

**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**

**2024**



**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**

**2024**





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

PORTARIA DECEA Nº 1.322/SNOT, DE 13 DE MAIO DE 2024.  
Protocolo COMAER nº 67600.010347/2024-58

Aprova a reedição 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 da atribuição que lhe confere o art. 4º da Portaria nº 651/GC3, de  
11 de dezembro de 2023, e considerando o que consta do Processo nº 67600.026477/2023-21,  
procedente do DECEA, resolve:

Art. 1º Aprovar a reedição 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 Revogar a Portaria DECEA nº 91/DGCEA, de 2 de agosto de 2013  
publicada no Boletim do Comando da Aeronáutica nº 163, de 26 de agosto de 2013.

Art. 3º Esta Instrução entra em vigor em 3 de junho de 2024.

(a)Ten Brig Ar ALCIDES TEIXEIRA BARBACOV  
Diretor-Geral do DECEA

(Publicado no BCA nº , de de 2024.)



## SUMÁRIO

<b>1</b>	<b>DISPOSIÇÕES PRELIMINARES .....</b>	<b>7</b>
1.1	<u>FINALIDADE .....</u>	7
1.2	<u>ÂMBITO E GRAU DE SIGILO.....</u>	7
1.3	<u>ABREVIATURAS .....</u>	7
1.4	<u>DEFINIÇÕES .....</u>	7
<b>2</b>	<b>DESCRIÇÃO DO DOCUMENTO.....</b>	<b>10</b>
2.1	<u>UTILIZAÇÃO.....</u>	10
<b>3</b>	<b>RESPONSABILIDADES .....</b>	<b>10</b>
3.1	<u>ELO DE COORDENAÇÃO DE STI NO DECEA.....</u>	10
3.2	<u>AUTORIDADE COMPETENTE DA OM .....</u>	10
3.3	<u>COMITÊ DE SEGURANÇA DA INFORMAÇÃO.....</u>	10
3.4	<u>SSSI - SEÇÃO DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO.....</u>	10
3.5	<u>PROPRIETÁRIO DO ATIVO DE INFORMAÇÃO .....</u>	11
3.6	<u>ELO DE SERVIÇO DE STI.....</u>	11
<b>4</b>	<b>PROCESSO DE GESTÃO DE VULNERABILIDADES DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO .....</b>	<b>13</b>
4.1	<u>DESCRIÇÃO DO PROCESSO .....</u>	13
4.2	<u>DIRETRIZES DO PROCESSO .....</u>	13
4.3	<u>CONTROLE DE MATURIDADE.....</u>	17
4.4	<u>FATORES CRÍTICOS DE SUCESSO .....</u>	19
<b>5</b>	<b>DESCRIÇÃO DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO ..</b>	<b>20</b>
5.1	<u>VISÃO GERAL DO PROCESSO.....</u>	20
5.2	<u>SUBPROCESSO "PLANEJAR EXECUÇÃO" .....</u>	21
5.3	<u>SUBPROCESSO "EXECUTAR ANÁLISE" .....</u>	22
5.4	<u>SUBPROCESSO "DEFINIR AÇÕES".....</u>	23
5.5	<u>SUBPROCESSO "MELHORIA CONTÍNUA".....</u>	24
<b>6</b>	<b>DISPOSIÇÕES FINAIS .....</b>	<b>26</b>
	<b>REFERÊNCIAS .....</b>	<b>27</b>
	<b>ANEXO A - GVUL01 - PLANEJAMENTO DA ANÁLISE.....</b>	<b>29</b>
	<b>ANEXO B - GVUL02 - VULNERABILIDADES IDENTIFICADAS.....</b>	<b>30</b>
	<b>ANEXO C - GVUL03 - AÇÕES PARA TRATAMENTO DAS VULNERABILIDADES.....</b>	<b>31</b>
	<b>ANEXO D - GVUL04 - IDENTIFICAÇÃO, QUANTIFICAÇÃO E ANÁLISE DOS INDICADORES DO PROCESSO.....</b>	<b>32</b>
	<b>ANEXO E - FERRAMENTAS DE VARREDURA DE VULNERABILIDADES.....</b>	<b>33</b>





## **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 Organizações Militares Subordinadas, sendo considerado ostensivo o seu grau de sigilo.

### **1.3 ABREVIATURAS**

COMTICEA	–	Comitê de Segurança da Informação do DECEA
DCA	–	Diretriz do Comando da Aeronáutica
DECEA	–	Departamento de Controle do Espaço Aéreo
DTI	–	Diretoria de Tecnologia da Informação da Aeronáutica
GVUL	–	Gestão de Vulnerabilidades de Ativos de Tecnologia da Informação
ICA	–	Instrução do Comando da Aeronáutica
MCA	–	Manual do Comando da Aeronáutica
NSCA	–	Norma de Sistema do Comando da Aeronáutica
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) e no Glossário de Segurança da Informação (Portaria GSI/PR nº 93, de 18 de outubro de 2021).

Para efeito desta Instrução, entende-se por:

#### **1.4.1 AMEAÇAS**

Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas na confidencialidade, integridade e disponibilidade e, conseqüentemente, causando impactos aos negócios de uma organização.

#### **1.4.2 ANÁLISE DE VULNERABILIDADES**

Consiste na avaliação e identificação de falhas e potenciais ameaças de segurança numa infraestrutura tecnológica.

### 1.4.3 ATIVO DE INFORMAÇÃO

Todo elemento que é composto de processos que manipulam a informação, a partir da própria informação, do meio em que ela é armazenada e dos equipamentos em que ela é manuseada, transportada e descartada. O termo ativo possui essa denominação por ser considerado um elemento de valor para um indivíduo ou Organização.

### 1.4.4 COMMON VULNERABILITY AND EXPOSURES (CVE)

Sigla em inglês traduzido para Exposições e Vulnerabilidades Comuns (CVE), possui um número do CVE, que é um identificador usado por fornecedores como a Microsoft, RedHat e Adobe para catalogar vulnerabilidades individuais dos quais patches são providos como solução. Muitas vezes, novos ataques e explorações são documentados em um CVE muito antes do fornecedor admitir o problema ou liberar uma atualização ou *patch* para resolver a situação. Estas exposições e vulnerabilidades, disponibilizadas e mantidas pela MITRE Corporation, podem ser acessadas pelo público pela URL: <https://cve.mitre.org/>.

### 1.4.5 COMMON VULNERABILITY SCORING SYSTEM (CVSS)

Sigla em inglês traduzido para Sistema Comum de Pontuação de Vulnerabilidade (CVSS), é um padrão livre utilizado para classificar a gravidade e o risco de segurança da informação que a vulnerabilidade apresenta no sistema de computadores. O CVSS fornece uma pontuação de gravidade que varia de 0 a 10, sendo que quanto maior a pontuação, maior o risco.

### 1.4.6 CUSTODIANTE

Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação.

### 1.4.7 ELOS DE COORDENAÇÃO DO STI

São os setores pertencentes aos Órgãos de Direção-Geral e de Direção Setorial (ODGS) e ao GABAER, responsáveis pela coordenação de suas atividades de TI junto ao Órgão Central. Esses setores terão a sua constituição estabelecida nos Regulamentos e/ou Regimentos Internos das OM a que estão subordinados, e são regulados segundo a NSCA 7-7 “Estrutura e Competências do STI no COMAER”.

### 1.4.8 ELOS DE SERVIÇOS DO STI

São os setores de TI das OM do COMAER que executam atividades rotineiras de manutenção de TI, reportando-se aos seus respectivos Elos de Coordenação, conforme descrito no NSCA 7-7 “Estrutura e Competências do STI no COMAER”.

### 1.4.9 EXCEÇÃO DE VULNERABILIDADE

É uma vulnerabilidade não corrigida e que foi incluída em uma lista de exceção para ser tratada como uma aceitação de risco devido à falta de suporte do fabricante do equipamento ou uma tecnologia muito antiga e que não possui mais atualizações. As OM podem justificar um requisito operacional para não mitigar ou corrigir uma vulnerabilidade de

segurança da informação de um sistema de informação sob sua responsabilidade com base na gestão e na criação de um plano para aprovação.

#### 1.4.10 GESTÃO DE VULNERABILIDADE

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.

#### 1.4.11 HOST

Um computador ou dispositivo de TI como, por exemplo, estação de trabalho, roteador, *switch*, *gateway* e *firewall*.

#### 1.4.12 ID CVE

Identificação para um CVE específico

#### 1.4.13 LOG

Registro de atividades gerado por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por IDSs.

#### 1.4.14 PATCHES

Um *patch* é um programa criado para atualizar ou corrigir um *software*.

#### 1.4.15 PENTEST

Acrônimo de teste de penetração (*PENetration TEST*).

#### 1.4.16 PROPRIETÁRIO DAS INFORMAÇÕES

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

#### 1.4.17 VULNERABILIDADE

Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

## **2 DESCRIÇÃO DO DOCUMENTO**

### **2.1 UTILIZAÇÃO**

**2.1.1** Para a utilização desta Instrução, as Organizações Militares devem estar estruturadas e alinhadas de acordo com o estabelecido pela Política de Segurança da Informação do Comando da Aeronáutica (DCA 14-8), bem como devem possuir uma Seção de Segurança de Sistemas da Informação (SSSI) responsável pela garantia do cumprimento da Diretriz de Segurança da Informação do Departamento de Controle do Espaço Aéreo (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 vigentes do COMAER e da Administração Pública Federal.

### **3 RESPONSABILIDADES**

#### **3.1 ELO DE COORDENAÇÃO DO STI NO DECEA**

**3.1.1** O Elo de Coordenação do STI no DECEA é o Subdepartamento Técnico, que possui as seguintes responsabilidades:

- a) Normatizar e manter atualizado o Processo de Gestão de Vulnerabilidades de Ativos de Tecnologia da Informação no âmbito do DECEA; e
- b) Acompanhar o processo de implantação das ações corretivas e preventivas.

#### **3.2 AUTORIDADE COMPETENTE DA OM – CHEFES DOS SUBDEPARTAMENTOS DO DECEA, CHEFES, DIRETORES E COMANDANTES DAS ORGANIZAÇÕES SUBORDINADAS AO DECEA**

**3.2.1** A Autoridade Competente da OM tem por responsabilidade:

- a) Designar e aprovar os representantes de cada área/setor para compor o Comitê de Segurança da Informação ou estrutura equivalente na OM; e
- b) Orientar e supervisionar as atividades do Comitê.

#### **3.3 COMITÊ DE SEGURANÇA DA INFORMAÇÃO**

**3.3.1** O Comitê de Segurança da Informação ou estrutura equivalente terá em sua composição os representantes de cada área/setor, que possui as seguintes responsabilidades:

- a) Indicar os responsáveis pela execução das atividades de análise de vulnerabilidades no âmbito da OM.
- b) Promover a integração dos responsáveis pelo Processo de Gestão de Vulnerabilidades.
- c) Monitorar o processo de gestão de vulnerabilidades.
- d) Propor reuniões para tratar de assuntos pertinentes do processo de gestão de vulnerabilidades da OM.
- e) Encaminhar as decisões deliberadas em reuniões à Autoridade Competente da OM; e
- f) Encaminhar os registros do processo de gestão de vulnerabilidades ao SDTE.

#### **3.4 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO**

**3.4.1** As Seções de Segurança de Sistemas da Informação são as Seções locais de SI das OM Subordinadas ao DECEA, que possui as seguintes responsabilidades:

- a) Aprovar as ações corretivas e preventivas;
- b) Analisar e avaliar as vulnerabilidades;
- c) Tratar, conjuntamente com os Elos de Serviços do STI e os Proprietários de Ativos de Informação, as vulnerabilidades encontradas nos ativos; e
- d) Apoiar o SDTE na geração de indicadores de desempenho.

### **3.5 PROPRIETÁRIOS DE ATIVOS DE INFORMAÇÃO**

**3.5.1** Os Proprietários de Ativos de Informação são pessoas ou Organizações que tem por responsabilidade:

- a) Tratar, conjuntamente com a SSSI e os Elos de Serviços do STI, as vulnerabilidades encontradas nos ativos.

### **3.6 ELOS DE SERVIÇOS DO STI**

**3.6.1** Os Elos de serviços do STI no DECEA são os setores de TI das OM subordinadas ao DECEA, que tem por responsabilidade:

- a) Tratar, conjuntamente com a SSSI e os Proprietários de ativos de Informação, as vulnerabilidades encontradas nos ativos.

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

### **4.1 DESCRIÇÃO DO PROCESSO**

**4.1.1** De acordo com os itens III, IV e V do art. 9º da IN nº 3, combinado com o item 6.17 da DCA 7-2/2022, as Organizações subordinadas ao DECEA devem possuir uma estrutura de gestão de vulnerabilidades em seus sistemas de informação instalados, visando reduzir riscos resultantes de vulnerabilidades conhecidas. Adicionalmente, o Departamento de Controle do Espaço Aéreo deve estabelecer e 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 DIRETRIZES DO PROCESSO**

**4.2.1** O processo de gestão de vulnerabilidades sempre deve estabelecer mecanismos de manter atualizado o *software* e *patches* de fabricante ou fornecedor oficial para permitir o rastreamento das vulnerabilidades mais recentes.

**4.2.2** As OM subordinadas ao DECEA devem apresentar ao SDTE, periodicamente, as métricas de gerenciamento de vulnerabilidades definidas nesta Instrução, GVUL04 - Identificação, Quantificação e Análise dos Indicadores do Processo, com o objetivo de mensurar o grau de vulnerabilidade e ameaça de determinado ativo de informação.

**4.2.3** Os ativos de informação que fazem parte dos serviços da Organização devem possuir um gerenciamento de vulnerabilidades para identificação e análise dos resultados da varredura.

**4.2.4** As avaliações de risco das vulnerabilidades devem ser realizadas anualmente, no mínimo, e sempre que houver mudanças nos sistemas.

**4.2.5** As OM que criam aplicativos de software, é altamente recomendável que eles implantem analisadores de código para revisar seu código de software para possíveis vulnerabilidades.

**4.2.6** Os ativos de informação das OM devem ser CLASSIFICADOS por tipo de ambiente, por tipo de sistema, por ID CVE, CVSS/Gravidade e por tipo de vulnerabilidade.

**4.2.7** O CVE identifica e fornece informações sobre vulnerabilidades de segurança de software, que pode ser obtido por meio da seguinte URL: <https://cve.mitre.org/cve/>.

**4.2.8** As equipes SSSI das OM devem determinar e manter atualizado o valor percentual dos ativos de informação vulneráveis por gravidade e CVSS.

**4.2.9** As OM devem utilizar as pontuações CVSS para quantificar o risco e a urgência de uma vulnerabilidade.

**4.2.10** A atribuição de todas as vulnerabilidades com base na pontuação CVSSv2 ou CVSSv3 estática da vulnerabilidade possuem a gravidade: Muita Baixa, Baixa, Média, Alta ou Muito Alta.

**4.2.11** O nível de severidade das vulnerabilidades CVSS v2 e CVSSv3 estão classificados de acordo com a tabela abaixo:

Nível de Severidade	Faixa de Pontuação CVSS v2	Faixa de Pontuação CVSS v3
Muito Alto (Crítico)	—	A pontuação da vulnerabilidade mais alta está entre 9 e 10,0
Alto	A pontuação da vulnerabilidade mais alta está entre 7 e 10	A pontuação da vulnerabilidade mais alta está entre 7 e 8,9
Médio	A pontuação da vulnerabilidade mais alta está entre 4 e 6,9	A pontuação da vulnerabilidade mais alta está entre 4 e 6,9
Baixo	A pontuação da vulnerabilidade mais alta está entre 0 e 3,9	A pontuação da vulnerabilidade mais alta está entre 0,1 e 3,9
Muito Baixo (Informações)	—	A pontuação da vulnerabilidade mais alta está em 0

**Tabela 1 – Fonte: <https://nvd.nist.gov/vuln-metrics/cvss>**

**4.2.12** As vulnerabilidades sem CVEs devem ser corrigidas de acordo com sua gravidade baseada em CVSS. Esta pontuação pode ser obtida por meio da seguinte calculadora: <https://nvd.nist.gov/vuln-metrics/cvss/> ou <https://www.first.org/cvss/>

**4.2.13** O CVSS deve ser usado para medir a gravidade de uma vulnerabilidade, não devendo em hipótese alguma ser usado sozinho para avaliar o risco.

**4.2.14** Os relatórios elaborados desta Instrução devem ser classificados com acesso restrito e o envio destes, ao Subdepartamento Técnico do DECEA, deve ser feito através da Rede Mercúrio conforme preconizada na ICA 205-47 - Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica.

**4.2.15** O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou *host* impactado tem para o negócio da Organização. O formulário sugerido para realizar o tratamento das vulnerabilidades é o GVUL03 - Ações para Tratamento de Vulnerabilidades.



**4.2.16** As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados da tabela abaixo:

Nível de Severidade	Prazo de Correção	Descrição do Risco
Muito Alto (Crítico)	2 dias	Condição totalmente inaceitável e medidas imediatas devem ser tomadas para eliminar o risco e mitigar seus impactos
Alto	30 dias	Pessoas mal-intencionadas podem facilmente obter o controle do <i>host</i> que pode comprometer toda a rede ou coletar informações altamente confidenciais. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos, acesso com <i>backdoors</i> , execução de <i>rootkits</i> e acesso a uma lista de todas as contas de usuário no <i>host</i> .
Médio	90 dias	Pessoas mal-intencionadas podem obter acesso às configurações de segurança no <i>host</i> , como acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços
Baixo	120 dias	Pessoas mal-intencionadas podem coletar informações confidenciais do <i>host</i> , como versões de software instaladas, que podem revelar vulnerabilidades conhecidas
Muito Baixo (Informações)	180 dias	Pessoas mal-intencionadas podem coletar informações sobre o <i>host</i> por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades

**Tabela 2 – Nível de severidade e prazo de correção das vulnerabilidades**

**4.2.17** Quando as vulnerabilidades não puderem ser corrigidas dentro do prazo de seu nível de severidade conforme a Tabela 2, as OM devem enviar um relatório ao SDTE contendo, no mínimo:

- Nome do ativo da informação e a vulnerabilidade não corrigida dentro do prazo de correção;
- A justificativa pelo não cumprimento do prazo;
- Os controles de segurança existentes do ativo da informação, se houver;
- Novo prazo de correção; e
- Plano de ação para o tratamento de correção das vulnerabilidades.

**4.2.18** As vulnerabilidades não corrigidas, que forem incluídas na lista de exceção pela equipe de SSSI das Organizações, deverão ser tratadas como “Aceitação de Risco” de acordo com a ICA 7-26 – Processo de Gestão de Riscos de Segurança e Tecnologia da Informação do Departamento de Controle do Espaço Aéreo.

**4.2.19** Quando as exceções das vulnerabilidades forem aceitas, as OM devem estabelecer processos para lidar com essas situações e criar um plano para remediar o problema dentro de um prazo aprovado.

**4.2.20** O prazo de aprovação das exceções de vulnerabilidades não deve ultrapassar 365 dias.

**4.2.21** Quando novas vulnerabilidades são identificadas, as OM devem realizar uma análise de risco para determinar o risco que apresentam ao sistema segundo a ICA 7-26 – Processo de Gestão de Riscos de Segurança e Tecnologia da Informação do Departamento de Controle do Espaço Aéreo.

**4.2.22** As OM devem realizar um constante monitoramento das vulnerabilidades, dos patches e das possíveis ameaças aos ativos de informação.

**4.2.23** As Organizações subordinadas ao DECEA devem informar as vulnerabilidades e suas correções a todos os usuários afetados.

**4.2.24** As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de verificação de vulnerabilidades de rede e *host*, verificação de logs de patches, testes de invasão/penetração (*Pentest*) e verificação das definições de configuração.

**4.2.25** Todo teste de invasão ou o teste de penetração (*Pentest*) deve ser realizado por meio de aprovação e coordenação do Subdepartamento Técnico do DECEA.

**4.2.26** Somente as correções de vulnerabilidades que foram efetivamente testadas e aprovadas devem ser implantadas em produção.

**4.2.27** Quando correções de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser realizadas por um processo de gestão de mudanças conforme a ICA 7-24 - Processo de Gestão de Mudanças de Ativos de Tecnologia da Informação do Departamento de Controle do Espaço Aéreo, para que os controles de segurança adequados sejam implementados para teste, avaliação de riscos e reparação.

**4.2.28** Todos os ativos de informação devem incluir configurações de log para permitir o monitoramento e análise de todas as atividades ilegais e não autorizadas que possam afetar ou que sejam relevantes para a segurança da informação.

**4.2.29** As informações de eventos de registros e seus recursos devem ser protegidos contra acesso não autorizado e adulteração.

### **4.3 CONTROLE E MATURIDADE DO PROCESSO**

#### **4.3.1 MEDIÇÃO DO NÍVEL DE MATURIDADE**

##### **4.3.1.1 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, bem como 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.

**4.3.1.2** A tabela 3 apresenta as metas para a evolução dos níveis de maturidade:

**Tabela 3 - Metas para a Evolução dos Níveis de Maturidade**

<b>Nível de Maturidade</b>	<b>Metas</b>
2 – Repetível e Intuitivo	<ul style="list-style-type: none"><li>• Possuir uma normativa interna do DECEA para gestão de vulnerabilidades de segurança da informação</li><li>• Iniciar a implantação e testes do processo em pelo menos 50% das Organizações Subordinadas ao DECEA</li></ul>
3 – Processo Definido	<ul style="list-style-type: none"><li>• Implantar o processo em todas as Organizações Subordinadas ao DECEA</li><li>• Capacitar todos os chefes das seções de segurança da informação</li></ul>
4 – Gerenciado e Mensurável	<ul style="list-style-type: none"><li>• Criar um painel para acompanhamento, através de indicadores gerenciais do processo, a fim de garantir a tomada de decisão pela Direção do DECEA</li></ul>
5 – Otimizado	<ul style="list-style-type: none"><li>• Realizar uma reunião semestral de análise crítica para melhoria contínua do processo</li><li>• Possuir sistema informatizado para emissão de relatórios automatizados</li></ul>

**4.3.1.3** Cada Organização deverá elaborar e encaminhar ao Subdepartamento Técnico do DECEA um Relatório de Evolução dos Níveis de Maturidade, que deverá ser atualizado anualmente e sempre que houver alteração no nível de maturidade.

**4.3.1.4** O Relatório de Evolução dos Níveis de Maturidade deverá conter, no mínimo:

- a) O nível de maturidade e a meta atual;
- b) As mudanças e justificativas em relação ao nível de maturidade; e
- c) O prazo de evolução dos níveis de maturidade;

#### 4.3.2 ACOMPANHAMENTO DO PROCESSO POR INDICADORES

**Tabela 4 – Acompanhamento do Processo**

<b>Objetivos do Processo</b>	<b>Indicadores do Processo</b>
<ul style="list-style-type: none"><li>• Reduzir a ocorrência e o impacto das vulnerabilidades técnicas; e</li><li>• Aprovar planos de ação com custos eficientes para vulnerabilidades críticas.</li></ul>	<ul style="list-style-type: none"><li>• Quantidade de novas vulnerabilidades identificadas (comparado com o exercício anterior);</li><li>• Quantidade de vulnerabilidades identificadas por nível de criticidade;</li><li>• Quantidade de exceções de vulnerabilidades aprovadas;</li><li>• Quantidade de vulnerabilidades conhecidas e não corrigidas há mais de 180 dias;</li><li>• Percentual de vulnerabilidades críticas identificadas que possuem planos de ação desenvolvidos;</li><li>• Percentual de exceções de vulnerabilidades aprovadas;</li><li>• Tempo médio das vulnerabilidades em aberto (descobertas, mas ainda não corrigidas).</li></ul>

#### 4.4 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 à sua exploração.

## 5 DESCRIÇÃO DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

O processo de Gestão de Vulnerabilidades 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.

**5.1.4** Com a aprovação do SDTE, todos os formulários descritos nesta Instrução poderão ser reproduzidos e automatizados em ferramentas de software apropriadas.

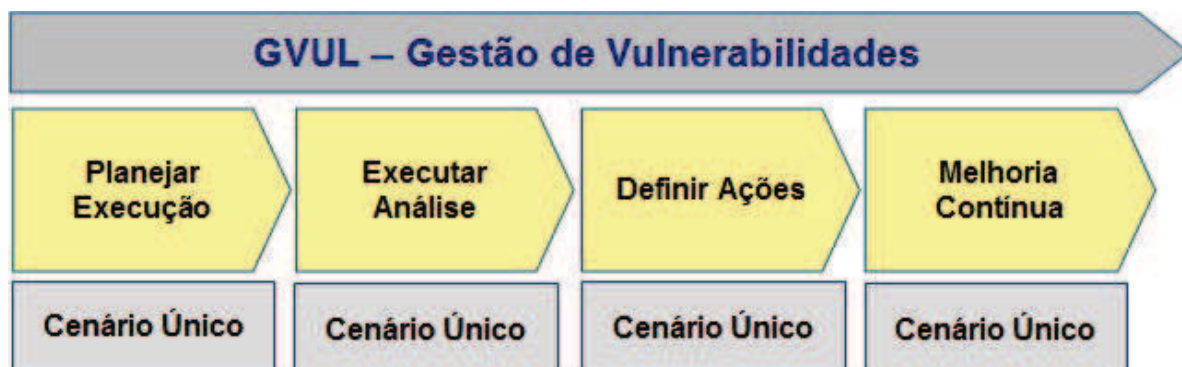
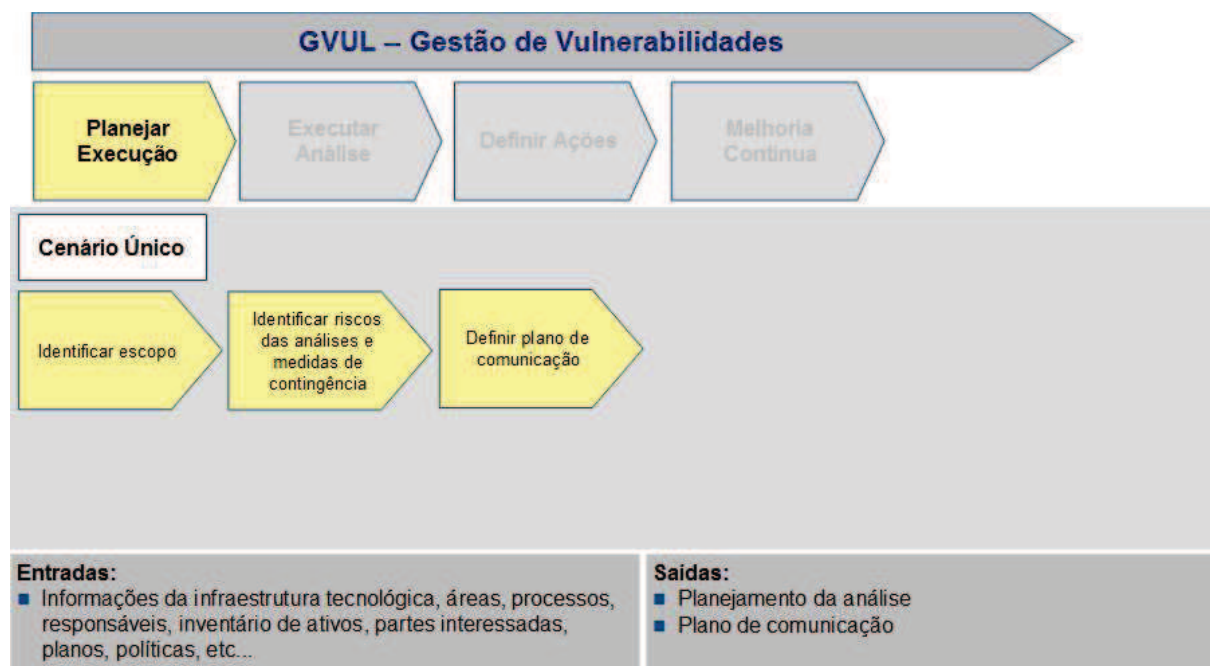


Figura 1 - Visão Geral do Processo de Gestão de Vulnerabilidades

## 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:

- ativos de informação;
- localização (física e lógica); e
- 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”

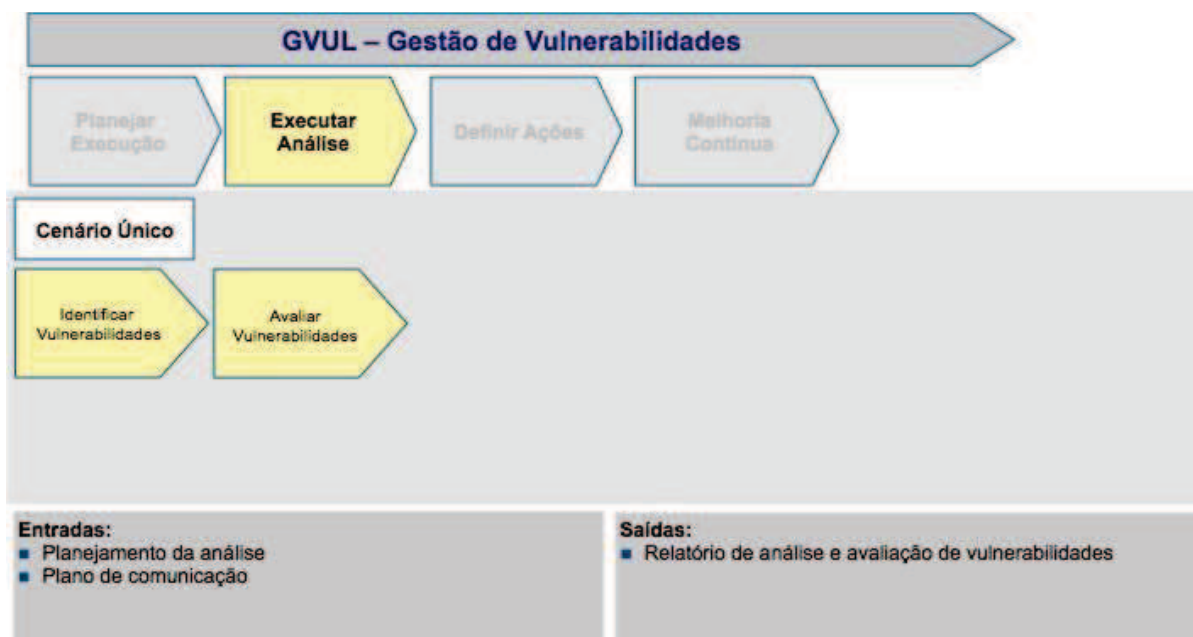
**5.2.5.1** Durante a fase de planejamento da análise é necessário definir um plano de comunicação das áreas e responsáveis pelos ativos de informação do escopo, contendo:

- 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.

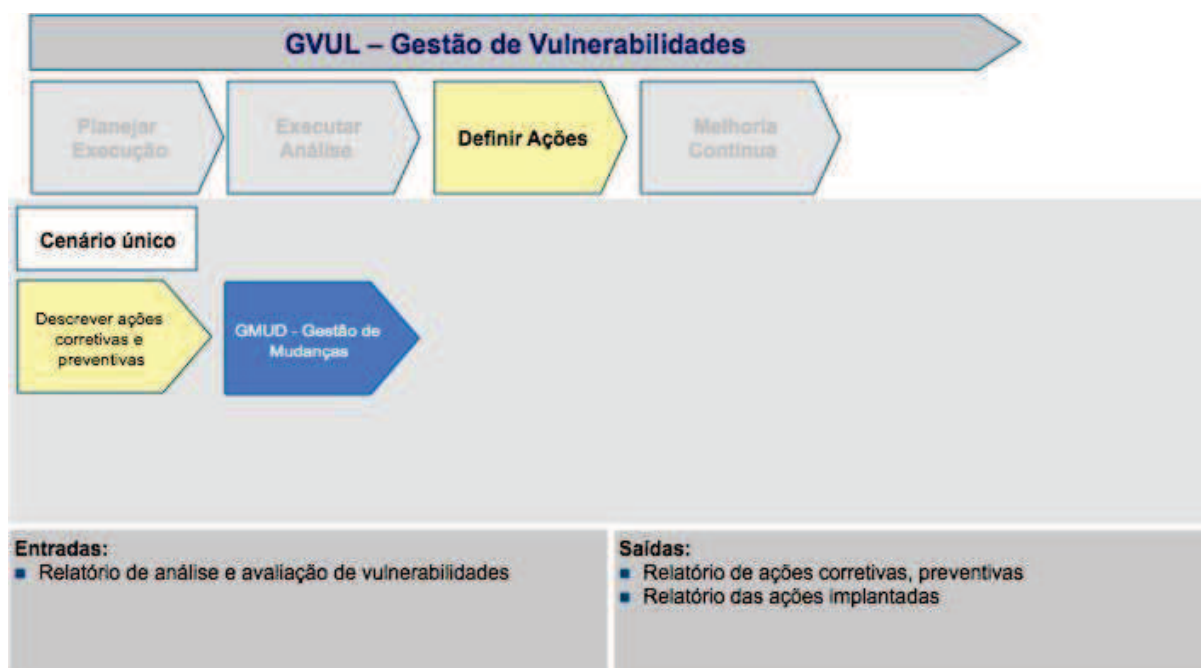
### 5.3.3 ETAPA “AVALIAR VULNERABILIDADES”

**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”

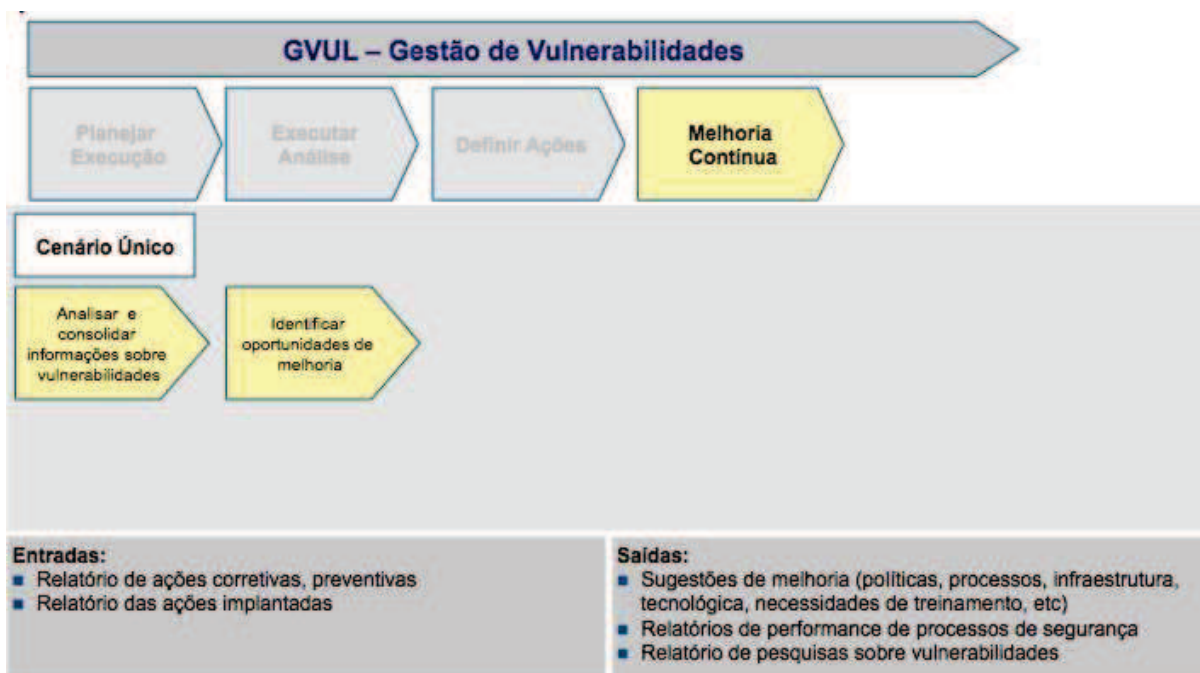
**5.4.2.1** Para cada vulnerabilidade identificada, a equipe técnica deverá apontar um ou mais controles de segurança que deverão ser implementados, o responsável pela implementação e a data desejada para implementação das ações de segurança.

**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.

**5.5.2.2** Com a aprovação do SDTE, cada Organização Militar poderá desenvolver ou adquirir uma ferramenta de gestão de vulnerabilidades para medição dos indicadores de processo com o objetivo de permitir um acompanhamento sistemático das atividades desenvolvidas, assim como subsidiar o gestor na tomada de decisão.

## **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.

## **6DISPOSIÇÕES FINAIS**

**6.1** O processo e os procedimentos de gestão de ativos apresentados neste documento são de caráter geral e devem ser revisados periodicamente a cada 36 meses, ou quando fato relevante demandar atualização extemporânea.

**6.2** Esta Instrução do Comando da Aeronáutica está em conformidade com as diretrizes da DTI – Órgão Central do Sistema de Tecnologia da Aeronáutica – e deve ser revisada e atualizada sempre que forem atualizadas e 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.

## REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27002. **Tecnologia da Informação: Técnicas de segurança: Código de práticas para a gestão da segurança da informação.** Rio de Janeiro, RJ, 2022.

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, 2023.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 1.274 /SNOT, de 1º de março de 2024. Aprova a reedição da “Diretriz do Comando da Aeronáutica que dispõe sobre a Segurança da Informação do Departamento de Controle do Espaço Aéreo” = **DCA 7-2**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2024, n. 53, 18 mar. 2024.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 58/DGCEA, de 24 de maio de 2013. “Aprova a edição da Diretriz que estrutura a gerência de configuração de tecnologia da informação no Âmbito do Departamento de Controle do Espaço Aéreo (DECEA)” = **DCA 7-4**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 132, 12 jul. 2013.

BRASIL Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria GABAER nº 273/GC3, de 18 de abril de 2022. Aprova a Diretriz que estabelece a “Política de Segurança da Informação do Comando da Aeronáutica” = **DCA 14-8**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 74, 18 abr. 2022.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 950/SNOT, de 30 de maio de 2023. Aprova a reedição da Instrução do “Processo de Gestão de Mudanças de Ativos de Tecnologia da Informação do DECEA”. = **ICA 7-24**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n.109, 16 jun. 2023.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 59/DGCEA, de 24 de maio de 2013. Aprova a edição da Instrução acerca do “Processo de Gestão de Riscos de Segurança e Tecnologia da Informação do Departamento de Controle do Espaço Aéreo” = **ICA 7-26**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2013, n. 120, 26 jun. 2013.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 1.077/SNOT, de 21 de agosto de 2023. Aprova a edição da Instrução relativa ao “Processo de Controle de Acesso à Rede Interna do DECEA” = **ICA 7-30**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2023, n. 165, 06 set. 2023.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 745 /DGCEA, de 14 de fevereiro de 2023. Aprova a reedição do “Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo” = **MCA 7-1**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 39, 01 mar. 2023.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº 8/3SC2, de 14 de abril de 2003. “Aprova a Reedição do Manual de Abreviaturas, Siglas e Símbolos da Aeronáutica” = **MCA 10-3**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2003, n. 74, 22 abr. 2003.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº 2/3SC2, de 30 de janeiro de 2001. “Aprova a reedição do Manual que dispõe sobre padronização do uso de termos, palavras, vocábulos e expressões de uso corrente no âmbito do Comando da Aeronáutica” = **MCA 10-4**. Boletim Externo Ostensivo, Rio de Janeiro, RJ, 2001.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº45/CEMAER, de 22 de novembro de 2022. “Estrutura e Competências do Sistema de Tecnologia da Informação do Comando da Aeronáutica” = **NSCA 7-7**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 224, 07 dez. 2022.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 248, 27 dez. 2018 - Seção 1.

BRASIL. Instrução Normativa GSI nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 101, 28 maio 2020 – Seção 1.

BRASIL. Instrução Normativa GSI nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 101, 31 maio 2021 - Seção 1.

BRASIL. Portaria GSI\_PR Nº 93, de 18 de outubro de 2021. Glossário de Segurança Institucional da Presidência da República. Glossário de Segurança da Informação. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 197, 19 out. 2021, Seção 1.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br. **Cartilha de Segurança para Internet**. São Paulo, SP, 2012.

FIRST. **Common Vulnerability and Exposures (CVE)**. CVE List Home. Disponível em: <https://cve.mitre.org/cve/>. Acesso em: 22/06/2023.

FIRST. **Common Vulnerability Scoring System (CVSS)**. The Common Vulnerability Scoring System SIG. Disponível em: <https://www.first.org/cvss/>. Acesso em: 22/06/2023.

National Institute of Standards and Technology (NIST). National Vulnerability Database (NVD). **Common Vulnerability Score System (CVSS)**. Disponível em: <https://nvd.nist.gov/vuln-metrics/cvss/>. Acesso em 22/06/2023.

ANEXO A - GVUL01 – PLANEJAMENTO DA ANÁLISE


<div>COMANDO DA AERONÁUTICA</div> <div>DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO</div> <div>&lt;inserir nome da OM por extenso&gt;</div>				
	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	Período	Canal/Evento
Encaminhar o Planejamento da Análise	Analista da SSSI	Chefe da SSSI	Mensal	
Aprovar o Planejamento da Análise	Chefe da SSSI	Comandante Proprietário do Ativo	Mensal	
Informar a Execução da Análise	Chefe da SSSI	Proprietário do Ativo Áreas Usuárias	Mensal	
Encaminhar o Resultado da Análise e Recomendações	Chefe da SSSI	SDTE	Trimestral	
Encaminhar a Análise de Indicadores do Processo	Chefe da SSSI	SDTE	Trimestral	







## ANEXO D - GVUL04 – IDENTIFICAÇÃO, QUANTIFICAÇÃO E ANÁLISE DOS INDICADORES DO PROCESSO

<b>COMANDO DA AERONÁUTICA</b> <b>DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO</b> <u>&lt;inserir nome da OM por extenso&gt;</u>				
	<b>CÓDIGO DO REGISTRO</b>	<b>DATA</b>	<b>CLASSIFICAÇÃO</b>	<b>LOCALIDADE</b>
	GVUL04			
<b>ASSUNTO</b>		Identificação, Quantificação e Análise dos Indicadores do Processo		
<b>1 MEDIÇÃO DOS INDICADORES</b>				
<b>Indicador</b>		<b>Quantitativo</b>	<b>Observações</b>	
Quantidade de novas vulnerabilidades				
Quantidade de vulnerabilidades por nível de criticidade		[total de vulnerabilidades por criticidade]	[informar quais vulnerabilidades foram encontradas, fornecer detalhes daquelas que possuem maior risco e as recomendações para correção]	
Quantidade de exceções de vulnerabilidades aprovadas.				
Quantidade de vulnerabilidades conhecidas e não corrigidas há mais de 180 dias				
Percentual de vulnerabilidades críticas identificadas que possuem planos de ação desenvolvidos				
Percentual de exceções de vulnerabilidades aprovadas				
Tempo médio das vulnerabilidades em aberto				
<b>2 ANÁLISE DOS INDICADORES</b>				
<b>3 AÇÕES DE MELHORIA CONTÍNUA</b>				

**ANEXO E – FERRAMENTAS DE VARREDURA DE VULNERABILIDADES**

Esta Instrução tem como objetivo apenas divulgar uma lista de ferramentas comerciais mais utilizadas para busca e avaliação de vulnerabilidades, bem como auxiliar no desenvolvimento das atividades do Processo de Gestão de Vulnerabilidades. A escolha e a utilização de um determinado fornecedor ou ferramenta de varredura de vulnerabilidades é uma decisão de cada OM e que deve ser tomada baseada em fatores inerentes às atividades de segurança da informação desenvolvidas pelos Elos de Serviço de STI.

Segue abaixo uma tabela com uma lista de ferramentas de varredura de vulnerabilidades mais utilizadas para análise e execução de testes.

<b>Ferramenta</b>	<b>URL</b>	<b>Plataforma</b>	<b>Nota</b>
Acunetix	<a href="https://acunetix.com">https://acunetix.com</a>	Windows e Linux	Pode ser configurado para usar o OpenVAS. Possui versão Demo.
Aircrack-ng	<a href="https://www.aircrack-ng.org">https://www.aircrack-ng.org</a>	Windows, Linux, NetBSD, Solaris e OS X	Conjunto completo de ferramentas para avaliar a segurança da rede WiFi e em linha de comando.
Burp Suite	<a href="https://portswigger.net/burp">https://portswigger.net/burp</a>	Windows, Linux e Mac	Software desenvolvido para realização de testes de segurança de aplicações web. Gratuito e capacidade limitada.
Core Impact	<a href="https://www.coresecurity.com">https://www.coresecurity.com</a>	Versão Trial	Teste de penetração com o objetivo de explorar vulnerabilidades e mitigar os riscos. Possui avaliação gratuita.
Invicti	<a href="https://www.invicti.com">https://www.invicti.com</a>	Demo	Período de avaliação experimental é de 2 semanas, no máximo 5 URLs de destino.
Kali Linux	<a href="https://www.kali.org/">https://www.kali.org/</a>	Diversas versões (Arm, ISO, Máquinas virtuais, Cloud, USB etc)	Distribuição de teste de penetração que possui diversas ferramentas de varredura exploração de falhas.

Ferramenta	URL	Plataforma	Nota
Metasploit Pro	<a href="https://www.metasploit.com">https://www.metasploit.com</a>	Windows e Linux	Teste de penetração para ajudá-lo a simular ataques do mundo real, coletar dados e corrigir <i>exploits</i> encontrados.
Nessus	<a href="https://tenable.com">https://tenable.com</a>	Windows, Linux e Mac	Ferramenta de verificação de vulnerabilidades. Gratuito e capacidade limitada.
Nexpose	<a href="https://www.rapid7.com">https://www.rapid7.com</a>	Windows e Linux	Ferramenta de verificação de vulnerabilidades em código aberto. Pode ser incorporada a um <i>MetaSploit Framework</i> . Gratuito e capacidade limitada.
Nikto	<a href="https://cirt.net">https://cirt.net</a>	Windows e Linux	Ferramenta de varredura de vulnerabilidades para aplicações em servidores web. É gratuito online e em código aberto (GPL).
Nmap	<a href="https://nmap.org">https://nmap.org</a>	Windows, Linux e Mac	Utilitário gratuito e de código aberto para descoberta de rede, administração e auditoria de segurança.
OpenVas	<a href="https://www.openvas.org">https://www.openvas.org</a>	Linux	Scanner de vulnerabilidade completo em código aberto, desenvolvido e mantido pela Greenbone Networks GmbH.
OWAP ZAP	<a href="https://www.zaproxy.org">https://www.zaproxy.org</a>	Windows, Linux e Mac	Scanner de aplicativos Web. em código aberto e gratuito.
QualysGuard	<a href="https://www.qualys.com">https://www.qualys.com</a>	SaaS	Ferramenta de busca de vulnerabilidades e configurações incorretas em aplicações <i>web</i> . Atualmente, se chama Qualys Cloud Platform.

Ferramenta	URL	Plataforma	Nota
Retina	<a href="https://www.beyondtrust.com">https://www.beyondtrust.com</a>	Windows, Linux, Unix e Mac	Software de código aberto baseado na Web que cuida do gerenciamento de vulnerabilidades a partir de um local central. Utiliza gerenciamento Endpoint.
SQLMap	<a href="https://sqlmap.org">https://sqlmap.org</a>	Todos os sistemas operacionais	Ferramenta de teste de penetração de código aberto que automatiza o processo de detecção e exploração de falhas de <i>SQL Injection</i> e o controle de servidores de banco de dados.
Tripwire IP360	<a href="https://www.tripwire.com">https://www.tripwire.com</a>	Demo	Solução de gerenciamento de vulnerabilidades para identificar a rede e nuvem.
Uniscan	<a href="https://sourceforge.net/projects/uniscan/">https://sourceforge.net/projects/uniscan/</a>	Linux	Scanner de vulnerabilidade de inclusão de arquivo remoto, inclusão de arquivo local e execução de comando remoto.
W3f	<a href="https://w3af.org">https://w3af.org</a>	Linux, BSD ou Mac	Varredura e exploração de falhas de recursos <i>web</i>
Websecurify	<a href="https://websecurify.com">https://websecurify.com</a>	Windows, Linux e Mac	Gratuito e capacidade limitada.
Wireshark	<a href="https://www.wireshark.org/">https://www.wireshark.org/</a>	Windows, Linux e Mac	Analizador de protocolo de rede que identifica a ameaça.