECIFICAÇÃO DO *SOFTWARE* PARA GESTÃO DAS POLÍTICAS, os documentos requeridos pelo SGSI devem ser protegidos e controlados seguindo as especificações da Norma ABNT NBR ISO/IEC 27001:2006. Portanto, um sistema de informação deve ser estabelecido para definir as ações de gestão dos documentos normativos de segurança da informação para:

a) aprovar documentos para adequação antes de sua emissão;

b) analisar criticamente, atualizar (quando necessário) e reaprovar documentos;

c) assegurar que as alterações e a situação da revisão atual dos documentos sejam identificadas;

d) assegurar que as versões pertinentes de documentos aplicáveis estejam disponíveis nos locais de uso;

e) assegurar que os documentos permaneçam legíveis e prontamente identificáveis;

f) assegurar que os documentos estejam disponíveis àqueles que deles precisam e sejam transferidos, armazenados e finalmente descartados conforme os procedimentos aplicáveis à sua classificação;

g) assegurar que documentos de origem externa sejam identificados;

h) assegurar que a distribuição de documentos seja controlada;

i) prevenir o uso não intencional de documentos obsoletos;

j) aplicar identificação adequada nos casos em que sejam retidos para qualquer propósito; e

k) estabelecer e manter registros para fornecer evidências do SGSI.

6.2 Este sistema deverá possuir uma interface intuitiva e deverá ser acessado via web.

7 REGISTROS GERADOS

Documentos Normativos de Segurança da Informação armazenados.

8 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada constatando-se que todo o fluxo de elaboração, revisão, aprovação e divulgação foram seguidos, respeitando o controle de segregação de funções.

9 FLUXOGRAMA

Não aplicável.

10 DOCUMENTOS DE REFERÊNCIA

10.1 DCA 7-2 Política de Segurança da Informação do DECEA, 2010.

10.2 DCA 14-8 Política de Segurança da Informação do COMAER, 2006.

10.3 PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, 2010.

10.4 ABNT NBR ISO/IEC 27001 Sistema de Gestão de Segurança da Informação, 2006.

11 ANEXOS

Não aplicável.

Anexo B - Norma de Gestão de Cópias de Segurança da Informação

SUMÁRIO

1 OBJETIVO

Esta Norma estabelece as diretrizes para a gestão de cópia de segurança da informação dos dados custodiados por todas as Organizações Militares subordinadas ao DECEA. Tem como propósito prover uma base comum para elaboração de procedimentos e instruções para realização de cópias de segurança, restauração, armazenamento e transporte de mídias de cópias de segurança da informação.

2 APLICAÇÃO

Esta Norma de Segurança da Informação é de aplicação no Departamento de Controle do Espaço Aéreo e suas Organizações Subordinadas.

3 DEFINIÇÕES

Os conceitos e definições estão listados na MCA 7-1 Glossário de Segurança da Informação do DECEA.

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 CÓPIAS DE SEGURANÇA

A cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso de perda dos dados originais.

3.2 MÍDIAS

Meios difundidos de cópias de segurança incluem CD-ROM, DVD, disco rígido externo, fitas magnéticas, flash de memória, entre outros que porventura surjam com o avanço tecnológico.

3.3 RESTAURAÇÃO

Restauração dos dados originais a partir de um dispositivo de cópia de segurança.

4 RESPONSABILIDADES

4.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

4.1.1 Elaborar as diretrizes para a correta cópia de segurança da informação e fiscalizar o cumprimento desta Norma para a gestão de Cópias de Segurança da Informação.

4.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

4.2.1 Implementar as diretrizes presentes nesta Norma de Cópias de Segurança da Informação

4.3 STI – SEÇÃO DE TECNOLOGIA DA INFORMAÇÃO

4.3.1 Executar os procedimentos de administração das cópias de segurança da informação.

5 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

Deve-se definir com o Chefe, Diretor ou Comandante de cada Organização Militar subordinada ao DECEA quais dados deverão ter cópias de segurança da informação.

5.1 CÓPIA DE SEGURANÇA DA INFORMAÇÃO DOS DADOS

5.1.1 REALIZAÇÃO DA CÓPIA DE SEGURANÇA DA INFORMAÇÃO

5.1.1.1 As mídias de cópias de segurança devem ser identificadas. A identificação deve conter, no mínimo, a data da cópia de segurança da informação e o código da mídia.

5.1.1.2 Antes da realização de modificações impactantes nos dados, deve ser feita uma cópia de segurança da informação total das informações e configurações, a fim de preservar os dados originais caso ocorram falhas no processo de modificação.

5.1.1.3 A realização operacional da cópia de segurança da informação deverá ser detalhada em um procedimento de cópias de segurança da informação de cada Organização Militar subordinada ao DECEA. Cada Organização Militar deve elaborar um procedimento de segurança da informação com as instruções de como é realizada a cópia de segurança em sua Organização Militar, em conformidade com as diretrizes contidas nesta Norma de Segurança da Informação.

5.1.1.4 Deve ser preenchido um formulário diário de cópia de segurança da informação. Esse formulário deve conter os seguintes requisitos: informações de periodicidade, tipo de cópia de segurança, tempo de retenção, número da mídia, conteúdo da cópia, dia de execução, resultado de teste na mídia, erros em procedimentos de cópia, tempo de retenção da cópia e local onde deverá ser armazenada a cópia de segurança.

5.1.1.5 A necessidade de parada nos serviços de Tecnologia da Informação deve ser observada e programada.

5.1.2 REALIZAÇÃO DOS TESTES DAS MÍDIAS

5.1.2.1 Os testes das mídias de cópias de segurança devem ser definidos no procedimento de cópias de segurança da informação de cada Organização Militar subordinada ao DECEA.

5.1.2.2 As mídias de cópia de segurança devem ser periodicamente testadas de acordo com o procedimento de segurança da informação de cada Organização Militar subordinada ao DECEA.

5.1.2.3 Deve ser preenchido um formulário de testes de mídias de cópias de segurança da informação. Esse formulário deve conter as seguintes informações: data, resultado e conteúdo do teste de mídia, situação física da mídia e operador que realizou o teste na mídia.

5.1.3 TEMPO DE RETENÇÃO DOS DADOS E CLASSIFICAÇÃO DOS DADOS

5.1.3.1 Os dados copiados devem ser armazenados em conformidade com a legislação em vigor preconizada no RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica".

5.1.3.2 O tempo de retenção, específico para cada tipo de dado, deverá ser definido formalmente pelo proprietário da informação em conjunto com o servidor e deverá ser descrito em um Formulário de Cópia de Segurança da Informação.

5.1.3.3 Os dados devem ser classificados em conformidade com o RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica".

5.2 INFORMAÇÕES DE CÓPIAS DE SEGURANÇA DA INFORMAÇÃO

5.2.1 INFORMAÇÕES

5.2.1.1 As informações de cópias de segurança devem ser identificadas em formulários específicos para cada ativo de informação de tecnologia.

5.2.1.2 As informações contidas no Formulário de Cópia de Segurança da Informação deverão ser definidas formalmente pelo proprietário da informação em conjunto com o custodiante do ativo de informação tecnológico.

5.2.1.3 O Formulário de Cópia de Segurança da Informação deverá conter as informações de periodicidade, tipo de cópia de segurança, tempo de retenção, número da mídia, conteúdo da cópia, dia de execução, resultado de teste na mídia, erros em procedimentos de cópia, tempo de retenção da cópia e local onde deverá ser armazenada a cópia de segurança.

5.3 RESTAURAÇÃO DOS DADOS

5.3.1 RESTAURAÇÃO DAS INFORMAÇÕES

5.3.1.1 Somente o proprietário da informação, conforme regulamentado na DCA 7-2 "Política de Segurança da Informação do DECEA" poderá autorizar a restauração da mesma, utilizando o procedimento de segurança da informação definido por cada Organização Militar subordinada ao DECEA.

5.3.1.2 Caso uma área não proprietária de uma informação solicite a restauração da mesma, o proprietário da informação deverá ser notificado para ciência e autorização do procedimento.

5.3.1.3 De acordo com uma boa prática de segurança, a informação deve ser restaurada em local diferente do ambiente lógico da rede por exemplo da informação original, sempre que

possível, de modo a evitar falhas no processo de restauração, no qual uma informação é restaurada substituindo a informação anterior.

5.4 ARMAZENAMENTO DAS MÍDIAS

5.4.1 ARMAZENAMENTO INTERNO E EXTERNO

5.4.1.1 As mídias de cópia de segurança da informação deverão ser armazenadas em local protegido, controlado e com número de identificação na mídia.

5.4.1.2 As mídias de cópia de segurança da informação deverão ser armazenadas em conformidade com as especificações do fabricante da mídia.

5.4.1.3 As mídias devem receber a classificação e o tratamento da informação de acordo com o valor dos dados que armazenam.

5.4.1.4 As mídias de cópia de segurança da informação devem ser armazenadas em local que garanta a sua integridade física e lógica.

5.4.1.5 As mídias de cópia de segurança da informação contendo informações vitais para o negócio da Organização Militar devem preferencialmente ser armazenadas a uma distância mínima de cinco quilômetros em relação às informações originais.

5.4.1.6 As mídias de cópia de segurança contendo informações classificadas devem possuir o rótulo de classificação, conforme descrito no RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica".

5.4.1.7 As mídias de cópia de segurança da informação contendo informações confidenciais devem ser armazenadas em local separado das demais.

5.4.1.8 O acesso às mídias de cópia de segurança da informação classificadas como confidenciais deve ser controlado, registrado e formalmente autorizado pelo chefe de cada Organização Militar.

5.5 DO TRANSPOSTE DAS MÍDIAS

5.5.1 TRANSPORTE INTERNO E EXTERNO

5.5.1.1 As mídias de cópia de segurança da informação devem ser transportadas de forma registrada e controlada.

5.5.1.2 As mídias de cópia de segurança da informação devem ser transportadas de forma protocolada, por pessoa formalmente autorizada e em recipiente lacrado (que revele qualquer tentativa de acesso indevido).

5.5.1.3 O conjunto de mídias de cópia de segurança da informação contendo informações classificadas como confidenciais devem ser separadas, em uma ou mais mídias, e devem transportadas por vias distintas.

5.6 DESCARTE

5.6.1 DESCARTE DAS MÍDIAS

5.6.1.1 As mídias de cópia de segurança da informação devem ser descartadas no período especificado pelo fabricante no seu tempo de validade.

5.6.1.2 O conteúdo da mídia a ser descartada deverá ter tratamento de acordo com a RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica".

5.6.1.3 As mídias contendo informações sensíveis para o negócio de cada Organização Militar subordinada ao DECEA devem ser destruídas de forma que a informação não possa ser recuperada.

5.6.1.4 As mídias de cópia de segurança da informação contendo informações sensíveis para os negócios cada Organização Militar subordinada ao DECEA devem ter sua data de descarte registrada.

6 REGISTROS GERADOS

Não aplicável.

7 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada constatando que as atividades do item 5 estão sendo realizadas. Deve-se verificar as evidências da execução das atividades do item 5, ou seja, a execução das atividades de realização da cópia, do teste, da restauração e do descarte da mídia.

8 FLUXOGRAMA

Não aplicável.

9 DOCUMENTOS DE REFERÊNCIA

9.1 PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, 2010.

9.2 DCA 7-2 Política de Segurança da Informação do DECEA, 2010.

9.3 DCA 14-8 Política de Segurança da Informação do COMAER, 2006.

9.4 RCA 205-1 Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica, 2006.

10 ANEXOS

Não Aplicável

Anexo C - Norma de Gestão de Mudanças

SUMÁRIO

1 OBJETIVO

Garantir que alterações em sistemas operacionais e/ou sistemas e/ou aplicativos sejam planejadas, aprovadas, executadas e registradas, minimizando o risco de impactos em disponibilidade, integridade e confiabilidade.

2 APLICAÇÃO

Esta Norma de Segurança da Informação é de aplicação no Departamento de Controle do Espaço Aéreo e suas Organizações Subordinadas.

3 DEFINIÇÕES

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

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 GESTÃO DE MUDANÇAS

Processo de gerenciamento de mudanças em sistemas operacionais, serviços, sistemas, aplicativos e outros.

3.2 AVALIAÇÃO DE IMPACTO DE MUDANÇA

Documento que indique os possíveis impactos gerados por uma determinada mudança nos ativos de informação tecnológicos.

3.3 PLANO DE RESTAURAÇÃO

Documento que indique os passos que devem ser realizados para recuperação de um ativo em caso de falha.

3.4 PLANO DE COMUNICAÇÃO DE MUDANÇA

Definição da forma de comunicação e das pessoas que devem ser alertadas de alguma mudança nos ativos de informação tecnológicos.

4 RESPONSABILIDADES

4.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

Elaborar as diretrizes para a gestão de mudanças e fiscalizar o cumprimento desta Norma.

4.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Implementar as diretrizes presentes nesta Norma.

5 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

5.1 PLANEJAMENTO DE MUDANÇAS

Todas as alterações em sistemas de informação devem ser planejadas e registradas. O planejamento de todas as mudanças deve conter as seguintes informações:

a) ativo a ser modificado;

b) criticalidade do ativo;

c) motivo da mudança;

d) detalhes técnicos do que se deseja mudar;

e) avaliação de impactos da mudança;

f) indicação do Plano de Restauração do ativo em caso de falha;

g) indicação do Plano de Comunicação aos Envolvidos;

h) definição de data e hora (apropriados) para execução da mudança; e

i) aprovação do responsável pelo ativo.

5.2 MUDANÇAS EM ATIVOS CRÍTICOS

Para mudanças em ativos de informações que contêm informações críticas para a Organização Militar, além do planejamento de mudança, testes devem ser executados em um ambiente de homologação adequado.

5.3 COMUNICAÇÃO AOS ENVOLVIDOS

O responsável pelo ativo, antes da aprovação de uma mudança, deve executar o Plano de Comunicação aos Envolvidos. Este Plano deve orientar os envolvidos diretamente na mudança do ativo que sofrerá as alterações.

5.4 APROVAÇÃO DE MUDANÇAS

Nenhuma mudança deve ser realizada sem a devida aprovação do ativo. O responsável pelo ativo deve aprovar mudanças baseado nas informações de "PLANEJAMENTO DE MUDANÇAS".

NOTA: Quando aplicável, o responsável pelo ativo deve estar atento às questões relativas a "Licenciamento" e "Direitos Autorais" antes de sua aprovação de mudança.

5.5 AVALIAÇÃO DE MUDANÇA

Após a realização de uma mudança, deve ser verificado o funcionamento adequado do sistema de informação.

5.6 MUDANÇAS DESNECESSÁRIAS

As mudanças só devem ocorrer em situações em que exista uma razão de negócio válida.

NOTA: Atualizações de sistemas às versões mais atuais nem sempre são de interesse do negócio, pois podem introduzir vulnerabilidades e instabilidades não existentes na versão corrente.

6 REGISTROS GERADOS

Não aplicável.

7 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada constatando-se que as atividades do item 5 foram realizadas.

8 FLUXOGRAMA

Não aplicável.

9 DOCUMENTOS DE REFERÊNCIA

9.1 PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, 2010.

9.2 DCA 7-2 Política de Segurança da Informação do DECEA, 2010.

9.3 DCA 14-8 Política de Segurança da Informação do COMAER, 2006.

9.4 ABNT NBR ISO/IEC 27001 Sistema de Gestão de Segurança da Informação, 2006.

10 ANEXOS

Não aplicável.

Anexo D - Norma de Gestão de Riscos de Tecnologia e Segurança da Informação

SUMÁRIO

1 OBJETIVO

Esta Norma tem como objetivo definir as diretrizes para o processo de Gestão de Riscos de tecnologia e segurança da informação.

2 CAMPO DE APLICAÇÃO

Esta Norma de Segurança da Informação é de aplicação no Departamento de Controle do Espaço Aéreo e suas Organizações Militares subordinadas.

3 DEFINIÇÕES

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

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 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.

3.2 GESTÃO DE RISCOS

Conjunto de atividades coordenadas para conhecer e controlar uma organização no que se refere a riscos, conforme conceituação contida na Norma ABNT NBR ISO/IEC 27005:2008.

3.3 PDCA

A metodologia de gestão de segurança da informação baseia-se no processo de melhoria contínua, denominado ciclo "PDCA" (*Plan-Do-Check-Act*), estabelecido pela Norma ABNT NBR ISO/IEC 27001:2006.

3.4 SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI)

Sistema que classifica e gerencia os ativos em relação ao risco, também classifica as informações, objetivos, controles e grau de segurança requeridos pelo DECEA, de acordo com a Norma ABNT NBR ISO/IEC 27001:2006.

4 RESPONSABILIDADES

4.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

4.1.1 Realizar a gestão de riscos de tecnologia e segurança da informação no âmbito do DECEA e de suas Organizações Militares subordinadas, provendo diretrizes e ferramentas tecnológicas para a análise e avaliação de riscos.

4.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO

4.2.1 Realizar a análise de riscos nos ativos de informação de responsabilidade de sua Organização Militar.

4.2.2 Seguir as diretrizes da ASSICEA para realizar a análise de riscos.

4.2.3 Encaminhar os relatórios de análises de riscos para a ASSICEA.

5 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

5.1 DIRETRIZES PARA A GESTÃO DE RISCOS

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).

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.

5.2 SISTEMA DE GESTÃO DE RISCOS DA ABNT NBR ISO/IEC 27005:2008

Nos itens abaixo, será apresentada uma abordagem sistemática do processo de Gestão de Riscos de Tecnologia e Segurança da Informação com o objetivo de manter os riscos em níveis aceitáveis. O processo de gestão de riscos é composto pelas seguintes atividades:

a) definição do contexto;

b) análise e avaliação de riscos;

c) tratamento dos riscos;

d) aceitação dos riscos;

e) monitoramento e análise crítica de riscos; e

f) comunicação dos riscos.

5.2.1 DEFINIÇÃO DO CONTEXTO

5.2.1.1 Deve-se definir o escopo de aplicação da Gestão de Riscos de Tecnologia e Segurança da Informação a fim de delimitar o âmbito de atuação. Esse escopo pode abranger a Organização Militar Subordinada, área, processo, ou ativo de informação.

5.2.1.2 Nesta atividade, deve-se estabelecer os critérios de avaliação e de aceitação do risco.

5.2.2 ANÁLISE E AVALIAÇÃO DE RISCOS

5.2.2.1 Nesta atividade, inicialmente serão identificados os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados.

5.2.2.2 Deve-se realizar o mapeamento de ativos de informação realizando a identificação desses ativos de informação e seu responsável dentro do escopo estabelecido.

5.2.2.3 Devem-se identificar os riscos associados ao escopo definido, considerando:

a) ameaças envolvidas;

b) vulnerabilidades existentes nos ativos de informação; e

c) controles de segurança da informação já adotados.

5.2.2.4 Devem-se estimar os riscos identificados para cada ativo de informação, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de confidencialidade, integridade e disponibilidade.

5.2.2.5 Devem-se avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos na definição do contexto.

5.2.2.6 Devem-se relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos na definição de contexto.

5.2.3 TRATAMENTO DOS RISCOS

5.2.3.1 Devem-se relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos na definição de escopo.

5.2.3.2 Devem-se determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou aceitar o risco, observando:

a) eficácia dos controles de segurança da informação já existentes;

b) restrições organizacionais, técnicas e estruturais em cada Organização Militar subordinada ao DECEA;

c) requisitos legais; e

d) análise custo/benefício.

5.2.3.3 Deve-se elaborar um plano para o tratamento dos riscos, relacionando, no mínimo, controles de segurança da informação, os responsáveis pela implantação dos controles de segurança da informação, prioridades e prazos de execução necessários à sua implantação.

5.2.4 ACEITAÇÃO DOS RISCOS

Devem-se verificar os resultados do processo executado de gestão de riscos de tecnologia e segurança da informação, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação do Chefe, Diretor ou Comandante da Organização Militar Subordinada ao DECEA.

5.2.5 MONITORAMENTO E ANÁLISE CRÍTICA DOS RISCOS

Devem-se 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 de Tecnologia e Segurança da Informação.

5.2.6 COMUNICAÇÃO DOS RISCOS

Deve-se manter a chefia superior informada a respeito de todas as fases da gestão de riscos de tecnologia e segurança da informação, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas ou interessadas.

6 MELHORIA CONTÍNUA

Cada Organização Militar Subordinada ao DECEA deve propor à ASSICEA a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica.

As Organizações Militares subordinadas ao DECEA devem executar as ações corretivas ou preventivas aprovadas pelo Chefe, Diretor ou Comandante da Organização Militar para tratar os riscos identificados durante a atividade de análise e avaliação de riscos.

7 REGISTROS GERADOS

Não aplicável.

8 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada mediante a constatação de que todas as atividades do processo de gestão de riscos de tecnologia e segurança da informação foram seguidas.

9 FLUXOGRAMA

Não aplicável.

10 DOCUMENTOS DE REFERÊNCIA

10.1 DCA 7-2 Política de Segurança da Informação do DECEA, 2010.

10.2 DCA 14-8 Política de Segurança da Informação do COMAER, 2006.

10.3 PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, 2010.

10.4 ABNT NBR ISO/IEC 27001 Sistema de Gestão de Segurança da Informação, 2006.

10.5 ABNT NBR ISO/IEC 27005 Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação, 2008.

11 ANEXOS

Não aplicável.

Anexo E - Norma de Controle de Acesso Lógico das Redes de Telecomunicações

SUMÁRIO

1 OBJETIVO

Estabelecer diretrizes para implementação de controles de acesso lógico para as redes de telecomunicações gerenciadas pelo DECEA em conformidade com a ROCA 20-7 "Regulamento do Departamento de Controle do Espaço Aéreo".

2 APLICAÇÃO

Esta Norma de Segurança da Informação é de aplicação no Departamento de Controle do Espaço Aéreo e suas Organizações Militares subordinadas.

3 DEFINIÇÕES

Os conceitos e definições estão listados na MCA 7-1 "Glossário de Segurança da Informação do DECEA".

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 CONTROLE DE ACESSO LÓGICO

Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso às informações.

3.2 REDE DE TELECOMUNICAÇÕES

Uma rede de telecomunicações pode ser composta de várias sub-redes, dependendo do tipo de serviço que é provido ao usuário final. As redes de telecomunicações estão sendo aperfeiçoadas para suportar a transmissão de informações com a introdução de novas tecnologias, tanto do lado dos equipamentos da rede (elementos de rede) quanto dos meios de transmissão (redes de transporte) e dos sistemas de operação para gerenciamento de Redes de Telecomunicações.

3.3 USUÁRIO

Servidor militar ou civil, prestador de serviço ou fornecedor do DECEA e das suas Organizações Militares subordinadas que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação, formalizada por meio da assinatura do Termo de Responsabilidade.

3.4 QUEBRA DE SEGURANÇA DA INFORMAÇÃO

Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

3.5 TERMO DE RESPONSABILIDADE

Termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e autenticidade e a legalidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

4 RESPONSABILIDADES

4.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

Estabelecer as diretrizes de controle de acesso lógico para as redes de telecomunicações e fiscalizar o cumprimento dessas diretrizes.

4.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO.

Implementar as diretrizes estabelecidas e comunicar à ASSICEA os incidentes de segurança da informação quando da ocorrência mediante ao não cumprimento das diretrizes de controle de acesso lógico.

5 DIRETRIZES PARA IMPLANTAÇÃO DAS REDES DE TELECOMUNICAÇÕES

5.1 GESTÃO DE ATIVOS

5.1.1 O DECEA e suas Organizações Militares subordinadas devem identificar e classificar os respectivos requisitos de segurança da informação dos ativos de informação.

5.1.2 Os requisitos de segurança da informação dos ativos de informação devem ser definidos por meio de critérios que atendam à disponibilidade, à integridade, à confidencialidade e à autenticidade da informação.

5.1.3 O inventário dos ativos de informação que compõem as redes de telecomunicações deve incluir todas as informações necessárias que permitam a recuperação de um ativo de informação após um incidente de segurança da informação grave ou um desastre, incluindo: identificar o valor de cada ativo de informação, tipo de ativo, formato, determinar com clareza e objetividade o conteúdo do ativo de informação, localização, informações sobre cópias de segurança da informação, informações sobre licenças, a classificação da informação deste ativo e a importância do ativo de informação para o negócio do DECEA.

5.1.4 Na elaboração e administração do inventário de ativos de informação deve-se identificar o(s) responsável(is) – proprietário(s) e custodiante(s) – de cada ativo de informação.

5.1.5 O inventário de ativos de informação deve ser completo, cobrindo todos os ativos de telecomunicações de valor, incluindo informações de recursos de rede, serviços e rede de aplicações.

5.1.6 Os requisitos de segurança da informação dos ativos de informação devem ser categorizados, no mínimo, em cinco categorias de controle de segurança da informação: a) tratamento da informação; b) controles de acesso físico e lógico; c) gestão de risco de segurança da informação; d) tratamento e resposta a incidentes de segurança da informação; e f) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação.

5.2 SEGURANÇA EM RECURSOS HUMANOS

5.2.1 Todo servidor militar ou civil, prestador de serviço ou fornecedor do DECEA e de suas organizações militares subordinadas, deve assinar o Termo de Responsabilidade para ser liberado o acesso aos recursos da rede de telecomunicações. Este Termo deve ser elaborado pela própria Organização Militar e armazenado de modo seguro.

5.2.2 Os direitos de acesso de todo servidor militar ou civil, prestador de serviço ou fornecedor do DECEA às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades.

5.3 GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

5.3.1 As Organizações Militares subordinadas ao DECEA devem elaborar um procedimento de segurança da informação para as atividades de sistemas associados a recursos de processamento e comunicação das informações, tais como procedimentos de inicialização e desligamento de computadores, geração de cópias de segurança da informação, manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e das salas de computadores.

5.3.2 Deve-se adotar a Norma de Segurança da Informação de Gestão de Mudanças para avaliação do impacto das alterações no ambiente e para controlar os recursos de processamento da informação e sistemas.

5.3.3 Deve ser estabelecido um procedimento de segurança da informação referente à administração e execução de funções ou áreas de responsabilidade críticas para o negócio do DECEA e suas organizações militares subordinadas mantendo a segregação de funções.

5.3.4 Os recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

5.3.5 Devem ser implantados nas redes de telecomunicações controles de segurança da informação para prevenir, detectar e remover código malicioso e controlar códigos móveis.

5.3.6 Um sistema centralizado para gerência de *software* de antivírus das redes de telecomunicações deve ser implantado.

5.3.7 Deve-se adotar a Norma de Segurança da Informação de Cópias de Segurança para todos os sistemas críticos das redes de telecomunicações.

5.3.8 Os ativos de informação presentes nas redes de telecomunicações devem ser monitorados e os eventos de segurança da informação devem ser registrados conforme orientação da ASSICEA.

5.3.9 O monitoramento das redes de telecomunicações deve ser utilizado para checar a eficácia dos controles de segurança da informação adotados e para verificar a conformidade com esta Norma de segurança da informação de controle de acesso lógico das redes de telecomunicações. Além disso, um sistema de controle, monitoração e restrição de acesso ao conteúdo da internet deve ser implementado nas redes de telecomunicações.

5.3.10 As conexões da rede com outras redes externas, principalmente a Internet, devem ser protegidas por controles de segurança da informação especificados pela ASSICEA.

5.3.11 Um sistema de prevenção de intrusos (IPS) e um sistema de detecção de intrusos (IDS) deve ser implementado nas redes de telecomunicações.

5.3.12 Uma solução de correlação de eventos de segurança da informação e um servidor de logs dedicado (Log Server) devem ser implementados nas redes de telecomunicações.

5.4 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

5.4.1 Deve ser elaborado um procedimento de segurança da informação para notificação e resposta dos diferentes tipos de incidentes de segurança da informação e fragilidades que possam ter impacto na segurança dos ativos de informação do DECEA e de suas Organizações Militares subordinadas.

5.4.2 Todos os servidores militares ou civis, prestadores de serviço ou fornecedores que desempenham atividades no âmbito do DECEA e das suas Organizações Militares subordinadas devem ser alertados sobre sua responsabilidade de notificar, o mais rapidamente possível, qualquer incidente de segurança da informação.

5.4.3 Deve ser criada uma equipe de resposta a incidente para avaliar, responder, tratar e aprender com incidentes de segurança da informação. Essa equipe deve ser autorizada a tomar decisões imediatas sobre como lidar com os incidentes de segurança da informação.

5.4.4 Todas as responsabilidades e procedimentos devem estar definidos para o manuseio efetivo de incidentes de segurança da informação e fragilidades, uma vez que estes tenham sido notificados.

5.4.5 Um processo de melhoria contínua deve ser aplicado a respostas, monitoramento, avaliação e gestão total de incidentes de segurança da informação.

5.5 GESTÃO DE CONTINUIDADE DO NEGÓCIO

5.5.1 Deve-se adotar o processo de gestão de continuidade do negócio para minimizar o impacto sobre o DECEA e de suas Organizações Militares subordinadas em recuperar perdas de ativos de informação a um nível aceitável, por meio da combinação de ações de prevenção e recuperação.

5.5.2 Os planos de continuidade de negócio devem tratar as vulnerabilidades das Organizações Militares subordinadas ao DECEA, que podem conter informações sensíveis e que necessitar de proteção adequada.

5.5.3 As Organizações Militares subordinadas ao DECEA devem considerar durante o desenvolvimento e implementação do plano de continuidade de negócio a inclusão de um plano de reabilitação de emergência dos serviços de telecomunicações que garantam as comunicações dos serviços de telecomunicações essenciais para as atividades operacionais do DECEA.

5.5.4 Os Planos de continuidade de negócio devem ser testados, reavaliados e melhorados, de forma a manter todas as informações atualizadas.

5.6 CONFORMIDADE

Na ocorrência de desastres naturais, acidentes e outras emergências ou riscos, as Organizações Militares subordinadas ao DECEA devem dar prioridade às comunicações essenciais para manter as atividades críticas do DECEA em operação.

5.7 DOCUMENTAÇÃO

Toda a infraestrutura das redes de telecomunicações deve ser documentada e mantida atualizada.

5.8 MEDIDAS DE SEGURANÇA DA INFORMAÇÃO DE REDES DE TELECOMUNICAÇÕES CONTRA ATAQUES CIBERNÉTICOS

5.8.1 PROTEÇÃO DOS RECURSOS DE REDE

5.8.1.1 Os recursos de telecomunicações devem estar protegidos apropriadamente. Assim, pode-se evitar interferências significantes à entrega dos serviços das redes de telecomunicações, causados por comportamento inesperado. Este pode ser provocado, intencionalmente ou não, por programas maliciosos distribuídos por usuários de serviços das redes de telecomunicações gerenciadas pelo DECEA.

5.8.1.2 Para proteger recursos de rede IP (como servidores e roteadores) de ataques cibernéticos (por exemplo, ataques de negação de serviços), as Organizações Militares subordinadas ao DECEA devem ter mecanismos para filtrar as comunicações ou limitar a banda de comunicação IP, portas de comunicação e protocolos de aplicação. Dependendo do serviço de telecomunicações, tais mecanismos de filtragem de comunicações devem ser implementados em associação ao controle de processamento de sinais, autenticação de usuários e controle de acesso.

5.8.2 MEDIDAS CONTRA PERSONIFICAÇÃO DE ORIGEM

5.8.2.1 As Organizações Militares subordinadas ao DECEA devem implementar controles de segurança da informação para proteção contra personificação de endereços IP (IP Spoofing).

5.8.2.2 Para prevenir personificação de uma origem por meios privilegiados, convém que controles de segurança da informação apropriados contra acesso não autorizado sejam implementados nos sistemas de informação provendo autenticação de usuários e introduzindo controles de senha e/ou funções de autenticação forte, por exemplo: uso obrigatório de senhas

imprevisíveis sob certo tamanho e a introdução de senha única e autenticação forte por dispositivos de senha única.

5.9 MEDIDAS DE SEGURANÇA PARA CONGESTIONAMENTO DE REDE

5.9.1 MECANISMO DE DETECÇÃO E LIMITAÇÃO DE CONGESTIONAMENTO DE REDE

5.9.1.1 Os equipamentos críticos de telecomunicações devem possuir mecanismos para detectar congestionamento de rede e evitar a concentração das comunicações no caso de um congestionamento de rede.

5.9.1.2 Deve-se prever a gestão de capacidade dos equipamentos das redes de telecomunicações ajustando os limites de desempenho dos equipamentos de comunicação e implementando mecanismos para controlar o número de comunicações antes de atingir este limite. Além disso, todo o tráfego da rede deve ser processado por equipamentos distribuídos, quando possível.

5.9.2 COLETA PRÉVIA DE INFORMAÇÕES QUE PODEM CAUSAR CONGESTIONAMENTO:

As Organizações Militares subordinadas ao DECEA devem elaborar um procedimento de segurança da informação para reportar a coleta prévia de informações e manter as pessoas necessárias informadas.

5.9.3 MEDIDAS PARA MELHORA TEMPORÁRIA DA CAPACIDADE

Deve-se considerar a escala de uma potencial paralisação ou desastre para a utilização de um centro de processamento distribuído de rede, com a instalação de equipamentos complementares e as mudanças necessárias na configuração dos ativos de informação para se adaptar, caso ocorra um incidente grave ou até mesmo um desastre interrompendo as operações críticas das Organizações Militares subordinadas ao DECEA. Esta ação poderá ser incorporada em uma estratégia de Gestão de Continuidade das Operações, a fim de manter a operacionalidade dos sistemas críticos em face de eventuais óbices na operação desses sistemas.

5.9.4 COLETA PRÉVIA DE INFORMAÇÕES QUE ALERTEM O MAU FUNCIONAMENTO

Uma vez que desastres, acidentes e fenômenos sociais tendem a ser as causas de falhas em equipamentos de telecomunicações e congestionamento de redes, as Organizações Militares subordinadas ao DECEA devem considerar a adoção de medidas de antecipação, previstas em Planos de continuidade de negócios, recolhendo informações relevantes e acumulando o conhecimento de forma regular.

6 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

6.1 CONTROLE DE ACESSO LÓGICO

6.1.1 Um procedimento de segurança da informação de concessão e revogação de direitos de acesso a sistemas e serviços deve ser definido e implantado pelas Organizações Militares subordinadas ao DECEA.

6.1.2 Os usuários devem estar cientes de suas responsabilidades em relação à guarda das senhas de acesso, pois o compartilhamento de senhas compromete a rastreabilidade das ações realizadas nos sistemas e expõe o usuário autorizado às responsabilidades por atos prejudiciais executados por outra pessoa. Deve ser solicitado aos usuários um termo de sigilo das senhas.

6.1.3 A autorização de cada privilégio concedido deve ser registrada de forma a gerar evidências de sua execução por parte dos responsáveis, mantendo a rastreabilidade para o caso de incidentes de segurança ou de auditorias e para que os privilégios possam ser reavaliados posteriormente.

6.1.4 As modificações nos privilégios de acesso dos usuários de sistemas do DECEA e das Organizações Militares subordinadas devem ser registradas de forma a gerar evidências do controle sobre a concessão adequada desses privilégios, mantendo a rastreabilidade para o caso de incidentes de segurança da informação ou de auditorias.

6.1.5 Os registros de modificações de privilégios de acesso devem ser verificados periodicamente de modo a garantir que os privilégios não foram concedidos de maneira equivocada ou não autorizada, além de manter o controle de expiração dos privilégios concedidos.

6.1.6 Um procedimento de segurança da informação para formação e uso de senhas de acesso, deve ser elaborado pelo DECEA e suas Organizações Militares subordinadas. Este procedimento deve ser revisado e aprovado pela ASSICEA.

6.1.7 Um procedimento de segurança da informação para os serviços de rede de telecomunicações deve ser elaborado pelo DECEA e suas Organizações Militares subordinadas. Este procedimento deve prevenir acesso não autorizado aos serviços de rede e especificar que os usuários somente recebam acesso para os serviços que tenham sido especificamente autorizados a usar.

6.1.8 Os acessos de usuários remotos às redes de telecomunicações devem ser autenticados por uma solução de VPN – Virtual Private Network implementada pelas Seções de Segurança de Sistemas de Informação presentes nas Organizações Militares subordinadas ao DECEA. A solução empregada deve estar em conformidade com a ICA 200-8 “Medidas de Segurança para Equipamentos Cripotécnicos e de Comunicações”.

6.1.9 Devem ser implantados mecanismos de identificação automática de equipamentos para autenticar conexões (Identificação de equipamento em redes).

6.1.10 As portas de diagnóstico e configuração devem ser protegidas contra acessos não autorizados (Proteção e configuração de portas de diagnóstico remotas).

6.1.11 As redes de telecomunicações devem ser segregadas em domínios lógicos e os seus serviços devem ser segregados em redes virtuais (Segregação de redes).

6.1.12 As restrições de conexões dos usuários às redes de telecomunicações devem ser implementadas (Controle de conexão de rede).

6.1.13 Um procedimento de segurança da informação de mecanismos seguros de *logon* deve ser implementado no acesso às redes de computadores (Procedimentos seguros de entrada no sistema – *logon*).

6.1.14 Os usuários devem ter um identificador único na rede de computadores (Identificação e autenticação de usuário).

6.1.15 Devem ser implementadas, nas redes de telecomunicações, técnicas de autenticação que permitam validar a identidade de um usuário (Identificação e autenticação de usuário).

6.1.16 Um sistema de gerenciamento e manutenção de senhas deve ser implementado nas redes de telecomunicações.

6.1.17 Os mecanismos de restrição para o uso de programas utilitários de sistemas devem ser implementados nas redes de telecomunicações (Uso de utilitários de sistema).

6.1.18 Mecanismos de desconexão e desligamento automáticos de estações de trabalho em locais de alto risco devem ser implementados nas redes de telecomunicações (Desconexão de terminal por inatividade).

6.1.19 O DECEA e suas Organizações Militares subordinadas devem implementar restrições de horário para conexão às redes de telecomunicações (Limitação de horário de conexão).

6.1.20 Um procedimento de segurança da informação de acesso às informações e funções dos sistemas de aplicação deve ser implementado nas redes de telecomunicações (Restrição de acesso à informação).

6.1.21 O DECEA e suas Organizações Militares subordinadas devem abrigar isoladamente os sistemas de aplicações sensíveis e relevantes para atingir a missão da organização militar (Isolamento de sistemas sensíveis).

6.2 ELABORAÇÃO E ADMINISTRAÇÃO DE CONTAS DE ACESSO

6.2.1 A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário.

6.2.2 Disponibilizar ao usuário, que não exerce funções de administração da rede local, somente uma única conta institucional de acesso, pessoal e intransferível.

6.2.3 Utilizar conta de acesso, no perfil de administrador, somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

6.2.4 O DECEA e suas Organizações Militares subordinadas devem responsabilizar o usuário pela quebra de segurança da informação ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de um Termo de Responsabilidade.

6.2.5 A criação de contas de serviço exige regras específicas vinculadas a um processo automatizado.

6.2.6 As Seções de Segurança de Sistemas de Informação devem estabelecer regras para credenciamento, bloqueio e exclusão de contas de acesso de seus usuários, bem como para o ambiente de desenvolvimento.

6.3 ATIVOS DE INFORMAÇÃO

6.3.1 O DECEA e suas Organizações Militares subordinadas devem utilizar ferramentas de proteção contra acesso não autorizado aos ativos de informação que favoreçam, preferencialmente, a administração de forma centralizada.

6.3.2 O DECEA e suas Organizações Militares subordinadas devem respeitar o princípio do menor privilégio, para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação conforme o RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica".

6.3.3 Utilizar ativo de informação homologado pela ASSICEA nas aplicações de controle de acesso e de tratamento das informações sigilosas.

6.3.4 Registrar eventos relevantes, previamente definidos, para a segurança da informação e rastreamento de acesso às informações sigilosas.

6.3.5 Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

6.3.6 O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.

6.3.7 As Seções de Segurança de Sistemas de Informação presentes nas Organizações militares subordinadas ao DECEA devem estabelecer regras para o uso da internet, do correio eletrônico e de mensagens instantâneas.

6.4 REDES DE TELECOMUNICAÇÕES

6.4.1 O DECEA e suas Organizações Militares subordinadas devem conceder credenciais de acesso à rede de telecomunicações após a data de contratação ou de entrada em exercício do usuário.

6.4.2 Excluir credenciais de acesso à rede de telecomunicações quando houver desligamento do usuário.

6.4.3 Registrar os acessos à rede de telecomunicações de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido pela Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo.

6.4.4 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem à rede de telecomunicações.

6.4.5 Manter, na rede de telecomunicações, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

6.4.6 Utilizar a legislação específica presente no RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica" para a concessão de acesso às informações sigilosas, no âmbito da rede de telecomunicações, por meio de canal seguro.

6.4.7 Gravar o acesso remoto à rede de telecomunicações em *logs* para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada.

7 REGISTROS GERADOS

Não aplicável.

8 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada constatando a implantação dos requisitos de segurança da informação nas redes de telecomunicações.

9 FLUXOGRAMA

Não aplicável.

10 DOCUMENTOS DE REFERÊNCIA

10.1 DCA 7-2 Política de Segurança da Informação do DECEA, 2010.

10.2 PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, 2010.

10.3 DCA 102-1 Requisitos Básicos das Redes de Comunicações do COMAER, 2008.

10.4 DCA 21-2 Diretriz para Implantação do Centro de Gerenciamento Técnico do SISCEAB, 2009.

10.5 RCA 205-1 Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica, 2006.

10.6 ROCA 20-7 Regulamento do Departamento de Controle do Espaço Aéreo, 2010.

10.7 ABNT NBR ISO/IEC 27002 Código de Práticas para a Gestão da Segurança da Informação, 2005.

11 ANEXOS

Não aplicável

Anexo F - Norma de Auditoria Interna de Conformidade de Segurança da Informação

SUMÁRIO

1 OBJETIVO

Garantir que o Departamento de Controle do Espaço Aéreo e suas unidades subordinadas operem continuamente, de acordo com as políticas, normas, procedimentos e instruções de trabalho determinados pelo Sistema de Gestão de Segurança da Informação.

2 APLICAÇÃO

Esta Norma inclui o planejamento, a elaboração de relatórios, a execução e o acompanhamento de uma auditoria interna do SGSI e se aplica ao DECEA e a todos as unidades subordinadas que fazem parte do Sistema de Gestão de Segurança da Informação.

3 DEFINIÇÕES

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

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 AUDITORIA

Processo sistemático, documentado e independente para obter evidências de auditoria e avaliá-las objetivamente, de modo a determinar a extensão na qual os critérios da auditoria são atendidos.

3.2 LISTA DE VERIFICAÇÃO

Questionário estruturado ou Plano de Trabalho para orientar e auxiliar os auditores nos testes das Organizações Militares a serem auditadas.

3.3 EVIDÊNCIA DE AUDITORIA

Informações recolhidas da unidade auditada, tais como: registros, documentos escritos, impressos de computador, entrevistas e observações.

3.4 OBSERVAÇÃO DE AUDITORIA

Recomendação da auditoria consultiva que tem o objetivo de melhorar o processo avaliado.

3.5 RECOMENDAÇÃO DE AUDITORIA

Ação corretiva que se propõe a abordar um ou mais itens de auditoria identificados, que devem ser abordados antes da certificação ou recertificação do Sistema de Gestão de Segurança da Informação.

3.6 PLANO DE AUDITORIA

Planejamento da auditoria, contemplando datas, envolvidos, unidades e auditores.

3.7 RELATÓRIO DE AUDITORIA

Relatório formal com os principais resultados e conclusões da auditoria.

3.8 RISCO DE AUDITORIA

Potencial de uma auditoria não cumprir os seus objetivos, por exemplo, pelo uso de informações não confiáveis, incompletas ou imprecisas.

3.9 PROGRAMAÇÃO DA AUDITORIA

Diário das auditorias planejadas por unidade.

3.10 ESCOPO DA AUDITORIA

Partes da Organização Militar que serão auditadas.

3.11 TESTE DE AUDITORIA

Verificação realizada pelos auditores para verificar se um controle é eficaz e adequado para mitigar um ou mais riscos para a organização.

3.12 PAPÉIS DE TRABALHO DOS AUDITORES

Documentos escritos, gravações e qualquer outra evidência gerada pelos auditores durante a auditoria, incluindo a lista de verificação.

3.13 AUDITORIA DE CONFORMIDADE

Tipo de auditoria específica para avaliar a extensão que a auditoria atingiu em conformidade com os requisitos estabelecidos.

3.14 AUDITORIA DO SGSI

Auditoria centrada na organização do Sistema de Gestão da Segurança da Informação (SGSI).

3.15 AUDITORIA BASEADA EM RISCO

Auditoria planejada com base em uma avaliação de análise de riscos.

4 RESPONSABILIDADES

4.1 DIRETOR–GERAL

Conceder autoridade para que o Representante da ASSICEA execute a auditoria.

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

4.2.1 Nomear um ou mais Auditores Líderes e as suas devidas Equipes de Auditoria (o representante da ASSICEA também pode ser o Auditor Líder).

4.2.2 Juntamente com o Auditor Líder, revisar as ações corretivas e preventivas e fazer seus devidos acompanhamentos, de acordo com o Relatório de Auditoria Interna.

4.2.3 Manter a confidencialidade das informações obtidas durante a auditoria.

4.3 AUDITOR LÍDER

4.3.1 Preparar um Plano de Auditoria para servir de base para a realização da auditoria.

4.3.2 Preparar um Plano de Notificação para servir de base para a divulgação dos resultados da auditoria.

4.3.3 Coordenar o planejamento da auditoria com as unidades, agendando data e hora com seus "coordenadores".

4.3.4 Planejar a auditoria, preparar os documentos de trabalho e repassar para a equipe de auditores.

4.3.5 Consolidar todas as evidências coletadas durante a auditoria e gerar o Relatório de Auditoria.

4.3.6 Alertar os setores auditados, com agilidade, sobre as não-conformidades críticas encontradas.

4.3.7 Coordenar a Reunião de Fechamento da Auditoria Interna.

4.4 GRUPO DE AUDITORES

4.4.1 Fornecer o suporte necessário ao Auditor Líder na realização da auditoria.

4.4.2 Realizar auditorias em setores com suporte da lista de verificação.

4.4.3 Levantar não-conformidades, recomendações ou observações.

4.4.4 Manter a confidencialidade das informações levantadas durante a auditoria.

4.4.5 Agir de forma ética durante todo o processo de auditoria.

4.5 AUDITADOS

4.5.1 Agendar e organizar com os membros da sua Organização Militar a data de auditoria, para que possa receber a equipe de auditores com prontidão.

4.5.2 Fornecer todas as informações necessárias para os auditores.

4.5.3 Receber o Relatório de Auditoria, planejar, agir e acompanhar as ações corretivas sugeridas.

5 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

5.1 DISPOSIÇÃO GERAL

5.1.1 Um programa de auditoria deve ser criado no início de cada ano contendo todas as auditorias programadas para o ano.

5.1.2 As auditorias internas devem ser programadas para ser realizadas pelo menos duas vezes ao ano.

5.1.3 O auditor interno deve ser uma pessoa sem relação com a Organização Militar subordinada ao DECEA que irá auditar. De preferência deve ser alguém da equipe da ASSICEA.

5.1.4 Todos os membros da equipe de auditoria interna devem ser designados pela ASSICEA.

5.1.5 O Auditor Líder deve fiscalizar as atividades de sua equipe.

5.1.6 Uma notificação de auditoria deve ser enviada para a unidade a ser auditada pelo menos quinze dias antes da auditoria.

5.2 PLANEJAMENTO E PREPARAÇÃO DA AUDITORIA

5.2.1 O programa de auditoria anual deve ser elaborado pela ASSICEA e deve ser aprovado pelo Diretor-Geral do DECEA.

5.2.2 O programa de auditoria anual deve incluir:

a) escopo e objetivo da auditoria;

b) unidades a serem auditadas e seus respectivos representantes;

c) membros da equipe auditora;

d) data, hora e local da auditoria; e

e) distribuição dos auditores em relação às unidades a serem auditadas.

5.3 REUNIÃO DE PREPARAÇÃO DE AUDITORIA

5.3.1 Uma reunião de preparação de auditoria deve ser realizada pelo menos uma semana antes do período de auditoria.

5.3.2 A reunião de preparação de auditoria deve tratar obrigatoriamente, entre outros assuntos, dos seguintes aspectos:

a) assegurar a disponibilidade de todos os recursos envolvidos;

b) verificar aspectos logísticos necessários; e

c) revisar o escopo.

5.4 REUNIÃO DE ABERTURA DE AUDITORIA

5.4.1 Antes do início do período de auditoria deve ser realizada uma reunião de abertura.

5.4.2 Para a reunião de abertura deve ser convocada a presença do auditor líder, da equipe auditora e dos representantes das Organizações Militares a serem auditadas.

5.4.3 A reunião de abertura de auditoria deve tratar, entre outros assuntos, dos seguintes aspectos:

a) objetivo e escopo da auditoria;

b) confirmação do plano de auditoria; e

c) esclarecimento e resolução de qualquer dúvida ou pendência.

5.5 EXECUÇÃO DA AUDITORIA

5.5.1 Os auditores devem realizar a auditoria utilizando os seguintes documentos como base:

a) Lista de Auditoria: contém elementos específicos que devem ser auditados em determinada organização, por exemplo, os documentos normativos de segurança da informação publicados pelo DECEA.

b) Lista de Requisitos do SGSI: contém elementos relacionados com os requisitos do SGSI da ABNT NBR ISO/IEC 27001:2006; e

c) Lista de Requisitos de Controles: contém elementos relacionados a controles encontrados no Apêndice A da ABNT NBR ISO/IEC 27001:2006.

5.5.2 Os resultados de auditoria devem ser coletados mediante entrevistas, análises de documentos e observações das atividades e devem ser anotados nas listas citadas no item acima.

5.5.3 Evidências de não-conformidades devem ser anotadas.

5.5.4 Recomendações ou observações que possam refletir positivamente sobre o SGSI também devem ser anotados.

5.6 RELATÓRIO DE AUDITORIA

5.6.1 As equipes de auditores devem fazer, para cada unidade auditada, uma reunião de consolidação.

5.6.2 A equipe de auditores deve analisar todos os resultados obtidos e classificar cada evidência como não-conformidades, recomendações ou observações.

5.6.3 Todas as não-conformidades, recomendações ou observações devem possuir sua devida evidência objetiva.

5.6.4 A reunião de consolidação geral deve contemplar os seguintes aspectos:

a) análise dos resultados;

b) consolidação de todas as conclusões;

c) classificação das conclusões; e

d) elaboração de relatório de recomendações e de auditoria.

5.6.5 A classificação dos resultados deve ser realizada observando os seguintes critérios:

5.6.5.1 Não-conformidades maiores:

a) quando um requisito do SGSI não é atendido;

b) quando um ou mais requisitos da ABNT NBR ISO/IEC 27001:2006 não é atendido; e

c) quando um requisito não atendido tem influência direta ao negócio.

5.6.5.2 Não-conformidades menores:

a) quando um ou mais requisitos da ABNT NBR ISO/IEC 27001:2006 é ou são parcialmente atendidos.

5.6.5.3 Recomendações:

a) quando um processo pode em algum contexto ocorrer na quebra dos requisitos de segurança da informação da ABNT NBR ISO/IEC 27001:2006.

5.6.5.4 Observações:

a) sugestões de melhorias no processo.

5.6.5.5 Resultados Positivos:

a) processo que vai além do que é exigido.

5.6.6 Os auditores devem seguir um código de conduta ao escrever suas conclusões, conforme os itens abaixo:

a) o relatório deve ser conciso e apresentado de modo construtivo;

b) os resultados devem estar dentro do escopo de auditoria; e

c) o relatório deve ser imparcial.

5.6.7 As informações geradas pelas equipes de auditoria devem ser consolidadas pelo seu Auditor Líder.

5.6.8 As informações geradas pelos auditores líderes devem ser consolidadas pela ASSICEA, gerando, assim, o Relatório de Auditoria Interna.

5.6.9 O relatório de auditoria deve ser mantido e controlado pela ASSICEA.

5.7 REUNIÃO DE FECHAMENTO

5.7.1 O Auditor Líder presidirá a reunião de fechamento junto com sua equipe de auditores.

5.7.2 O Auditor Líder deverá expor cada um dos resultados encontrados durante a auditoria.

5.7.3 Todos os presentes à reunião de fechamento devem garantir a confidencialidade dos itens tratados durante a mesma.

5.7.4 Todas as dúvidas e esclarecimentos devem ser resolvidos durante a reunião.

5.8 ACOMPANHAMENTO DE AÇÕES CORRETIVAS

5.8.1 Os responsáveis pelas Organizações Militares subordinadas ao DECEA que possuam necessidades de ações corretivas devem elaborar um plano para solucioná-las.

5.8.2 O prazo para execução de ações corretivas deve ser acordado com a ASSICEA.

5.8.3 A aprovação das ações corretivas deve ser realizada pela ASSICEA.

5.8.4 O Auditor Líder deve ficar responsável por validar se a ação corretiva foi realizada após o término de implantação.

5.8.5 O Auditor Líder deve fazer um segundo acompanhamento, 3 (três) meses após a implantação da ação corretiva, para verificar sua eficácia.

5.9 QUALIFICAÇÃO DOS AUDITORES

5.9.1 Os Auditores devem possuir atributos pessoais que lhes permitam agir em conformidade com os princípios da auditoria. Além disso, cada auditor deve ser:

a) Ético, justo, verdadeiro, sincero, honesto e discreto;

b) Disposto a considerar ideias, alternativas ou pontos de vista; e

c) Diplomático, observador, perceptivo, versátil, persistente e decisivo.

5.9.2 Os auditores devem possuir conhecimentos e habilidades específicas para:

a) aplicar princípios de auditoria;

b) planejar e organizar os trabalhos;

c) realizar auditoria dentro do prazo esperado;

d) coletar informações de forma eficiente;

e) preparar relatórios de auditoria; e

f) comunicar eficientemente.

5.9.3 Os auditores devem possuir conhecimentos em Situações Organizacionais. O conhecimento deve abranger:

a) estrutura, funções e relações; e

b) processos de negócios do DECEA.

5.9.4 Os auditores devem possuir conhecimentos de Sistema de Gestão de Segurança da Informação, como, por exemplo:

a) terminologia de segurança da informação;

b) princípios de segurança da informação; e

c) ferramentas de gestão de segurança da informação.

6 REGISTROS GERADOS

Não aplicável.

7 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada por meio da análise do documento de auditoria entregue pelo Auditor Líder.

8 FLUXOGRAMA

Não aplicável.

9 DOCUMENTOS DE REFERÊNCIA

9.1 DCA 7-2 Política de Segurança da Informação do DECEA, 2010.

9.2 DCA 14-8 Política de Segurança da Informação do COMAER, 2006.

9.3 PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, 2010.

9.4 ABNT NBR ISO 19011 Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental, 2002.

9.5 ABNT NBR ISO/IEC 27001 Sistema de Gestão de Segurança da Informação, 2006.

10 ANEXOS

Não aplicável.

Anexo G - Norma de Gerenciamento de Configuração

SUMÁRIO

1 OBJETIVO

Identificar, controlar e auditar os elementos de Tecnologia da Informação e os ativos de informação (*hardware*, *software*, documentação, licenças etc.), mantendo uma base de dados (designada por CMDB – *Configuration Management Data Base*) com o objetivo de fornecer informação segura e atualizada sobre os itens de configuração (IC).

2 APLICAÇÃO

Esta Norma de Segurança da Informação é de aplicação no Departamento de Controle do Espaço Aéreo e suas Organizações subordinadas.

3 DEFINIÇÕES

Os conceitos e definições estão listados na MCA 7-1 "Glossário de Segurança da Informação do DECEA".

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 GERENCIAMENTO DE CONFIGURAÇÃO

Processo de gerenciamento de configurações em ativos de tecnologia da informação.

3.2 IC – ITENS DE CONFIGURAÇÃO

São todos os componentes de TI e os serviços prestados com eles. Podem incluir PC, *software*, componentes de rede, servidores, documentação, procedimentos e todos os outros componentes de TI que a organização utiliza.

3.3 CMDB – *CONFIGURATION MANAGEMENT DATABASE*

É a base de dados que registra todos os IC mantendo os seus registros em termos das suas versões, situações e relações entre eles (por exemplo, um gravador de DVD que faz parte de um dado PC ou ainda um dado *software* que está instalado num determinado servidor).

4 RESPONSABILIDADES

4.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

Elaborar as diretrizes para o gerenciamento de configurações e fiscalizar o cumprimento desta Norma.

4.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Implementar as diretrizes presentes nesta Norma.

5 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

5.1 PLANEJAMENTO DO GERENCIAMENTO DE CONFIGURAÇÕES

5.1.1 Determinar o objetivo e a extensão do Gerenciamento de Configuração;

5.1.2 Examinar e entender as instruções existentes, padrões e processos a respeito das organizações subordinadas ao DECEA;

5.1.3 Desenvolver a nomenclatura para os itens de configuração (IC), se não existirem;

5.1.4 Estabelecer um fluxo de trabalho para processos operacionais;

5.1.5 Especificar uma base de tempo e um processo para a implantação das atividades do Gerenciamento da Configuração (identificação da configuração, checagem, documentação do status das mudanças, auditorias);

5.1.6 Analisar os requisitos de integração com o uso de produtos de terceiros; e

5.1.7 Criar o desenho do sistema de gerenciamento da configuração (CMDB, localização, as interfaces para o sistema, as ferramentas de suporte etc).

5.2 IDENTIFICAÇÃO DA CONFIGURAÇÃO

A configuração da infraestrutura da Tecnologia da Informação deve ser dividida em itens de configuração (IC) identificados sem ambiguidade, de modo que estes possam ser verificados eficazmente, monitorados e reportados de acordo com os requisitos do negócio. O grau de detalhe deve ser determinado da forma mais eficiente, em linha com os requisitos práticos e individuais da instituição.

5.3 CONTROLE DOS ITENS DE CONFIGURAÇÃO (IC)

5.3.1 Registro dos novos IC e suas versões.

5.3.2 Documentar as mudanças dos IC (atualização do status, mudanças dos atributos do IC, mudanças das responsabilidades, controle de licença, relacionamento com outros IC etc).

5.3.3 Documentar IC modificados com base nas mudanças efetuadas.

5.3.4 Proteger a integridade de dados da configuração.

5.4 PROVA DE STATUS DA CONFIGURAÇÃO

5.4.1 A prova do status é fornecida periodicamente em forma de relatórios. Como regra geral, envolve a seguinte informação:

5.4.1.1 Identificação única dos itens de configuração incluindo o status atual (instalado, em testes, em desenvolvimento etc.);

5.4.1.2 A linha de base da configuração, a liberação e seu status atual;

5.4.1.3 Nome do responsável pelas mudanças; e

5.4.1.4 Para os problemas não solucionados, devem ser encaminhadas requisições para mudança, de acordo com o estabelecido no Anexo C – Norma de Gestão de Mudanças desta Instrução em relação aos itens individuais de configuração.

5.5 VERIFICAÇÃO DA CONFIGURAÇÃO E AUDITORIA

5.5.1 Confirmar que os processos da gerência da configuração são aderentes aos objetivos planejados;

5.5.2 Confirmar que a consistência e a integridade dos dados estejam asseguradas; e

5.5.3 Confirmar que as mudanças em itens de configuração sejam incorporadas de uma maneira oportuna, conforme determinado no Anexo C – Norma de Gestão de Mudanças desta ICA.

6 REGISTROS GERADOS

Não aplicável.

7 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada constatando que todos os requisitos do item 5.5 foram cumpridos.

8 FLUXOGRAMA

Não aplicável.

9 DOCUMENTOS DE REFERÊNCIA

9.1 DCA 7-2 Política de Segurança da Informação do DECEA, 2010.

9.2 PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, 2010;

9.3 PCA 7-14 Plano Diretor de Tecnologia da Informação do DECEA, 2010;

10 ANEXOS

Não aplicável.

Anexo H - Norma de Gestão de Incidentes de Segurança da Informação

SUMÁRIO

1 OBJETIVO

Disciplinar a gestão de incidentes de segurança da informação no Departamento de Controle do Espaço Aéreo e suas Organizações Subordinadas.

2 APLICAÇÃO

Esta Norma de Segurança da Informação é de aplicação no Departamento de Controle do Espaço Aéreo e suas Organizações Militares subordinadas.

3 DEFINIÇÕES

Os conceitos e definições estão listados na MCA 7-1 "Glossário de Segurança da Informação do DECEA".

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 EVENTO DE SEGURANÇA DA INFORMAÇÃO

É a ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles de segurança da informação, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

3.2 INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Um incidente de segurança da informação é indicado por um único ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

3.3 ETIR – EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES DE TELECOMUNICAÇÕES E SISTEMAS DE INFORMAÇÃO

Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes de telecomunicações e sistemas de informação.

3.4 TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

É o serviço que consiste em receber, filtrar, classificar e responder a solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

4 RESPONSABILIDADES

4.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

4.1.1 Elaborar as diretrizes para a gestão de incidentes de segurança da informação e fiscalizar o cumprimento desta Norma.

4.1.2 O Chefe da ASSICEA é o responsável pela Gestão de Incidentes de Segurança da Informação no DECEA e em suas Organizações Militares subordinadas, bem como pelo relacionamento com o CTIR.FAB.

4.1.3 Com o advento da ocorrência de um incidente de segurança da informação grave, deve acionar o CTIR.FAB para ser informado ao CTIR.GOV e este comunique às autoridades policiais competentes para a adoção dos procedimentos legais quando julgar necessário.

4.1.4 Gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes de Telecomunicações e Sistemas de Informação – ETIR, no DECEA em suas Organizações Militares subordinadas.

4.1.5 Indicar o Chefe da Equipe de Tratamento e Resposta a Incidentes em Redes de Telecomunicações e Sistemas de Informação (ETIR) no DECEA.

4.2 SSSI - SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

4.2.1 Seguir as diretrizes desta Norma no processo de Gestão de Incidentes de Segurança da Informação.

4.2.2 Comunicar a ocorrência de incidentes de segurança da informação em redes de telecomunicações e sistemas de informação à ASSICEA, com o objetivo de permitir que sejam aplicadas soluções integradas, bem como a geração de estatísticas.

4.2.3 Tratar os incidentes de segurança da informação que acontecerem no âmbito da sua Organização Militar em conformidade com as diretrizes da ASSICEA.

5 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

5.1 DIRETRIZES DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

5.1.1 NOTIFICAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

O DECEA deve assegurar que as fragilidades e eventos de segurança da informação associados aos sistemas de informação nas redes de telecomunicações sejam comunicados, permitindo a tomada de ações corretivas em tempo hábil.

5.1.2 NOTIFICANDO FRAGILIDADES DE SEGURANÇA DA INFORMAÇÃO

5.1.2.1 Todos os servidores militares e civis, prestadores de serviço e fornecedores de sistemas e serviços de informação devem ser instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços nas redes de telecomunicações do DECEA.

5.1.2.2 O mecanismo de notificação deve ser fácil, acessível e disponível sempre que possível, para que ocorra a notificação de eventos de segurança da informação. Recomenda-se colocar um *link* na página *web* da Organização Militar com um formulário disponível para o usuário relatar o incidente de segurança da informação.

5.1.2.3 Todos os servidores militares e civis, prestadores de serviço e fornecedores devem receber treinamento para a notificação de incidentes de segurança da informação.

5.1.3 RESPONSABILIDADES E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

5.1.3.1 A equipe de tratamento de incidentes deve elaborar um procedimento de segurança da informação para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

5.1.3.2 As responsabilidades de todos os servidores militares e civis, prestadores de serviço e fornecedores devem estar estabelecidas em um procedimento de segurança da informação.

5.1.4 APRENDENDO COM OS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

5.1.4.1 Devem ser estabelecidos mecanismos para permitir que indicadores dos tipos, quantidade, impactos e custos dos incidentes de segurança da informação sejam quantificados e monitorados nas redes de telecomunicações do DECEA e em sistemas de informação administrados pelo DECEA.

5.1.5 COLETA DE EVIDÊNCIAS DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

5.1.5.1 Durante o tratamento de um incidente de segurança da informação as evidências devem ser coletadas e armazenadas em conformidade com o Anexo B –Norma de Gestão de Cópias de Segurança da Informação desta ICA.

5.1.5.2 Um procedimento de segurança da informação deve ser elaborado para a atividade de coleta e apresentação de evidências com o propósito de estabelecer uma ação disciplinar para os incidentes de segurança da informação tratados no âmbito do DECEA e em suas Organizações Militares subordinadas.

5.2 DIRETRIZES DA EQUIPE DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DO DECEA

5.2.1 FUNDAMENTOS LEGAIS

5.2.1.1 Conforme preconizada a ROCA 20-7 “Regulamento do Departamento do Controle do Espaço Aéreo”, o DECEA têm a competência de gerenciar as atividades relacionadas com o controle do espaço aéreo, com a proteção ao voo, com o serviço de busca e salvamento e com

as telecomunicações do COMAER, proporcionando, também, o apoio logístico e a segurança de sistemas de informação necessários à realização dessas atividades. Consoante a ROCA 20-7, o DECEA deve ser o responsável por gerenciar os incidentes de segurança da informação nas redes de telecomunicações do COMAER e nos sistemas de informação administrados pelo DECEA.

5.2.1.2 Conforme preconizado na DCA 7-2 "Política de Segurança da Informação do DECEA" no item 6.15, o DECEA deve desempenhar e manter uma estrutura que promova atividades de gerenciamento de incidentes de segurança da informação em todas as suas Organizações Subordinadas; sendo assim, a criação de uma Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação em Redes de Telecomunicações e Sistemas de Informação, mundialmente conhecido como CSIRT® (do inglês *Computer Security Incident Response Team*) se faz necessária para implantar esta diretriz. Além disso, é necessário monitorar os ativos críticos do DECEA trabalhando proativamente, prevendo as medidas antes que um incidente aconteça, e acionar um plano de continuidade para tratar um incidente grave, garantindo assim a continuidade das operações no DECEA.

5.2.1.3 A criação das equipes de tratamento de incidentes de segurança da informação tem como fundamento legal a Norma Complementar nº 05/IN01/DSIC/GSIPR – Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), em conjunto com o 5º objetivo contido no PCA 7-11 "Plano Diretor de Segurança da Informação no DECEA".

5.2.2 DEFINIÇÃO DA MISSÃO DA ETIR

5.2.2.1 Prover a proteção e a defesa das redes de telecomunicações e sistemas de informação administrados pelo DECEA contra ataques cibernéticos visando Integrar Monitoramento, Análise, Controle, Gerenciamento e Resposta aos Sistemas de Informação do DECEA.

5.2.3 MODELO DE IMPLEMENTAÇÃO

5.2.3.1 O Chefe da ASSICEA deverá indicar o Oficial que será o chefe da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação em Redes de Telecomunicações e Sistemas de Informação administrados pelo DECEA.

5.2.3.2 Este Oficial será o responsável por elaborar os procedimentos de segurança da informação referentes à missão do ETIR, gerenciar as atividades e distribuir tarefas para a equipe ETIR.

5.2.3.3 A Equipe gerencial deverá ficar alocada no Rio de Janeiro, de preferência no núcleo do Centro de Gerenciamento Técnico do Sistema de Controle do Espaço Aéreo Brasileiro, conforme preconiza a DCA 21-2. A referida Equipe prestará serviço para todas as organizações militares no âmbito do Estado do Rio de Janeiro, a fim de fornecer ações integradas e indicadores de desempenho para a direção do DECEA.

5.2.3.4 Para garantir o perfeito funcionamento das redes de telecomunicações e dos sistemas de informação administrados pelo DECEA, esta Equipe gerencial deverá exercer as suas atividades em regime 24 por 7 (24 horas por dia nos 7 dias da semana).

5.2.3.5 As Organizações Militares: CINDACTA I, CINDACTA II, CINDACTA III, CINDACTA IV, SRPV-SP, ICEA, PAME-RJ, CISCEA, ICA, CGNA, 1º GCC e GEIV, por meio da SSSI – Seção de Segurança de Sistemas de Informação –, deverão tratar os incidentes

de segurança da informação reportando todas as ações para o Centro Gerencial da ETIR, no Rio de Janeiro, e para a Assessoria de Segurança de Sistemas da Informação do Controle do Espaço Aéreo.

5.2.3.6 As Equipes distribuídas nas seguintes Organizações Militares: CINDACTA I, CINDACTA II, CINDACTA III, CINDACTA IV, SRPV-SP, ICEA, PAME-RJ, CISCEA, ICA, CGNA, 1º GCC e GEIV serão responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade.

5.2.3.7 A Equipe gerencial situada no Rio de Janeiro será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes descentralizadas situadas nas seguintes Organizações Militares: CINDACTA I, CINDACTA II, CINDACTA III, CINDACTA IV, SRPV-SP, ICEA, PAME-RJ, CISCEA, ICA, CGNA, 1º GCC e GEIV, além de ser a responsável, perante todo o COMAER, pelas informações que serão distribuídas para o Chefe da ASSICEA comunicar ao CTIR.FAB.

5.2.4 AUTONOMIA DA ETIR

5.2.4.1 Nesse primeiro momento de implementação da ETIR, o seu modelo de autonomia será compartilhada, na qual a Equipe trabalhará em acordo com os outros setores do DECEA a fim de participar do processo de tomada de decisão sobre quais medidas devem ser adotadas. Assim que obtiver maior maturidade no processo de gerenciamento, a autonomia do seu trabalho poderá ser atualizada para uma autonomia completa, ou seja, não precisará consultar outras áreas do DECEA ou de suas Organizações Militares subordinadas para tomar algum tipo de ação ou decisão no tratamento de incidentes de segurança da informação.

5.2.4.2 A ETIR participará no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório. Neste caso, a Equipe poderá recomendar os procedimentos de segurança da informação a serem executados ou as medidas de recuperação durante um ataque cibernético e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros do DECEA e de suas Organizações Militares subordinadas.

5.2.4.3 O Oficial chefe da ETIR deverá indicar os membros do processo decisório e definir explicitamente em um procedimento de segurança da informação suas responsabilidades nesse processo.

5.2.4.4 A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança da informação ocorridos no DECEA e em suas Organizações Subordinadas ao Chefe da ASSICEA, que fará a integração com o CTIR.FAB, e este fará a integração com o CTIR.GOV a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

6 REGISTROS GERADOS

Não aplicável.

7 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada constatando que todas as diretrizes do item 5.1 foram cumpridas.

8 FLUXOGRAMA

Não aplicável.

9 DOCUMENTOS DE REFERÊNCIA

9.1 DCA 7-2 Política de Segurança da Informação do DECEA, de 2010.

9.2 DCA 21-2 Diretriz para Implantação do Centro de Gerenciamento Técnico do SISCEAB, de 2009.

9.3 ROCA 20-7 Regulamento do Departamento de Controle do Espaço Aéreo, de 2010.

9.4 ABNT NBR ISO/IEC 27002 Código de Práticas para a Gestão da Segurança da Informação, de 2005.

9.5 ISO/IEC 18044:2004 Tecnologia da Informação – Técnicas de segurança – Gestão de Incidentes de Segurança da Informação, de 2004.

10 ANEXOS

Não aplicável.