MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-27

PROCESSO DE GESTÃO DE VULNERABILIDADES DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

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

TECNOLOGIA DA INFORMAÇÃO

ICA 7-27

PROCESSO DE GESTÃO DE VULNERABILIDADES DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

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

PORTARIA DECEA Nº 91/DGCEA, DE 2 DE AGOSTO DE 2013.

Aprova a edição da Instrução relativa ao Processo de Gestão de Vulnerabilidades de Ativos de Tecnologia da Informação do Departamento de Controle do Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere o art. 195, inciso IV, do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1049/GC3, de 11 de novembro de 2009, e o art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 369/GC3, de 9 de junho de 2010, resolve:

Art. 1º Aprovar a edição da ICA 7-27 "Processo de Gestão de Vulnerabilidades de Ativos de Tecnologia da Informação do Departamento de Controle do Espaço Aéreo", que com esta baixa.

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

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

(Publicado no BCA nº 163, de 26 de agosto de 2013.)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES 7
1.1 FINALIDADE 7
1.2 ÂMBITO E GRAU DE SIGILO 7
1.3 ABREVIATURAS 7
1.4 DEFINIÇÕES 7

2 DESCRIÇÃO DO DOCUMENTO 8
2.1 UTILIZAÇÃO 8

3 RESPONSABILIDADES 9
3.1 SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA 9
3.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO 9
3.3 PROPRIETÁRIO DOS ATIVOS DE INFORMAÇÃO 9
3.4 ELO DE SERVIÇO DE TI 9

4 PROCESSO DE GESTÃO DE VULNERABILIDADES DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO 10
4.1 DESCRIÇÃO DO PROCESSO 10
4.2 CONTROLE E MATURIDADE DO PROCESSO 10
4.3 FATORES CRÍTICOS DE SUCESSO 12

5 DESCRIÇÃO DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO 13
5.1 VISÃO GERAL DO PROCESSO 13
5.2 SUBPROCESSO “PLANEJAR EXECUÇÃO” 14
5.3 SUBPROCESSO “EXECUTAR ANÁLISE” 15
5.4 SUBPROCESSO “DEFINIR AÇÕES” 16
5.5 SUBPROCESSO “MELHORIA CONTÍNUA” 17

6 DISPOSIÇÕES FINAIS 19

REFERÊNCIA 20

Anexo A - GVUL01 – Planejamento da Análise 21
Anexo B - GVUL02 – Vulnerabilidades Identificadas 22
Anexo C - GVUL03 – Ações para Tratamento de Vulnerabilidades 23
Anexo D - GVUL04 – Identificação, Quantificação e Análise dos Indicadores do Processo 24

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução visa normatizar e estabelecer responsabilidades quanto ao Processo de Gestão de Vulnerabilidades de Ativos de Tecnologia da Informação aplicado no Departamento de Controle do Espaço Aéreo e suas Organizações Militares Subordinadas.

1.2 ÂMBITO E GRAU DE SIGILO

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

1.3 ABREVIATURAS

DECEA	–	Departamento de Controle do Espaço Aéreo
GVUL	–	Gestão de Vulnerabilidades de Ativos de Tecnologia da Informação
OM	–	Organização Militar
SDTE	–	Subdepartamento Técnico do DECEA
SSSI	–	Seção de Segurança de Sistemas da Informação
TI	–	Tecnologia da Informação

1.4 DEFINIÇÕES

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

Para efeito desta Instrução, entende-se por:

1.4.1 ATIVO DE INFORMAÇÃO

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

1.4.2 GESTÃO DE VULNERABILIDADES

Sistemática para obter informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliando a exposição da Organização Militar a estas vulnerabilidades e tomar as medidas apropriadas para lidar com os riscos associados (Fonte: ABNT NBR ISO/IEC 27002:2005).

1.4.3 VULNERABILIDADE

Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (Fonte: ABNT NBR ISO/IEC 27002:2005).

2 DESCRIÇÃO DO DOCUMENTO

2.1 UTILIZAÇÃO

2.1.1 Como pré-condição para a utilização deste Processo, as Organizações Militares devem estar estruturadas de acordo com o estabelecido pelo Plano Diretor de Segurança da Informação do DECEA (PCA 7-11), ou seja, devem possuir uma Seção de Segurança de Sistemas da Informação (SSSI) responsável pela garantia do cumprimento da Política de Segurança da Informação do DECEA (DCA 7-2).

2.1.2 As Seções de Segurança de Sistema da Informação de cada OM devem seguir as diretrizes estabelecidas pela Instrução aqui apresentada e pelos documentos normativos de segurança da informação dela derivados.

3 RESPONSABILIDADES

3.1 SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA

3.1.1 Normatizar e manter atualizado o Processo de Gestão de Vulnerabilidades de Ativos de Tecnologia da Informação no âmbito do DECEA.

3.1.2 Acompanhar o processo de implantação das ações corretivas e preventivas.

3.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO

3.2.1 Aprovar as ações corretivas e preventivas.

3.2.2 Analisar e avaliar as vulnerabilidades.

3.2.3 Definir e implantar ações corretivas e preventivas.

3.2.4 Apoiar o SDTE na geração de indicadores.

3.3 PROPRIETÁRIO DOS ATIVOS DE INFORMAÇÃO

3.3.1 Acompanhar o processo de implantação das ações corretivas e preventivas.

3.4 ELO DE SERVIÇO DE TI

3.4.1 Responsável por executar a implementação das ações corretivas e preventivas.

4 PROCESSO DE GESTÃO DE VULNERABILIDADES DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

4.1 DESCRIÇÃO DO PROCESSO

4.1.1 De acordo com o item 4.1.4, letra "g", 23, do Plano Diretor de Segurança da Informação do Departamento de Controle do Espaço Aéreo, está prevista a criação de uma estrutura de gestão de vulnerabilidades em sistemas de informação instalados no âmbito do DECEA, visando reduzir riscos resultantes de vulnerabilidades conhecidas. Adicionalmente, o item 6.17 da Política de Segurança da Informação do Departamento de Controle do Espaço Aéreo estabelece que o DECEA deve estruturar-se para promover atividades de gestão de riscos de segurança da informação em todas as Organizações Subordinadas, com vistas ao levantamento do impacto e probabilidades de ocorrência dos referidos riscos nos ativos de informação, bem como para identificar ameaças associadas às vulnerabilidades destes ativos, medir os níveis de risco e selecionar os controles necessários ao seu tratamento. Portanto, faz-se necessário o estabelecimento de um processo para gestão de vulnerabilidades nas Organizações Subordinadas, a fim de padronizar os procedimentos correlatos.

4.1.2 O processo de gestão de vulnerabilidades permite identificar falhas de segurança em tempo hábil, e, ao promover ações imediatas de melhoria na infraestrutura de Tecnologia da Informação, aplicações web, sistemas e processos, a Organização poderá antecipar-se ao risco de ataques.

4.2 CONTROLE E MATURIDADE DO PROCESSO

4.2.1 MEDIÇÃO DO NÍVEL DE MATURIDADE

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

0 – Não Existente: A Organização não considera os impactos no negócio associados a vulnerabilidades de segurança e a incertezas de projetos de desenvolvimento. O gerenciamento de vulnerabilidades não tem sido identificado como relevante para a aquisição de soluções e entrega de serviços de TI.

1 – Inicial/*Ad Hoc*: As vulnerabilidades e riscos de TI são considerados e tratados de maneira *Ad Hoc*. As vulnerabilidades relacionadas à TI são eventualmente tratadas. Existe um entendimento emergente de que as vulnerabilidades são importantes e precisam ser tratadas.

2 – Repetível e Intuitivo: Uma abordagem de avaliação de vulnerabilidades imatura e em desenvolvimento existe e é implementada. O gerenciamento de vulnerabilidades é normalmente de alto nível e é tipicamente aplicado apenas a projetos importantes ou em resposta a problemas. Os processos de correção das vulnerabilidades estão no início de sua implementação.

3 – Processo Definido: O gerenciamento de vulnerabilidades segue um processo definido e documentado. As decisões para acompanhar o processo de gerenciamento de vulnerabilidades e receber treinamento são deixadas a critério individual. A metodologia para a avaliação de vulnerabilidades é convincente e bem estruturada e garante que os principais riscos para o negócio sejam identificados. Um processo para corrigir as vulnerabilidades é normalmente instituído.

4 – Gerenciado e Mensurável: A avaliação e o gerenciamento de vulnerabilidades são procedimentos padronizados. As exceções ao processo de gerenciamento de vulnerabilidades são relatadas. As vulnerabilidades são avaliadas em termos de projeto individual e também regularmente a respeito da operação de TI como um todo. Existe a capacidade de monitorar a posição dos riscos associados às vulnerabilidades e tomar decisões informadas referentes à exposição que se deseja assumir. Todas as vulnerabilidades identificadas têm um proprietário nomeado. Além disso, um banco de dados de gerenciamento de vulnerabilidades é estabelecido, e parte dos processos de gerenciamento de vulnerabilidades é automatizado.

5 – Otimizado: O gerenciamento de vulnerabilidades já alcançou um estágio no qual há processo estruturado, executado e bem gerenciado. Boas práticas são aplicadas no contexto organizacional. A busca, a análise e o relatório de dados de gerenciamento de vulnerabilidades são automatizados.

4.2.1.2 A tabela 1 apresenta as metas para a evolução dos níveis de maturidade:

Tabela 1 - Metas para a Evolução dos Níveis de Maturidade

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

4.2.2 ACOMPANHAMENTO DO PROCESSO POR INDICADORES

Tabela 2 – Acompanhamento do Processo

Objetivos do Processo	Indicadores do Processo
• Reduzir a ocorrência e o impacto das vulnerabilidades técnicas; e • Aprovar planos de ação com custos eficientes para vulnerabilidades críticas.	• Quantidade de novas vulnerabilidades identificadas (comparado com o exercício anterior); • Quantidade de vulnerabilidades identificadas por nível de criticidade; e • Percentual de vulnerabilidades críticas identificadas que possuem planos de ação desenvolvidos.

4.3 FATORES CRÍTICOS DE SUCESSO

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

a) garantir cumprimento das responsabilidades atribuídas no processo;

b) garantir cumprimento dos procedimentos relacionados ao processo;

c) acompanhamento da situação do processo e apresentação de relatórios periódicos;

d) garantir comunicação eficiente e eficaz do processo para todas as partes interessadas e envolvidas; e

e) garantir constante atualização quanto ao surgimento de novas vulnerabilidades e técnicas associadas a sua exploração.

5 DESCRIÇÃO DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

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

5.1 VISÃO GERAL DO PROCESSO

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

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

5.1.3 No caso do processo de gestão de vulnerabilidades em tela, ele é composto por 4 (quatro) subprocessos a seguir descritos: Planejar Execução, Executar Análise, Definir Ações e Melhoria Contínua, conforme ilustrado na figura 1.

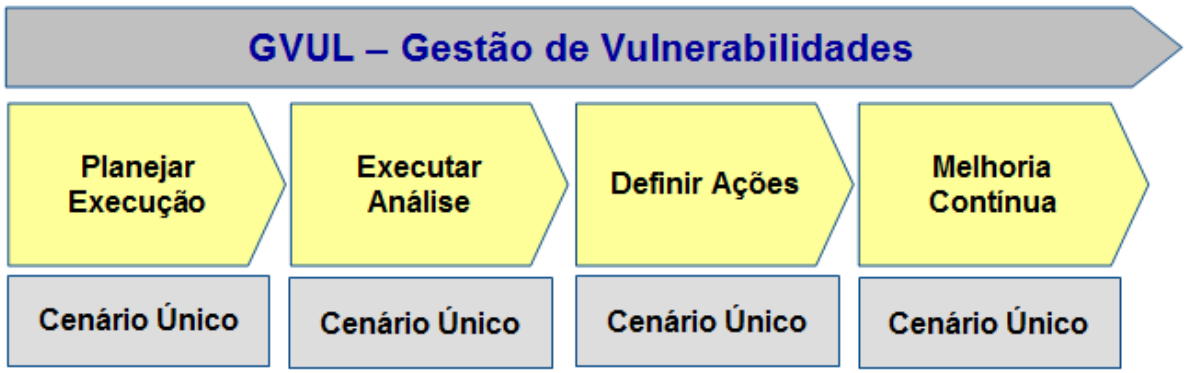

Figura 1 - Visão Geral do Processo de Gestão de Vulnerabilidades

5.2 SUBPROCESSO “PLANEJAR EXECUÇÃO”

5.2.1 Este subprocesso, ilustrado na figura 2, trata do planejamento da execução da análise de vulnerabilidades no ambiente tecnológico.

5.2.2 Neste subprocesso, deverá ser identificado o escopo da análise, os riscos envolvidos da execução e o plano de comunicação para as partes envolvidas.

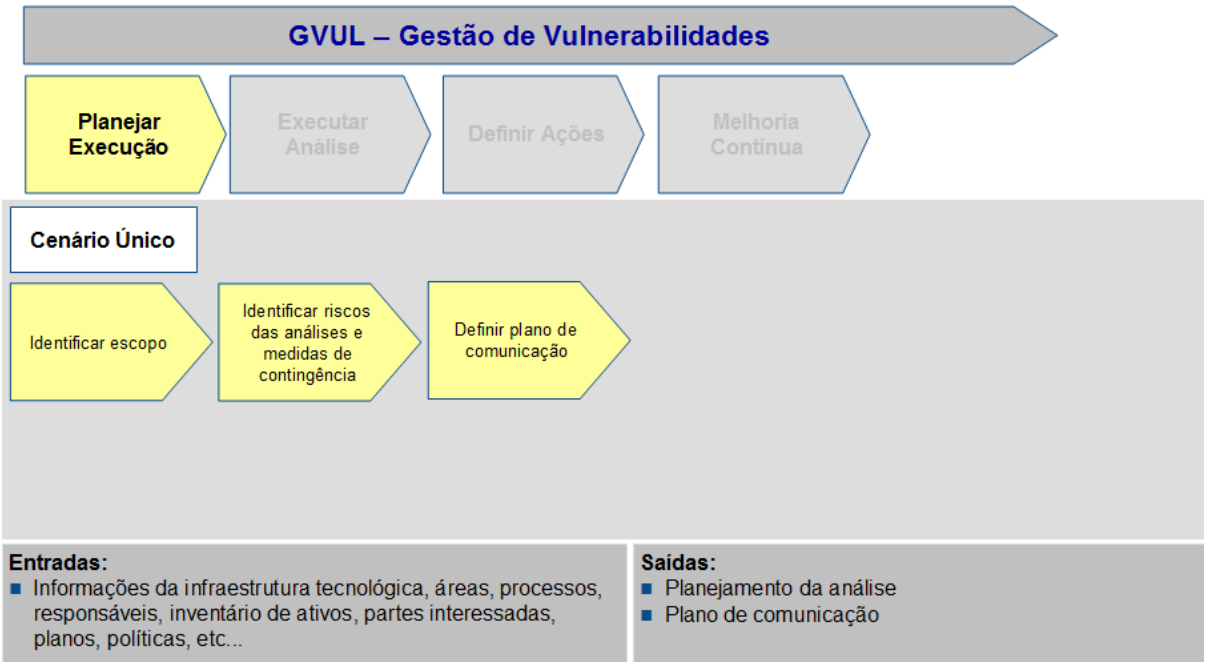

Figura 2 - Subprocesso para Planejar Execução

5.2.3 ETAPA “IDENTIFICAR ESCOPO”

5.2.3.1 Nesta etapa, devem ser inseridas as informações da análise de vulnerabilidade com o nome do elaborador do relatório da análise e o período da execução da mesma.

5.2.3.2 Esta etapa tem como objetivo identificar o escopo (interno e externo) da análise de vulnerabilidades. Deverão ser identificados:

a) ativos de informação;

b) localização (física e lógica); e

c) responsáveis (proprietário e custodiante).

5.2.3.3 Estas informações deverão ser transcritas nos itens 1 e 3 do documento Planejamento da Análise (GVUL01), conforme modelo do Anexo A.

5.2.4 ETAPA "IDENTIFICAR RISCOS DAS ANÁLISES E MEDIDAS DE CONTINGÊNCIA"

5.2.4.1 Uma vez identificado o escopo da análise de vulnerabilidades, é necessária a realização de uma análise de riscos em função das vulnerabilidades para avaliar os impactos das implantações dos respectivos controles de segurança.

5.2.4.2 Estas informações deverão ser transcritas no item 3 do documento Planejamento da Análise (GVUL01), padronizado no Anexo A.

5.2.5 ETAPA "DEFINIR PLANO DE COMUNICAÇÃO"

5.2.5.1 Durante a fase de planejamento da análise é necessário definir um plano de comunicação das áreas e responsáveis pelos ativos de informação do escopo, contendo:

a) Ação de comunicação;

b) Responsável;

c) Público-alvo;

d) Periodicidade; e

e) Canal/Evento.

5.2.5.2 Esta comunicação é mandatória, não podendo ser dispensada, e deverá ser transcrita no item 4 do documento Planejamento da Análise (GVUL01), padronizado no Anexo A.

5.3 SUBPROCESSO "EXECUTAR ANÁLISE"

5.3.1 Uma vez definido o planejamento e o Plano de Comunicação, a análise de vulnerabilidades se iniciará, sendo necessário executar os procedimentos para identificar e avaliar as vulnerabilidades, conforme ilustrado na figura 3.

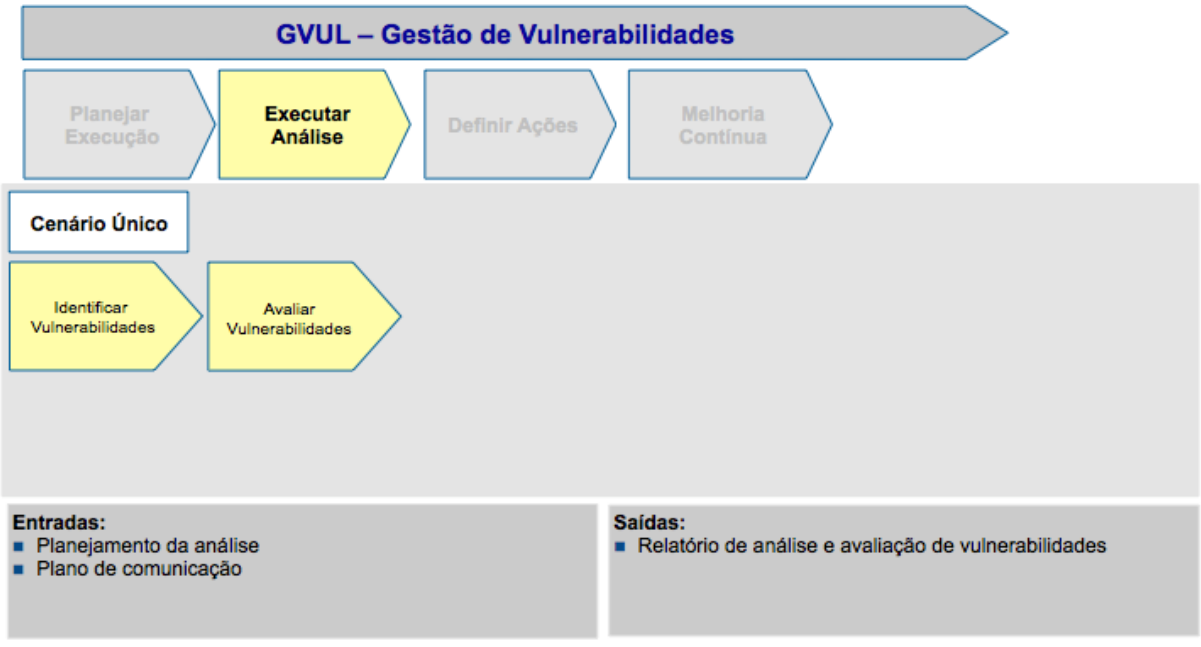

Figura 3 - Subprocesso para Executar a Análise

5.3.2 ETAPA “IDENTIFICAR VULNERABILIDADES”

5.3.2.1 Nesta etapa, a equipe técnica responsável deverá identificar e documentar as vulnerabilidades encontradas em cada ativo de informação.

5.3.2.2 Essas informações deverão ser transcritas no documento Vulnerabilidades Identificadas (GVUL02), padronizado no Anexo B.

5.3.3 ETAPA “AVALIAR VULNERABILIDADES”

5.3.3.1 Após a identificação e documentação das vulnerabilidades identificadas, a equipe técnica responsável pela análise deverá avaliar as vulnerabilidades informando o impacto (Alto, Médio ou Baixo) de cada uma para o ambiente tecnológico do escopo.

5.3.3.2 Essas informações deverão ser transcritas no documento Vulnerabilidades Identificadas (GVUL02), padronizado no Anexo B.

5.4 SUBPROCESSO “DEFINIR AÇÕES”

5.4.1 Após a identificação e avaliação das vulnerabilidades identificadas, deverão ser definidas e implementadas as ações necessárias para tratar as vulnerabilidades identificadas, conforme ilustrado na figura 4.

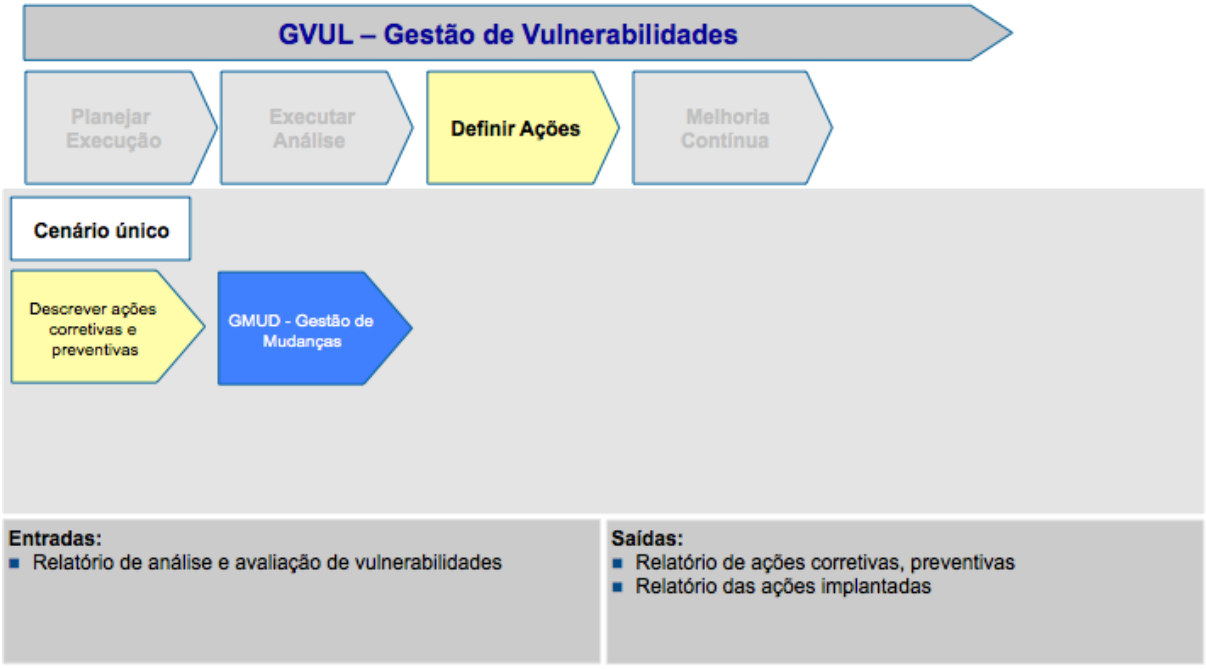

Figura 4 - Subprocesso para Definir Ações

5.4.2 ETAPA "DESCREVER AÇÕES CORRETIVAS E PREVENTIVAS"

5.4.2.1 Para cada vulnerabilidade identificada, a equipe técnica devera apontar um ou mais controles de segurança que deverão ser implementados, o responsável pela implementação e a data desejada para implementação das ações de segurança.

5.4.2.2 Essas informações deverão ser transcritas no documento Ações para Tratamento de Vulnerabilidades (GVUL03), padronizado no Anexo C.

5.4.2.3 Após a elaboração do documento Ações para Tratamento de Vulnerabilidades (GVUL03), as ações deverão ser implementadas a partir do processo de Gestão de Mudanças.

5.5 SUBPROCESSO "MELHORIA CONTÍNUA"

5.5.1 Após o tratamento das vulnerabilidades através dos controles de segurança da informação, é necessário consolidar as informações sobre vulnerabilidades e identificar oportunidades de melhorias no processo, conforme ilustrado na figura 5.

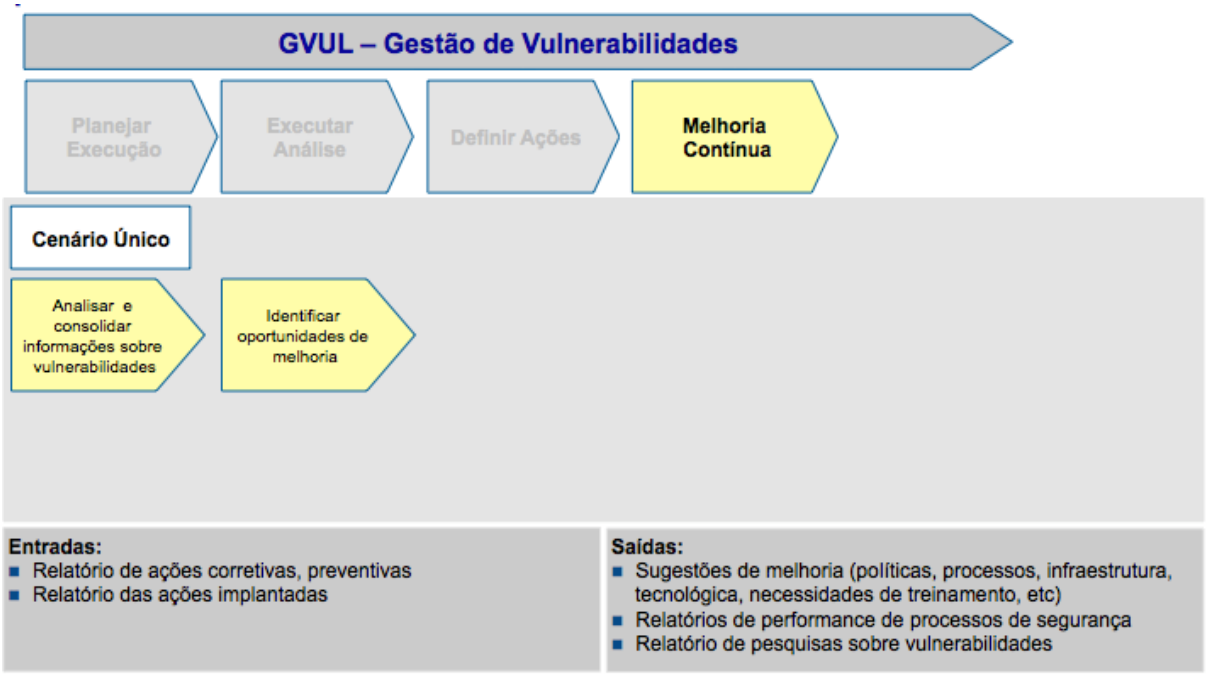

Figura 05 - Subprocesso para Melhoria Contínua

5.5.2 ETAPA “ANALISAR E CONSOLIDAR INFORMAÇÕES SOBRE VULNERABILIDADES”

5.5.2.1 Nesta etapa, deve-se identificar e quantificar os indicadores do processo no documento Identificação, Quantificação e Análise dos Indicadores do Processo (GVUL04), padronizado no Anexo D.

5.5.3 ETAPA “IDENTIFICAR OPORTUNIDADES DE MELHORIA”

5.5.3.1 Nesta etapa, deve-se analisar as informações consolidadas do processo, através dos seus indicadores, e identificar oportunidades de melhoria. Essas informações deverão ser transcritas no documento Identificação, Quantificação e Análise dos Indicadores do Processo (GVUL04), padronizado no Anexo D.

6 DISPOSIÇÕES FINAIS

6.1 O Processo de Segurança da Informação apresentado neste documento é de caráter geral e deve ser revisado a cada trinta e seis meses, ou quando fato relevante demandar atualização extemporânea.

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

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

REFERÊNCIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27002. *Tecnologia da informação: Técnicas de segurança: Código de pratica para a gestão da segurança da informação*. Rio de Janeiro, RJ, 2005.

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

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

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

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

BRASIL. Comando da Aeronáutica. Estado Maior da Aeronáutica. *Estrutura e Competência do Sistema de Tecnologia da Informação do Comando da Aeronáutica*: **NSCA 7-7**. Brasília, DF, 2004.

Anexo A - GVUL01 – Planejamento da Análise

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GVUL01			
ASSUNTO	Planejamento da Análise de Vulnerabilidades			

1 INFORMAÇÕES GERAIS

Nome do Elaborador	Período da Análise

2 IDENTIFICAÇÃO DO ESCOPO DA ANÁLISE

Nome do Ativo de Informação	Localização		Responsáveis	
	Física	Lógica	Proprietário	Custodiante

3 IDENTIFICAÇÃO DOS RISCOS E MEDIDAS DE CONTINGÊNCIA

Risco Envolvido com a Análise	Medida de Contingência a ser Adotada

4 MATRIZ DE COMUNICAÇÃO DO PROCESSO

Ação	Responsável	Público-Alvo	Periodicidade	Canal/Evento
Encaminhar o Planejamento da Análise	Analista da SSSI	Chefe da SSSI	Mensalmente	
Aprovar o Planejamento da Análise	Chefe da SSSI	Comandante Proprietário do Ativo	Mensalmente	
Informar a Execução da Análise	Chefe da SSSI	Proprietário do Ativo Áreas Usuárias	Mensalmente	
Encaminhar o Resultado da Análise e Recomendações	Chefe da SSSI	SDTE	Mensalmente	
Encaminhar a Análise de Indicadores do Processo	Chefe da SSSI	SDTE	Mensalmente	

Anexo B - GVUL02 – Vulnerabilidades Identificadas

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
DECEA	GVUL02			
ASSUNTO	Vulnerabilidades Identificadas			

1 MATRIZ DE VULNERABILIDADES

Ativo de Informação	Vulnerabilidade	Impacto

Anexo C - GVUL03 – Ações para Tratamento de Vulnerabilidades

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GVUL03			
ASSUNTO	Ações para Tratamento de Vulnerabilidades			

1 MATRIZ DE AÇÕES PARA TRATAMENTO DE VULNERABILIDADES

Ativo de Informação	Vulnerabilidade	Ação de Tratamento	Responsável	Data

Anexo D - GVUL04 – Identificação, Quantificação e Análise dos Indicadores do Processo

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GVUL04			
ASSUNTO	Identificação, Quantificação e Análise dos Indicadores do Processo			

1 MEDIÇÃO DOS INDICADORES

Indicador	Quantitativo	Observações
Quantidade de novas vulnerabilidades		
Quantidade de vulnerabilidades por nível de criticidade		
Percentual de vulnerabilidades críticas identificadas que possuem planos de ação desenvolvidos		

2 ANÁLISE DOS INDICADORES

3 AÇÕES DE MELHORIA CONTÍNUA