

**MINISTÉRIO DA DEFESA  
COMANDO DA AERONÁUTICA**



**TECNOLOGIA DA INFORMAÇÃO**

**NSCA 7-13**

**SEGURANÇA DA INFORMAÇÃO E DEFESA  
CIBERNÉTICA NAS ORGANIZAÇÕES DO COMANDO  
DA AERONÁUTICA**

**2022**

**MINISTÉRIO DA DEFESA  
COMANDO DA AERONÁUTICA  
COMANDO-GERAL DE APOIO**



**TECNOLOGIA DA INFORMAÇÃO**

**NSCA 7-13**

**SEGURANÇA DA INFORMAÇÃO E DEFESA  
CIBERNÉTICA NAS ORGANIZAÇÕES DO COMANDO  
DA AERONÁUTICA**

**2022**



**MINISTÉRIO DA DEFESA**  
**COMANDO DA AERONÁUTICA**  
**COMANDO-GERAL DE APOIO**

**PORTARIA COMGAP Nº 42/ADLG, DE 2 DE MAIO DE 2022**

Aprova a reedição da Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica.

**O CHEFE DO ESTADO-MAIOR DO COMANDO-GERAL DE APOIO**, no uso da delegação de competência estabelecida na alínea “b” do inciso I do art. 1º da Portaria COMGAP Nº 109/SSRH, de 08 de dezembro de 2021, e considerando o que consta do Processo nº 67131.000594/2022-58, resolve:

Art. 1º Aprovar a reedição da NSCA 7-13 “Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica”.

Art. 2º A entrada em vigor do presente ato, conforme disposto no parágrafo único do art. 4º do Decreto 10.139, de 28 de novembro de 2019, será na data de sua publicação.

Art. 3º Revoga-se a Portaria nº 31/3EM, de 06 de maio de 2013, publicada no BCA nº 88, de 9 de maio de 2013.

**Maj Brig Ar WALCYR JOSUÉ DE CASTILHO ARAUJO**  
Chefe do Estado-Maior do COMGAP

(Publicado no BCA nº 081, 3 de maio de 2022)

## SUMÁRIO

<b>1</b>	<b>DISPOSIÇÕES PRELIMINARES.....</b>	<b>9</b>
1.1	FINALIDADE.....	9
1.2	CONCEITUAÇÕES.....	16
1.3	ÂMBITO .....	16
<b>2</b>	<b>OBJETIVOS.....</b>	<b>17</b>
<b>3</b>	<b>PROCEDIMENTOS DE SEGURANÇA .....</b>	<b>18</b>
3.1	CONTROLE DE ACESSO FÍSICO.....	18
3.2	CONTROLE DE ACESSO LÓGICO .....	18
3.3	MEIOS DE PROTEÇÃO CONTRA PROGRAMAS MALICIOSOS.....	18
3.4	SERVIÇOS DE REDE DA INTRAER E DA INTERNET.....	19
3.5	COMPUTAÇÃO MÓVEL .....	19
3.6	DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS APLICATIVOS .....	20
3.7	INSPEÇÕES DE SISTEMAS .....	20
3.8	COLABORADORES TERCEIRIZADOS.....	21
3.9	MONITORAMENTO DE ATIVIDADES .....	21
3.10	INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.....	22
3.11	PLANO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO .....	22
3.12	SOLUÇÕES TÉCNICAS BASEADAS EM REDES SEM FIO .....	22
3.13	EMPREGO DE VOIP .....	23
3.14	EMPREGO DE VIDEOCONFERÊNCIA.....	23
3.15	COMPUTAÇÃO EM NUVEM.....	23
3.16	TRATAMENTO DE DADOS PESSOAIS .....	24
<b>4</b>	<b>POLÍTICAS DE SEGURANÇA .....</b>	<b>25</b>
<b>5</b>	<b>COMPETÊNCIAS.....</b>	<b>26</b>
5.1	DO ÓRGÃO CENTRAL DO STI .....	26
5.2	DOS ELOS DE COORDENAÇÃO DO STI.....	26
5.3	DO CIAER.....	26
5.4	DOS ELOS ESPECIALIZADOS DO STI .....	27
5.5	DOS ELOS DE SERVIÇOS E USUÁRIOS DO STI .....	27
5.6	DO SERVIÇO DE ATENDIMENTO AOS USUÁRIOS DE TECNOLOGIA DA INFORMAÇÃO (SAUTI).....	27
<b>6</b>	<b>ATRIBUIÇÕES.....</b>	<b>28</b>
<b>7</b>	<b>DISPOSIÇÕES FINAIS .....</b>	<b>29</b>
	<b>REFERÊNCIAS .....</b>	<b>30</b>

<b>Anexo A - Política de uso de Recursos Computacionais .....</b>	<b>34</b>
<b>Anexo B - Política de Administração de Recursos Computacionais .....</b>	<b>39</b>
<b>Anexo C - Política de Manipulação de Informações Classificadas .....</b>	<b>43</b>
<b>Anexo D - Política de Antivírus e Códigos Maliciosos .....</b>	<b>45</b>
<b>Anexo E - Política de Firewall e Recursos Computacionais Localizados em Zonas Desmilitarizadas (DMZ) .....</b>	<b>48</b>
<b>Anexo F - Política de Segurança Física .....</b>	<b>48</b>
<b>Anexo G - Política de Segurança dos Serviços de Rede .....</b>	<b>51</b>
<b>Anexo H - Política de Segurança em Servidores .....</b>	<b>53</b>
<b>Anexo I - Política de Acesso Remoto.....</b>	<b>55</b>
<b>Anexo J - Política de Segurança Lógica .....</b>	<b>56</b>
<b>Anexo K - Política de Inspeção.....</b>	<b>58</b>
<b>Anexo L - Política de Backup .....</b>	<b>60</b>
<b>Anexo M - Política de Gestão de Ativos .....</b>	<b>66</b>

## PREFÁCIO

Não está longe o tempo que a manutenção da segurança das informações armazenadas em um sistema de tecnologia da informação (TI) era uma tarefa mais *Simples*. Basicamente, a preocupação restringia-se às senhas e aos níveis de permissão de acesso aos arquivos dos usuários.

Com o surgimento da *Internet* ocorreram grandes mudanças em todas as áreas do conhecimento humano, trazendo avanços nas tecnologias de comunicação e de informação, o que ampliou a gama necessária de procedimentos e de soluções técnicas que visam proteger as informações dos sistemas de TI.

A implantação de protocolos e de serviços da *Internet* nas Organizações do COMAER fez surgir a INTRAER, a INTRANET (rede com protocolos e serviços da *Internet*) do COMAER. A nova rede trouxe grandes benefícios para as OM do Comando, mas também introduziu vulnerabilidades que afetam a segurança dos sistemas de TI.

Além disso, a similaridade entre as funcionalidades da INTRAER e aquelas presentes na *Internet* trouxe para os usuários da rede corporativa a falsa impressão de informalidade e de que poderiam utilizar os recursos de TI disponibilizados pela Organização da mesma forma que utilizavam os seus computadores pessoais, em suas residências, no acesso à *Internet*. Esta postura equivocada dos usuários aumenta o nível de risco a que são expostos os sistemas de TI, pois facilitam a concretização de eventuais ameaças.

A DTI, Órgão Central do Sistema de Tecnologia da Informação, em busca de uma melhoria em seus processos, vem, a cada dia, procurando determinar os fatores que podem vir a impactar o emprego dos recursos e sistemas de TI no apoio à atividade-fim do COMAER.

A partir da identificação das vulnerabilidades existentes nas redes, nos sistemas e nas instalações de TI, é possível prever como “*hackers*” e outros agentes de ameaças podem gerar impactos nos recursos e sistemas de TI do COMAER.

A garantia de um nível adequado de segurança das informações dos sistemas de TI tornou-se um fator crítico para o apoio às atividades do COMAER, constituindo-se a presente norma num passo importante para nortear a implantação, nas suas Organizações, dos procedimentos e soluções técnicas de segurança em suas redes locais de comunicação de dados.

## **1 DISPOSIÇÕES PRELIMINARES**

### **1.1 FINALIDADE**

Orientar as Organizações do COMAER quanto aos princípios de segurança da informação que devem ser seguidos a fim de garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações armazenadas, processadas ou em trânsito a fim de garantir a Defesa do Escopo Cibernético do Comando da Aeronáutica.

### **1.2 CONCEITUAÇÕES**

#### **1.2.1 ACESSO DEDICADO À *INTERNET***

Circuito de comunicação fornecido por um provedor de acesso físico à *Internet*.

#### **1.2.2 ACESSO À *INTERNET***

Estação de trabalho com acesso, via canalização de dados, à rede local de computadores de uma OM do COMAER, possuindo acesso aos sistemas e serviços disponibilizados na INTRAER.

#### **1.2.3 ACESSO REMOTO À INTRAER**

Acesso à INTRAER originado fora de rede local de OM do COMAER.

#### **1.2.4 ADMINISTRADOR DE REDE**

É o militar ou civil designado pelo Comandante/Chefe/Diretor para administrara rede local de computadores de uma Organização Militar.

#### **1.2.5 *ADWARE***

Do inglês *Advertising Software*. Tipo específico de *spyware*. Programa projetado especificamente para apresentar propagandas. Pode ser usado de forma legítima, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil).

#### **1.2.6 ANALISTA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO**

É o militar ou servidor civil designado pelo Comandante/Chefe/Diretor para desempenhar as atividades inerentes à Segurança em Tecnologia da Informação local.

#### **1.2.7 APAGAMENTO SEGURO**

Processo por meio do qual os dados eliminados ficam definitivamente irre recuperáveis.

#### **1.2.8 ATIVOS DE TECNOLOGIA DA INFORMAÇÃO**

Patrimônio composto de ativos físicos, ativos de informação e ativos de *software*.

### 1.2.9 AUTENTICIDADE

Propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

### 1.2.10 BACKDOOR

Qualquer mecanismo inserido no sistema, intencionalmente ou acidentalmente, com o objetivo de permitir o acesso não documentado ao sistema ou aos seus dados. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

### 1.2.11 BIOMETRIA

Reconhecimento do indivíduo a partir de características de partes do seu corpo, por exemplo: a face, a palma da mão, as impressões dos dedos das mãos, a retina ou a íris dos olhos.

### 1.2.12 BOTNETS

Rede formada por diversos computadores zumbis (infectados com *bots*). Permite potencializar as ações danosas executadas pelos *bots* e ser usada em ataques de negação de serviço, esquemas de fraude, envio de *spam*, entre outros. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

### 1.2.13 BOTS

Tipo de malware que, além de incluir funcionalidades de *worms*, dispõe de mecanismos de comunicação com o invasor, os quais permitem que o computador infectado seja controlado remotamente. O processo de infecção e propagação do *bot* é similar ao do *worm*, ou seja, o *bot* é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

### 1.2.14 CAVALO-DE-TRÓIA (TROJANS)

Tipo de malware que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

### 1.2.15 CONFIDENCIALIDADE

Propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

### 1.2.16 CONTA DE USUÁRIO

Identificação individual de usuário, constituída por um código de usuário acompanhado de uma senha, a qual define os direitos de acesso do usuário aos Recursos Computacionais do COMAER.

### 1.2.17 CONTROLE

Conjunto de políticas, processos, procedimentos, estrutura organizacional e funções de *software* e/ou *Hardware* que precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. (Fonte: ABNT NBR ISO/IEC 27002:2013).



### **1.2.18 CONTROLE DE ACESSO**

Conjunto de procedimentos de segurança que balizam os direitos de acesso e restrições para papéis específicos dos usuários acessarem os Recursos Computacionais, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados. (Fonte: ABNT NBR ISO/IEC 27002:2013).

### **1.2.19 CRIPTOGRAFIA**

Arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

### **1.2.20 CTIR.FAB (CENTRO DE TRATAMENTO DE INCIDENTES EM REDES DE COMPUTADORES DA FORÇA AÉREA BRASILEIRA)**

Sigla designativa para o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Força Aérea Brasileira, subordinado ao Órgão Central do Sistema de Tecnologia da Informação (STI) do COMAER e mantido pelo Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER). (Fonte: ICA 7-42/2016 e DCA 11-130/2020)

### **1.2.21 DISPONIBILIDADE**

Propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

### **1.2.22 DMZ (DEMILITARIZED ZONE)**

Uma área na rede de uma empresa que é acessível à rede pública (*Internet*), mas não faz parte da sua rede interna. Geralmente, esses servidores possuem números de IP acessíveis pela rede externa, o que os torna alvos de ataques. Para assegurar que os riscos são minimizados, um sistema de detecção e prevenção de intrusos deve ser implementado nessa *DMZ*.

### **1.2.23 ELOS DE COORDENAÇÃO DO SISTEMA DE TECNOLOGIA DAINFORMAÇÃO DO COMAER – STI**

São os setores pertencentes aos Órgãos de Direção-Geral, de Direção Setorial (ODGS) e aos Órgãos de Assistência Direta e Imediata ao Comandante da Aeronáutica, responsáveis pela coordenação de suas atividades de TI junto ao Órgão Central do STI.

### **1.2.24 ELOS ESPECIALIZADOS DO STI**

São aqueles que, por atribuições regimentais ou por terem sido instituídos em ato específico, executam atividades ou serviços especializados de TI de interesse do COMAER.

### **1.2.25 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.

#### **1.2.26 ELOS USUÁRIOS DO STI**

São todos os militares e servidores civis que utilizam as ferramentas disponibilizadas pelo STI, nos seus locais de trabalho ou nas operações, para o tratamento das informações de interesse do COMAER, tendo a sua autorização, credenciamento e apoio técnico, coordenados pelos seus respectivos Elos de Serviço.

#### **1.2.27 ESTAÇÕES DE TRABALHO**

Designação genérica dos microcomputadores conectados ou não à rede dedados, que são utilizados pelos usuários.

#### **1.2.28 “HACKER”**

Termo de origem inglesa, que significa popularmente indivíduo que elabora e/ou modifica *software* ou *Hardware* de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas, com o intuito de violar sistemas de TI. O correto termo para o *hacker* mal-intencionado é “*CRACKER*”, que não será utilizado nesta publicação.

#### **1.2.29 INCIDENTE DE SEGURANÇA**

Um *Simples* ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações donegócio e ameaçar a segurança da informação.

#### **1.2.30 INFORMAÇÃO CLASSIFICADA**

Informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

#### **1.2.31 INTEGRIDADE**

Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

#### **1.2.32 NÃO REPÚDIO**

Habilidade de provar a ocorrência de um evento ou ação e suas entidades originárias (Fonte: ISO/IEC 27000:2018)

#### **1.2.33 KEYLOGGERS**

Tipo específico de *spyware*, com a capacidade de capturar e de armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de *Internet banking*. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021)

#### **1.2.34 LOG**

Registros de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação a serem mantidos e analisados criticamente, a intervalos regulares. (Fonte: ABNT NBR ISO/IEC 27002:2013).

#### **1.2.35 LOG-ON**

Procedimento seguro de entrada no sistema e acesso aos sistemas e aplicações. (Fonte: ABNT NBR ISO/IEC 27002:2013).

#### **1.2.36 LOG-OFF**

Ato de saída de um sistema de TI ou aplicação.

#### **1.2.37 MALWARE/ PROGRAMA MALICIOSO**

*Software* malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de *software* costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como *e-mail* ou sites. Entre os exemplos de malware estão os vírus, *worms*, *trojans*(ou cavalos de Troia), *spyware*, *adware* e *botnets*. (Fonte: Portaria GSI/PR N° 93, de 18 de outubro de 2021).

#### **1.2.38 MODEM**

Do inglês *Modulator/Demodulator*. Dispositivo responsável por converter os sinais do computador em sinais que possam ser transmitidos no meio físico de comunicação como, por exemplo, linha telefônica, cabo de TV, ar e fibra ótica. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil).

#### **1.2.39 PATCHES**

Atualizações de programas e sistemas operacionais disponibilizados pelos fabricantes, com a finalidade de corrigir erros (*bugs*) constatados durante o tempo de vida do *software* ou sistemas operacionais. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil).

#### **1.2.40 PLANO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO**

Documentação dos procedimentos e das informações necessárias para que o COMAER mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente. (Fonte: Portaria GSI/PR N° 93, de 18 de outubro de 2021).

#### **1.2.41 PORT-SCAN**

O ato de sistematicamente fazer varreduras de portas (local onde informações entram e saem) de Recursos Computacionais.

#### **1.2.42 PROGRAMA MALICIOSO**

O termo refere-se a qualquer código ou programa mal-intencionado que execute ações inesperadas ou não autorizadas, podendo causar danos a um sistema de computador ou comprometer a segurança de uma informação valiosa disponível neste sistema. (Fonte: NBR ISO/IEC 27002 – Código de Práticas para Gestão de Segurança da Informação).

#### **1.2.43 RECURSOS COMPUTACIONAIS**

São os equipamentos, as instalações, as redes de computadores, os programas de computador e os bancos de dados administrados, mantidos ou operados pelo COMAER, que para efeito desta Norma, correspondem ao conjunto formado pelos ativos físicos, de informação e de *software*.

#### **1.2.44 RECURSOS COMPUTACIONAIS CORPORATIVOS**

Recursos computacionais disponibilizados e utilizados no âmbito do COMAER cuja gerência é efetuada por um ODGSA.

#### **1.2.45 RECURSOS COMPUTACIONAIS LOCAIS**

Recursos computacionais existentes, utilizados e administrados no âmbito de cada Organização Militar, cuja gerência é efetuada pelo Setor de TI dessa Organização.

#### **1.2.46 ROOTKIT**

Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado em um computador (*root* ou *Administrator*), mas, sim, para manter o acesso privilegiado em um computador previamente comprometido. (Fonte: Portaria GSI/PR N° 93, de 18 de outubro de 2021).

#### **1.2.47 SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS)**

Refere-se a um mecanismo que, sigilosamente, ouve o tráfego na rede para detectar atividades anormais ou suspeitas e, deste modo, reduz os riscos de intrusão. Existem duas famílias distintas de *IDS*: os *N-IDS* (*network based intrusion detection system* ou sistema de detecção de intrusões de rede), que garantem a segurança dentro da rede e os *HIDS* (*host based intrusion detection system* ou sistema de detecção de intrusões no *host*), que asseguram a segurança no *host*. (Fonte: Portaria GSI/PR N° 93, de 18 de outubro de 2021).

#### **1.2.48 SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**

Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. (Fonte: Portaria GSI/PR N° 93, de 18 de outubro de 2021).

#### **1.2.49 SENHA**

Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser e que possui o direito de acessar o recurso em questão. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil).

#### **1.2.50 SERVIDOR**

Recurso computacional que desempenha alguma função de prestação de serviço de rede, tais como armazenamento de dados, impressão, acesso para usuários e outros.

#### **1.2.51 SISTEMAS DE TI CRÍTICOS**

São equipamentos, programas e serviços disponibilizados pela área de TI, cuja perda de operacionalidade, ainda que temporária, produz impacto considerável na capacidade da Organização em cumprir a sua missão.

#### **1.2.52 SMART CARD**

É um cartão que funciona como mídia armazenadora. Em seus *chips* são armazenadas as chaves privadas dos usuários. O acesso às informações neles contidas é feito por meio de senha pessoal, determinada pelo titular.

#### **1.2.53 SPAM**

Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil).

#### **1.2.54 SPYWARE**

Tipo de *malware*. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. *Keylogger*, *screenlogger* e *adware* são alguns tipos específicos de *spyware*. (Fonte: Portaria GSI/PR N° 93, de 18 de outubro de 2021).

#### **1.2.55 SSH (SECURE SHELL)**

Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferências de arquivos e outros. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil).

#### **1.2.56 REDES SEM FIO**

Soluções técnicas de rede, cujo objetivo é estabelecer conectividade entre estações em uma rede local ou entre segmentos de redes locais, sem a utilização dos tradicionais cabos de pares trançados ou ópticos. O padrão adotado na implementação de redes sem fio é o recomendado na norma *IEEE 802.11 (Institute of Electrical and Electronics Engineers)* e suas variantes. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil).

#### **1.2.57 TOKEN**

Algo que o usuário possui e controla (tipicamente uma chave, senha e/ou módulo criptográfico) e que é utilizado para autenticar a identidade do requerente e/ou a requisição em si. (Fonte: Portaria GSI/PR N° 93, de 18 de outubro de 2021).

#### **1.2.58 VIDEOCONFERÊNCIA**

Solução técnica baseada em recursos de rede de dados que permite o contato audiovisual entre pessoas ou grupos de pessoas que estão em lugares diferentes, através do uso de câmeras de videoconferência e de *software* específicos, baseados nos padrões preconizados nas normas do ITU (International Telecommunication Union).

#### **1.2.59 VÍRUS**

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil)

#### **1.2.60 VOIP**

O termo *VoIP*, ou *Voice Over IP* ou Voz Sobre IP refere-se a soluções tecnológicas que permitem a digitalização de voz e a sua transmissão por redes de dados que utilizam o protocolo IP (*Internet Protocol*). Estas soluções são utilizadas, principalmente, para apoiar atividades de telefonia e videoconferência.

#### **1.2.61 REDE PRIVADA VIRTUAL / VIRTUAL PRIVATE NETWORK (VPN)**

Refere-se à construção de uma rede privada, utilizando redes públicas (por exemplo, a *Internet*) como infraestrutura. Esses sistemas utilizam criptografia e

outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado seja interceptado enquanto estiver passando pela rede pública. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

#### **1.2.62 VULNERABILIDADES**

Condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha. (Fonte: Portaria GSI/PR Nº 93, de 18 de outubro de 2021).

#### **1.2.63 WORM**

Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferentemente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores. (Fonte: Cartilha de Segurança para *Internet* do Comitê Gestor da *Internet* no Brasil).

### **1.3 ÂMBITO**

Esta Norma se aplica a todas as Organizações do COMAER.

## **2 OBJETIVOS**

**2.1** Elencar os princípios básicos a fim de garantir os níveis adequados de segurança da informação de ativos físicos, dos ativos de *software* e dos ativos de informação de interessado COMAER.

**2.2** Conscientizar os usuários de TI do COMAER e os colaboradores terceirizados, sobre a importância de conhecer e aplicar as normas e os procedimentos de segurança da informação preconizados nas legislações inerentes ao assunto, tanto as publicadas na esfera do COMAER, quanto as publicadas em outras esferas governamentais.

**2.3** Estabelecer as condições para operacionalização dos procedimentos de classificação, de processamento, de envio, de armazenamento e de descarte das informações sensíveis que integram os sistemas de TI.

**2.4** Orientar quanto ao emprego adequado de certificados digitais, em conformidade com a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), a fim de garantir a autenticidade e o não repúdio das transações que envolvem os ativos de informação de interesse do COMAER.

**2.5** Definir os requisitos de segurança da informação nas atividades de contratação, de desenvolvimento, de operação e de manutenção de sistemas aplicativos de TI em conformidade com as normas de segurança da informação estabelecidas no COMAER.

**2.6** Conscientizar o público interno do Comando da Aeronáutica sobre as vulnerabilidades e riscos aos quais estão submetidos os recursos computacionais da Organização ou pessoais, seja para defesa da infraestrutura crítica da informação, seja para possível resposta a ações ofensivas perpetradas por elementos adversos.

### 3 PROCEDIMENTOS DE SEGURANÇA

#### 3.1 CONTROLE DE ACESSO FÍSICO

**3.1.1** As instalações que hospedam sistemas de TI devem ter seu acesso controlado e restrito aos elementos devidamente autorizados, a fim de garantir a integridade, a confidencialidade e a disponibilidade das informações. Estas instalações deverão ser providas de sistemas de acesso baseadas no uso de biometria e de circuito fechado de câmeras, devendo o registro dos acessos permanecer arquivado por no mínimo 90 dias.

**3.1.2** Os critérios utilizados para controle de acesso físico serão estabelecidos em instrução específica emitida pelo Órgão Central do STI.

#### 3.2 CONTROLE DE ACESSO LÓGICO

**3.2.1** O acesso lógico aos sistemas de TI deve ser protegido por meio das medidas dedicadas de segurança, tais como senhas seguras ou, quando necessário, de dispositivos de segurança adicionais, tais como *smart cards*, *tokens* e interfaces com biometria.

**3.2.2** Os usuários de sistemas de TI devem preservar a confidencialidade de suas senhas pessoais de acesso aos sistemas e, conseqüentemente, responder por todos os atos praticados utilizando as senhas em questão.

**3.2.3** A necessidade de utilização de dispositivos de segurança adicionais, tais como *smart cards*, *tokens* e interfaces com biometria, ficará sujeita à avaliação por parte do CIAER, mediante solicitação direta do Comandante, Chefe ou Diretor da OM.

**3.2.4** Os critérios utilizados para o controle de acesso lógico serão estabelecidos em instrução específica emitida pelo Órgão Central do STI.

#### 3.3 MEIOS DE PROTEÇÃO CONTRA PROGRAMAS MALICIOSOS

**3.3.1** Deverão ser instalados e configurados, pelos Elos de Serviço, nos equipamentos servidores e nas estações de trabalho de TI, o *software* antivírus corporativo e outros utilitários de *software* indicados pelo Órgão Central que previnam ou mitiguem ataques gerados por programas maliciosos.

**3.3.2** O Órgão Central do STI é responsável pela padronização e fornecimento do *software* de antivírus corporativo, assessorado pelo Núcleo do Centro de Defesa Cibernética da Aeronáutica - NuCDCAER. Os setores de TI das Organizações Militares poderão adquirir produtos distintos do padronizado, desde que autorizado pelo respectivo ODGSA e pelo Órgão Central do STI, e com os recursos previstos no planejamento financeiro da respectiva OM e que seja integrado aos sistema de monitoramento de vulnerabilidades padronizado no COMAER e gerenciado pelo CTIR.FAB.

**3.3.3** É vedado para qualquer fim, seja para uso pessoal ou institucional, o acesso a redes sociais via INTRAER.

**3.3.4** É vedada a utilização de serviços de mensagem instantânea (*chat* ou bate-papo) que trafeguem informações pela *Internet* (hospedados e mantidos por entidades externas ao COMAER), por estes serem, comprovadamente, grandes difusores de programas maliciosos, cabendo ao Chefe do Elo de Serviço de TI a responsabilidade pelo cumprimento deste item.

**3.3.5** Está autorizado o uso de serviços de mensagem instantânea (*chat* ou bate-



papo), de âmbito interno da Organização (rede local) ou entre Organizações (INTRAER), exclusivamente para uso institucional, hospedados e mantidos pela Organização, desde que se utilizem de *Softwares* homologados divulgados na página do Órgão Central do STI na INTRAER.

### **3.4 SERVIÇOS DE REDE DA INTRAER E DA INTERNET**

**3.4.1** Os serviços de rede da INTRAER e da *Internet*, disponibilizados pelas Organizações, deverão ser utilizados somente para apoio às atividades de interesse do COMAER, de acordo com a NSCA 7-1 e a ICA 7-5.

**3.4.2** O Chefe do Setor de TI da OM (Elo de Serviço de TI) deverá negar o acesso aos serviços de rede da INTRAER e da *Internet* quando os mesmos envolverem procedimentos suspeitos que contrariem as leis em vigor no país ou a moral e os bons costumes, ou que venham a prejudicar a realização das atividades de interesse do COMAER, ou que provoquem danos à imagem do COMAER e das demais instituições governamentais, ou, ainda, que causem prejuízos morais ou financeiros a terceiros.

**3.4.3** A entrada em operação de sistemas ou serviços que façam uso de recursos da INTRAER ou da *Internet* só poderá ocorrer a partir de aprovação prévia do Órgão Central do STI.

**3.4.4** É proibida a implantação nas redes locais que integram a INTRAER de sistemas de TI e demais serviços de rede, cuja operação venha a impactar de maneira efetiva o acesso a sistemas de TI de interesse do COMAER ou da Administração Federal, mesmo que os sistemas impactantes sejam restritos ao âmbito da rede local de sua implantação.

**3.4.5** A instalação de um acesso remoto à INTRAER, qualquer que seja o local da implantação, só poderá ocorrer a partir de aprovação prévia do Órgão Central do STI.

**3.4.6** A entrada em operação de acessos dedicados à *Internet* que venham a ser implantados nas Organizações do COMAER só deverá ocorrer a partir de aprovação prévia do Órgão Central do STI.

**3.4.7** A Organização Militar que porventura originar a difusão de vírus ou outro tipo de ameaça eletrônica na INTRAER terá o seu acesso bloqueado à Rede de Dados do Comando da Aeronáutica, por determinação do Órgão Central do STI. O Órgão Central do STI também entrará em contato com a Organização orientando, caso julgue conveniente, seu Comandante, Chefe ou Diretor a instaurar sindicância para apuração de autoria e enviará equipe especializada para auxiliar nos trabalhos de investigação de danos e autoria, bem como na eliminação da ameaça.

### **3.5 COMPUTAÇÃO MÓVEL**

**3.5.1** A utilização de computadores portáteis será precedida de medidas que visem à orientação dos usuários dos equipamentos e, se necessário, do emprego de soluções de criptografia de dados, respeitando normativas gerenciais e técnicas existentes no COMAER. É vedado o uso de computador portátil para trato de assuntos sigilosos, conforme item 3.4.7.1, do RCA 205-1/2006 – Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica.

**3.5.2** É vedada a utilização de computadores pessoais (particulares) na rede das organizações do COMAER.

**3.5.2.1** Excepcionalmente, em situações particulares, por solicitação do Comandante/Chefe/Diretor, poderá ser autorizado o uso de computadores pessoais nas

redes locais, desde que expressamente autorizado pelo respectivo ODGSA.

### **3.6 DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS APLICATIVOS**

**3.6.1** As instalações físicas e os recursos de TI empregados no desenvolvimento, na realização dos testes e na geração das versões de produção dos sistemas de TI não devem ser os mesmos, estabelecendo-se o maior grau de segregação possível entre esses ambientes.

**3.6.2** Os processos de desenvolvimento e manutenção de sistemas aplicativos devem ser acompanhados pelo setor da Organização envolvida, responsável pela segurança das informações, o qual realizará os testes necessários para detectar vulnerabilidades nos sistemas.

**3.6.3** As especificações técnicas para o desenvolvimento, implantação e manutenção de sistemas de TI deverão ser contempladas com os controles de segurança previstos na Norma NBR ABNT ISO/IEC 27002:2013, com a devida customização para as peculiaridades de cada projeto.

### **3.7 INSPEÇÕES DE SISTEMAS**

**3.7.1** Devem ser estabelecidos registros em mídia que permitam, posteriormente, a realização de inspeções em atividades de:

- 1) administração e manutenção dos ambientes operacionais dos sistemas servidores;
- 2) administração e manutenção de sistemas de redes locais, metropolitanas e de longa distância; e
- 3) desenvolvimento, operação e manutenção de sistemas aplicativos.

**3.7.2** É responsabilidade dos Elos de Coordenação do STI a estruturação de equipe de inspetores, no âmbito de seus Grandes Comandos, tomando como base o padrão estabelecido pelo *framework COBIT* ou outro que seja estabelecido pelo Órgão Central do STI, a fim de permitir a realização anual de Inspeção na Área da Segurança da Informação nas respectivas Organizações Militares subordinadas.

**3.7.3** A Inspeção deverá ser realizada em três momentos, a saber:

**3.7.4** Pré-operacional – inspeção realizada antes da implantação de um novo sistema, procedimento ou equipamento; sua segurança e o impacto que este causará na infraestrutura devem ser analisados.

**3.7.3.1** Periódica – inspeção realizada em intervalos de tempos pré-definidos, e com a devida autorização do Comandante, Chefe ou Diretor da OM inspecionada, devendo ser verificados, de forma minuciosa, os procedimentos de acordo com as normas de segurança da informação em vigor, com o objetivo de identificar eventuais falhas e corrigi-las antes de causarem qualquer tipo de prejuízo.

**3.7.3.2** Emergencial – sempre que houver uma falha de segurança, esta inspeção deve ser realizada para evidenciar as causas da vulnerabilidade e buscar formas de corrigir o problema.

**3.7.5** Os inspetores serão pessoas estranhas ao local no qual será realizada a inspeção, de forma a evitar vícios e comprometimentos que possam afetar o processo de inspeção.

**3.7.6** As Organizações Militares deverão sofrer processos de inspeção com uma periodicidade mínima de 02 (dois) anos.

**3.7.7** O Relatório de Inspeção de Sistemas, deverá ser elaborado em duas vias, onde deverão ser apontadas todas as incorreções e irregularidades observadas pela equipe de inspetores.

**3.7.8** Uma via do Relatório de Inspeção de Sistemas deverá ser encaminhada para a OM inspecionada para resposta no prazo de 30 (trinta) dias.

**3.7.9** Uma via do Relatório de Inspeção de Sistemas deverá ser mantida nos arquivos do Órgão Central do STI por 10 (dez) anos para eventuais consultas.

### **3.8** COLABORADORES TERCEIRIZADOS

**3.8.1** Os dispositivos legais utilizados para a contratação de colaboradores terceirizados devem contemplar cláusulas que estabeleçam controles de segurança para os sistemas de TI envolvidos, principalmente as relativas ao estabelecimento de termo de confidencialidade entre as contratadas, conforme normativas estabelecidas na ICA 200-4/2007 (Processo de Concessão de Credencial de Segurança de Pessoa Jurídica).

**3.8.2** Todos os contratos em vigor, que envolvam direta ou indiretamente acesso a dados sigilosos, também deverão ser revisados pelo CIAER a fim de assegurar que recursos críticos não estejam sendo acessados por pessoal terceirizado não credenciado.

### **3.9** MONITORAMENTO DE ATIVIDADES

**3.9.1** Devem ser estabelecidos, pelo Órgão Central do STI, e implementados pelos Elos de Serviço, procedimentos de monitoramento das atividades de TI, realizadas pelos usuários e técnicos de sistemas da área, inclusive pelos colaboradores terceirizados, a fim de permitir uma avaliação permanente do nível de segurança da informação.

**3.9.2** No caso deste monitoramento de atividades – para produção de conhecimento de inteligência – requerer procedimentos invasivos, o mesmo deverá ser precedido de conhecimento formal ao Comandante, Chefe ou Diretor da OM a ser monitorada e somente poderá ser realizada pelo CIAER, conforme definido pela ICA 200-8/2019 – Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações.

**3.9.2.1** Não obstante, com fins de promover o incremento da capacidade de proteção cibernética através da busca de vulnerabilidades, o NuCDCAER e o CIAER, este último representado pela Divisão de Inteligência Cibernética, poderão aplicar técnicas, táticas e procedimentos de exploração cibernética, de forma manual ou automatizada, sem necessidade de autorização da OM, nem necessidade de comunicação prévia, durante ou posterior, visto que a busca por vulnerabilidades de toda INTRAER de forma automatizada acontecerá diariamente, coordenada pelo NuCDCAER.

**3.9.3** O CTIR.FAB é o responsável pelo tratamento, controle, monitoramento, análise forense e resposta a incidentes de segurança, estando sob coordenação do Órgão Central do STI, que dará ciência imediata ao CIAER, ao respectivo Elo de Coordenação do STI e ao Comandante, Chefe ou Diretor da OM envolvida de incidentes de segurança da informação ocorridos.

**3.9.4** O CTIR.FAB é operado pelo Núcleo do Centro de Defesa Cibernética da

Aeronáutica (NuCDCAER), que se encontra na estrutura organizacional do Centro de Computação da Aeronáutica de Brasília.

**3.9.5** O NuCDCAER absorveu também as demais atividades de Defesa Cibernética desempenhadas pelo CCA-BR previstas na NSCA 7-6/2016, na ICA 7-42/2016 e na ICA 7-49/2020.

**3.9.6** O CTIR.FAB é o responsável pela definição do plano de respostas a incidentes e deverá abranger os seguintes aspectos: preparação e treinamento de uma equipe; identificação do incidente; contenção do incidente; eliminação do incidente; reconstituição de forma a torná-lo operacional; notificação ao Órgão Central do STI de Notas Técnicas que tratem dos incidentes ocorridos no âmbito do COMAER.

**3.9.7** A definição das regras para o funcionamento do CTIR.FAB é de competência do Órgão Central do STI.

**3.9.8** O CTIR.FAB deverá enviar relatórios semestrais a respeito dos incidentes de segurança ocorridos no âmbito do COMAER para o Órgão Central do STI, de modo que este Órgão possa contabilizar estatisticamente esses eventos e usá-los no planejamento das ações necessárias preventivas para eliminação ou diminuição dos incidentes de segurança da informação.

### **3.10 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

**3.10.1** Os incidentes de Segurança da Informação devem ser reportados tão logo sejam observados pelo Elo do STI à ETIR responsável pela OM, devendo as informações relevantes serem enviadas para o *e-mail* [abuse@fab.mil.br](mailto:abuse@fab.mil.br).

**3.10.2** O Elo que reportar o incidente deverá preservar, tanto quanto possível, as evidências do incidente observado, visando possibilitar procedimentos específicos de análise ligados ao fato, a fim de garantir a legitimidade do procedimento e das evidências coletadas.

**3.10.3** A Instrução que estabelece os parâmetros de funcionamento do CTIR.FAB e o processo de atendimento aos incidentes de Segurança da Informação e a prática forense computacional necessária na etapa de coleta de evidências é a ICA 7-42 - Gerenciamento de Incidentes de Segurança em Redes de Computadores no Comando da Aeronáutica.

**3.10.4** O Órgão Central do STI produzirá e divulgará conhecimento baseado na análise dos relatórios estatísticos referentes aos atendimentos a incidentes de Segurança da informação, objetivando eliminar a falha de segurança explorada ou minimizar a ocorrência dessas situações.

### **3.11 PLANO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO**

**3.11.1** Cada um dos sistemas de TI considerados críticos pelo COMAER deve estar protegido por um Plano de Continuidade de Negócios em Segurança da Informação. A competência para a elaboração e a implantação desse Plano pertence ao gestor do sistema, seja Elo de Coordenação ou Elo Especializado do STI..

**3.11.2** Os critérios utilizados para a confecção de Planos de Continuidade de Negócio em Segurança da Informação serão definidos em legislação complementar emitida pelo Órgão Central do STI.

### **3.12 SOLUÇÕES TÉCNICAS BASEADAS EM REDES SEM FIO**

**3.12.1** O emprego de redes sem fio para estabelecer conectividade entre estações ou redes que integram a INTRAER só poderá ser efetivado com autorização do Órgão Central do STI.

**3.12.2** Os critérios utilizados para a emissão de autorização para uso de redes sem fio serão estabelecidos em instrução específica emitida pelo Órgão Central do STI.

**3.12.3** O emprego de redes sem fio como solução técnica de TI para atender a atividades ou sistemas de interesse do COMAER só poderá ser efetivado com autorização do Órgão Central do STI, mesmo que estas atividades ou sistemas estejam isolados da INTRAER e que sua operação tenha caráter temporário.

### **3.13** EMPREGO DE VOIP

**3.13.1** Os projetos que visam o emprego de *VoIP* como solução técnica para atender necessidades de Organizações do COMAER deverão ser submetidos ao DECEA para análise e aprovação, com antecedência mínima de 90 (noventa) dias de sua data prevista de entrada em operação.

**3.13.2** Os critérios utilizados para emissão de autorização para uso de *VoIP* serão estabelecidos em instrução específica emitida pelo Órgão Central de Telecomunicações (DECEA).

### **3.14** EMPREGO DE VIDEOCONFERÊNCIA

**3.14.1** Os projetos que visam à implantação de soluções de videoconferência para atender a necessidades de Organizações do COMAER deverão ser submetidos à DTI, Órgão Central do STI, para análise e aprovação, com antecedência mínima de 90 (noventa) dias de sua data prevista de entrada em operação.

**3.14.2** Os critérios utilizados para emissão de autorização para uso de videoconferência serão estabelecidos em instrução específica emitida pela DTI, Órgão Central do STI.

**3.14.3** Está autorizado o uso de serviços de videoconferência ou *VoIP* de âmbito interno da Organização (rede local) ou entre Organizações (INTRAER), desde que seja informado ao Órgão Central do STI a solução utilizada.

**3.14.4** Está autorizado o uso de serviços de videoconferência ou *VoIP* via *Internet*, para assuntos exclusivos da OM, desde que se utilize uma solução com criptografia comercial e que não sejam tratados assuntos sigilosos.

**3.14.5** O sistema de videoconferência de âmbito interno da Organização (rede local) e entre Organizações (INTRAER) de qualquer teor de assunto e as videoconferências onde serão tratadas assuntos sigilosos deverão ser os padronizados e mantidos pela DTI.

**3.14.6** O uso de redes sociais para assuntos institucionais exclusivos da OM pode ser implantado, desde que se utilize ponto de acesso à *Internet* não conectado à INTRAER e que não sejam tratados assuntos sigilosos.

### **3.15** COMPUTAÇÃO EM NUVEM

**3.15.1** A implementação de soluções e serviços com hospedagem em nuvem devem seguir as regras previstas na Norma NBR ABNT ISO/IEC 27017 e da IN GSI N° 5/2021, desde que não sejam hospedados dados e informações sigilosas.

**3.15.2** A utilização de quaisquer serviços hospedados em nuvem por alguma Organização Militar do COMAER requererá autorização prévia do respectivo ODGSA,

com assessoramento do Órgão Central de STI.

### **3.16     TRATAMENTO DE DADOS PESSOAIS**

**3.16.1**       As orientações para o tratamento de dados pessoais no âmbito do COMAER estão estabelecidas na DCA 16-6/2021 - Governança da Proteção de Dados Pessoais do Comando da Aeronáutica, que preconiza a extensão a todos os tipos de dados pessoais, não somente àqueles apontados da Lei 13.709 de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

#### **4 POLÍTICAS DE SEGURANÇA**

**4.1** Aplicar-se-ão a todas as Organizações do Comando da Aeronáutica, as Políticas definidas nos Anexos A, B, C, D, E, F, G, H, I, J e K desta NSCA, as quais são adaptadas da legislação em vigor, constante das referências.

## 5 COMPETÊNCIAS

### 5.1 DO ÓRGÃO CENTRAL DO STI

São competências do Órgão Central do STI:

- a) estabelecer normas, padrões e metodologias relativas à Segurança da Informação, que estejam em conformidade com a legislação brasileira e com os padrões aceitos internacionalmente;
- b) receber e avaliar sob o ponto de vista de Segurança da Informação, as propostas, enviadas pelos Elos de Coordenação do STI, relativas a sistemas aplicativos e a serviços de TI, que pretendem fazer uso dos recursos da INTRAER ou da *Internet*;
- c) emissão de Notas Técnicas, no âmbito do COMAER, com o propósito de difundir as informações necessárias a fim de que um dado incidente de segurança não ocorra novamente;
- d) encaminhar ao CIAER cópia dos Relatórios de Incidentes do CTIR.FAB; e
- e) informar aos Elos de Coordenação do STI da existência de procedimentos de monitoramentos invasivos nas áreas de competência de cada ODGSA.

### 5.2 DOS ELOS DE COORDENAÇÃO DO STI

São competências dos Elos de Coordenação do STI:

- a) estabelecer procedimentos adequados para a identificação, a avaliação e o gerenciamento dos riscos associados à segurança dos sistemas de TI na sua área de responsabilidade, conforme norma específica a ser emitida pelo Órgão Central do STI;
- b) encaminhar ao Órgão Central do STI as propostas de sistemas aplicativos e de serviços de TI que pretendem fazer uso dos recursos da INTRAER ou da *Internet*;
- c) estabelecer um plano de resposta a incidentes envolvendo a segurança dos sistemas de TI na sua área de responsabilidade de acordo com a orientação emanada no item 3.10.2 desta NSCA;
- d) estabelecer procedimentos, na sua área de responsabilidade, que garantam aos técnicos e aos usuários de sistemas de TI, inclusive aos colaboradores terceirizados, o conhecimento das normas de segurança da informação, respeitadas as particularidades de cada cargo ou função exercida;
- e) assessorar as Organizações do COMAER na sua área de responsabilidade quanto aos procedimentos para a monitoração das atividades de TI executadas nas suas instalações; e
- f) adequar a estrutura organizacional dos seus Elos do STI subordinados, de modo a contemplar um setor responsável pela segurança da informação dos sistemas de TI sob sua responsabilidade.

### 5.3 DO CIAER



Estabelecer normas, padrões e metodologias que regularizem o emprego de equipamentos criptotécnicos e de comunicações, conforme estabelecido na ICA 200-8, denominada de Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações.

#### **5.4 DOS ELOS ESPECIALIZADOS DO STI**

São competências dos Elos Especializados do STI:

- a) estabelecer procedimentos adequados para a identificação, a avaliação e o gerenciamento dos riscos associados à segurança dos sistemas de TI sob sua área de responsabilidade; estabelecer um plano de resposta a incidentes envolvendo a segurança dos sistemas de TI sob sua responsabilidade;
- b) estabelecer procedimentos que garantam aos seus técnicos de TI, inclusive aos colaboradores terceirizados, o conhecimento das normas de segurança da informação, respeitadas as particularidades de cada cargo ou função exercida; e
- c) notificar ao Órgão Central do STI as informações relativas aos incidentes de segurança ocorridos no âmbito do COMAER bem como as providências adotadas para saná-los.

#### **5.5. DOS ELOS DE SERVIÇOS E USUÁRIOS DO STI**

É competência dos Elos de serviços e usuários do STI a adequação de suas atividades de TI, de modo a cumprir o estabelecido nos procedimentos de segurança descritos e nas demais normas relativas à segurança das informações dos sistemas de TI.

Todo Elo de serviço do STI deverá procurar implantar o conteúdo da cartilha “Boas práticas em segurança da informação – 4ª edição, 2012” ou versão mais atualizada, disponível no site do Tribunal de Contas da União ([www.tcu.gov.br](http://www.tcu.gov.br)), e verificar seus procedimentos de segurança conforme a ICA 200-5/2009 “Gerenciamento de Plano de Segurança Orgânica do Comando da Aeronáutica”.

Todo usuário do STI deverá tomar conhecimento do conteúdo da cartilha de segurança, disponível no site [www.cert.br](http://www.cert.br), a fim de dotá-lo do conhecimento mínimo necessário a respeito do tema segurança da informação.

#### **5.6 DO SERVIÇO DE ATENDIMENTO AOS USUÁRIOS DE TECNOLOGIA DA INFORMAÇÃO (SAUTI)**

- a) registrar os dados referentes aos incidentes de Segurança da Informação relatados pelos Elos do STI;
- b) acionar o CTIR.FAB para tratamento do incidente de segurança; e
- c) enviar ao Órgão Central do STI relatório estatístico trimestral referente aos atendimentos a incidentes de Segurança da Informação.

## **6 ATRIBUIÇÕES**

Aos Comandantes, Chefes e Diretores incumbe garantir, no âmbito de suas Organizações, o cumprimento dos procedimentos de segurança descritos nesta NSCA, bem como a capacitação dos usuários e do efetivo dos Elos de Serviço de TI de suas respectivas OM quanto à aplicação do preconizado nas Normas das séries ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27005:2019 e respectivas atualizações, fazendo uso dos recursos financeiros devidamente planejados em instrumentos de planejamento, tais como os Planos Diretores de Tecnologia da Informação e os Programas de Trabalho Anuais de cada Organização Militar.

## **7 DISPOSIÇÕES FINAIS**

**7.1** Esta publicação substitui a NSCA 7-13/2013, aprovada pela Portaria COMGAP nº 31/3EM, de 06 de maio de 2013.

**7.2** Esta Norma entrará em vigor na data da publicação da Portaria de Aprovação.

**7.3** O comandante da OM é responsável pelo fiel cumprimento das normas contidas deste documento, bem como pela aplicação dos procedimentos cabíveis decorrentes do não cumprimento no âmbito de Organização.

**7.4** Caberá à SEFA a instauração de procedimentos de ressarcimento ao erário no caso em que estes danos forem comprovados, bem como o encaminhamento desse processo ao TCU.

**7.5** Os casos não previstos nesta NSCA serão submetidos à apreciação do Comandante-Geral de Apoio.

**7.6** O Centro de Defesa Cibernética da Aeronáutica - CDCAER, no ato de sua criação, assumirá os papéis, responsabilidades e competências atribuídos ao NuCDCAER nesta Norma.

## REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27001. **Tecnologia da informação**: Técnicas de segurança: Sistemas de gestão de segurança da informação: Requisitos. ABNT: Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27002 **Tecnologia da informação**: Técnicas de segurança: Código de prática para controles de segurança da informação. ABNT: Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27005. **Tecnologia da informação**, Técnicas de segurança: Gestão de Riscos de Segurança da Informação. ABNT: Rio de Janeiro, 2019.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. PORTARIA EMAER nº 31/6SC, de 27 de outubro de 2006. Aprova a Norma de Sistema do Comando da Aeronáutica que estabelece o Gerenciamento do Ciclo de Vida dos Sistemas de Tecnologia da Informação da Aeronáutica: NSCA 7-4. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 203, 1º nov. 2006.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria nº 650/GC3, de 31 de julho de 2007. Aprova a edição da instrução que versa sobre a concessão de credencial de segurança de pessoa jurídica - ICA 200-4. **BSA**, Rio de Janeiro, 15 jun. 2007.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria nº 2, de 02 de março de 2009. Aprova a edição da instrução que versa sobre o gerenciamento de plano de segurança orgânica do Comando da Aeronáutica - ICA 200-5. **BSA**, Rio de Janeiro, 25 maio 2009.

BRASIL. Comando da Aeronáutica. Departamento de Ciência e Tecnologia Aeroespacial. Portaria DCTA nº 272/DTI, de 11 de agosto de 2014. Aprova a edição da instrução que dispõe sobre a política de segurança em tecnologia da informação e uso dos recursos computacionais do DCTA - ICA 7-34. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 168, 05 set. 2014.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº 050/3SC, de 21 de dezembro de 2015. Aprova a reedição da Norma de Sistema do Comando da Aeronáutica que estabelece a estrutura e as competências do Sistema de Tecnologia da Informação do Comando da Aeronáutica: **NSCA 7-7. Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 236, 23 dez. 2015.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria nº1869/GC3, de 15 de dezembro de 2015. Aprova a edição da instrução para a salvaguarda de assuntos sigilosos da aeronáutica (ISAS) - ICA 205-47. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 232, 17 out. 2015.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº 051/3SC, de 21 de dezembro de 2015. Aprova a reedição da Instrução que trata do Uso da Rede Mundial de Computadores - INTERNET – no Comando da Aeronáutica: **ICA**

**7-5. Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 236, 23 dez. 2015.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. Portaria nº 145/3EM, de 10 de agosto de 2016. Aprova a reedição da norma de sistema que define as atribuições específicas para os centros de computação da aeronáutica - NSCA 7-6. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 136, 15 ago. 2016.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº 41/3SC, de 9 de setembro de 2016. Aprova a edição da Instrução que tratado Gerenciamento de Incidentes de Segurança em Redes de Computadores no Comando da Aeronáutica. ICA 7-42. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 158, 16 set. 2016.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. Portaria COMGAP nº 60/ADNP, de 20 de agosto de 2020. Aprova a edição da Instrução que dispõe sobre a Visita de Assessoria Técnica em Segurança da Informação (VAT-SEG) nas Organizações do COMAER: ICA 7-49. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 154, 27 ago 2020.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria GABAER Nº 197/GC3, de 15 de dezembro de 2021. Aprova a Diretriz que dispõe sobre a Governança da Proteção de Dados Pessoais do Comando da Aeronáutica: DCA 16-6. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 232, 20 dez. 2021.

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, n. 74, 20 abr. 2022.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. Portaria COMGAP nº 38/ADLG, de 21 de abril de 2022. Aprova a reedição da norma de sistema do comando da aeronáutica que trata do funcionamento do serviço de atendimento aos usuários de tecnologia da informação do Comando da Aeronáutica (SAUTI) - NSCA 7-8. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 77, 27 abr. 2022.

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. Disponível: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215>. Acesso em: 02 maio 2022.

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. Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172>. Acesso em: 02 maio 2022.

BRASIL. Instrução Normativa GSI nº 5, de 30 de agosto de 2021. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684>. Acesso em: 02 maio 2022.

BRASIL. Instrução Normativa GSI nº 6, de 23 de dezembro de 2021. Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal. Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-6-de-23-de-dezembro-de-2021-370081858>. Acesso em: 02 maio 2022.

BRASIL. Ministério da Economia. **Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019**. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. Disponível em: [https://www.in.gov.br/materia/-/asset\\_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535](https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70267659/do1-2019-04-05-instrucao-normativa-n-1-de-4-de-abril-de-2019-70267535). Acesso em 02 maio 2022.

BRASIL. Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**: seção 1, Brasília, DF, n. 156, de 17 ago. 2009.

BRASIL. Norma Complementar nº 07/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. **Diário Oficial da União**: seção 1, Brasília, DF, n. 134, de 16 jul. 2014.

BRASIL. Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**: seção 1, Brasília, DF, n. 162, de 24 ago. 2010.

BRASIL. Norma Complementar nº 09/IN01/DSIC/GSIPR, Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. **Diário Oficial da União**: seção 1, Brasília, DF, n. 134, de 16 jul. 2014.

BRASIL. Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. **Diário Oficial da União**: seção 1, Brasília, DF, nº 30, de 10 fev. 2012.

BRASIL. Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de *Software* Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. **Diário Oficial da União**: seção 1, Brasília, DF, n. 224, de 21 nov. 2012.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria**

**GSIPR nº 93, de 18 de outubro de 2021.** Aprova o Glossário de Segurança da Informação. Disponível em: <https://www.jusbrasil.com.br/diarios/documentos/1300227607/portaria-n-93-19-10-2021-ato-publicado-no-dou> . Acesso em: 02 maio 2022.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**, 4. ed. - Brasília: TCU, 2012. Disponível em: [https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp%3FfileId%3D8A8182A24F0A728E014F0B226095120B&sa=U&ved=2ahUKEwjb7IPh\\_rH3AhVRJ7kGHTARCSIQFnoECAQQAQ&usg=AOvVaw0B9JYsVycqjKyyGogs7-Pn](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp%3FfileId%3D8A8182A24F0A728E014F0B226095120B&sa=U&ved=2ahUKEwjb7IPh_rH3AhVRJ7kGHTARCSIQFnoECAQQAQ&usg=AOvVaw0B9JYsVycqjKyyGogs7-Pn). Acesso em 26 abr. 2022.

BRASIL. Comitê Gestor da *Internet* no Brasil. **Cartilha de Segurança para Internet**. 4. Ed. São Paulo: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-Internet.pdf>. Acesso em: 26 abr. 2022.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Glossário de Segurança da Informação**: Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1>. Acesso em 26 abr. 2022.

BRASIL **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm) . Acesso em: 02 maio 2002

*INTERNATIONAL ORGANIZATION FOR STANDARDIZATION* - ISO/IEC 27002. **Information Security, cybersecurity and privacy protection - Information security controls**. Suíça, 2022.

*INTERNATIONAL ORGANIZATION FOR STANDARDIZATION* - ISO/IEC 27000. **Information technology - Security techniques - Information security Management systems - Overview and vocabulary**. Suíça, 2018.

## **Anexo A - Política de uso de Recursos Computacionais**

Para uso dos Recursos Computacionais do COMAER deve ser observado o que se segue

### **1 RECURSOS COMPUTACIONAIS**

**1.1** Os recursos computacionais do COMAER têm por finalidade servir à pesquisa, ao desenvolvimento, ao ensino e às atividades técnicas, administrativas e operacionais de interesse do serviço.

**1.2** O uso dos recursos computacionais do COMAER também está sujeito às leis federais.

**1.3** Quanto ao uso da *Internet* no COMAER, os usuários também devem observar, além dos normativos internos, as normas e recomendações do Comitê Gestor da *Internet* no Brasil (CGI.BR).

### **2 AUTORIZAÇÃO DE USO**

**2.1** O usuário, para utilizar os recursos computacionais do COMAER, deve solicitar ao Elo de Serviço de sua OM a abertura de uma conta de usuário, a qual o identificará univocamente.

### **3 CONTAS DE USUÁRIOS**

**3.1** A solicitação de abertura de Contas de usuário, tanto em recursos computacionais locais como em recursos computacionais corporativos, se dá pelo preenchimento da Ficha de Cadastro de usuário, conforme estabelecido por cada OM do COMAER, que deve ser assinada pelo usuário solicitante e por seu responsável, sendo o Chefe da Seção, onde o usuário está desempenhando suas atividades, o responsável pela solicitação da criação de conta de usuário.

**3.2** O responsável pela solicitação da Conta de usuário deve providenciar a abertura desta conta junto à Equipe de TI da OM.

**3.3** As fichas de Cadastro de usuário devem ficar arquivadas junto à Seção de Tecnologia da Informação da OM.

**3.4** Para a abertura de Contas de usuário em recursos computacionais locais, a OM responsável poderá definir procedimentos adicionais, além dos aqui previstos

### **4.1 USO DAS CONTAS DE USUÁRIOS**

**4.1.1** A Conta de usuário e a respectiva senha são atribuídas a um único usuário. Elas são intransferíveis e não devem ser compartilhadas, assumindo o usuário da senha integral responsabilidade pela sua guarda e sigilo, bem como pelo uso indevido de terceiros.

**4.1.2** As senhas devem ser tratadas como informação classificada do COMAER.

**4.1.3** O usuário é responsável, individualmente, pela sua Conta de usuário e por todas as atividades desenvolvidas através dela, nos recursos computacionais do COMAER.

**4.1.4** As senhas utilizadas pelos usuários devem atender, no mínimo, os seguintes requisitos:



- a) não devem conter nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas;
- b) não devem conter palavras que façam parte de dicionários, ou seja, nomes de músicas, filmes e outros; e
- c) ter no mínimo oito caracteres, priorizando a utilização de frases complexas no lugar de palavras ou a utilização de maiúsculas e minúsculas, números, sinais de pontuação e símbolos; e
- d) não devem fazer parte de bases públicas de senhas previamente comprometidas.

**4.1.5** As contas de usuário e senhas não devem ser inseridas em mensagens de *e-mail* ou qualquer outra forma de comunicação eletrônica, escritas em papel, bilhetes colados nos Recursos Computacionais ou guardadas em qualquer local.

**4.1.6** Não deve ser usada senha única para Contas de usuários diferentes e para sistemas autônomos diferentes.

**4.1.7** Todas as senhas de usuário, após o primeiro acesso aos recursos computacionais, devem ser imediatamente trocadas.

**4.1.8** Todas as senhas existentes em recursos computacionais recebidos de terceiros devem ser substituídas.

**4.1.9** Senhas suspeitas de terem sido descobertas deverão ser imediatamente trocadas.

**4.1.10** O acesso a um recurso computacional, após 3 (três) tentativas com erros de Conta de usuários e/ou senha, deverá ser bloqueada. A reativação da Conta de usuário deverá ser solicitada à Equipe de TI da OM.

## **4.2 USO DOS RECURSOS COMPUTACIONAIS**

**4.2.1** O usuário é responsável pelos eventuais arquivos e informações de cunho pessoal que possam existir nos recursos computacionais do COMAER, sendo que os mesmos, para todos os efeitos, não estão sujeitos a qualquer regime de privacidade e são passíveis de monitoramento e inspeção pelo CTIR.FAB ou pela Equipe de Segurança em TI da respectiva OM, em consonância com as normas e legislação vigente.

**4.2.2** O usuário é responsável pelo uso da informação a que tiver acesso, bem como pela sua distribuição.

**4.2.3** Toda informação armazenada nos recursos computacionais ou transmitida, pela Rede Local ou pela INTRAER, será tratada e considerada pertencente à respectiva OM.

**4.2.4** O usuário é responsável pelo *backup* e recuperação das informações existentes em sua estação de trabalho e pelo armazenamento das correspondentes mídias

**4.2.5** Quando utilizar recursos computacionais portáteis do COMAER, o usuário deve realizar cópia de segurança, não conectá-los em redes externas não pertencentes ao COMAER (ou se necessário, prover os cuidados adequados), não permitir seu uso por terceiros (exceto sob consentimento explícito do responsável), provê-los de mecanismo de trava física e lógica e, em hipótese alguma, deixá-los desprotegidos em áreas públicas, devolvendo-os ao setor responsável após o seu uso.

**4.2.6** O usuário deve comunicar, imediatamente, ao seu chefe imediato e ao responsável direto pelo recurso computacional do local onde o fato tenha ocorrido,

qualquer violação das regras contidas nesta Norma ou prejuízos causados por terceiros, a eles próprios e aos recursos computacionais do COMAER.

**4.2.7** Os Administradores de Segurança de TI das OM, ou, na sua ausência os Administradores de Rede das OM, preferencialmente, deverão possuir telefones celulares funcionais cujo número deverá ser divulgado para acioNamento a qualquer tempo.

**4.2.8** Qualquer mau funcionamento de um sistema deverá ser imediatamente reportado à Equipe de TI da OM, pois a demora neste ato poderá levar a sérios danos aos sistemas, e até mesmo à indisponibilidade dos Recursos Computacionais envolvidos.

**4.2.9** Informações a respeito de medidas de segurança são confidenciais e não devem ser reveladas para pessoas não autorizadas.

**4.2.10** Os Recursos Computacionais somente poderão se conectar fisicamente às redes de dados do COMAER.

**4.2.11** Todas as mídias removíveis, independentes da fonte, devem ser verificadas com programa antivírus antes de serem utilizadas.

**4.2.12** Os usuários são responsáveis por eventuais disseminações de vírus em seus sistemas sempre que não observarem as medidas previstas na Política de Antivírus e Códigos Maliciosos (Anexo D), e desta forma notificar imediatamente à Equipe de TI da OM, caso ocorra algum incidente.

**4.2.13** O usuário deve observar o estabelecido na política para recebimento (download) de arquivos, por *e-mail* ou qualquer outro meio eletrônico, disposto na alínea h da Política de Antivírus e Códigos Maliciosos (Anexo D).

**4.2.14** É vedado ao usuário de recursos computacionais:

- a) utilizar os recursos computacionais para fins diversos dos funcionais ou institucionais, em desacordo com esta Norma e com as demais publicações vigentes no COMAER;
- b) efetuar acesso não autorizado, atacar ou monitorar os recursos computacionais ou redes de dados, utilizando recurso da rede local da OM ou outros meios;
- c) tentar ou efetuar acesso não autorizado a arquivos confidenciais do COMAER;
- d) próprio acesso, por meio do monitoramento do barramento de dados, ou das redes de dados existentes no COMAER;
- e) tentar ou efetuar a interferência em serviços de outros usuários ou o seu bloqueio, utilizando recursos da rede local da OM ou outros meios;
- f) violar ou tentar violar os sistemas de segurança dos recursos computacionais do COMAER, como quebrar ou tentar adivinhar contas de usuário ou senha de terceiros;
- g) utilizar *Softwares* em desacordo com o estabelecido no item 4.4 deste Anexo A;
- h) instalar ou manter programas maléficos dentro da rede ou de servidores tais como vírus, *worms*, cavalos-de-tróia (*trojans*), *adware*, *spywares*, mail

bombs, *backdoor*, *keyloggers*, *bots*, *botnets*, *botnets* e assemelhados, que possam colocar em risco os recursos computacionais;

i) utilizar serviços de redes sociais, mensagens instantâneas ou de bate-papo disponíveis na *INTERNET* (aqueles hospedados e mantidos por entidade externa ao COMAER) sem autorização expressa do Órgão Central do STI;

j) interromper processos de rastreamento de vírus;

k) utilizar, armazenar ou distribuir, nas redes de comunicação e nos recursos computacionais do COMAER, informações indesejadas, tais como, correntes de cartas, circulares e similares, materiais obscenos, ofensivos, ilegais, não éticos, comercial privado, propagandas, ameaças, difamação, injúria, racismo, *spam* ou outro que venham a causar molestamento, tormento ou danos a terceiros;

l) utilizar, armazenar ou distribuir material com conteúdo que incentive ou instrua a invasão de recursos computacionais ou redes de computadores;

m) instalar, alterar, configurar ou excluir os recursos computacionais, tanto de *Hardware* como de *Software*, existentes tanto nas redes locais como na INTRAER;

n) remanejar recursos computacionais sem a prévia autorização do responsável por seu Setor Funcional e sem o prévio conhecimento da Equipe de TI da OM;

o) acessar simultaneamente um mesmo recurso computacional. Caso o usuário identifique um acesso simultâneo deverá imediatamente comunicar à Equipe de TI da OM, sob pena de responder por sua omissão;

p) fazer má utilização dos recursos computacionais, expondo-os a choques elétricos ou magnéticos, líquidos e outros fatores que possam provocar danos aos mesmos;

q) realizar a transferência de qualquer informação ou documento classificado, existente nos recursos computacionais do COMAER, sem a prévia autorização do Responsável por seu Setor Funcional, sem a devida proteção criptográfica e sem a utilização da Rede de Comunicação de Dados Sigilosos (Rede Mercúrio), mantida e normatizada pelo CIAER;

r) utilizar processo criptográfico em arquivos contendo informação ou documentos, mesmo que de caráter pessoal, residentes nos recursos computacionais de propriedade do COMAER, sem que para isso tenha autorização;

s) utilizar processo criptográfico em arquivos contendo informação ou documento não ostensivo residentes nos recursos computacionais, diferente do padrão definido, sem conhecimento do Chefe da Equipe de TI da OM ou de quem por ele tenha sido investido nesse poder;

t) impedir ou dificultar, de alguma forma, a realização das atividades de monitoramento e inspeção dos recursos computacionais do COMAER; e

u) realizar qualquer outro procedimento de uso dos recursos

computacionais não previsto neste Anexo, que possa afetar de forma negativa o COMAER, outras organizações e seus usuários.

#### **4.3 USO DE SOFTWARE**

**4.3.1** O usuário deve respeitar os direitos de propriedade intelectual, em particular os que se referem à lei em vigor que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País.

**4.3.2** O usuário deve observar que toda e qualquer utilização dos recursos computacionais do COMAER deverá estar de acordo com todas as obrigações contratuais assumidas pelo COMAER, inclusive no que respeita às limitações definidas nos contratos de *Software* e outras licenças.

**4.3.3** Os *Softwares* cedidos por produtores ou seus representantes legais, a título de demonstração ou teste, deverão estar acompanhados de contratos específicos formalizados.

**4.3.4** O *Software* de propriedade do usuário ou por ele contratado de terceiros, deverá estar acompanhado do seu contrato específico formalizado ou seu termo de responsabilidade, juntamente com o comprovante de registro do produto, quando da utilização do mesmo no âmbito do COMAER e sua utilização só poderá ser realizada com a autorização da Equipe de TI da OM.

**4.3.5** Os *Softwares* classificados como de domínio público (*freeware*) seguirão orientação específica de cada Elo de Serviço, desde que o *Software* seja gratuito para uso corporativo.

**4.3.6** É vedado ao usuário de qualquer *Software*:

- a) escrever, gerar, compilar, copiar, propagar, executar ou tentar introduzir nos recursos computacionais do COMAER, códigos ou *Software* contendo processos destrutivos;
- b) invadir recursos computacionais do COMAER, com exceção daqueles usuários cuja função esteja relacionada com a utilização destas ferramentas para os fins de monitoramento e inspeção, na forma prevista nesta Norma;
- c) utilizar os *Softwares* do COMAER em atividades particulares;
- d) explorar, sem autorização, aplicações e sistemas corporativos para obter dados ou alterar dados;
- e) norma, que possa afetar de forma negativa o COMAER, outras organizações e usuários; e
- f) possuir senha de administrador de estação de trabalho, a fim de que não efetue instalação de *Software*.

## **Anexo B – Política de Administração de Recursos Computacionais**

Na administração dos recursos computacionais do COMAER, os Elos do STI, por meio de suas respectivas Equipes de TI, devem observar as regras descritas abaixo e aplicá-las no âmbito de suas respectivas OM do Comando da Aeronáutica.

**1.1** Definir, implementar e manter um único Sistema de Cadastro de Contas de usuários contendo informações cadastrais de todas as contas existentes na sua OM de origem, seja em recursos computacionais corporativos, seja em recursos computacionais locais.

**1.1.1** Priorizar, quando possível, a integração com o Servidor de Autenticação de Login Único do STI.

**1.2** Abrir, administrar e encerrar contas de usuários.

**1.2.1** Garantir que durante a abertura de conta o usuário assine um Termo de Compromisso e Manutenção de Sigilo, declarando ler e cumprir a presente norma, além de cumprir as leis de direitos autorais e as legislações de proteção de dados

**1.3** Prover uma única conta para cada usuário, mantendo-a igual em todos os recursos computacionais locais nos quais ele vier a ter acesso, quando viável tecnologicamente.

**1.4** Validar anualmente as contas de usuários na sua rede local.

**1.5** Consultar, periodicamente, os Chefes dos Setores Funcionais quanto às atualizações das informações cadastrais pertinentes aos seus usuários.

**1.6** Manter mecanismos para exigir dos usuários a mudança de senha sempre que evidências de comprometimento foram identificadas ou em intervalos de até 360 (sessenta) dias. Nestes casos, a troca de senha deverá ser realizada e cada OM deverá definir mecanismos próprios para trocas de senhas.

**1.7** Manter mecanismos para impedir a repetição de senhas considerando as seis últimas senhas utilizadas.

**1.8** Prover meios para moderar a utilização de mensagem instantânea ou de bate-papo disponíveis na *INTERNET* que sejam hospedados e mantidos por entidades externas ao COMAER e não autorizados pelo Órgão Central do STI.

**1.9** Prover mecanismos para bloquear a conta de usuário após 3 (três) tentativas de acesso a um recurso computacional com erros de conta de usuário e/ou senha.

**1.10** Prover meios para suspender as sessões de uma estação de trabalho, após um período de inatividade de 10 (dez) minutos, e para encerrar as sessões, após um período de suspensão de 10 (dez) minutos.

**1.11** Prover a segurança e a integridade dos recursos computacionais disponíveis, dos serviços aos usuários e dos dados armazenados nas máquinas servidoras sob sua responsabilidade, atentando para os requisitos previstos nas normas vigentes de Proteção de Dados.

**1.12** Agendar e realizar o processo de execução de cópias de segurança (*backup*) de Servidores e armazenar as mídias correspondentes conforme procedimento definido nesta Norma.

**1.13** Manter os recursos computacionais sempre atualizados, pesquisando, obtendo

e aplicando, sempre que possível, os pacotes de correção e atualização disponibilizados pelos fabricantes, atentando também para os pacotes de terceiros que sejam dependências dos recursos computacionais utilizados nas redes locais.

**1.14** Suspender temporariamente o acesso de qualquer usuário a todo e qualquer recurso computacional sob sua responsabilidade, nos casos de suspeita de violação desses recursos computacionais. Se comprovada a violação dos recursos, pelo usuário, deverá ser encaminhada pela Chefia da Equipe de TI da OM, Parte Administrativa ao Comandante, Chefe ou Diretor da OM, para que sejam tomadas as medidas cabíveis, determinando a abertura de sindicância ou mesmo inquérito, sob pena de que a Chefia da Equipe de TI ou mesmo o Comandante da Unidade responderem solidariamente pelos danos causados. Nos casos em que forem comprovados danos ao erário, o processo deverá ser encaminhado à SEFA para providências.

**1.14.1** Isolar da rede local os recursos computacionais com suspeita de violação e seguir os procedimentos de perícia forense digital propostos pelo NuCDCAER, caso seja oportuno.

**1.14.2** Se comprovada a violação dos recursos, pelo usuário, deverá ser encaminhada pela Chefia da Equipe de TI da OM, Parte Administrativa ao Comandante, Chefe ou Diretor da OM, para que sejam tomadas as medidas cabíveis, determinando a abertura de sindicância ou mesmo inquérito, sob pena de que a Chefia da Equipe de TI ou mesmo o Comandante da Unidade responderem solidariamente pelos danos causados. Nos casos em que forem comprovados danos ao erário, o processo deverá ser encaminhado à SEFA para providências.

**1.15** Suspender temporariamente serviços de rede local em caso de violação ou suspeita de violação dos recursos computacionais locais, informando o fato ao Comando/Chefia/Direção da OM.

**1.16** Difundir constantemente as normas e procedimentos para uso de recursos computacionais, estabelecidos no Anexo “A” desta norma.

**1.17** Analisar a rede local sob a sua responsabilidade, utilizando *Software* ou equipamento apropriado, com o objetivo de garantir um desempenho adequado sem, no entanto, afetar ou alterar qualquer configuração de outra rede local, que não esteja sob a sua responsabilidade.

**1.18** Configurar o servidor de *e-mail* para gerar automaticamente estatísticas de uso de cada usuário, sempre que possível.

**1.19** Realizar alterações de emergência na rede de comunicação de dados para prevenir mudanças inadvertidas que podem levar à negação de serviços, revelação de informação não autorizada e outros problemas análogos.

**1.20** Realizar monitoramento e inspeção na utilização dos recursos computacionais locais, quando autorizado pelo Comando/Chefia/Direção da respectiva OM, visando preservar a integridade das informações institucionais e a imagem do COMAER, podendo fiscalizar:

- a) conteúdo de mensagens transmitidas e recebidas;
- b) arquivos residentes em discos;
- c) programas de computadores instalados;
- d) fluxo de pacotes na rede local;

- e) arquivos específicos de controle;
- f) programas de computador em execução; e
- e) outros recursos computacionais.

**1.21** Limitar a área reservada aos usuários no servidor de *e-mail* e estabelecer um prazo máximo para a manutenção de mensagens não superior a 180 (cento e oitenta) dias, dando ciência destes fatos aos usuários. Ao término deste prazo, as mensagens deverão ser retiradas do sistema e tratadas conforme critério da OM.

**1.22** Evitar esforços para evitar o acesso simultâneo de mais de um usuário a um mesmo recurso computacional, evitando assim possíveis acessos não autorizados..

**1.23** Impedir, durante o registro de senhas, a utilização de senhas comuns, fracas ou comprometidas. Comparar a senha escolhida com bases públicas de senhas previamente comprometidas, palavras de dicionários, caracteres repetidos, entre outros.

**1.23.1** Informar ao usuário a política de senhas em uso.

**1.24** Responsabilizar-se por outras tarefas inerentes à sua função que forem determinadas pelo Comando/Chefia/Direção.

**1.25** Prover a interface de usuário para acesso aos recursos computacionais utilizando *logon* e protetores de tela ajustados e padronizados institucionalmente para ativação após no máximo 10 (dez) minutos de inatividade e desativados automaticamente com o uso da senha.

**1.26** Conceder privilégios de sistema para atender o mínimo necessário à realização das atividades dos usuários, reavaliando-os periodicamente para que os privilégios desnecessários sejam revogados.

**1.27** Instalar em todos os recursos computacionais utilizados pelos usuários um *Software* antivírus homologado e atualizado, de preferência corporativo, conforme estabelecido na Política de Antivírus e Códigos Maliciosos (Anexo D).

**1.28** Desabilitar a opção de execução automática de arquivos anexados dos *Softwares* clientes de correio eletrônico.

**1.29** Modems e quaisquer outros dispositivos de conexão remota à rede deverão ser desinstalados ou desabilitados nos Recursos Computacionais.

**1.30** Zelar para que os sistemas multiusuários ou sistemas de dados incluam ferramentas automatizadas para verificação do estado de segurança dos sistemas. Estas ferramentas devem incluir meios para registro, detecção e correção de problemas de segurança.

**1.31** Zelar para que os desenvolvedores de aplicativos garantam que seus programas suportam autenticação de usuários individuais, e não de grupos.

**1.32** Prover meios para que arquivos com registro de eventos sejam mantidos por pelo menos 2 (dois) anos. Durante este período estes arquivos devem ser mantidos seguros e à disposição apenas de pessoas autorizadas, assim como protegidos contra alterações. Para prover evidências para investigação, medidas legais e ações disciplinares, estas informações devem ser capturadas sempre que um crime, ou abuso relativo a redes de computadores for detectado. As informações relevantes devem ser mantidas armazenadas *off-line* até que sejam necessárias. Estas informações incluem: registro de acesso aos arquivos, registros de execução de

aplicativos, assim como cópias de todos os arquivos potencialmente envolvidos.

**1.33** Dar ciência aos usuários que todas as atividades relacionadas ao uso dos recursos computacionais do COMAER são passíveis de registro, monitoramento e inspeção, em compatibilidade com as normas vigentes de Proteção de Dados.

**1.34** Ajustar o tamanho máximo permitido para envio e/ou de mensagens e/ou arquivos segundo necessidades de sua OM.

**1.35** Desativar caixas postais não acessadas por um período de mais de 60 (sessenta) dias, desde que não justificado.

**1.36** Configurar o *Software* de *e-mail* para pedir senha ao entrar na conta de correio.



### **Anexo C - Política de Manipulação de Informações Classificadas**

Para o armazenamento e tramitação seguros de informações classificadas (sensíveis), deve-se observar o disposto a seguir:

- a) dados e informações classificadas deverão ser transmitidos por meio eletrônico, desde que obrigatoriamente criptografado, em sistema de cifra de alta confiabilidade, com algoritmo de Estado, homologado pelo CIAER conforme preconizado a Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (Fonte: ICA 205-47/2015).
- b) os acessos às informações classificadas devem ser registrados e exigir a autenticação do usuário, do Recurso Computacional e do ponto de acesso.
- c) sendo possível, o sistema deverá emitir avisos para o Administrador de Rede Local no caso de tentativas de acessos não autorizados aos dados classificados.
- d) a transmissão de dados classificados somente poderá ocorrer com a utilização de um mecanismo de criptografia, utilizando-se de um programa de encriptação de dados, observando-se o disposto na RCA 205-1.
- e) dados classificados e mantidos nos Recursos Computacionais do COMAER deverão estar criptografados através do programa de criptografia, a qual observa o disposto no RCA 205-1.
- f) as cópias de segurança (*backup*) devem ser mantidas de acordo com a Política de Segurança Lógica, que se encontra detalhada no Anexo “J” desta Instrução.
- g) informações classificadas devem ser tratadas conforme preconizado na Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ICA 205-47/2015).
- h) toda exclusão de informações classificadas deverá ser executada através de um processo de apagamento seguro.
- i) quando os recursos computacionais não estiverem sendo utilizados e as informações neles contidos forem classificadas, estas deverão ser apagadas, conforme item anterior. Caso seja necessário que estas informações permaneçam no recurso computacional, o mesmo deverá ser armazenado em local seguro, com acesso restrito ao pessoal responsável.
- j) em caso de extravio de recursos computacionais contendo informações classificadas, o Setor de Inteligência da OM deverá ser imediatamente comunicado pelo Comando/Chefia/Direção da OM via parte reservada, e todas as chaves compartilhadas em outros recursos deverão ser trocadas.
- k) deverá ser aberto, a critério do Comandante, Chefe ou Diretor da OM, processo de sindicância para apuração do extravio de recursos computacionais.
- l) deverá ser aberto Boletim de Ocorrência na Delegacia mais próxima da ocorrência do extravio caso o mesmo tenha ocorrido *exterNamente* às dependências da OM.
- m) deve existir uma ferramenta para verificação regular e automática da integridade e autenticidade dos dados classificados em uso para alertar os

administradores de rede sobre toda e qualquer alteração.

n) sempre que a encriptação for usada, a versão original do documento deverá ser apagada após a execução do processo de deciptação e verificado o correto restabelecimento da versão original.

o) chaves de encriptação usadas pelo COMAER são sempre tratadas como informações classificadas e, portanto, não podem ser reveladas para consultores, trabalhadores temporários ou similares. O acesso a estas chaves deve ser restrito ao pessoal autorizado e a quem tem a necessidade de usá-las.

p) não deverá ser feita a impressão de informações classificadas em dispositivos de impressão de rede.

q) até onde o sistema operacional permitir, o manuseio de informações classificadas ou críticas deve ser registrado quanto a quaisquer eventos relacionados à segurança.

r) Elaborar o Relatório de Impacto de Proteção de Dados (RIPD) nos processos, projetos e serviços que utilizarem informações classificadas contendo dados pessoais para fins de defesa nacional, segurança do Estado, que poderão ou deverão ser solicitados pela Autoridade Nacional de Proteção de Dados (ANPD) nos casos previstos na Lei Geral de Proteção de Dados Pessoais (LGPD). (Fonte: DCA 16-6/2021).

### **Anexo D - Política de Antivírus e Códigos Maliciosos**

Com relação a esta política, são definidos os requisitos abaixo relacionados à prevenção, detecção e erradicação de vírus, contaminações e códigos maliciosos nos recursos computacionais.

- a) todos os computadores do COMAER devem ter instalado um programa antivírus, fornecido ou recomendado pelo Órgão Central do STI, devidamente licenciado e atualizado.
- b) preferencialmente, o servidor que executa o antivírus corporativo na OM deve ser dedicado.
- c) os computadores infectados devem ser fisicamente desconectados da rede até que seja garantida a sua descontaminação.
- d) o programa antivírus deve ser configurado para que seja periodicamente atualizado e executado em intervalos regulares, de preferência de maneira automática.
- e) o *Software* antivírus emitirá alerta quando ocorrer a detecção de malware. O CTIR.FAB deve possuir acesso ao servidor principal do antivírus corporativo, de modo a ter acesso às informações de detecção de malware.
- f) sempre que possível, habilitar no recurso computacional a opção de verificação automática de vírus nas mídias removíveis.
- g) os recursos computacionais, sempre que possível, deverão estar protegidos contra códigos maliciosos do tipo *adware*, *spyware*, cavalo-de-tróia (*trojans*), *worms*, *backdoors*, *keyloggers*, *bots*, *botnets*, *rootkit* e outros que possam surgir.
- h) fica estabelecida a seguinte política para download (recebimento) de arquivos, por *e-mail* ou qualquer outro meio eletrônico:
  - excepcionalmente, e quando estritamente necessário ao exercício das atividades funcionais do usuário, será permitido o recebimento de arquivos comerciais, tais como imagens, textos e outros, que deverão ser rastreadas (“escaneados”) por antivírus antes de serem abertos;
  - é estritamente proibido o carregamento de qualquer arquivo executável recebido pelos usuários, colaboradores ou prestadores de serviços com extensões do tipo *EXE*, *.COM*, *.SCR*, ou outros que possam comprometer o sistema através da execução de comandos maliciosos, vírus, *trojans* e outros similares, e
  - quando se tratar de atualização de *Software*, que envolva arquivos deste tipo, a Equipe de TI da OM será a responsável por executar o serviço.
- i) o NuCDCAER poderá assessorar o Órgão Central do STI na criação, edição e coordenação da implantação das políticas gerais da ferramenta de antivírus.
- j) o CCA-BR poderá, junto a representantes dos ODGSA, assessorar o Órgão Central do STI na definição de cronogramas de implantação e

atualização da ferramenta do antivírus no COMAER.

k) cabe aos Elos de Serviço que possuem servidores de antivírus descentralizados executarem o cronograma de implantação e atualização da ferramenta do antivírus nas OM apoiadas.

l) o CCA-BR poderá informar ao Órgão Central do STI e aos ODGSA o panorama de instalação e atualização da ferramenta de antivírus, para devidas providências em suas OM subordinadas.

m) cabe ao CCA-BR acompanhar a disponibilidade dos servidores de antivírus no COMAER, bem como, notificar os responsáveis visando o restabelecimento do serviço.

n) as OM que decidirem pela não utilização do antivírus em algum dispositivo de sua OM deverão informar a motivação ao Órgão Central do STI e serão responsáveis pelas ameaças decorrentes desta decisão..

o) é de responsabilidade da OM reportar ao CCA-BR qualquer dificuldade de instalação e atualização do antivírus.

p) é responsabilidade da OM que possua algum servidor de antivírus descentralizado designar apoio técnico local com vistas a facilitar a comunicação com CCA-BR.

q) o CCA-BR deve possuir acesso de administrador em todos os servidores de antivírus.

r) cabe ao CCA-BR capacitar os Elos De Serviços, quanto a instalação, configuração e atualização da ferramenta de antivírus.

### **Anexo E - Política de *Firewall* e Recursos Computacionais Localizados em Zonas Desmilitarizadas (DMZ)**

As Organizações do COMAER deverão adotar medidas de defesa em profundidade e configurar servidores de *firewall*, *IPS/IDS* (do inglês, *Intrusion Prevention System* ou Sistema de Prevenção de Intrusão) e *WAF* (do inglês, *Web Application Firewall* ou *firewall* de aplicação *web*) em suas respectivas Redes de Comunicação de Dados Locais e Rede Corporativa de comunicação de dados, de forma a atender ao que se segue:

- a) o *firewall* deverá intermediar as comunicações entre as Redes Locais das OM e as demais (*Internet*, *INTRAER* ou outras) de forma a minimizar os incidentes de segurança e o seu uso abusivo;
- b) o ponto de entrada e saída da rede das Redes Locais das OM deverá ser controlado e monitorado por *IDS*, com configuração condizente com os serviços de TI prestados pela organização;
- c) o *firewall* deverá adotar a posição de negação padrão, bloqueando todo e qualquer tráfego entre as redes, exceto aqueles serviços necessários para as atividades funcionais;
- d) sempre que possível, deverá adotar medidas de defesa em profundidade utilizando-se de mecanismos diversos de proteção contra falhas de defesa; e
- e) sempre que for necessária a liberação de algum serviço para a *INTERNET*, este deverá ser disponibilizado em uma zona desmilitarizada (*DMZ*) onde serão feitos os controles necessários para a proteção e monitoração de tentativas de invasão, negação de serviços, dentre outros.
- f) a solução de *IDS/IPS* pode estar inclusa em uma solução de *firewall*;
- g) sempre que o *firewall*, *IDS*, *IPS* ou *WAF* possuir registro que indique a possibilidade de um incidente de segurança, o administrador deverá notificar o CTIR.FAB através do *e-mail* [abuse@fab.mil.br](mailto:abuse@fab.mil.br) com as evidências do evento suspeito;
- h) durante atividades realizadas pelo CIAER ou pelo NuCDCAER em que haja a necessidade de acesso à rede local, as regras de *firewall* devem ser ajustadas de modo a permitir este acesso.
- i) sempre que tomar conhecimento de alguma ameaça cibernética, o NuCDCAER poderá propor a implementação de bloqueios criação de assinaturas nas soluções de *firewall*, *IPS* e *WAF*;
- j) sempre que for necessária a liberação de algum serviço para a *INTERNET*, *INTRAER* ou a outra rede externa à Organização Militar, o serviço deverá estar disponibilizado em uma zona desmilitarizada (*DMZ*) onde serão feitos os controles necessários (com *firewall*, *IPS/IDS* e *WAF*) para a proteção e monitoração de tentativas de invasão, negação de serviços, dentre outros.

### **Anexo F - Política de Segurança Física**

Todos os usuários de recursos computacionais do COMAER, ou terceiros, conectados ou não às redes locais de comunicação de dados de uma OM, devem observar os procedimentos descritos a seguir:

- a) os equipamentos de conectividade (roteadores, switches, servidores e outros dispositivos de interconexão) deverão estar em salas exclusivas e com acesso restrito às Equipes de TI das respectivas redes de comunicação de dados. Equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo classificados somente poderão estar ligados a redes de computadores seguras e que sejam fisicamente e logicamente isoladas de qualquer outra, observando-se o disposto no RCA 205-1/2006.
- b) estes equipamentos deverão possuir, na medida do possível, quadros de alimentação exclusivos que deverão permanecer trancados e com acesso restrito a pessoas habilitadas e com a devida ciência do Chefe da Equipe de TI da OM.
- c) as salas onde esses equipamentos estão localizados deverão ser providas de mecanismos de tranca e, de controle de acesso pessoal, preferencialmente, com reconhecimento biométrico; usuários não credenciados não poderão ter acesso a estes equipamentos.
- d) as salas onde esses equipamentos estão localizados deverão ser providas de mecanismos de monitoramento e controle ambiental de forma a minimizar ameaças potenciais como roubo, fogo, explosivos, fumaça, poeira, vibração, efeitos químicos, temperatura, umidade, dentre outros. Deve-se, ainda, manter as salas e os recursos computacionais limpos, organizados e conservados, sendo proibido o consumo de alimentos, bebidas, cigarros e similares nestes locais.
- e) para a conexão de computadores ao backbone sempre adotar switches ou equipamentos equivalentes que possibilitem o controle de portas.
- f) os Recursos Computacionais deverão passar por processo de manutenção preventiva periódica para evitar falhas de *Hardware*. Todas as manutenções preventivas ou corretivas deverão ser documentadas para que haja um histórico dos problemas ocorridos e das respectivas soluções.
- g) caso haja necessidade da entrada de outra pessoa em salas de acesso restrito, que não dos membros das equipes locais de TI, ela deverá ser acompanhada por pelo menos um dos membros da referida equipe.
- h) a alimentação elétrica para os Recursos Computacionais deverá ser exclusiva, constante e em níveis adequados ao funcionamento desses recursos, bem como possuir aterramento apropriado à proteção contra surtos e sobretensões, seguindo-se as recomendações fornecidas pelo fabricante de cada equipamento.
- i) os equipamentos de interconexão da Rede Local de cada OM devem estar alimentados por no-break com autonomia mínima de 20 (vinte) minutos a plena carga.
- j) o cabeamento interno das Redes Locais, bem como os de interconexão entre redes, deverá estar encapsulado em conduítes e/ou calhas que o

protejam de interrupções acidentais, e deverão estar identificados para que não sejam expostos indevidamente. O acesso ao cabeamento deverá somente ser permitido à pessoa autorizada e qualificada para tal.

k) nenhum recurso computacional poderá ser movimentado sem o expresso consentimento dos detentores do material carga e com o conhecimento e aval do Chefe de TI da OM, para que o mesmo execute os procedimentos de segurança que forem necessários, em função da destinação do equipamento e dos dados nele armazenados, estabelecidos nesta Política. Deve-se, ainda, manter um registro de entrada e saída contendo horário, data e nome do responsável pela movimentação destes recursos.

l) a manutenção dos equipamentos, da Rede de Comunicação de Dados Locais das OM do COMAER, deverá ser feita preferencialmente nas dependências da própria Organização à qual pertence o equipamento, com a supervisão de um ou mais membros da Equipe de TI da OM.

m) quando qualquer equipamento necessitar ser retirado do seu local de origem, para manutenção, ou qualquer outro fim, que não seja o uso de um sistema nele contido, este deverá ter todos os arquivos (de configuração e/ou dados) apagados de forma segura, quer estejam em disco (usando técnicas para sobrescrever um disco para garantir que qualquer dado previamente existente torne-se completamente ilegível), memórias ou qualquer outro meio de armazenamento, para que o mesmo não comprometa a segurança interna da respectiva rede. Esta operação deverá ser executada quantas vezes forem necessárias, de forma a impossibilitar a recuperação de informações anteriormente armazenadas.

n) as Organizações Militares do COMAER, através das suas Equipes de TI, deverão manter um controle rígido sobre os usuários e os equipamentos que estão conectados às suas respectivas Redes de Comunicação de Dados Locais, de forma a impedir qualquer conexão de recursos computacionais não autorizados àquelas redes.

o) as Organizações Militares do COMAER, através das suas Equipes de TI, deverão manter um inventário atualizado dos recursos computacionais com no mínimo as seguintes informações: Local e usuário para contato; detalhamento do *Hardware* e sistema operacional utilizados; principais funções e aplicativos.

p) as Organizações Militares do COMAER, através das suas equipes de TI, deverão manter os seus recursos computacionais com os respectivos gabinetes lacrados, permitindo assim, constatar a ocorrência de possíveis violações. Estes equipamentos somente poderão ser abertos pelas Equipes de TI responsáveis.

q) em caso de violação do lacre, a Equipe de TI da OM deverá ser acionada para a execução de vistoria especializada. A não comunicação imediata da violação do lacre por parte do detentor da carga à Equipe de TI da OM implica na sua responsabilização.

r) mídias de *backup* devem ser armazenadas em compartimentos à prova de fogo e água e separados fisicamente do local do sistema copiado, preferencialmente em outro prédio.

s) as Organizações Militares do COMAER deverão proteger todos os equipamentos de conexão de rede com dispositivo anti-roubo, desde que localizados em ambientes abertos.

t) no desligamento ou demissão de Servidor civil ou afastamento do militar, solicitar a devolução de bens de propriedade da organização, condicionando esta devolução ao desimpedimento de sua ficha pelo Setor de TI da OM e, consequentemente, sendo pré-requisito para o seu desligamento.

u) todos os recursos computacionais deverão ser desligados no final de expediente de trabalho, quando não houver previsão de utilização dos mesmos.

v) os servidores de rede, switches e outros equipamentos de conectividade existentes na Organização Militar do COMAER, deverão estar ligados 24 (vinte e quatro) horas por dia, sete dias por semana. Caso sejam desligados por motivos de manutenção programada ou força maior, os usuários deverão ser comunicados previamente.



### **Anexo G - Política de Segurança dos Serviços de Rede**

Na disponibilização dos serviços de rede deve ser observado o que se segue:

- a) os servidores conectados à Rede Local, a princípio, são privativos para uso da comunidade de usuários interna, devendo estar protegidos contra acessos indevidos.
- b) os servidores que disponibilizam serviços para a comunidade de usuários externa deverão estar na zona desmilitarizada (*DMZ*), e sempre ser monitorados contra tentativas de invasão e negação de serviços.
- c) cada serviço deverá ser disponibilizado em um ou mais Servidores dedicados, sendo que este deverá, sempre que possível, comportar apenas um serviço.
- d) a responsabilidade pela manutenção dos serviços é do chefe da equipe de TI da OM que os hospedam.
- e) serviços ou protocolos inseguros devem ser atualizados para suas versões mais recentes e seguras ou substituídos por equivalentes mais seguros, sempre que existirem, antes de serem disponibilizados na rede local da OM.
- f) o protocolo *SNMP* (*Simple Network Management Protocol* - Protocolo *Simples* de Gerência de Rede) é de uso exclusivo dos Administradores de Rede, dos membros da equipe de Segurança da Informação da OM, dos Elos Especializados do STI e do CTIR.FAB.
- g) o acesso ao serviço *DNS* (*Domain Name System* - Sistema de Nomes de Domínios) deve ser limitado à consulta para a resolução de nomes. A transferência de zonas de domínio internas deverá ser somente para Servidores secundários.
- h) deve-se isolar o Servidor *DNS* de Rede Local do Servidor *DNS* de *INTERNET*, protegendo-o contra acessos externos à rede local da OM.
- i) o serviço de banco de dados deverá ter uma política específica, em conformidade com a Política de Manipulação de Informações Classificadas (Anexo C).
- j) em caso de comprometimento da segurança cibernética de um Servidor, o incidente deve ser reportado para a Equipe de Tratamento de Incidentes (ETIR) responsável, e a equipe de TI da OM deve adotar os procedimentos sugeridos por aquela ETIR. Quando se tratar de crime envolvendo o espaço cibernético, todos os vestígios deverão ser preservados segundo orientações da ETIR para posterior realização de perícia forense computacional.
- k) todos os *Softwares* dos recursos computacionais deverão estar atualizados com os patches mais recentes previamente testados em ambiente isolado.
- l) os logs de serviços, dos sistemas operacionais dos servidores e de acessos a switches e roteadores, devem ser mantidos por um período mínimo de 6 (seis) meses. Qualquer atividade suspeita deve ser comunicada à Equipe de Tratamento de Incidentes (ETIR) responsável pela OM.
- m) deverá ser definida pelo Órgão Central do STI uma topologia para

implementação de um serviço de sincronização de relógios (NTP – *Network Time Protocol* – Protocolo de Tempo para redes), para uso na INTRAER, no prazo de 01 (um) ano, a contar da data da publicação desta Instrução.

n) a responsabilidade da manutenção, monitoração de funcionamento e segurança, bem como, da aplicação dos patches dos sistemas é do Chefe da Equipe de TI da OM, no âmbito das suas respectivas sub-redes e domínios.

o) Caso haja a necessidade de manutenções remotas, a possibilidade deve ser avaliada pela equipe responsável para cada caso, considerando os riscos envolvidos e as medidas de segurança disponíveis.

### **Anexo H - Política de Segurança em Servidores**

Todos os servidores de rede do COMAER ou de terceiros, e que não sejam acessados externamente à rede local de uma OM devem obedecer os procedimentos descritos abaixo:

- a) todos os servidores devem ser gerenciados pelos Administradores de Rede Locais, que devem manter manuais atualizados de configuração segura destas máquinas de maneira a refletir o descrito nesta Política.
- b) servidores corporativos devem ser configurados para carregar seus sistemas exclusivamente a partir do disco rígido interno. Todos os outros meios que puderem ser usados para a carga do sistema devem ser desabilitados, exceto em situações temporárias necessárias e definidas pelo Chefe da Equipe de TI da OM.
- c) não devem existir múltiplas contas de acesso ao servidor para um mesmo usuário, com exceção dos Administradores de Rede Local. Contas padrão como root e administrador, quando não utilizadas, devem ser desativadas.
- d) nenhum programa deve ser executado no Servidor pelo usuário a partir de uma estação de trabalho, exceto aqueles definidos e permitidos claramente pelo Administrador de Rede Local.
- e) as sessões de uma estação de trabalho devem ser suspensas pelo Administrador de Rede Local após um período de inatividade, e encerradas após um período pré-determinado depois do tempo esgotado, de acordo com o previsto no item 1.9 do Anexo B desta Instrução.
- f) todas as funções de segurança e as alterações e inclusões de *Software* devem ser feitas a partir do Servidor e apenas pelo Administrador de Rede Local.
- g) o acesso físico ao servidor via console não deve ser uma prática rotineira. O acesso lógico de usuários ao servidor, após as devidas configurações de acessibilidade, deverá ser somente através da rede. O mesmo deve ser realizado somente por protocolos de acesso seguros como SSH, RDP.
- h) os arquivos classificados devem ser mantidos criptografados segundo a Política de Manipulação de Informações Classificadas (Anexo C). Isto inclui arquivos de senha, arquivos-chave e arquivos com dados confidenciais.
- i) todas as transações devem ser registradas, tais como as tentativas de entrada mal sucedidas no sistema, operação/acesso não autorizados, suspensão e encerramento de sessão (acidental ou deliberada), mudanças na atribuição de *Software* e de segurança, entrada/saídas do sistema (logons/logoffs), outras atividades designadas (por exemplo, acessos aos arquivos classificados) e, opcionalmente, todas as atividades, por um período de 6 (seis) meses.
- j) os usuários devem possuir diretórios próprios para armazenamento de arquivos.
- k) não devem ser transferidos programas e arquivos para as áreas públicas; o mesmo vale para as macros e bibliotecas de macros, salvo necessidade de divulgação pública e o referido programa ou arquivo não venha a

comprometer a segurança do Servidor ou da rede local da OM.

l) O número de tentativas de validação de senhas deve ser limitado a uma quantidade máxima de 3 (três). Caso seja extrapolado este limite, a conta à qual a senha está vinculada deverá ser bloqueada. A reativação desta conta deverá ser solicitada ao Chefe da Equipe de TI da OM.

m) caso seja necessário, um procedimento adicional de identificação de usuários poderá ser usado, dependendo das informações a serem acessadas.

n) os servidores corporativos devem estar registrados em um documento mantido em poder dos Chefes da Equipe de TI das respectivas OM, contendo no mínimo as seguintes informações: localização do Servidor e o contato do Administrador de Rede Local; *Hardware* do Servidor; versão do sistema operacional e *Softwares* instalados; função principal e aplicação a que se destina.

o) alterações de configurações de Servidores em operação devem seguir os procedimentos padronizados e documentados de acordo com o planejamento estabelecido pela Equipe de TI da OM.

p) serviços e aplicações que não serão usados devem ser desabilitados ou desinstalados do Servidor sempre que possível.

q) acessos aos serviços devem ser registrados e protegidos.

r) relações de confiança entre sistemas oferecem riscos à segurança e, portanto, devem ser substituídas, sempre que possível, por outros métodos mais seguros de comunicação.

s) os Servidores de rede devem estar fisicamente localizados em ambientes de acesso controlado, conforme definido na Política de Segurança Física (Anexo F).

t) quando da instalação de um novo Servidor, roteador ou switch, as senhas originais devem ser substituídas, assim como as contas padrões devem ser renomeadas ou desativadas.

u) os eventos relacionados à segurança devem ser reportados à Equipe de Tratamento de Incidentes (ETIR) responsável pela OM por meio do *e-mail* abuse@fab.mil.br com as evidências do evento suspeito, que tomará as ações de tratamento necessárias. Medidas corretivas serão prescritas conforme necessidade. Eventos relacionados à segurança incluem, mas não se limitam: ataques de port-scan; evidência de acessos não autorizados a contas privilegiadas; ocorrências anômalas que não são relacionadas a aplicações específicas do recurso computacional.

v) bloquear a execução de scripts nos servidores, exceto aqueles analisados e autorizados pelo administrador da rede local. Esta premissa pode ser reavaliada com frequência, no mínimo, semestral. O bloqueio é motivado pela possibilidade de impacto na disponibilidade, autenticidade e integridade dos sistemas hospedados no respectivo servidor, necessitando de análise cuidadosa pelo administrador da rede local.

w) o sistema operacional dos servidores deve ser atualizado sempre que houver novas versões disponíveis que sejam compatíveis com os serviços em execução.

### Anexo I - Política de Acesso Remoto

Todos os usuários que necessitem utilizar acessos remotos a uma rede local de uma OM, devidamente autorizados pelo Elo de Coordenação do ODGSA, observadas as regras emanadas pelo Órgão Central do STI, devem observar os procedimentos descritos a seguir.

- a) as implementações de acesso remoto coberto por esta Política incluem, mas não se limitam a serviços, tais como, modems, ISDN (Integrated Service Digital *Network* – Rede Digital de Serviços Integrados), frame relay, VPN (Virtual Private *Network*) e SSH (Secure Shell).
- b) somente serão permitidos acessos remotos à INTRAER através de conexões passando pelos *firewalls* corporativos e locais, devendo ser obrigatoriamente registrados e mantidos por no mínimo 6 (seis) meses.
- c) não é permitido que de equipamentos da rede local de uma OM originem-se conexões de redes que não sejam controladas pelos *firewalls* corporativos, tais como acesso discado, wireless e equivalentes.
- d) o acesso remoto à rede local de uma OM deve ser, obrigatoriamente, controlado através de um esquema de autenticação forte como códigos e senhas com validade de acesso ou chaves públicas.
- e) não serão permitidos os acessos remotos provenientes de redes externas à rede local de uma OM, bem como aos recursos computacionais, através de contas com privilégios de Administrador, Supervisor ou Superusuário. O acesso, como Administrador, Supervisor ou Superusuário, só poderá ser feito via console ou através da rede local de uma OM por intermédio de um protocolo seguro utilizando criptografia forte.
- f) para a devida proteção de informações e detalhes de uso aceitável quando acessando a rede local de uma OM, deve-se seguir o previsto nos Anexos A e C desta Norma.
- g) todo acesso remoto deve utilizar-se de algoritmos criptográficos, de acordo com a definição feita pelo CIAER, e de códigos de autenticação, assinaturas digitais ou outro sistema que permita a identificação do usuário no acesso à rede local da OM.
- h) não é permitido realizar acesso discado a sistemas internos ou externos, exceto quando, para atender uma necessidade excepcional e temporária, esse acesso seja justificado e devidamente autorizado pelo Elo de Coordenação de TI do ODGSA envolvido, observados os requisitos emanados pelo Órgão Central do STI. O acesso à INTRAER por intermédio do uso da *INTERNET* somente poderá ser realizado mediante uso de solução desenvolvida pelo CIAER. Caso não haja a possibilidade de uso de solução desenvolvida pelo CIAER, o Órgão Central do STI poderá autorizar o uso de soluções distintas.
- i) o uso de tecnologias baseadas em propagação de ondas eletromagnéticas, em rede, deve ser autorizado pelo Elo de Coordenação de TI do ODGSA, observadas as regras emanadas pelo Órgão Central do STI.

### **Anexo J - Política de Segurança Lógica**

Todos os recursos computacionais utilizados no COMAER, corporativos ou de terceiros, conectados ou não à rede local de uma OM, que mantenham ou não dados importantes e/ou classificados, devem observar os procedimentos descritos a seguir:

- a) para ter acesso ao serviço disponibilizado pelas Redes de Dados locais e pela INTRAER, o usuário necessita ser cadastrado e a partir de então, identificar-se através de uma Conta de usuário e uma senha.
- b) o nível de acesso aos arquivos (programas e dados), quanto à leitura, escrita e execução, deve ter uma atribuição individual, por grupo ou pública, definida conforme a necessidade de cada usuário ou grupo de usuários, no momento da abertura da conta de acesso aos recursos computacionais disponibilizados nas referidas redes.
- c) o acesso aos recursos computacionais somente deverá ser feito pelo usuário quando necessário e expressamente autorizado pelo Comandante, Chefe ou Diretor e pela sua Chefia Funcional.
- d) a permissão de acesso total ou equivalente deve ser removida dos diretórios compartilhados nos recursos computacionais utilizados como Servidores, salvo aqueles que deverão ser disponibilizados ao público externo nos Servidores alocados na *DMZ*, com a permissão única de leitura.
- e) o controle de acesso aos dados armazenados deve ser definido tanto em nível de arquivos como de diretórios, devendo ser usada a política de menor privilégio necessário, ou seja, cada usuário deve ter apenas o nível de acesso e privilégio suficiente para a execução de suas atividades.
- f) as Organizações Militares do COMAER, por meio das suas Equipes de TI, deverão providenciar as cópias de segurança das informações armazenadas em cada servidor sob sua responsabilidade, com o intuito de prover uma recuperação rápida de dados armazenados em caso de falha ou interrupção de algum serviço.
- g) as cópias de segurança não deverão, em hipótese alguma, ser armazenadas no mesmo espaço físico do Servidor e no mesmo prédio. A periodicidade das cópias deverá ser baseada no seu grau de criticidade para operações do dia-a-dia, podendo exigir, conforme o entendimento do Elo de Coordenação de TI respectivo, periodicidade diária, semanal ou mensal.
- h) o agendamento do processo de execução das cópias de segurança deverá ser feito, obrigatoriamente, pela Equipe de TI da OM.
- i) a disponibilidade da rede deve ser mantida fazendo-se cópias de segurança programadas e regulares. Todos os recursos de segurança, atributos e diretórios, devem ser respeitados e mantidos pelo procedimento de cópias de segurança.
- j) tanto as cópias quanto as funções de recuperação devem ser testadas regularmente.
- k) se um sistema de controle de acesso falhar, este deve negar todos os

privilégios aos usuários até a eliminação da falha.

- l) para os sistemas isolados, o usuário será o responsável pelo processo de execução das cópias de segurança, enquanto que para sistemas multiusuários, a Equipe de TI da OM será a responsável.
- m) todas as informações classificadas (sensíveis), valiosas ou críticas armazenadas nos recursos computacionais e em uma rede deverão ser periodicamente copiadas, baseando-se no seu grau de criticidade para operações do dia-a-dia, podendo exigir, periodicidade diária, semanal ou mensal.
- n) o armazenamento do conjunto de mídias de *backup* de Servidores é de responsabilidade da Equipe de TI da OM, assim como o das estações de trabalho é de responsabilidade do usuário.

### **Anexo K - Política de Inspeção**

Na condução de inspeção de segurança em recursos computacionais do COMAER devem ser observados os seguintes critérios, além daqueles do item 3.7 desta Norma:

- a) todos os Recursos Computacionais pertencentes à INTRAER, bem como os recursos computacionais das Organizações Militares deverão sofrer inspeções para verificação da implementação e cumprimento desta Norma de Segurança, com a ciência prévia do Comando/Chefia/Direção da OM onde eles estejam localizados.
- b) O NuCDCAER e o CIAER, através da Divisão de Inteligência Cibernética, poderão inspecionar as Organizações a qualquer tempo, com fins de promover o incremento da capacidade de proteção cibernética através da busca de vulnerabilidades. Poderão aplicar técnicas, táticas e procedimentos de exploração manual ou automatizada, sem necessidade de autorização da OM, nem necessidade de comunicação prévia, durante ou posterior.
- c) quando necessário, ou com o propósito de ser executada a inspeção, Equipe de Segurança em TI da OM e do NuCDCAER ou do CIAER deverão ter acesso irrestrito aos Recursos Computacionais, com a ciência do Comando/Direção/Chefia da organização inspecionada.
- d) os inspetores terão acesso a todas as informações, sejam elas eletrônicas, cópias de segurança e outras, que possam ter sido transmitidas, produzidas ou armazenadas nos recursos computacionais da organização inspecionada, devendo ser levada em consideração a credencial de segurança dos inspetores.
- e) os inspetores terão acesso a todas as áreas de trabalho onde se encontram os Recursos Computacionais, tais como laboratórios, salas diversas, manutenção e outras.
- f) os inspetores terão acesso físico e lógico aos sistemas que monitoram e armazenam os logs da rede.
- g) a Inspeção deverá ser feita com aviso prévio ao Chefe da Equipe de TI da OM e este, além de manter sigilo sobre o processo, deverá acompanhar os inspetores em todos os procedimentos executados.
- h) conforme atribuições previstas na NSCA 7-6/2016, na ICA 7-42/2016 e na ICA 7-49/2020, o NuCDCAER, por meio do CTIR.FAB e de suas demais seções, poderá manter um monitoramento remoto constante da INTRAER em qualquer ponto do backbone, incluindo Redes Locais, sem necessidade de prévio aviso a qualquer usuário.
- i) todo esforço deverá ser feito para impedir que as inspeções causem falhas operacionais ou interrupção dos serviços.
- j) todo recurso computacional existente no COMAER é passível de monitoramento e inspeção pelo NuCDCAER, conforme atribuições previstas na NSCA 7-6/2016, na ICA 7-42/2016 e na ICA 7-49/2020.
- k) considerando que os Recursos Computacionais pertencem ao COMAER ou



são utilizados em atividades desenvolvidas em prol deste Comando, fica entendido que não existe renúncia ao direito de privacidade por parte do usuário.

### **Anexo L – Política de *Backup***

Dos princípios gerais:

- a) a Política de *Backup* e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação do COMAER.
- b) a Política de *Backup* do COMAER está alinhada ao Programa de Privacidade e Segurança da Informação do Governo Federal, disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/PPSI>.
- c) a Política de *Backup* e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
- d) as rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
- e) as rotinas de *backup* devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
- f) as rotinas de *backup* devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.
- g) o armazenamento de *backup*, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de *backup* em um local remoto ao da sede da organização para armazenar cópias extras dos principais *backups*, a exemplo dos *backups* de dados de serviços críticos.
- h) a infraestrutura de rede de *backup* deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
- i) manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de *backup*.
- j) em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Da frequência e retenção dos dados:

- a) os *backups* dos serviços de TI críticos das organizações do COMAER devem ser realizados utilizando-se as seguintes frequências temporais, conforme a criticidade identificada do sistema:

I – Diária;

II – Semanal;

III – Mensal;

IV – Anual.

- b) os serviços de TI críticos das Organizações devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I – diária: 2 meses;

II – Semanal: 4 meses;

III – Mensal: 1 ano;

IV – Anual: 5 anos.

c) os serviços de TI NÃO críticos das Organizações devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I – Diária: 1 meses;

II – Semanal: 2 meses;

III – Mensal: 6 meses;

IV – Anual: 2 anos.

d) especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

e) os ativos envolvidos no processo de *backup* são considerados ativos críticos para a organização.

f) a solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada [pelo(s) responsável(s)], com a anuência prévia e formal [do(s) responsável(s)], refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I – Escopo (dados digitais a serem salvaguardados);

II – Tipo de *backup* (completo, incremental, diferencial);

III – Frequência temporal de realização do *backup* (diária, semanal, mensal, anual);

IV – Retenção;

V – RPO;

VI – RTO.

g) a alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Chefe da Equipe de TI da OM. A aprovação para execução da alteração depende da anuência do Comandante da OM.

h) os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de *backup* deverão zelar pelo cumprimento das diretrizes estabelecidas.

Tipo de *backup*:

I – Completo (full);

II – Incremental;

### III – Diferencial.

- a) salvo indicação em contrário, o *backup* dos dados do sistema será feito de acordo com a seguinte programação padrão:
- b) *backup* incremental diário (segunda a sábado), armazenado no local.
- c) *backup* completo semanal (sábado a domingo), armazenado externamente. Sempre que possível, os *backups* devem ser iniciados às 12h da manhã de sábado para permitir mais tempo durante o fim de semana para realizar o *backup* e tempo suficiente para lidar com quaisquer problemas que possam surgir durante o processo de *backup*.

#### Do uso da rede:

- a) o administrador de *backup* deve considerar o impacto da execução das rotinas de *backup* sobre o desempenho da rede de dados das Organizações, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI das Organizações.
- b) a execução do *backup* deve concentrar-se, preferencialmente, no período de janela de *backup*.
- c) o período de janela de *backup* deve ser determinado pelo administrador de *backup* em conjunto com a área técnica responsável pela administração da rede de dados das Organizações.

#### Do transporte e armazenamento

- a) as unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:
  - 1. A criticidade do dado salvaguardado;
  - 2. O tempo de retenção do dado;
  - 3. A probabilidade de necessidade de restauração;
  - 4. O tempo esperado para restauração;
  - 5. O custo de aquisição da unidade de armazenamento de *backup*;
  - 6. A vida útil da unidade de armazenamento de *backup*.
- b) o administrador de *backup* deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.
- c) podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.
- d) a execução das rotinas de *backup* deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
- e) no caso de desligamento do usuário (de forma permanente ou temporária), o *backup* de seus arquivos deverá ser mantido por, no mínimo, 30 dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.
- f) as unidades de armazenamento dos *backups* devem ser acondicionadas em

locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de *backup*. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

- g) quando da necessidade de descarte de unidades de armazenamento de *backups*, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.
- h) a fitas de *backup* serão transportadas e armazenadas conforme determinações dos respectivos PCA que regulam o serviço.
- i) a mídia será claramente identificada e armazenada em uma área segura acessível apenas para pessoa(s) autorizada(s).
- j) a mídia não será deixada sem supervisão durante o transporte.
- k) *backups* completos diários serão mantidos por [informar período, ex.:1 semana] e armazenado no local em um cofre à prova de água ou fogo fisicamente protegido, localizado em uma sala fora do data center.
- l) as fitas de *Backups* serão mantidos por um período conforme item “Da frequência e retenção dos dados” e enviado a um local de armazenamento de mídia externo fisicamente protegido. Depois do período de retenção, as fitas serão devolvidas à TI e serão reutilizadas ou destruídas.

#### Dos testes de *backup*

- m) os *backups* serão verificados periodicamente:
- n) os testes serão realizados, por amostragem, pelo menos na metade do tempo de retenção dos *backups*, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar *backups* bem-sucedidos.
- o) os logs de *backup* serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do *backup*.
- p) Ações corretivas serão tomadas quando os problemas de *backup* forem identificados, a fim de reduzir os riscos associados a *backups* com falha.
- q) a TI manterá registros de *backups* e testes de restauração para demonstrar conformidade com esta política.
- r) os testes devem ser realizados em todos os *backups* produzidos independente do ambiente.
- s) deve-se verificar se foi atendido os níveis de serviço pactuados, tais como os *Recovery Time Objective – RTOs*. (Tempo de Recuperação Objetivo)
- t) os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do *backup* e se o procedimento foi concluído com sucesso
- u) Quaisquer exceções a esta política serão totalmente documentadas e

aprovadas por Comitê responsável na Organização.

#### Procedimento de restauração de *backup*

a) o atendimento de solicitações de restauração de arquivos, *e-mails* e demais formas de dados deverá obedecer às seguintes orientações:

1. a solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de SAU ou solicitação formal.
2. a restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de *backup*.
3. a solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.
4. o operador de *backup* terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

b) o cronograma de restauração de dados:

1. o tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço entre as áreas de negócio e de TIC, é proporcional ao volume de dados necessários para o *restore*.
2. *backups* externos serão disponibilizados de acordo com a prioridade para restauração de acordo com a criticidade de cada sistema e o tipo de evento (catastrófico ou não catastrófico) onde esta definição deverá ser de cada Responsável pela Sustentação do Sistema.

c) diretrizes para restauração de dados:

1. a restauração de dados tem que ser formalizada pelo Responsável pelo Negócio de Acordo de Nível de Serviço entre as áreas de negócio e de TIC.
2. todo processo iniciado de Restauração deve ser notificado na abrangência do Sistema. Sistemas Internos a OM devem ser notificados pela TI da OM à OM. Restauração de Sistema que afetem toda a FAB devem ser notificados pelo STI.
3. após a restauração dos dados as mesmas notificações devem ser realizadas informando o público dos efeitos advindos da restauração, ou seja, volta ao ar com perda de dados, volta ao ar com recuperação bem sucedida ou outro caso.

#### Do Descarte da Mídia

a) a mídia de *backup* será retirada e descartada conforme descrito neste documento:

1. a TI garantirá que a mídia não contenha mais imagens de *backup* ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.
2. a TI garantirá a destruição física da mídia antes do descarte.

#### Das Responsabilidades

- a) o administrador de *backup* e o operador de *backup* ou pessoas designadas formalmente para tais tarefas na OM devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de *backup*.
- b) são atribuições do administrador de *backup*:
  1. propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
  2. providenciar a criação e manutenção dos *backups*;
  3. Configurar as soluções de *backup*;
  4. manter as unidades de armazenamento de *backups* preservadas, funcionais e seguras;
  5. definir os procedimentos de restauração e neles auxiliar;

#### Procedimentos Relevantes

- a) as TI das OM deverão ter publicados formalmente procedimento que reforcem e apoiem as declarações políticas acima. Note que é uma prática recomendada abrigar políticas e procedimentos em documentos separados para manter o conteúdo focado e reduzir o número de vezes que a política deve ser reprovada pela alta administração.

#### Não conformidade

- a) é de responsabilidade do setor de TI da OM declarar formalmente as responsabilidades e as consequências (legais e/ou disciplinares) para o não cumprimento da política pelos agentes públicos ou terceiros relacionados aos procedimentos de *backups* da OM através de, por exemplo, Normas Padrão de Ação (NPA) relacionadas ao tema.
- b) neste documento formal deverão constar os nome ou funções responsáveis pelo *backup*, quais os sistemas e suas propriedades de *backup* e restauração, detalhes técnicos de plataformas de *backup*, rotinas de acesso às fitas, transportes, responsáveis pela área de Negócio, entre outros tópicos já mencionados nesta Política de *Backup*.
- c) em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

## Anexo M – Política de Gestão de Ativos

Dos princípios gerais

- a) a Política de Gestão de Ativos de informação deve estar alinhada com a Política de Segurança da Informação do COMAER.
- b) a Política de Gestão de Ativos está alinhada ao Programa de Privacidade e Segurança da Informação do Governo Federal, disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/PPSI>.
- c) a Política de Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
- d) o processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.
- e) as rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.
- f) o processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.
- g) o registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.
- h) caberá a DTI implantar um sistema centralizado de Gestão de Ativos no COMAER.
- i) caso autorizado pela DTI, outras OM poderão implantar seus sistemas de Gestão de Ativos desde que estes sejam integrados a plataforma centralizada.

Os seguintes ativos de informação devem ser considerados no processo de inventário:

- a) ativos físicos;
- b) *hardwares*;
- c) *softwares*.

Diretrizes:

- a) informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.
1. a categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização.



2. a organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo *Hardware* ou *Software*.

3. o inventário também deverá incluir atualizações ou remoções do sistema de informação.

4. o CTIR-FAB deverá ter acesso a todos os sistemas que façam ou gerem dados relativos Gestão de Ativos no COMAER visando integrar a Política de Segurança da Informação.

b) das responsabilidades do proprietário do processo (recomenda-se a leitura ao Art. 9º da IN GSI/PR nº 3/2021)

1. identificar potenciais ameaças aos ativos de informação;

2. identificar vulnerabilidades dos ativos de informação;

3. consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

4. avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

5. indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na política de controle de acesso e catalogadas no sistema de gestão de ativos.

6. os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.

7. todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

8. os ativos de informação do COMAER sob cautela de usuários da FAB pertencem à FAB assim como as informações geradas por estes sistemas.

c) criticidade do ativo de informação:

1. a criticidade dos ativos de informação críticos da organização é determinado pelo:

a) requisitos legais;

b) pelo valor financeiro;

c) pelo seu potencial de agregar valor ao negócio;

d) por sua vida útil.

d) classificação das informações:

1. todos os ativos de informação devem ser classificados de acordo com sua criticidade.

2. as informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação do COMAER devem ser classificados de acordo com a legislação pertinente (recomenda-se leitura da LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011), podendo ser classificado em uma das seguintes categorias:

- a) **ultrassecreta:** São passíveis de classificação como ultrassegredos, dentre outros, dados, informações ou documentos referentes à soberania e à integridade territorial nacionais, a planos e operações, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade ou do Estado.
  - b) **segreda:** São passíveis de classificação como segredos, dentre outros, dados, informações ou documentos referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não autorizado possa acarretar dano grave à segurança do COMAER, da sociedade ou do Estado.
  - c) **reservada:** São passíveis de classificação como confidenciais, dentre outros, dados, informações ou documentos que, no interesse do COMAER, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança do COMAER, da sociedade ou do Estado.
1. os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de informações usados pela organização.

**Manipulação de mídia:**

- 1. a mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.
- 2. a mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados.
- 3. a mídia contendo informações confidenciais e internas do COMAER devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

#### Procedimentos Relevantes

- a) as TI das OM deverão ter publicados formalmente procedimento que reforcem, detalhem e apoiem as declarações políticas acima.
- b) neste documento formal deverão constar os nomes ou funções responsáveis pela classificação das informações, quais os sistemas e suas propriedades sustentam a Política de Gestão de Ativos.
- c) em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.