1. **DCA 14-8 – Política de Segurança da Informação do COMAER**

Este é o documento central que estabelece a política institucional de segurança da informação para todo o Comando da Aeronáutica. Define conceitos como confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade e controle de acesso, além de prever diretrizes para proteção de ativos de informação, gerenciamento de riscos, uso de criptografia, controle de acesso e responsabilidades dos usuários.

- **Abrange diretamente a manutenção de sigilo e as normas de segurança da informação, incluindo em ambiente digital, sendo referência para demais normas e procedimentos internos**.

2. **NSCA 7-13 – Segurança da Informação e Defesa Cibernética nas Organizações do COMAER**

Norma detalhada que operacionaliza a política de segurança da informação, estabelecendo procedimentos específicos para:

- Controle de acesso físico e lógico;
- Proteção contra programas maliciosos;
- Monitoramento de atividades e resposta a incidentes;
- Manipulação de informações classificadas (sigilosas), com referência explícita ao Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RCA 205-1);
- Regras para terceirizados, continuidade de negócios, uso de redes sem fio, VoIP, videoconferência, entre outros.
- Possui anexos específicos sobre manipulação de informações classificadas, uso de recursos computacionais, segurança lógica, auditoria, antivírus, firewall, etc.
- É a principal norma operacional sobre sigilo e segurança de TI no COMAER.

3. **NSCA 7-1 – Uso da Rede de Dados do COMAER – INTRAER**

Estabelece critérios, procedimentos e atribuições para uso da rede de dados interna do COMAER (INTRAER), incluindo:

- Restrições relativas à segurança das informações;
- Proibições quanto ao armazenamento ou processamento de informação classificada sem autorização;
- Regras para controle de acesso, autenticação, privacidade, monitoramento e responsabilidade dos usuários;

- **Reforça a necessidade de sigilo e segurança no uso dos sistemas de rede e comunicação interna**.

4. **OTCA 009/DTI/2019 – Padronização do Acesso à Internet no COMAER (Acesso Não Funcional)**

Define requisitos técnicos e procedimentos para acesso não funcional à internet, incluindo:

- Exigência de consentimento e assinatura de termo de responsabilidade e conhecimento da Política de Segurança da Informação;
- Citação expressa da DCA 14-8, NSCA 7-1, NSCA 7-13 e legislação federal (Lei de Acesso à Informação, Marco Civil da Internet, etc.);
- Procedimentos para guarda de registros de acesso, sigilo de dados e cumprimento das normas de segurança da informação;
- **Estabelece o compromisso formal de sigilo e cumprimento das normas de segurança de TI**.

5. **ICA 7-5 – Uso da Rede Mundial de Computadores – INTERNET – no COMAER**

Regula o uso da internet no âmbito do COMAER, estabelecendo:

- Procedimentos para acesso, monitoramento, uso responsável e seguro;
- Regras para proteção de informações institucionais, inclusive sigilosas, no ambiente externo;
- Complementa as normas de segurança e sigilo para o uso da internet.

Documento	**Tema Central**	**Abrangência sobre Sigilo/Security TI**
DCA 14-8	Política institucional de segurança da informação	Abrange toda a gestão de sigilo e segurança
NSCA 7-13	Procedimentos operacionais de segurança e defesa cibernética	Detalha sigilo, resposta a incidentes, controles
NSCA 7-1	Uso da rede interna (INTRAER) e segurança das informações	Regras práticas para sigilo e segurança em rede
OTCA 009/DTI/2019	Padronização de acesso à internet, termo de responsabilidade, integração das normas de segurança	Exige compromisso formal com sigilo e normas
ICA 7-5	Uso da internet, proteção e monitoramento de informações	Complementa regras de sigilo e segurança

Resumo

Conclusão:
Os documentos DCA 14-8, NSCA 7-13, NSCA 7-1, OTCA 009/DTI/2019 e ICA 7-5 são os que regem diretamente a manutenção de sigilo e as normas de segurança de tecnologia da informação no âmbito do COMAER. Eles estabelecem desde princípios e diretrizes institucionais até procedimentos operacionais, responsabilidades, controles técnicos e administrativos, e exigências legais para proteção das informações e dos sistemas de TI

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-5

USO DA REDE MUNDIAL DE COMPUTADORES - INTERNET - NO COMANDO DA AERONÁUTICA

2015

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO-MAIOR DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-5

USO DA REDE MUNDIAL DE COMPUTADORES - INTERNET - NO COMANDO DA AERONÁUTICA

2015

MINISTÉRIO DA DEFESA
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.

O CHEFE DO ESTADO-MAIOR DA AERONÁUTICA, no uso das atribuições que lhe confere o inciso IV do Art. 14 do Regulamento do Estado-Maior da Aeronáutica, aprovado pela Portaria nº 756/GC3, de 19 de novembro de 2007, tendo em vista o disposto no item 1.3.3 da NSCA 5-1/2011, aprovada pela Portaria COMGEP nº 864/5EM, de 23 de novembro de 2011, e considerando o que consta do Processo nº 67131.001274/2015-96, resolve:

Art. 1º Aprovar a reedição da ICA 7-5 - Uso da rede Mundial de Computadores - INTERNET - no Comando da Aeronáutica, elaborada pela Diretoria de Tecnologia da Informação da Aeronáutica.

Art. 2º Esta Instrução entra em vigor na data de sua publicação no Boletim do Comando da Aeronáutica.

Art. 3º Revoga-se a Portaria EMAER Nº 025/3SC3, de 17 de dezembro de 2001, publicada no Boletim Externo Ostensivo do EMAER nº 019, de 28 de dezembro de 2001.

Ten Brig do Ar HÉLIO PAES DE BARROS JÚNIOR
Chefe do Estado-Maior da Aeronáutica

(Publicado no BCA nº 236, de 23 de dezembro de 2015)

SUMÁRIO

PREFÁCIO

O dinamismo e a quantidade de informações disponibilizadas na rede mundial de computadores (INTERNET) se tornaram indispensáveis para o funcionamento das Organizações da Aeronáutica, potencializando a eficiência administrativa e a atualização de conhecimentos individuais.

Além do estabelecido para o uso da rede interna da Aeronáutica - INTRAER, o uso da INTERNET demanda medidas complementares, principalmente para a segurança dos ativos físicos, de *software* e de informação, tanto as de caráter geral, quanto às específicas que forem necessárias, visando prover as condições adequadas para a salvaguarda de interesses determinados ou coletivos, o que se constitui em responsabilidade de todos, conforme previsto na DCA 14-8 - "Política de Segurança da Informação do Comando da Aeronáutica".

Com a nova estrutura do Sistema de Tecnologia da Informação (STI) e com o crescimento do volume de utilização da INTERNET nos últimos anos, tornou-se necessária a revisão da ICA 7-5 - USO DA REDE MUNDIAL DE COMPUTADORES - INTERNET - NAS ORGANIZAÇÕES DA AERONÁUTICA, de 27 dez 2001, que complementa a NSCA 7-1 - USO DA INTRANET NAS ORGANIZAÇÕES DA AERONÁUTICA - INTRAER, instrumentos indispensáveis para a racional utilização dos recursos de comunicação de dados que apóiam as atividades de Tecnologia da Informação (TI) de interesse da Aeronáutica.

1 DISPOSIÇÕES PRELIMINARES

1.1. FINALIDADE

Esta Instrução tem por finalidade estabelecer critérios, procedimentos e atribuições para uso da Rede Mundial de Computadores - INTERNET - nas Organizações do COMAER.

1.2. CONCEITUAÇÕES

1.2.1. ACESSO

Ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade (Fonte: Norma Complementar 07/IN01/DSIC/GSIPR, de 06 de maio de 2010).

1.2.2. ACESSO À CAIXA POSTAL

Interface entre um cliente e um sistema de correio (Fonte: e-PING - Padrões de Interoperabilidade de Governo Eletrônico, Documento de referência, versão 2013).

1.2.3. ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

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

1.2.3.1. Ativos Físicos

Patrimônio da Instituição, composto de equipamentos computacionais (ex: processadores, monitores, *laptops*, *modems*), equipamentos de comunicação (ex: roteadores, *switchs*, *hubs*, PABX, aparelhos de *fac-símile*, secretárias eletrônicas), mídias removíveis (ex: fitas, discos rígidos, *pendrives*) e outros recursos tecnológicos (ex: impressoras, *no-breaks*, estabilizadores).

1.2.3.2. Ativos da Informação

Patrimônio composto de bases de dados e arquivos, documentação de sistemas, informações sobre pesquisas, manuais de usuários, material de treinamento, procedimentos de suporte e operação, planos de continuidade, procedimentos de recuperação de sistemas, trilhas de auditoria e informações armazenadas.

1.2.3.3. Ativos de *Software*

Patrimônio composto de aplicativos, sistemas operacionais, ferramentas de desenvolvimento e utilitários.

1.2.4. CANALIZAÇÃO DE DADOS

Infraestrutura de telecomunicações utilizada para o tráfego de dados, voz e imagem.

1.2.5. DOMÍNIO NA INTERNET

Nome que serve para localizar e identificar conjuntos de computadores na INTERNET. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na INTERNET. Sem o uso desse conceito seria necessária a memorização dos endereços dos computadores na INTERNET, os quais são denominados "endereços IP" (***I****NTERNET* ***P****rotocol*). (Fonte: www.governoeletronico.gov.br).

1.2.6. "HACKER"

Indivíduo que elabora e modifica *software* ou *hardware* de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas. Originário do inglês, o termo é usado em português sem modificação, referindo-se, na maioria das vezes, a programadores maliciosos que agem com o intuito de violar, de modo ilegal ou imoral sistemas de tecnologia da informação, podendo, nesses sistemas, causar danos. (Fonte: Glossário das Forças Armadas, 2007).

1.2.7. "HIPERLINK"

Termo de origem inglesa que, em português significa ligação entre um documento e outro(s) documento(s) ou outro(s) recurso(s). (Fonte: w3shools.com).

1.2.8. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Um evento ou uma série de eventos indesejados ou inesperados que podem vir a comprometer a confidencialidade ou a integridade ou a disponibilidade de ativos físicos, de software ou de informação, todos de interesse da Instituição. (Fonte: Glossário das Forças Armadas - 2007).

1.2.9. "MALWARE"

Termo de origem inglesa (***ma****licious soft****ware***), cuja tradução é "*software* malicioso", significando um tipo de programa para ser infiltrado ilicitamente em um computador alheio, a fim de causar dano ou permitir a obtenção de informações ou controle da outra máquina. Nesse grupo encontram-se os vírus, os vermes, os cavalos de tróia e os *spywares*. (Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil - www.cartilha.cert.br/conceitos/sec6.html).

1.2.10. ORGANIZAÇÃO PROVEDORA DOS SERVIÇOS DE TI (OPSTI)

De acordo com a NSCA 102-1/2013 - Reestruturação da Infraestrutura de Provimento de Acesso à INTERNET no COMAER, a conexão física com a INTERNET para Organizações pertencentes ao SISCEAB se fará, obrigatoriamente, por meio de link de dados disponibilizado em OM subordinadas ao Órgão Central de Telecomunicações - DECEA, também designadas como OPSTI. A relação das OPSTI e dos Órgãos Regionais está contida na mesma NSCA 102-1/2013.

1.2.11. PROVEDORES DE ACESSO REGIONAIS

De acordo com a NSCA 102-1/2013 - Reestruturação da Infraestrutura de Provimento de Acesso à INTERNET no COMAER, para os casos em que os recursos da rede local são compartilhados entre o acesso à INTRAER e à INTERNET, o acesso à INTERNET

deve ser realizado, sempre que possível, por meio dos provedores de acesso regionais. A relação das OPSTI e dos Órgãos Regionais está contida na mesma NSCA 102-1/2013.

Estas Organizações, conforme item 3.1, alínea "f" da NSCA 102-1/2013, são também chamadas de Organizações Provedoras de Acesso - OPA e são aquelas que permitem o acesso de outras organizações à rede mundial de computadores. É de competência do Órgão Central do STI credenciar os Órgãos Regionais.

1.2.12. SUBDOMÍNIO NA INTERNET

Nome que faz referência a uma parte de um domínio na INTERNET, identificando computadores que constituem uma parte ou um subconjunto do conjunto de computadores designado por um domínio na INTERNET. (Fonte: Empresa Brasileira de Hospedagem de Sites - www.rjhost.com.br).

1.3. ÂMBITO

Esta Norma se aplica a todas as Organizações do COMAER.

2 OBJETIVOS

Para o acesso à INTERNET, bem como para a divulgação das informações obtidas, os requisitos a serem atendidos pelas Organizações do COMAER foram estabelecidos nesta ICA em correspondência com os seguintes objetivos:

a) orientar o uso da INTERNET na Aeronáutica;

b) garantir os níveis adequados de segurança da informação nos acessos à INTERNET realizados pelas OM do COMAER; e

c) estabelecer as medidas de proteção à segurança das informações, adequada ao uso da INTERNET, contra acessos indevidos.

3 PROCEDIMENTOS

3.1. ACESSO DAS OM DO COMAER À INTERNET

3.1.1. As organizações do COMAER deverão acessar à INTERNET por meio dos acessos regionais mantidos pelo Órgão Central do STI.

3.1.2. Eventualmente, o Órgão Central do STI poderá autorizar a implantação, em caráter provisório, de acessos à INTERNET implantados em OM do COMAER, distintos dos acessos regionais, podendo a OM solicitante contratar serviço comercial de provedor da localidade, desde que instale em sua rede local os equipamentos de segurança padronizados para a conexão com a INTERNET. Se estes produtos forem adquiridos pela própria OM, as especificações devem ser aprovadas pelo Órgão Central do STI, antes de se tornar operacional a conexão com a INTERNET.

3.1.3. A solicitação de autorização para implantação, em OM do COMAER, de acessos provisórios à INTERNET deverá ser feita pela Organização interessada ao seu respectivo Elo de Coordenação do STI que, caso seja de parecer favorável à implantação do acesso, a submeterá ao Órgão Central do STI.

3.1.4. O ônus pelo aluguel de canalização, pelos demais serviços de telecomunicações necessários ao acesso físico à INTERNET e pela solução de segurança (*hardware*, *software* e demais serviços) utilizada na sua proteção são de responsabilidade da OM onde será implantado o ponto de acesso provisório àquela Rede.

3.1.5. Todo acesso à INTERNET deve ter sua liberação condicionada à identificação e autenticação do usuário, composto de *login* pessoal e senha individual, não sendo permitido o acesso por meio de identificação funcional ou senha compartilhada.

3.1.6. Todo usuário da INTERNET no COMAER deverá assinar um Termo de Responsabilidade e de conhecimento da Política de Segurança da Informação do COMAER e das políticas de segurança da informação definidas pelas respectivas Organizações (conforme Exemplo do Anexo A).

3.1.7. Todo o tráfego de dados com acesso à INTERNET deve ser protegido por ferramentas contra *softwares* maliciosos (*malware*). A padronização das ferramentas será realizada pelo Órgão Central do STI, conforme consta na NSCA 7-13/2013 - Segurança da Informação e Defesa Cibernética nas Organizações do COMAER.

3.1.8. A utilização de programas obtidos da INTERNET é de responsabilidade da própria Organização, devendo respeitar as condições de licenciamento e suporte técnico a que o programa está submetido.

3.1.9. A utilização do acesso à INTERNET está restrita ao atendimento das necessidades de serviço da Organização do COMAER.

3.1.10. É vedado o emprego do acesso à INTERNET para:

a) causar prejuízos morais ou financeiros a terceiros;

b) explorar vulnerabilidades de outros sítios da INTERNET, promovendo ataques do tipo daqueles realizados por "*hackers"*;

c) fazer uso de serviços de mensagem instantânea, de sítios de batepapo e de serviços associados às redes sociais, exceto quando autorizados por meio de documento oficial emitido pelo Órgão Central do STI;

d) expressar discriminação, preconceito ou apologia ao vício ou ao emprego ou utilização de ações, procedimentos ou práticas condideradas ilegais ou contrários à moral e aos bons costumes;

e) realizar procedimentos que se configurem como crimes, tais como pirataria, pedofilia, assédio, difamação ou outros quaisquer que contrariem as leis em vigor ou a moral e os bons costumes;

f) provocar danos à imagem do COMAER e das demais instituições governamentais; e

g) prejudicar a realização de atividades de interesse do COMAER.

3.1.11. As Organizações do COMAER detentoras de acessos provisórios à INTERNET deverão monitorar o seu uso pelo pessoal devidamente autorizado, mediante credencial de segurança, e habilitado, providenciando para que sejam corrigidas as discrepâncias observadas.

3.2. PUBLICAÇÃO DE PÁGINAS *WEB* NA INTERNET

3.2.1. A publicação de páginas *web* na INTERNET só poderá ser efetivada quando autorizada por meio de documento oficial emitido pelo Órgão Central do STI.

3.2.2. O registro de qualquer domínio na INTERNET, por parte de organizações do COMAER, somente poderá ser efetivado mediante autorização emitido pelo Órgão Central do STI.

3.2.3. As Organizações do COMAER deverão utilizar subdomínios do domínio *aer.mil.br* para publicar suas páginas *web* na INTERNET.

3.2.4. Na eventualidade de surgirem condições especiais que requeiram o registro de domínios na INTERNET, fora do domínio *aer.mil.br*, estes só poderão ser efetivados quando autorizados, por meio de documento oficial emitido pelo Órgão Central do STI. Uma vez autorizados, o Órgão Central do STI efetuará o registro do domínio junto ao *registro.br*.

3.2.5. A solicitação de autorização para publicação de páginas *web* na INTERNET e perfis de mídia social deverá ser feita pela Organização interessada ao seu respectivo Elo de Coordenação do STI que, caso seja de parecer favorável à publicação da página, a submeterá ao Órgão Central do STI, para avaliação quanto ao nível de segurança da informação e quanto às necessidades de canalização de dados, bem como ao CECOMSAER para a avaliação da identidade digital, recomendada pelo Governo Federal; cabe ressaltar que o conteúdo exposto é de inteira resposnabilidade do Comandante/Chefe/Diretor da Organização Militar (OM).

3.2.6. No que diz respeito à avaliação e necessidades da canalização de INTERNET, sempre que necessário, o Órgão Central do STI consultará o DECEA e solicitará o atendimento às demandas identificadas.

3.2.7. As páginas publicadas pelas Organizações do COMAER na INTERNET deverão ser, obrigatoriamente, hospedadas nos equipamentos servidores dos Centros de Computação da Aeronáutica.

3.2.8. O acesso às páginas *web* das Organizações do COMAER, publicadas na INTERNET, far-se-á, exclusivamente, a partir da página portal do COMAER na INTERNET (portal único do COMAER).

3.2.9. Os casos em que os domínios são outros que não o *aer.mil.br* ou o *fab.mil.br*, poderá ser realizado acesso diretamente por essas páginas, até que seja viabilizada a adaptação dessas Organizações à utilização do portal único do COMAER.

3.3. SISTEMAS APLICATIVOS NA INTERNET

3.3.1. A entrada em operação de sistemas, páginas e aplicativos móveis, cujo acesso será feito a partir da INTERNET, só poderá ser efetivada quando autorizada por meio de documento oficial emitido pelo Órgão Central do STI.

3.3.2. A solicitação de autorização para entrada em operação de sistemas aplicativos disponibilizados na INTERNET deverá ser feita pela Organização interessada ao seu respectivo Elo de Coordenação do STI que, caso seja de parecer favorável à entrada em operação do sistema, a submeterá ao Órgão Central do STI, para avaliação quanto ao nível de segurança da informação e quanto às necessidades de canalização de dados.

3.3.3. Os sistemas aplicativos disponibilizados na INTERNET deverão ser, obrigatoriamente, hospedados nos equipamentos servidores dos Centros de Computação da Aeronáutica.

3.3.4. A realização de ajustes, determinados pelo Órgão Central do STI, no sistema aplicativo disponibilizado na INTERNET será de responsabilidade da OM interessada.

3.4. ACESSO A SISTEMAS DE TI DA INTRAER A PARTIR DA INTERNET

3.4.1. O acesso a sistemas de TI da INTRAER a partir da INTERNET só poderá entrar em operação quando autorizado por meio de documento oficial emitido pelo Órgão Central do STI.

3.4.2. A solicitação de autorização para entrada em operação de um acesso a sistemas de TI da INTRAER a partir da INTERNET deverá ser feita pela Organização interessada ao seu respectivo Elo de Coordenação do STI que, caso seja de parecer favorável, a submeterá ao Órgão Central do STI, para avaliação quanto ao nível de segurança da informação e quanto às necessidades de canalização de dados.

3.4.3. As soluções técnicas de criptografia utilizadas para garantir a segurança das comunicações no emprego de canalização de dados, no ambiente da INTERNET, para o acesso a sistemas de TI da INTRAER deverão ser homologadas pelo CIAER.

3.4.4. Os acessos a sistemas de TI da INTRAER a partir da INTERNET deverão ser projetados de modo a utilizar a interface entre as duas redes presentes nos Centros de Computação da Aeronáutica.

3.4.5. A realização de ajustes, determinados pelo Órgão Central do STI, nos acessos autorizados será de responsabilidade da OM interessada.

4 COMPETÊNCIAS

4.1. DO ÓRGÃO CENTRAL DO STI

4.1.1. Avaliar, quanto ao nível de segurança das informações e quanto às necessidades de canalização de dados, as solicitações, encaminhadas pelos Elos de Coordenação do STI, relativas ao uso da INTERNET pelas OM do COMAER, que tratam da instalação de acessos provisórios, da publicação de páginas, da disponibilização de sistemas aplicativos e do acesso a sistemas de TI da INTRAER.

4.1.2. Autorizar a entrada em operação de acessos à INTERNET, no âmbito do COMAER.

4.1.3. Autorizar a publicação de páginas *web* na INTERNET, no âmbito do COMAER.

4.1.4. Autorizar a entrada em operação de sistemas aplicativos disponibilizados na INTERNET por OM do COMAER.

4.1.5. Autorizar o acesso a sistemas de TI da INTRAER a partir da INTERNET.

4.1.6. Dotar os Centros de Computação da Aeronáutica da infraestrutura (equipamentos, programas e canalização de dados) necessária, bem como de níveis adequados de capacitação de pessoal, adequados ao funcionamento dos seus acessos à INTERNET.

4.1.7. Gerenciar a atribuição de endereços IP para a conexão de computadores das OM do COMAER à INTERNET.

4.1.8. Gerenciar o registro de domínios e subdomínios da INTERNET para atender às Organizações do COMAER.

4.1.9. Produzir e disseminar conhecimentos acerca de incidentes de segurança da informação resolvidos e em andamento, objetivando prevenir ocorrência futuras.

4.2. DOS ELOS DE COORDENAÇÃO DO STI

4.2.1. Analisar as solicitações encaminhadas pelas OM do COMAER, no contexto sob sua área de responsabilidade funcional, relativas ao uso da INTERNET, quando tratar de instalação de acessos provisórios, da publicação de páginas, da disponibilização de sistemas aplicativos e do acesso a sistemas de TI da INTRAER.

4.2.2. Encaminhar as solicitações analisadas e consideradas adequadas ao Órgão Central do STI.

4.2.3. Fiscalizar, periodicamente, as páginas web já publicadas e aprovadas.

4.3. DO CECOMSAER

4.3.1. Elaborar e manter atualizado o Portal da Força Aérea na INTERNET.

4.3.2. Padronizar as informações de Comunicação Social da Aeronáutica divulgadas pela INTERNET.

4.3.3. Fazer a triagem, selecionar e encaminhar às OM detentoras da informação solicitada as correspondências eletrônicas recebidas pela INTERNET e endereçadas ao Comando da Aeronáutica.

4.3.4. Responder as correspondências eletrônicas endereçadas ao Comandante da Aeronáutica.

4.3.5. Analisar o conteúdo das propostas de páginas para a INTERNET ("*web sites*") apresentado pelas OM do COMAER.

4.3.5.1. As páginas para a INTERNET no COMAER serão consideradas adequadas à Identidade Padrão de Comunicação Digital quando estiverem de acordo com o Guia de estilo de sítios e portais da identidade padrão da Força Aérea Brasileira, em alinhamento à Instrução Normativa SECOM-PR n° 8 de 19 de dezembro de 2014 Art. 3º, que versa sobre as propriedades digitais dos órgãos e entidades do Poder Executivo Federal.

4.3.5.2. As páginas para a INTERNET no COMAER necessitam observar o Manual de operação do Portal único da Força Aérea Brasileira.

4.3.6. Estabelecer conexão ("*hiperlinks*") entre o Portal da Força Aérea e as páginas web cujas propostas tenham sido aprovadas pelo CECOMSAER.

4.4. DO CIAER

4.4.1. Assessorar o Órgão Central do STI na avaliação de soluções técnicas de criptografia utilizadas para garantir a segurança das comunicações em acessos à INTERNET.

4.5. DOS CENTROS DE COMPUTAÇÃO DA AERONÁUTICA

4.5.1. Operar os acessos à INTERNET sob sua responsabilidade garantindo os níveis de segurança da informação estabelecidos pelo Órgão Central do STI, bem como a disponibilidade dos acessos para atender às páginas *web* e aos sistemas aplicativos hospedados.

4.5.2. Prover o CECOMSAER do apoio técnico necessário ao trato das suas competências referentes ao emprego da INTERNET.

4.5.3. Gerar relatórios estatísticos relativos à utilização do acesso à INTERNET sob sua responsabilidade, por solicitação das Organizações do COMAER usuárias do acesso.

4.5.4. Apoiar os Elos de Serviço na resolução de incidentes de segurança da informação.

4.6. DOS ELOS DE SERVIÇO DO STI

4.6.1. Operar o acesso provisório à INTERNET sob sua responsabilidade garantindo os níveis de segurança da informação estabelecidos pelo Órgão Central do STI.

4.6.2. Gerar relatórios estatísticos relativos à utilização do acesso provisório à INTERNET sob sua responsabilidade.

4.6.3. Manter atualizadas as informações contidas nas páginas *web* das suas Organizações e nos demais serviços, que estão publicadas na INTERNET.

4.6.4. Efetuar, respeitando os prazos estabelecidos pelo Órgão Central do STI, as correções necessárias nos sistemas aplicativos disponibilizados na INTERNET pela sua Organização.

4.6.5. Registrar, mediante o Sistema de Atendimento aos Usuários de Tecnologia da Informação do Comando da Aeronáutica (SAUTI). A ocorrência de incidentes de segurança da informação.

4.7. DO SISTEMA DE ATENDIMENTO AOS USUÁRIOS DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA (SAUTI)

4.7.1. Registrar e categorizar os dados referentes aos incidentes de a segurança da informação relatados pelos Elos do STI.

4.7.2. Acionar o Elo Especializado responsável pelo atendimento ao usuário, referente aos incidentes de segurança da informação no âmbito do STI.

4.7.3. Enviar ao Órgão Central do STI relatório gerencial, constando de indicadores estatísticos, referente aos incidentes de segurança da informação registrados no âmbito do STI.

5 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

5.1. Os incidentes de segurança da informação devem ser reportados tão logo sejam observados pelo Elo do STI ao Sistema de Atendimento ao Usuário de Tecnologia da Informação (SAUTI), ou diretamente ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Aeronáutica (CTIR.AER).

5.2. O Elo que reportar o incidente deverá preservar, tanto quanto possível, as evidências do incidente observado, conforme orientações a serem dadas pelo Órgão Central do STI, visando a possibilitar procedimentos específicos de análise ligados ao fato, a fim de garantir a legitimidade do procedimento e das evidências coletadas.

5.3. O atendimento aos incidentes de segurança da informação caberá a um dos Elos Especializados, conforme orientações do Órgão Central do STI, o qual coordenará, operacionalmente, a estrutura do CTIR.AER.

5.4. O Órgão Central do STI elaborará e manterá atualizadas as regulamentações específicas, estabelecendo os processos de atendimento aos incidentes de segurança da informação e de prática forense computacional, em auxílio à coleta de evidências no âmbito do STI.

5.5. O Órgão Central do STI produzirá e divulgará conhecimentos 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.

6 DISPOSIÇOES GERAIS

6.1. A Norma de Sistema que tem por finalidade orientar a reestruturação da infraestrutura de provimento de acesso à INTERNET para as Organizações Militares do Comando da Aeronáutica, com a consequente definição de ações e responsabilidades, é a NSCA 102-1/2013 - Reestruturação da Infraestrutura de Provimento de Acesso à INTERNET no COMAER.

6.2. As Organizações Provedoras de Serviços de Tecnologia da Informação (OPSTI), bem como os provedores de acesso regionais, encontram-se listados na mesma Norma, NSCA 102-1/2013.

7 DISPOSIÇOES FINAIS

7.1. Esta publicação substitui a ICA 7-5/2001, aprovada pela Portaria EMAER nº 025/3SC3, de 17 de dezembro de 2001.

7.2. Os casos não previstos serão submetidos à apreciação do Exmo. Sr. Chefe do Estado-Maior da Aeronáutica.

ANEXO 1

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇAO DA AERONAUTICA

Termo de Responsabilidade e de conhecimento da Política de Segurança da Informação do COMAER e das políticas de segurança da informação definidas pelas respectivas Organizações

(MODELO)

Declaro que tenho pleno conhecimento de minha responsabilidade quanto à proteção a ser mantida sobre os assuntos sigilosos a que, por força de função ou atividade, tenha ou venha a ter acesso, comprometendo-me a guardar o sigilo necessário, de acordo com o que preceitua a Lei n° 7.170, de 14 de dezembro de 1983, que em seu Art. 13 prevê:

"Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos.

Pena: reclusão de 3 a 15 anos.

Parágrafo único - incorre na mesma pena quem:

I - com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa;

II - com o mesmo objetivo, realiza atividade aerofotográfica ou de sensoreamento remoto, em qualquer parte do território nacional;

III - oculta ou presta auxílio a espião sabendo-o tal, para subtraí-lo à ação de autoridade pública;

IV - obtém ou revela, para fim de espionagem desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo."

Comprometo-me em manter o sigilo de todas as minhas senhas de acesso, as quais não deverão ser fornecidas a qualquer outra pessoa.

Comprometo-me a não permitir o acesso ao meu equipamento por qualquer outra pessoa, salvo em estrita necessidade do serviço, devidamente autorizado e sob minha total responsabilidade.

Comprometo-me a tratar de forma adequada todas as informações, documentos, softwares e instalações de caráter sigiloso com as quais venha a ter contato, não divulgando a terceiros conhecimentos restritos de qualquer natureza.

Comprometo-me a informar imediatamente à administração toda e qualquer quebra de sigilo ou de segurança, que venha a ter ciência, de forma voluntária ou não.

Comprometo-me a cumprir rigorosamente as normas de segurança em vigor no âmbito da DTI.

Estou ciente de que minha estação de trabalho poderá ser auditada pelos órgãos responsáveis, a qualquer tempo e sem aviso prévio, sendo que a nenhum diretório poderá ser negado o acesso.

Sei também que os computadores do COMAER, os seus sistemas de informação e as suas redes estão sujeitos ao monitoramento, a qualquer tempo, e que o uso dos seus recursos implica no consentimento para este monitoramento. Consequentemente, nenhuma expectativa de privacidade deve ser assumida com relação às informações transmitidas, recebidas ou armazenadas nas redes que integram a INTRAER.

Declaro ainda que estou ciente das determinações contidas nas seguintes legislações e suas atualizações, bem como das demais normas castrenses vigentes:

Termos de Uso das Mídias Sociais do COMAER, 2ª Edição.

DCA 14-7/2013 - Política do COMAER para a TI;

DCA 14-8/2013 - Política de segurança da informação do COMAER;

ICA 7-5/2001 - Uso da Rede Mundial de Computadores - INTERNET - no COMAER;

ICA 200-12/2013 - Avaliação de documentos classificados no COMAER;

NSCA 7-1/2012 - Uso da Rede de Dados do COMAER - INTRAER;

NSCA 7-13/2013 - Segurança de Sistemas de TI no COMAER;

FCA 200-6/2013 - Tratamento de informações classificadas no COMAER;

RICA 21-236/2011 - Regimento Interno da DTI;

Lei 9.609, de 19 de fevereiro de 1998 - Lei da propriedade intelectual de programa de computador;

Lei 12.527, de 18 de novembro de 2011 - Lei de acesso à informação (LAI);

Decreto 7.724, de 16 de maio de 2012 - Regulamenta a LAI.

Decreto 7.845, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada.

O descumprimento das mesmas ou de qualquer norma de segurança, poderá implicar nas sanções administrativas e legais julgadas cabíveis.

Rio de Janeiro, de de 2015.

Nome completo: _____

Assinatura: _____

Identidade/Órgão Expedidor: _____

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

NSCA 7-1

USO DA REDE DE DADOS DO COMANDO DA AERONÁUTICA - INTRAER

2012

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
COMANDO-GERAL DE APOIO

TECNOLOGIA DA INFORMAÇÃO

NSCA 7-1

USO DA REDE DE DADOS DO COMANDO DA AERONÁUTICA - INTRAER

2012

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
COMANDO-GERAL DE APOIO

PORTARIA COMGAP Nº 6/3EM, DE 22 DE MARÇO DE 2012.
Protocolo COMAER nº 67131.000033/2012-87.

Aprova a reedição da Norma de Sistema para Uso da Rede de Dados do Comando da Aeronáutica - INTRAER.

O COMANDANTE-GERAL DE APOIO, no uso de suas atribuições, que lhe conferem o Inciso IX do Art. 5º e o Inciso XI do Art. 9º do Regulamento do Comando-Geral de Apoio, aprovado pela Portaria n° 643/GC3, de 8 de setembro de 2010 e tendo em vista o disposto no item 3.3 da ICA 700-1/2006 "Implantação e Gerenciamento de Sistemas no Comando da Aeronáutica", resolve:

Art. 1º Aprovar a reedição da NSCA 7-1 "Norma de Sistema para Uso da Rede de Dados do Comando da Aeronáutica - INTRAER".

Art. 2º Esta Norma entra em vigor na data de sua publicação em Boletim do Comando da Aeronáutica.

Ten Brig Ar RICARDO MACHADO VIEIRA
Comandante-Geral de Apoio

(Publicado no BCA Nº 061, de 28 de março de 2012)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta norma tem por finalidade estabelecer os critérios, os procedimentos e as atribuições para uso da Rede de Dados do Comando da Aeronáutica (INTRAER).

1.2 CONCEITUAÇÕES

1.2.1 ACESSO

Ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade (Fonte: Norma Complementar 07/IN01/DSIC/GSIPR, de 06 de maio de 2010).

1.2.2 ACESSO À CAIXA POSTAL

Interface entre um cliente de correio e um sistema de correio (Fonte: e-PING – Padrões de Interoperabilidade de Governo Eletrônico, Documento de referência, versão 2012, de 21 de novembro de 2011).

1.2.3 ACESSO À INTRAER

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.

1.2.4 AUTENTICIDADE

Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. (Instrução Normativa GSI/PR no 1, de 13 de junho de 2008).

1.2.5 CORREIO ELETRÔNICO

Sistema usado para criar, transmitir e receber mensagem eletrônica e outros documentos digitais por meio de rede de computadores (Fonte: Câmara Técnica de Documentos Eletrônicos – CTDE do CONARQ - Glossário.- (Versão 5.1 – março de 2010).

1.2.6 CAIXA POSTAL ELETRÔNICA

Espaço em arquivo de computador para recebimento de mensagens de correio eletrônico.

1.2.7 CAIXAS POSTAIS INDIVIDUAIS-FUNCIONAIS

As caixas postais individuais-funcionais destinam-se à troca de mensagens, via correio eletrônico do Governo Federal, entre as pessoas que trabalham nas organizações abrangidas por esta Norma, isto é, mensagens pessoais (Fonte: “Caixas Postais Individuais-Funcionais no Governo Federal”, disponível no endereço eletrônico: http://www.e.gov.br/correios/cp_individ.htm).

1.2.8 CONFIDENCIALIDADE

Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado. (Fonte: Instrução Normativa GSI/PR no 1, de 13 de junho de 2008).

1.2.9 DISPONIBILIDADE

Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade. (Instrução Normativa GSI/PR no 1, de 13 de junho de 2008).

1.2.10 ENDEREÇO IP

IP - *Internet Proto*col (Protocolo de Internet): protocolo que permite a comunicação entre dispositivos na rede. De forma genérica, pode ser considerado como um conjunto de números que representa o local de um determinado equipamento (normalmente computadores) em uma rede privada ou pública (Fonte: e-PING – Padrões de Interoperabilidade de Governo Eletrônico, Documento de referência, versão 2012, de 21 de novembro de 2011).

1.2.11 DNS ("*DOMAIN NAME SYSTEM*")

DNS – Domain Name System (Sistema de Nomes de Domínio): forma como os nomes de domínio são encontrados e traduzidos no endereço de protocolo da Internet. Um nome de domínio é um recurso fácil de ser lembrado quando referenciado como um endereço na Internet (Fonte: e-PING – Padrões de Interoperabilidade de Governo Eletrônico, Documento de referência, versão 2012, de 21 de novembro de 2011).

1.2.12 INTEGRIDADE

Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. (Instrução Normativa GSI/PR no 1, de 13 de junho de 2008).

1.2.13 "*LOGIN*"

Conjunto de procedimentos que visam a permitir o acesso de um usuário a um computador, a um servidor ou a outro recurso da rede.

1.2.14 *"LOGOUT"*

Conjunto de procedimentos para desconectar um usuário de um computador, de um servidor ou de outro recurso da rede.

1.2.15 MENSAGEM ELETRÔNICA ("*E-MAIL"*)

Documento digital produzido ou recebido via sistema de correio eletrônico, incluindo anexos que possam ser transmitidos com a mensagem (Fonte: Câmara Técnica de Documentos Eletrônicos – CTDE do CONARQ - Glossário.- (Versão 5.1 – março de 2010).

1.2.16 SERVIDOR

Computador que oferece um serviço ou que compartilha com outros computadores em uma rede, recursos na forma de arquivos, impressoras, etc.

1.2.17 "*SPAM*"

Spam é o termo usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas, ou o uso de soluções de mensagens instantâneas, onde é possível transmitir diversos tipos de arquivos digitalizados, não somente sob a forma de anexos.

Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês Unsolicited Commercial E-mail) (Fonte: Cartilha de segurança para Internet 3.1 do cert.br, disponível em: http://cartilha.cert.br/spam/sec1.html#sec1).

1.3 ÂMBITO

Esta Norma se aplica a todas as Organizações do COMAER.

2 INTRAER

2.1 ESTRUTURA DA REDE

A INTRAER é composta pela integração das redes locais das Organizações do COMAER, por meio de infraestrutura de telecomunicações.

Em cada localidade onde existe uma concentração de OM do COMAER, foi implantada uma infraestrutura de telecomunicações, denominada Rede Metropolitana, que interliga as redes locais existentes.

Da mesma forma, todas as Redes Metropolitanas estão interligadas por uma infraestrutura de telecomunicações, em nível nacional, constituindo uma Rede de Longa Distância.

Cada Organização do COMAER é considerada provedora de acesso à INTRAER.

2.2 RESTRIÇÕES RELATIVAS À SEGURANÇA DAS INFORMAÇÕES

2.2.1 CARÁTER GERAL

É expressamente proibida a utilização dos recursos da INTRAER nas seguintes situações:

a) atividades ilegais, fraudulentas, ou maliciosas; político-partidárias; "*lobby*" ou proselitismo político ou religioso; propaganda de empresas ou instituições sem relação direta com a missão do COMAER; incitação à prática de crime ou de transgressão disciplinar;
b) atividades com o propósito de ganho pessoal ou comercial;
c) uso de recursos computacionais com o propósito de acessar ou divulgar informação inapropriada, ofensiva ou contrária aos bons costumes;
d) armazenamento ou processamento de informação classificada, sem a devida autorização;
e) obtenção, armazenamento, instalação e utilização de programas, sem o devido licenciamento junto à Empresa ou Instituição detentora legal dos seus direitos de uso;
f) liberação do acesso, por parte de indivíduos não expressamente autorizados, de recursos disponíveis na INTRAER, sejam estes recursos equipamentos, serviços de rede ou programas que foram licenciados para o COMAER;
g) atividades visando a modificação ou a substituição de programas padronizados pelo Órgão Central do STI para emprego nos servidores de rede ou nas estações de trabalho da INTRAER;
h) atividades visando a modificação ou a substituição de programas aplicativos homologados e padronizados pelos Elos de Coordenação do STI, na sua área de responsabilidade, para emprego nos servidores de rede ou nas estações de trabalho da INTRAER;
i) atividades visando divulgar identidade dos usuários e senhas ou, de outro modo, permitir ou capacitar qualquer indivíduo não autorizado para acessar um sistema de TI do COMAER;
j) uso não autorizado de identificação ou senha individual;

k) atividades que permitam visualizar, modificar ou remover arquivos ou qualquer outro tipo de informação de propriedade de usuários da rede, sem a devida autorização;
l) emprego de ferramentas que realizem análises na rede local, visando a obter informações sobre as máquinas servidoras, as máquinas clientes e os demais recursos da rede local, exceto quando expressamente autorizado pelo administrador da rede, exceto quando expressamente autorizado pelo Comandante da OM; e
m) emprego de ferramentas que realizem análises nas redes metropolitanas e de longa distância, visando obter informações sobre as máquinas servidoras, as máquinas clientes e os demais recursos das redes, exceto quando expressamente autorizado pelo Órgão Central do STI.

2.2.2 PÁGINAS *WEB*

2.2.2.1 Conteúdo

Embora o conteúdo das páginas *WEB* publicadas em cada um dos servidores das Organizações seja de responsabilidade do Comandante da OM, é necessário observar que alguns assuntos, por motivos evidentes, não devem ser divulgados em páginas de acesso irrestrito. Estes assuntos são:

a) planos ou Ordens referentes a operações militares;
b) referências que facilitem a obtenção de informações classificadas;
c) *links* de acesso a sistemas de propriedade das Organizações Militares, tais como correio eletrônico (webmail), SIGADAER, entre outros, evitando tentativas de ataques do tipo "*sql injection*" nesses sistemas; e
d) informações de cunho pessoal sobre os militares e seus familiares.

Para a divulgação de informações em páginas WEB deve ser observado também o disposto no item 3.4.6 da RCA 205-1 "REGULAMENTO PARA SALVAGUARDA DE ASSUNTOS SIGILOSOS DA AERONÁUTICA", de 7 de março de 2006.

2.2.2.2 Padrões

Além dos padrões já estabelecidos em legislação interna do COMAER, as páginas do COMAER na INTRAER devem atender também aos "Padrões Brasil e-Gov", disponíveis em www.governoeletronico.gov.br.

2.2.3 CORREIO ELETRÔNICO

Alguns princípios devem ser observados pelos usuários de correio eletrônico na INTRAER:

a) no envio de mensagens para tratar de assuntos de interesse do serviço deve ser respeitada a cadeia de comando estabelecida;
b) não é permitido o envio ou o encaminhamento de mensagens espúrias tais como as populares "correntes" ou as de cunho político ou religioso;
c) as mensagens que contiverem arquivos associados ("atachados") devem ser previamente analisadas por programas antivírus e só então enviadas; e

d) o "*spam*" (definido como tendo 10 (dez) ou mais endereços de destino) é expressamente proibido, exceto quando devidamente autorizado pelo Comandante da OM de origem da mensagem.

2.2.4 PRIVACIDADE

Os usuários da INTRAER devem estar cientes de que os computadores do COMAER, os seus sistemas de informação e as suas redes estão sujeitos ao monitoramento, a qualquer tempo, e que o uso dos seus recursos implica no consentimento para este monitoramento.

Consequentemente, nenhuma expectativa de privacidade deve ser assumida com relação às informações transmitidas, recebidas ou armazenadas nas redes que integram a INTRAER.

Os sistemas de informação e os dados que neles existem são bens do COMAER e devem ser protegidos contra a divulgação indevida e contra a perda de integridade, de disponibilidade e de confidencialidade.

Em particular, devem ser adotados adequadamente todos os procedimentos estabelecidos pelo Órgão Central do STI e pelo CIAER, quando necessário, devem ser adotadas medidas complementares, específicas de cada interessado, além daquelas preconizadas para uso geral ou recomendadas.

Em todos os níveis da rede, devem ser implementados os meios adequados de autenticação de usuários e de registro de suas atividades, de modo a possibilitar o conhecimento e a verificação de todas as ações realizadas. A autenticação e o registro são obrigatórios para qualquer que seja a modalidade de inicialização do sistema ou de acesso.

2.3 APLICATIVOS QUE UTILIZAM RECURSOS DA INTRAER

A utilização da INTRAER como infraestrutura de comunicação de dados para suporte ao tráfego de informações oriundas ou destinadas a sistemas aplicativos, desenvolvidos ou adquiridos sem autorização expressa do Órgão Central do STI, está sujeita aos seguintes fatores condicionantes:

a) o projeto do sistema aplicativo deve ser submetido ao Órgão Central do STI, para análise e aprovação, com antecedência mínima de 30 dias em relação à data prevista para a sua entrada em operação;

b) o processo de implantação do sistema deve ser acompanhado por representantes do Órgão Central do STI;

c) o sistema deve ser submetido a testes de comunicação, acompanhados por representantes do Órgão Central do STI, que comprovem sua capacidade de operar nas condições técnicas disponíveis na INTRAER;

d) a entrada em operação do aplicativo só deverá ocorrer com autorização expressa do Órgão Central do STI;

e) a implantação de sistemas aplicativos, cujo consumo de recursos de rede esteja limitado à rede local da OM interessada, poderá ser processada, desde que o sistema

não venha a sobrecarregar a rede da OM, prejudicando de forma acentuada o acesso a sistemas de interesse do COMAER que são operados naquela OM; e

f) a suspensão do suporte da INTRAER a um sistema aplicativo pode ocorrer, a qualquer tempo, em caráter temporário ou permanente, caso o aplicativo em questão passe a comprometer o desempenho da INTRAER e, principalmente, a adequada operacionalidade de sistemas de interesse do COMAER.

2.4 ACESSOS REMOTOS ÀS REDES QUE COMPÕEM A INTRAER

A implantação de qualquer acesso remoto a INTRAER (externo à rede local de uma OM) só poderá ocorrer com autorização expressa do Órgão Central do STI.

Para obter autorização para implantação do acesso remoto, a OM interessada deverá encaminhar ao Órgão Central do STI, via seu Elo de Coordenação de TI, com antecedência mínima de 180 dias, o projeto de implantação do acesso, informando a proposta de solução técnica a ser utilizada, os dispositivos de segurança das informações adotados e a responsabilidade pelos custos associados à implantação e à manutenção do acesso remoto pretendido.

2.5 COMPARTILHAMENTO DE RECURSOS DA INTRAER COM OUTRAS REDES

O compartilhamento de recursos (servidores, estações de trabalho, ativos de rede, etc.) utilizados na INTRAER com a Internet ou outras redes só poderá ocorrer com autorização expressa do Órgão Central do STI.

A solicitação para compartilhamento desses recursos deverá ser encaminhada pela OM interessada ao Órgão Central do STI, via seu Elo de Coordenação de TI, com antecedência mínima de 180 dias.

2.6 ENDEREÇOS IP E DNS

A atribuição e o controle de endereços IP competem ao Órgão Central do STI.

O padrão de nome de domínio a ser utilizado pela Organização é a sequência de letras minúsculas e algarismos correspondentes à sigla da OM, sem qualquer sinal gráfico (hífen, travessão, barra, espaço, sinais de pontuação, acentos gráficos, etc.), seguidos da expressão "**intraer**", como, por exemplo:

a) bagl.intraer;
b) comar1.intraer;
c) pamals.intraer; e
d) srpvmn.intraer.

2.7 CORREIO ELETRÔNICO

O correio eletrônico da INTRAER é um serviço de comunicação interna do COMAER, viabilizando as mensagens do tipo "*e-mail*", em complemento aos usuais telefonemas, radiogramas, correspondências postais, mensagens fax, etc.

As caixas postais eletrônicas são funcionais e atribuídas no sentido decrescente de nível hierárquico na Organização. Entretanto, também podem ser criadas caixas pessoais vinculadas à funcional.

A conta de autenticação que protege o acesso a qualquer caixa postal eletrônica é pessoal.

A cada caixa postal eletrônica corresponde a uma única conta de autenticação.

A página principal de cada OM na INTRAER deve conter um apontador de fácil identificação para a relação dos endereços de suas caixas postais funcionais.

2.7.1 CAIXAS POSTAIS FUNCIONAIS

Compete aos Comandantes, Diretores ou Chefes a concessão das caixas postais funcionais, cabendo ao responsável pela rede local controlar a utilização delas.

A formação do endereço das caixas postais funcionais deve ser uma sequência de letras minúsculas e algarismos que identifique a função, seguida do símbolo "a comercial - @" e da identificação da OM, mais a expressão "**intraer"**, apresentada no padrão de domínio DNS, por exemplo:

a) Chefe do Centro de Computação da Aeronáutica do Rio de Janeiro ch@ccarj.intraer; e

b) Chefe do Esquadrão de Pessoal da Base Aérea de Recife ep@barf.intraer.

Para a identificação correta da função deve ser consultado o MCA 10-3.

O campo "*Display Name"* deve conter a sigla correspondente ao endereço, grafado em letras maiúsculas, tal como consta do MCA 10-3.

2.7.2 CAIXAS POSTAIS INDIVIDUAIS-FUNCIONAIS

Compete aos Comandantes, Diretores ou Chefes a concessão das caixas postais individuais funcionais, cabendo ao responsável pela rede local controlar a utilização delas.

Para a INTRAER, a formação do endereço das caixas postais individuais funcionais deve ser uma sequência de letras minúsculas que identifique o nome-de-guerra e as iniciais do nome do militar (no caso de civis, o nome pelo qual é conhecido o funcionário), seguida do símbolo "a comercial - @" e da identificação da OM, mais a expressão **"intraer"**, como apresentada no padrão de domínio DNS, por exemplo:

a) 1º Ten.-Av. Marco Aurélio da SILVA, do CCA-RJ silvamas@ccarj.intraer.

O campo "*Display Name"* deve conter o posto ou a graduação e o nome-de-guerra do militar (ou CV e o nome do funcionário), em maiúsculas, de acordo com o disposto no MCA 10-3, como, por exemplo:

a) TEN SILVA.

Alternativamente, as regras para definição da formação do endereço das caixas postais individuais funcionais e do campo "*Display name*", deverão seguir o estabelecido no documento "Caixas Postais Individuais-Funcionais no Governo Federal", disponível no endereço eletrônico: http://www.governoeletronico.gov.br/acoes-eprojetos/e-ping-padroes-de-interoperabilidade/arquivo.

2.7.3 IDENTIFICAÇÃO DO EMISSOR

Todos os "*e-mails*" devem conter ao final, como assinatura, a identificação do remetente, com seu nome completo, posto ou graduação, quadro ou especialidade, função e OM, como, por exemplo:

a) MARCO AURÉLIO DA SILVA - 1º Ten Av
Chefe da Seção de Informática do CCA-RJ

3 ATRIBUIÇÕES

3.1 DO CIAER:

Compete ao CIAER - Órgão Central do Sistema de Inteligência do COMAER - , em coordenação com o Órgão Central do STI, orientar e controlar a utilização dos procedimentos de segurança da INTRAER.

3.2 DO ÓRGÃO CENTRAL DO STI:

Ao Órgão Central do STI compete:

a) a supervisão técnica e operacional da INTRAER; e
b) o estabelecimento de normas para administração e uso da INTRAER, inclusive para o planejamento, a aquisição, a manutenção, a utilização, a padronização, o controle de acesso, a segurança, a atribuição de endereços IP, o gerenciamento da rede e o treinamento dos operadores e dos usuários da INTRAER.

3.3 DOS CENTROS DE COMPUTAÇÃO DA AERONÁUTICA:

Compete aos CCA cooperarem com o Órgão Central do STI na operação e no controle de utilização da INTRAER e, ainda, apoiar o funcionamento das redes locais das OM.

3.4 DOS COMANDANTES, CHEFES OU DIRETORES DE OM:

Compete aos Comandantes, Chefes e Diretores de OM:

a) viabilizar o uso adequado da INTRAER no âmbito da OM;
b) cooperar com os CCA de sua área na operação e no controle do funcionamento da INTRAER, providenciando o atendimento do que lhe for solicitado;
c) autorizar o que lhe compete para o correto funcionamento da INTRAER;
d) implementar as medidas complementares de segurança e as demais que forem necessárias para o adequado funcionamento da rede local;
e) promover a capacitação adequada dos técnicos e dos usuários da INTRAER do efetivo de sua Organização;
f) incluir na ficha de desimpedimento, um campo para certificação, pelo setor de Tecnologia da Informação, da efetivação de cancelamento, de remoção ou de encerramento de acessos, senhas, caixas postais eletrônicas, arquivos, autorizações e afins, pertinentes ao pessoal movimentado da OM;
g) impedir a utilização de programas ou de sistemas irregulares em computadores da Organização;
h) fiscalizar a correta utilização da INTRAER no âmbito da OM; e
i) comunicar ao seu Elo de Coordenação do STI, as irregularidades ou as sugestões relativas ao funcionamento da INTRAER.

3.5 DOS ADMINISTRADORES OU GERENTES DE REDE LOCAL:

Compete aos Administradores ou Gerentes de Rede Local:

a) cuidar para o contínuo funcionamento da rede local;
b) supervisionar diariamente as operações da INTRAER;
c) cuidar da segurança local e cooperar com a segurança geral dos sistemas, instalações, equipamentos e redes que compõem a INTRAER;
d) implementar, executar e controlar os procedimentos de segurança, incluindo a realização de cópias e a guarda adequada dos meios de recuperação dos sistemas;
e) preservar a confidencialidade das informações disponíveis na rede local;
f) controlar a concessão e a utilização de senhas, autenticações, contas, acessos e afins de interesse local para uso da INTRAER;
g) realizar inspeções periódicas para avaliar o correto funcionamento da rede local e antecipar as medidas evolutivas necessárias; e
h) providenciar para que o Comandante, Diretor ou Chefe da OM tome pronto conhecimento das irregularidades que observar no funcionamento da INTRAER.

3.6 DOS USUÁRIOS:

Compete aos usuários da INTRAER:

a) manter sigilo e utilizar adequadamente senhas, autenticações, acessos, equipamentos, arquivos, programas e afins, para que não haja comprometimento nem da segurança, nem do funcionamento da INTRAER;
b) limitar o acesso à INTRAER somente às pessoas autorizadas e para os devidos fins;
c) controlar o acesso às instalações e aos equipamentos da INTRAER de sua responsabilidade;
d) utilizar somente programas regularizados e de uso autorizado na INTRAER;
e) utilizar somente programas e arquivos que tenham sido verificados previamente, quanto à existência de vírus de computador e demais *softwares* maliciosos;
f) realizar criteriosamente os procedimentos lógicos de "*login"* (conexão) e de "*logout"* (desconexão) da sua rede local;
g) responder pela utilização das estações de trabalho, programas e arquivos sob sua responsabilidade;
h) cuidar da armazenagem apropriada das cópias de mensagens que devam ser preservadas;
i) assegurar-se de que as mensagens enviadas estejam devidamente identificadas no campo de origem e no final do texto. Não sendo admitida qualquer tentativa de anonimato;
j) relatar qualquer irregularidade observada durante o uso da INTRAER, a seu superior ou ao Administrador ou ao Gerente da rede local;
k) verificar a autenticidade das mensagens de correio eletrônico sempre que julgar conveniente; e
l) verificar periodicamente o conteúdo de sua caixa postal eletrônica, providenciando a exclusão das mensagens desnecessárias.

4 DISPOSIÇÕES FINAIS

4.1 Os casos não previstos serão resolvidos pelo Exmo. Sr. Comandante-Geral de Apoio.

MINISTÉRIO DA DEFESA COMANDO DA AERONÁUTICA **DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA** ORDEM TÉCNICA DO COMANDO DA AERONÁUTICA			
DOCUMENTO Nº OTCA 009/DTI/2019	**GRAU DE SIGILO** OSTENSIVO	**EMISSÃO** 28 OUT 2019	**VALIDADE** PERMANENTE
ASSUNTO PADRONIZAÇÃO DO ACESSO À INTERNET NO COMAER – ACESSO NÃO FUNCIONAL		**DISTRIBUIÇÃO** ORGÃO CENTRAL DO STI ELOS DO STI	
ANEXOS: ANEXO A – Topologia de rede			

1. **DISPOSIÇÕES PRELIMINARES**

1.1. FINALIDADE

A presente Ordem Técnica do Comando da Aeronáutica (OTCA) tem por finalidade estabelecer os requisitos técnicos e procedimentos gerais para o acesso não funcional à Internet provido por Organização Militar do COMAER. São exemplos aplicáveis a esta OTCA:

a) Acesso à Internet provido por Hotéis de Trânsito (cabeado ou *Wi-Fi*);

b) Acesso *Wi-Fi* à Internet em Elo de Serviço do STI;

c) Acesso *Wi-Fi* à Internet em Exercício ou Operação; e

d) Qualquer tipo de ponto de acesso contratado e mantido por Organização da Aeronáutica.

Objetivos a serem alcançados com esta OTCA:

a) Padronização dos serviços de acessos não funcionais;

b) Adequação às legislações de TI em vigor; e

c) Centralização dos acessos à Internet para otimização dos gastos com contratos de Internet no COMAER e gestão eficiente destes *links*.

1.2. ÂMBITO

Esta OTCA aplica-se ao Órgão Central do STI e aos demais elos do STI.

1.3. ABREVIATURAS

COMAER – Comando da Aeronáutica.

LAMP – Linux, Apache, MySQL e PHP.

OM – Organização Militar.

STI – Sistema de Tecnologia da Informação do COMAER.

1.4. CONCEITUAÇÃO

Para efeito desta publicação, os termos e expressões abaixo têm as seguintes conceituações:

1.4.1. *ACCESS POINT:*

Access Point ou AP é um dispositivo de rede sem fio que realiza a interconexão entre dispositivos. Em geral se conecta a uma rede cabeada servindo de ponto de acesso para outra rede, como, por exemplo, a INTERNET.

1.4.2. BACKUP

Cópia de segurança de dados de servidores e sistemas.

1.4.3. CAPTIVE PORTAL

Captive Portal é uma página *web* que o usuário deve visualizar e interagir, antes de ter acesso a uma rede pública, na qual foi ingressada recentemente. É principalmente usado com propósito de autenticação.

1.4.4. DISPOSITIVOS MÓVEIS

É o nome dado ao equipamento eletrônico portátil, podendo ser facilmente transportado, dotado de capacidade computacional, de armazenamento e/ou de tecnologia de comunicação em redes, no qual é possível conectar-se à INTERNET ou a qualquer outro tipo de rede, por meio de uma Rede sem Fio ou cabeada.

Consistem em *notebooks*, *netbooks*, PDA, *smartphones*, *smartwatches*, *tablets*, *pendrives*, USB *drives*, HDs externos e cartões de memória, não se limitando a estes.

1.4.5. FIREWALL

Sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes.

1.4.6. HOTSPOT

Access Point de uso público, utilizado, geralmente, em locais com áreas comuns, tais como aeroportos, estabelecimentos comerciais, shoppings e outros.

1.4.7. LDAP

Light-weight Directory Access Protocol é uma versão simplificada de serviço de diretório que organiza as informações como uma árvore e permite pesquisas em diferentes componentes e dados. (Fonte: IETF RFC 2251/1997).

1.4.8. PROXY

É o servidor que atua como intermediário entre uma rede local e a Internet, visando a

segurança da informação e o controle de acesso.

1.4.9. RADIUS

Remote Authentication Dial In User Service é um protocolo de rede que permite a autenticação de usuários, autorização de acesso a serviços, além do monitoramento e gerenciamento de recursos providos em rede. (Fonte: IETF RFC 2865/2000).

1.4.10. REDE SEM FIO (*WIRELESS*)

Uma rede sem fio é tipicamente uma extensão de uma rede local convencional cabeada, criando-se o conceito de uma rede local sem fio (*Wireless Local Area Network – WLAN*). Uma WLAN converte pacotes de dados em onda de rádio ou infravermelho e os envia para outro equipamento *wireless* ou para um ponto de acesso que serve como uma conexão para uma LAN. Assim, uma Rede *Wireless* é um sistema que interliga vários equipamentos fixos ou móveis utilizando o ar como meio de transmissão. (Fonte: ICA 7-21/2012: Redes sem Fio Wi-Fi do Departamento de Controle do Espaço Aéreo).

1.4.11. SNMP

Simple Network Management Protocol – Protocolo Simples de Gerência de Rede é um protocolo de gerência típica de redes UDP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores (*switches*). O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, fornecer informações para o planejamento de sua expansão, dentre outras. (Fonte: ICA 7-21/2012: Redes sem Fio Wi-Fi do Departamento de Controle do Espaço Aéreo).

1.4.12. VLAN

É uma rede comutada, logicamente segmentada por funções ou aplicações, sem considerar a localização física dos usuários. (Fonte: ICA 102-15/2013: Controles de Segurança da Informação da Rede de Telefonia IP do COMAER).

1.4.13. “WI-FI”

Wi-Fi é uma marca registrada da *Wi-Fi Alliance*, que é utilizada por produtos e equipamentos utilizados em redes locais sem fio, também conhecidas como WLAN, que são baseados no padrão IEEE 802.11. (Fonte: ICA 7-21/2012: Redes sem Fio *Wi-Fi* do Departamento de Controle do Espaço Aéreo).

1.4.14. WPA2

O WPA2 ou IEEE 802.11i foi uma substituição da *Wi-Fi Alliance* em 2004 à tecnologia WPA, pois, embora fosse mais segura em relação ao padrão anterior WEP, a *Wi-fi Alliance* teve a intenção de fazer um novo certificado para redes sem fio mais confiável e também necessitava continuar o investimento inicial realizado sobre o WPA. O principal objetivo do WPA2 é suportar as características adicionais de segurança do padrão 802.11i que não estão incluídas nos produtos que suportam WPA. Assim como o WPA, o WPA2 provê autenticação e criptografia, propondo a garantia de confidencialidade, autenticidade e integridade em redes sem fio. (Fonte: ICA 7-21/2012: Redes sem Fio Wi-Fi do Departamento de Controle do Espaço Aéreo).

2. **DISPOSIÇÕES GERAIS**

2.1. CONSIDERAÇÕES **GERAIS**

Com a implementação da Concentração dos Serviços de Tecnologia da Informação nos Grupamentos de Apoio, conforme previsto na MCA 21-1/2015 – IMPLANTAÇÃO DE GRUPAMENTOS DE APOIO, MCA 11-2/2016 – MANUAL DE PROCEDIMENTOS PARA A CONCENTRAÇÃO DE SERVIÇOS DE TI NOS GRUPAMENTOS DE APOIO e na NSCA 102-1/2013 – RESTRUTURAÇÃO DA INFRAESTRUTURA DE PROVIMENTO DE ACESSO À INTERNET NO COMAER, enlaces de comunicação de alta velocidade foram implantados nos GAP para acesso à INTERNET, os quais foram providos com ferramentas de proteção de perímetro com capacidade de mitigar riscos associados à Segurança Cibernética, de modo a atender às regulamentações em vigor.

Contudo, se faz necessário padronizar os acessos NÃO funcionais das Organizações Militares do COMAER, com vistas a também adequá-los às legislações de TI vigentes no âmbito do Governo Federal, tais como o armazenamento de registros de acesso previstos pelo Art. 13da Lei nº 12.965 de 22 de abril de 2014 (Marco Civil da Internet), transcrito no item a seguir.

2.2. LEI Nº 12.965 DE 22 DE ABRIL DE 2014 (MARCO CIVIL DA INTERNET)

"ART. 13. NA PROVISÃO DE CONEXÃO À INTERNET, CABE AO ADMINISTRADOR DE SISTEMA AUTÔNOMO RESPECTIVO O DEVER DE MANTER OS REGISTROS DE CONEXÃO, SOB SIGILO, EM AMBIENTE CONTROLADO E DE SEGURANÇA, PELO PRAZO DE 1 (UM) ANO, NOS TERMOS DO REGULAMENTO.

§ 1º A RESPONSABILIDADE PELA MANUTENÇÃO DOS REGISTROS DE CONEXÃO NÃO PODERÁ SER TRANSFERIDA A TERCEIROS.

§ 5º EM QUALQUER HIPÓTESE, A DISPONIBILIZAÇÃO AO REQUERENTE DOS REGISTROS DE QUE TRATA ESTE ARTIGO DEVERÁ SER PRECEDIDA DE AUTORIZAÇÃO JUDICIAL, CONFORME DISPOSTO NA SEÇÃO IV DESTE CAPÍTULO.
§ 6º NA APLICAÇÃO DE SANÇÕES PELO DESCUMPRIMENTO AO DISPOSTO NESTE ARTIGO, SERÃO CONSIDERADOS A NATUREZA E A GRAVIDADE DA INFRAÇÃO, OS DANOS DELA RESULTANTES, EVENTUAL VANTAGEM AUFERIDA PELO INFRATOR, AS CIRCUNSTÂNCIAS AGRAVANTES, OS ANTECEDENTES DO INFRATOR E A REINCIDÊNCIA."

2.3. REQUISITOS DE ACESSO POR MEIO DE REDE SEM FIO (WI-FI)

São os seguintes os requisitos mínimos e os procedimentos padronizados para os ativos de rede e serviços de TI envolvidos com os acessos NÃO funcionais das Organizações Militares do COMAER:

2.3.1. REQUISITOS MÍNIMOS DOS *ACCESS POINT*

2.3.1.1. É mandatório que os equipamentos suportem o protocolo WPA2 ou superior.

2.3.1.2. O *Access Point* (AP) deverá possibilitar atualização de *firmware*, a fim de incorporar novos padrões e eventuais correções lançadas pelo fabricante.

2.3.1.3. O administrador de rede deve alterar as configurações padrão do *Access Point*, antes de torná-lo operacional, incluindo:

a) senhas;

b) SSID

c) chaves; e

d) SNMP communities.

2.3.1.4. O AP deve ser instalado em um local com acesso físico controlado a fim de evitar o *reset* físico do equipamento para restabelecer as configurações de fábrica.

2.3.1.5. Os protocolos de configuração que não serão necessários pelo AP, como HTTP, SNMP, *Telnet* etc., devem ser desabilitados e, sempre que possível, deve-se optar por um modo de configuração que não seja pela própria rede *Wireless*, mas sim pela rede cabeada ou ainda via conexão serial, a fim de minimizar as chances de que a sessão de configuração com o ap seja capturada imediatamente utilizando um cliente *Wireless*.

2.3.1.6. O tráfego de administração remota do *Access Point* através da rede deve ser protegido por meio de criptografia, habilitando protocolos seguros como HTTPS OU SSH.

2.3.1.7. O A*ccess Point* deve, preferencialmente, ter suporte para geração de eventos de segurança da informação, mediante a criação de logs de eventos.

2.3.1.8. Sempre que possível, um *banner* de advertência para login na interface de administração do *Access Point* deve ser implantado. A exibição de uma mensagem de advertência durante o logon na interface de administração do AP tem como propósito informar que o equipamento em questão pertence à organização militar e é de uso restrito para usuários autorizados, e que os acessos, eventualmente, estarão sendo auditados.

2.3.2. REQUISITOS DE REDE

2.3.2.1. Em hipótese alguma, essas redes de acesso poderão ter comunicação com a INTRAER. Caso não seja possível isolar fisicamente os equipamentos que disponibilizam o acesso *Wi-Fi* dos que fornecem acesso à INTRAER, estas deverão ser separada por meio de VLAN.

2.3.2.2. Todos os switches que fizerem parte da referida rede de acesso à Internet deverão ser gerenciáveis e **efetivamente** gerenciados. Ou seja, deverão ter a possibilidade de configuração de IP e suporte a VLAN, para possibilitar a segregação da rede e monitoramento. O setor de TI do elo de serviço apoiador deverá ter as credenciais para gerenciar e monitorar os switches.

2.3.2.3. As conexões de rede Wi-Fi com à Internet devem ser protegidas por *firewall*, conforme anexo A. O primeiro *firewall* (*Firewall Wi-Fi*) será o gateway dos usuários da rede sem fio e tem a função de fazer o filtro de conteúdo e iniciar a autenticação do usuário. O segundo firewall (*Firewall* INTRAER 2) tem a finalidade de segregar a rede sem fio da rede corporativa do COMAER.

2.3.2.4. A solução de *firewall* a ser utilizada é a solução padronizada para o STI, atualmente, o sistema utilizado é o Pfsense, de preferência, em sua versão mais atualizada.

2.3.2.5. A rede *wireless* deve ser segregada de modo a permitir a aplicação de controles de acesso que identifiquem os protocolos e serviços autorizados a trafegar.

2.3.2.6. A utilização de equipamentos *wireless*, com função de *Access Point*, que não sejam de propriedade da organização militar deve ser proibida.

2.3.2.7. Deverá ser utilizado o serviço DHCP do *firewall*, deixando o serviço em questão desativado nos *Access Points*.

2.3.2.8. O IP de saída para a Internet utilizado para a rede *wireless* deverá, sempre que possível, ser diferente do IP utilizado para os acessos funcionais, para facilitar futuros rastreamentos de usuários.

2.3.2.9. A topologia da solução deve atender o disposto no anexo A.

2.3.3. REQUISITOS DE CRIPTOGRAFIA E AUTENTICAÇÃO

2.3.3.1. O WPA2 ou superior deverá ser habilitado no *Access Point*.

2.3.3.2. Caso o AP não possua suporte ao WPA2 *Enterprise* ou superior, poderá ser utilizado WPA2 com chave compartilhada.

2.3.3.3. É mandatório no uso de, no mínimo, WPA2 com chave compartilhada, uma solução segura de autenticação para permitir que somente usuários autorizados possam acessar à internet. Após o ingresso na rede sem fio, deve ser solicitada a autenticação individual do usuário, utilizando para isso, a solução de *Captive Portal* padronizada pela DTI.

2.3.3.4. Deve ser utilizado o *software* Pfsense na versão atual com *Captive Portal (hotspot)* configurado permitindo o acesso à rede somente após a autenticação com o usuário e senha cadastrados.

2.3.3.5. O administrador do Pfsense deve realizar o cadastro dos usuários por meio de um servidor RADIUS ou LDAP.

2.3.3.6. Deve ser ativado um *proxy* transparente (*squid*) com filtragem de conteúdos inadequados como por exemplo: pornografia, site de apologia a drogas, violência ou crimes, tais como pedofilia.

2.3.4. PROCEDIMENTOS GERAIS DE CONFIGURAÇÃO DA SOLUÇÃO

2.3.4.1. Instalar um *firewall* PfSense **(PfSense Wi-Fi)**, na última versão estável. Esse *firewall* poderá ser instalado na forma de máquina virtual, utilizando a infraestrutura do Elo de Serviço e deverá ter suas interfaces de rede configuradas conforme figura do anexo A, ou seja, com no mínimo uma interface na VLAN de usuários Wi-Fi e outra interface na VLAN de acesso à Internet.

2.3.4.2. Instalar e configurar os seguintes pacotes dentro do PfSense:

a) sudo – Gerenciamento de acessos de administrador

b) Squid – Serviço de proxy

c) Squidguard – Filtro de URL

d) Lightsquid – Interface de visualização de logs de acesso

e) Freeradius – Pacote para gerenciamento das autenticações.

2.3.4.3. Configurar o módulo Captive Portal do PfSense, utilizando o Squid como proxy transparente para melhor controle de conteúdo e armazenamento.

2.3.4.4. Deverá ser criado um servidor LAMP (Linux, Apache, MySQL, PHP) para armazenar as informações de autenticação dos usuários. O padrão de configuração desse servidor deverá seguir a normatização da DTI.

2.3.4.5. Os *logs* de acesso deverão ser armazenados no próprio PfSense Wi-Fi, que deverá ser dimensionado para armazenar pelo menos 1 ano de *log* de conexões.

2.3.5. PROCEDIMENTOS GERAIS DE CADASTRO DE USUÁRIOS

2.3.5.1. Todo usuário deverá ser previamente cadastrado antes de ter o acesso autorizado, tendo, no mínimo, informações de CPF e nome completo registrados.

2.3.5.2. O *login* usuário a ser cadastrado deverá ser o CPF para brasileiros, e o número de passaporte para estrangeiros.

2.3.5.3. É obrigatório o conhecimento e o consentimento do **Termo de Responsabilidade e de conhecimento da Política de Segurança da Informação (Anexo B),** para usuários da rede que não integrem o COMAER. O acesso à Internet será fornecido, mediante a assinatura do termo.

2.3.5.4. A utilização de *VOUCHER* só será permitida, caso a solução de acesso associe o Voucher à identificação do usuário e registre os acessos.

2.3.6. REQUISITOS DE AUDITORIA

2.3.6.1. Todos os *logs* de acesso do usuário deverão ser armazenados por, no mínimo 12 meses, conforme requisitos da Lei nº 12.965, de 23 de abril de 2014.

2.3.6.2. Todos os *logs* de acesso do usuário devem ser gerados e armazenados, conforme requisitos da Lei nº 12.965, de 23 de abril de 2014.

2.3.7. RESPONSABILIDADES

2.3.7.1. O Elo de Serviço apoiador e OM solicitante do serviço serão responsáveis pela configuração e operação de todos os equipamentos e softwares que fazem parte da solução descrita nesta OTCA. Também serão responsáveis por garantir o cumprimento dos requisitos técnicos e procedimentos previstos nesta norma, de forma a manter conformidade com a Lei 12.965/2014.

2.3.7.2. Os setores de TI dos Elos de Serviço apoiador deverão se capacitar para prover os serviços da referida solução, incluindo, tecnologia de *Firewall* (*PfSense*), gerenciamento de *switches* e de *Access Point*s e servidores de autenticação, usando para isso, fontes de conhecimento e manuais na INTERNET e realizando os cursos da Cisco (CCNA) atualmente disponíveis via convênio do Exército (www.escom.eb.mil.br).

2.3.7.3. A DTI poderá ministrar treinamentos específicos para o setor de TI do Elo de Serviço apoiador, de forma a capacitá-los a configurar e operar a solução de acesso, mediante solicitação.

2.4. A DTI normatizará o padrão de configuração do servidor LAMP e do PfSense Wi-Fi.

3. **DISPOSIÇÕES FINAIS**

3.1. Qualquer solicitação de acesso à Internet nos termos desta OTCA deverá ser submetidos inicialmente para o Elo de Serviço apoiador. O Elo de Serviço apoiador, por sua vez, caso não tenha as capacidades para implementação da solução, poderão solicitar treinamento à DTI.

3.2. Os casos não previstos nesta instrução serão submetidos à apreciação do Diretor de Tecnologia da Informação da Aeronáutica.

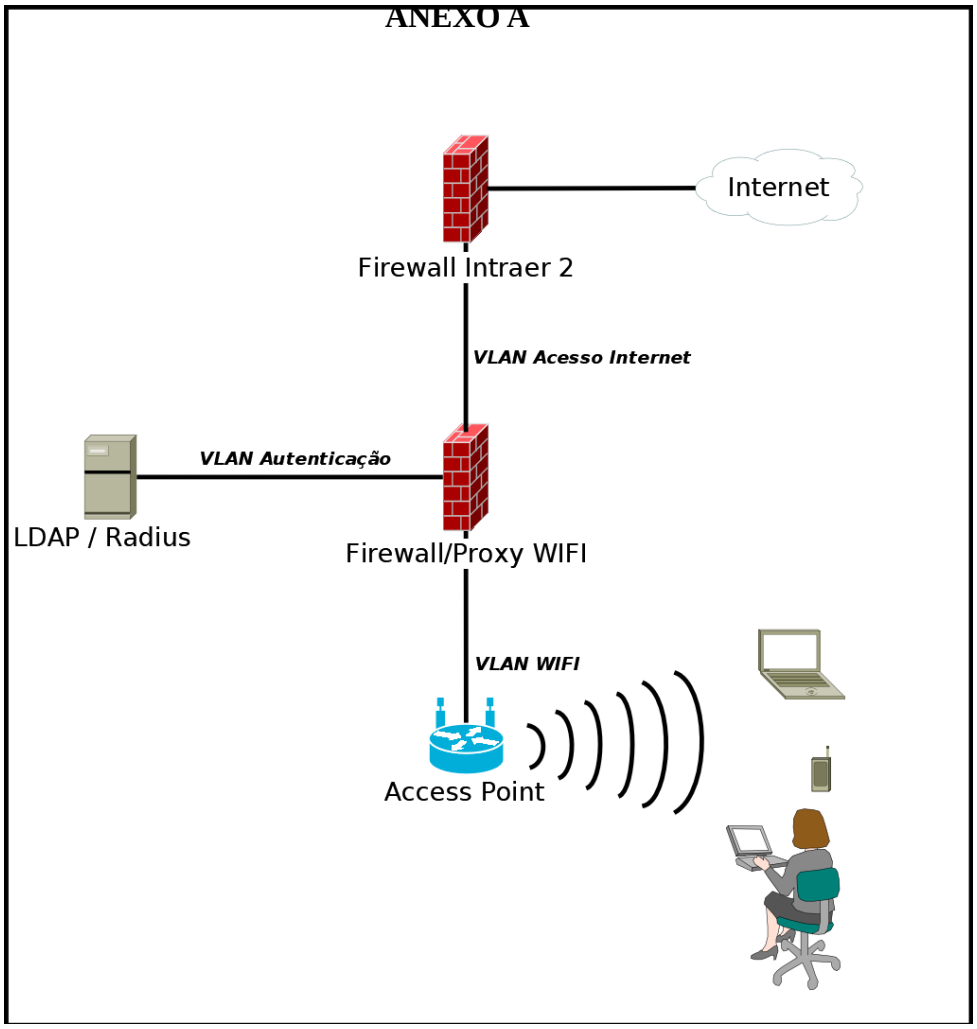
Brig Int **LUIZ FERNANDO** MORAES DA SILVA
Diretor de Tecnologia da Informação da Aeronáutica

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. CCE-093**.** *Comissão de Estudo Especial de Gestão de Projetos, Programas e Portfólio*. Rio de Janeiro, RJ, 2012.

BRASIL. Comando da Aeronáutica. Diretoria de Tecnologia da Informação da Aeronáutica. *Elaboração, Padronização e Controle de Publicações*: **OTCA 001/DTI**. Rio de Janeiro, RJ, 2016.

ANEXO A


Internet
Firewall Intraer 2
VLAN Acesso Internet
VLAN Autenticação
LDAP / Radius
Firewall/Proxy WIFI
VLAN WIFI
Access Point

ANEXO B

MINISTÉRIO DA DEFESA

COMANDO DA AERONÁUTICA

DIRETORIA DE TECNOLOGIA DA INFORMAÇAO DA AERONAUTICA

Termo de Responsabilidade e de conhecimento da Política de Segurança da Informação do

COMAER e das políticas de segurança da informação definidas pelas respectivas Organizações

Declaro que tenho pleno conhecimento de minha responsabilidade quanto à proteção a ser mantida sobre os assuntos sigilosos a que, por força de função ou atividade, tenha ou venha a ter acesso, comprometendo-me a guardar o sigilo necessário, de acordo com o que preceitua a Lei n°7.170, de 14 de dezembro de 1983, que em seu Art. 13 prevê:

"Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos.

Pena: reclusão de 3 a 15 anos.

Parágrafo único - incorre na mesma pena quem:

I - com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa;

II - com o mesmo objetivo, realiza atividade aerofotográfica ou de sensoreamento remoto, em qualquer parte do território nacional;

III - oculta ou presta auxílio a espião sabendo-o tal, para subtraí-lo à ação de autoridade pública;

IV - obtém ou revela, para fim de espionagem desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em

desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo."

Comprometo-me em manter o sigilo de todas as minhas senhas de acesso, as quais não deverão ser fornecidas a qualquer outra pessoa.

Comprometo-me a não permitir o acesso ao meu equipamento por qualquer outra pessoa, salvo em estrita necessidade do serviço, devidamente autorizado e sob minha total responsabilidade.

Comprometo-me a tratar de forma adequada todas as informações, documentos, softwares e instalações de caráter sigiloso com as quais venha a ter contato, não divulgando a terceiros conhecimentos restritos de qualquer natureza.

Comprometo-me a informar imediatamente à administração toda e qualquer quebra de sigilo ou de segurança, que venha a ter ciência, de forma voluntária ou não.

Comprometo-me a cumprir rigorosamente as normas de segurança em vigor no âmbito da DTI.

Estou ciente de que minha estação de trabalho poderá ser auditada pelos órgãos responsáveis, a qualquer tempo e sem aviso prévio, sendo que a nenhum diretório poderá ser negado o acesso.

Sei também que os computadores do COMAER, os seus sistemas de informação e as suas redes estão sujeitos ao monitoramento, a qualquer tempo, e que o uso dos seus recursos implica no consentimento para este monitoramento. Consequentemente, nenhuma expectativa de privacidade deve ser assumida com relação às informações transmitidas, recebidas ou armazenadas nas redes que integram a INTRAER.

Declaro ainda que estou ciente das determinações contidas nas seguintes legislações e suas atualizações, bem como das demais normas castrenses vigentes:

Termos de Uso das Mídias Sociais do COMAER, 2ª Edição.
DCA 14-7/2013 - Política do COMAER para a TI;
DCA 14-8/2013 - Política de segurança da informação do COMAER;
ICA 7-5/2001 - Uso da Rede Mundial de Computadores - INTERNET - no COMAER;
ICA 200-12/2013 - Avaliação de documentos classificados no COMAER;
NSCA 7-1/2012 - Uso da Rede de Dados do COMAER - INTRAER;
NSCA 7-13/2013 - Segurança de Sistemas de TI no COMAER;
FCA 200-6/2013 - Tratamento de informações classificadas no COMAER;
RICA 21-236/2011 - Regimento Interno da DTI;

Lei 9.609, de 19 de fevereiro de 1998 - Lei da propriedade intelectual de programa de computador;

Lei 12.527, de 18 de novembro de 2011 - Lei de acesso à informação (LAI);

Decreto 7.724, de 16 de maio de 2012 - Regulamenta a LAI.

Decreto 7.845, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada.

O descumprimento das mesmas ou de qualquer norma de segurança, poderá implicar nas sanções administrativas e legais julgadas cabíveis.

, de de 20 .

Nome completo: _____

Assinatura: _____

Identidade/Órgão Expedidor: _____

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-61

USO DAS REDES DE DADOS NO COMAER
(INTRAER E INTERNET)

2024

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-61

USO DAS REDES DE DADOS NO COMAER
(INTRAER E INTERNET)

2024

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA

PORTARIA DTI Nº103/SNOR, DE 15 DE MAIO DE 2024.

Protocolo COMAER nº 67131.001042/2024-29

Aprova a ICA 7-61 "Uso das Redes de Dados no COMAER (INTRAER E ITERNET)".

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA, no uso das atribuições que lhe confere o art. 5 da Portaria nº 634/GC3, de 11 de dezembro de 2023, e art. 11 do Regulamento da Diretoria de Tecnologia da Informação da Aeronáutica, aprovado pela Portaria nº 353/GC3, de 10 de agosto de 2022, resolve:

Art. 1º Aprovar o Uso das Redes de Dados no COMAER (INTRAER E INTERNET) – ICA 7-61, nos moldes da NSCA 5-1, conforme o disposto no Parágrafo único do art. 3° da Portaria nº 661/GC3, de 21 de dezembro de 2023.

Art. 2º Ficam revogados:

I – a Portaria COMGAP nº 6/3EM, de 22 de março de 2012, publicada no Boletim do Comando da Aeronáutica nº 61, de 28 de março de 2012

II – a Portaria EMAER nº 51/3SC, de 21 de dezembro de 2015, publicada no Boletim do Comando da Aeronáutica nº 236, de 23 de dezembro de 2015

III – a Portaria DTI nº 2/TIOP, de 4 de novembro de 2019, publicada no Boletim do Comando da Aeronáutica nº 203, de 7 de novembro de 2019; e

IV – a Portaria COMGAP nº 56/ADNP, de 24 de Julho de 2020, publica no Boletim do Comando da Aeronáutica nº 133, de 29 de julho de 2020.

Art. 3° Esta Portaria entra em vigor na data de sua publicação, por se trarar de urgência justificada no expediente administrativo, conforme parágrafo único do art. 4º, do Decreto nº 10.139, de 28 de novembro de 2019.

Brig Eng SÉRGIO RICARDO DE ASSIS
Diretor de Tecnologia da Informação da Aeronáutica

SUMÁRIO

PREFÁCIO

O avanço tecnológico trouxe mudanças significativas para sociedade. Neste sentido, a era digital modificou a forma de viver, nunca se acessou tantas informações de forma fácil e rápida. Em um pouco mais de 50 (cinquenta) anos, migrou-se da máquina de escrever para os computadores e com a criação da internet, disseminou-se a comunicação mundial.

Dessa forma, a Era Digital se consolidou mundialmente e veio melhorar as experiências de seus usuários. Todavia, simultaneamente, a preocupação com a cibersegurança explodiu no mundo, trazendo consigo a preocupação social com a proteção de dados pessoais em rede. Nessa seara, foi criada a LGPD (Lei Geral de Proteção de Dados Pessoais - Lei nº13.709).

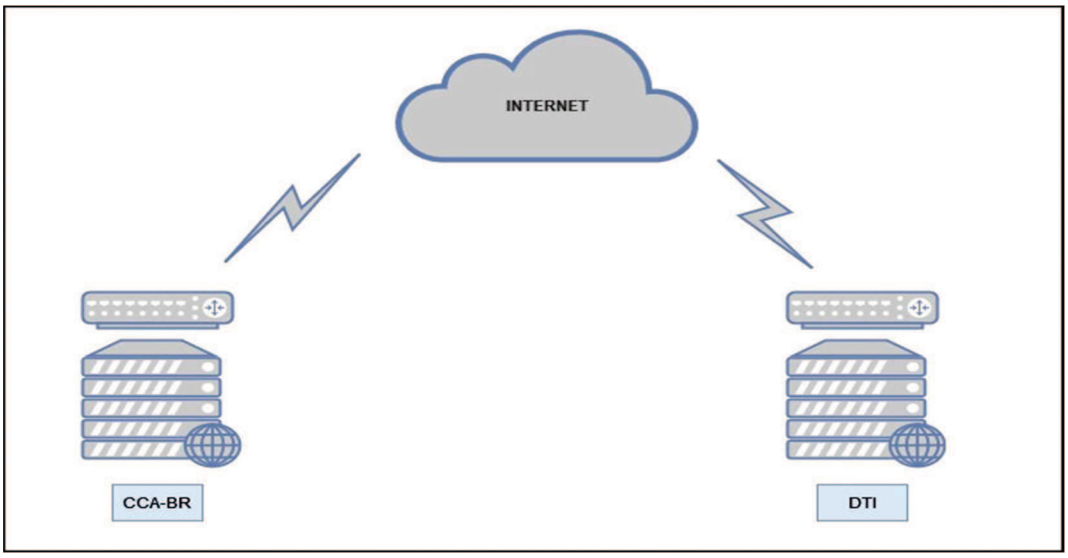
A tecnologia mudou a forma de pensar em sociedade e de se relacionar com as pessoas e com o mundo ao redor. A internet gera impactos na economia, força as empresas a otimizar seus processos e mudar o jeito de produzir produtos e serviços.

No COMAER não foi diferente, com o avanço tecnológico, surgiu a necessidade de criação de uma rede interna de comunicação de dados de TI, dessa forma surgiu a intraer. Essa rede é um instrumento indispensável para a racional utilização dos recursos de comunicação de dados que apoiam as atividades de Tecnologia da Informação (TI) de interesse da Aeronáutica.

Além do uso da intraer, a FAB utiliza a internet e por isso deve se preocupar com medidas complementares com o fito de estabelecer níveis de riscos aceitáveis para acessibilidade dessas redes. A cibersegurança visa prover as condições adequadas para a salvaguarda de interesses determinados ou coletivos, o que se constitui em responsabilidade de todos, conforme previsto na DCA 14-8 - "Política de Segurança da Informação do Comando da Aeronáutica".

A utilização da internet no COMAER oferece uma gama de possibilidades sobre a relação de trabalho colaborativo em rede. Na verdade, o acesso remoto da intraer, via internet, trouxe novas perspectivas de rompimento da barreira geográfica com a utilização da telemedicina, das reuniões por videoconferência e do *home office.*

O dinamismo e a quantidade de informações disponibilizadas na rede mundial de computadores (internet) se tornaram indispensáveis para o funcionamento das Organizações da Aeronáutica, potencializando a eficiência administrativa e a atualização de conhecimentos individuais. A intraer das OM é interligada pela internet que se conecta através dos links de Comutação de Rótulos Multiprotocolo executado por roteadores ou, como é mais conhecido, *Multiprotocol Label Switching* (MPLS), controlados pelo DECEA. A figura abaixo demonstra um exemplo de como funcionam essas conexões:



1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

A presente ICA tem por finalidade regular e doutrinar os critérios, os procedimentos, os níveis adequados de segurança da informação e as atribuições para uso da Rede de Dados intraer/internet no Comando da Aeronáutica.

1.2 CONCEITUAÇÕES

1.2.1 ACESSO

Ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade (Fonte: Norma Complementar 07/IN01/DSIC/GSIPR, de 06 de maio de 2010).

1.2.2 ACESSO À INTRAER

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

Consiste na capacidade de um computador acessar, à distância, um outro computador ou de uma rede de computadores e, assim, visualizar arquivos, o desktop e até controlar programas e as funcionalidades dos dispositivos acessados.

1.2.4 ACESSO SEGURO

Combinação de processos ou soluções de segurança projetados para impedir o acesso não autorizado aos ativos digitais de uma organização e a perda de dados confidenciais.

1.2.5 APLICATIVO

Trata-se de um software para computadores e/ou aparelhos móveis, que permite o desempenho de uma tarefa específica para usuários finais.

1.2.6 ATAQUE CIBERNÉTICO

Tentativas não autorizadas de explorar, roubar e/ou causar danos a informações confidenciais aproveitando-se de sistemas de computador vulneráveis. Visam causar danos ou obter o controle ou o acesso a documentos e sistemas importantes em uma rede de computadores pessoais ou comerciais. (MICROSOFT,2023)

1.2.7 ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

São todos os itens, físicos ou virtuais, que compõem a infraestrutura de TI. Ou seja, todo hardware, software, redes e outras tecnologias fundamentais para a continuidade das operações.

1.2.8 ATIVOS FÍSICOS

Patrimônio da Instituição, composto de equipamentos computacionais (ex: processadores, monitores, laptops, modems), equipamentos de comunicação (ex: roteadores, *switchs*, *hubs*, PABX, aparelhos de fac-símile, secretárias eletrônicas), mídias removíveis (ex: fitas, discos rígidos, *pendrives*) e outros recursos tecnológicos (ex: impressoras, *nobreaks*, estabilizadores).

1.2.9 ATIVOS DA INFORMAÇÃO

Patrimônio composto de bases de dados e arquivos, documentação de sistemas, informações sobre pesquisas, manuais de usuários, material de treinamento, procedimentos de suporte e operação, planos de continuidade, procedimentos de recuperação de sistemas, trilhas de auditoria e informações armazenadas.

1.2.10 ATIVOS DE SOFTWARE

Patrimônio composto de aplicativos, sistemas operacionais, ferramentas de desenvolvimento e utilitários.

1.2.11 AUTENTICAÇÃO

Processo de verificação da identidade de um objeto ou uma pessoa.

1.2.12 AUTENTICIDADE

Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. (Instrução Normativa GSI/PR no 1, de 13 de junho de 2008).

1.2.13 CANALIZAÇÃO DE DADOS

Infraestrutura de telecomunicações utilizada para o tráfego de dados, voz e imagem.

1.2.14 CONFIDENCIALIDADE

Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada. (Fonte: Instrução Normativa GSI/PR no 1, de 13 de junho de 2008).

1.2.15 CÓDIGO FONTE

Conjunto de arquivos de texto contendo todas as instruções que devem ser executadas, expressas de forma ordenada numa linguagem de programação.

1.2.16 DATACENTERS

Local físico que armazena máquinas de computação e seus equipamentos de hardware relacionados. Contém a infraestrutura de computação que os sistemas de TI exigem,

como servidores, unidades de armazenamento de dados e equipamentos de rede.

1.2.17 DISPONIBILIDADE

Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade. (Instrução Normativa GSI/PR no 1, de 13 de junho de 2008).

1.2.18 DNS ("DOMAIN NAME SYSTEM")

Define como os nomes de domínio são encontrados e traduzidos no endereço de protocolo da internet. Um nome de domínio é um recurso fácil de ser lembrado quando referenciado como um endereço na internet.

1.2.19 DOMÍNIO

Domínio é o nome de identificação único de um site na intraer/internet, por exemplo, "*.intraer"* ou "*fab.mil.br"*. Ele é formado pelo nome e pela extensão: "*fab"* é o nome do domínio e o "*.mil.br"* é a extensão.

1.2.20 ELOS DE SERVIÇO 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.

1.2.21 ELO ESPECIALIZADO 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.

1.2.22 ELOS DE COORDENAÇÃO DO 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.

1.2.23 E-MAIL (MENSAGEM ELETRÔNICA)

Documento digital produzido ou recebido via sistema de correio eletrônico, incluindo ou não, anexos que possam ser transmitidos junto a mensagem.

1.2.24 ENDEREÇOS IP

Protocolo de *Internet* ou *Internet Protocol* (IP) que permite a comunicação entre dispositivos na rede. De forma genérica, pode ser considerado como um conjunto de caracteres que representa o local de um determinado equipamento em uma rede privada ou pública.

1.2.25 ESTAÇÕES DE TRABALHO (*WORKSTATIONS*)

Computadores direcionados a atividades profissionais que, frequentemente, demandam bastante desempenho no processamento de dados.

Indivíduo que elabora e modifica software ou hardware de computadores, seja

desenvolvendo funcionalidades novas, seja adaptando as antigas. Originário do inglês, o termo é usado em português sem modificação, referindo-se, na maioria das vezes, a programadores maliciosos que agem com o intuito de violar, de modo ilegal ou imoral sistemas de tecnologia da informação, podendo, nesses sistemas, causar danos.

1.2.26 *HIPERLINK*, PÁGINAS *WEB* E PORTAL

a) *hiperlink* é trecho que está contido um conteúdo em uma página *Web* que direciona para outra página, sítio (*site*) ou mesmo para outro local da mesma página. Esse trecho de conteúdo pode estar contido em um texto, botão ou imagem**;**

b) página *web* **qualquer documento que faça parte de um sítio *web*** e que costuma conter ligações (igualmente chamadas hiperligações ou links) para facilitar a navegação entre os conteúdos; e

c) portal é uma plataforma *web* que **agrega informações de diferentes fontes** em uma única interface e apresenta as informações mais relevantes para cada usuário de acordo com seu contexto.

1.2.27 HOMOLOGADO

Aquilo que foi desenvolvido, acompanhado e implantado por intermédio de processo ou procedimento estabelecido pelo STI e aceito pelo demandante.

1.2.28 IMPLANTAÇÃO

Significa desenvolver um plano, introduzir ou estabelecer uma novidade, iniciar algo novo.

1.2.29 IMPLEMENTAÇÃO

Significa ação de pôr em prática um plano, entrada em vigor de acordo, assegurar a realização ou executar algo.

1.2.30 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Um evento ou uma série de eventos indesejados ou inesperados que podem vir a comprometer a confidencialidade ou a integridade ou a disponibilidade de ativos físicos, de software ou de informação, todos de interesse da Instituição.

1.2.31 INFRAESTRUTURA DE TELECOMUNICAÇÕES

Instalação planejada com o objetivo de conectar, interligar e fornecer suporte a toda a rede de comunicação da maneira mais adequada para o ambiente corporativo.

1.2.32 INFRAESTRUTURA DE TI

Infraestrutura de tecnologia da informação (TI) refere-se aos componentes necessários para executar e gerenciar ambientes de TI empresarial. Esses componentes incluem *hardware*, *software* e rede, além de um sistema operacional e armazenamento de dados.

1.2.33 INTEGRIDADE

Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

1.2.34 LAN - REDE DE ÁREA LOCAL

Redes de Área Local ou *Local Área Network* (LAN), interligam computadores presentes dentro de um mesmo espaço físico. Tornando possível a troca de informações e recursos entre os dispositivos participantes. São exemplos de redes locais as redes internas das OM.

1.2.35 LOBBY

Lobby é uma forma de comunicar, debater ou de tentar convencer parlamentares ou executivos do governo (além de funcionários próximos, como assessores e secretários) a tomar uma determinada decisão para atender a interesses particulares ou gerais.

1.2.36 LOGIN

Conjunto de procedimentos que visam a permitir o acesso de um usuário a um computador, a um servidor ou a outro recurso da rede.

1.2.37 LOGOUT

Conjunto de procedimentos para desconectar um usuário de um computador, de um servidor ou de outro recurso da rede.

1.2.38 MALWARE

Termo de origem inglesa *malicius software* (*MALWARE*), cuja tradução é "software malicioso", é um tipo de programa desenvolvido para ser infiltrado ilicitamente em um computador alheio, a fim de causar dano ou permitir a obtenção de informações ou controle da outra máquina.

1.2.39 MAN - REDE DE ÁREA METROPOLITANA

Rede de Área Metropolitana ou *Metropolitan Area Network* (MAN) tem a função de realizar conexão entre diferentes redes dentro de um raio de dezenas de quilômetros. Esse tipo de rede interliga computadores e usuários de unidades de uma empresa, através de conexão pública (link de internet).

1.2.40 MENSAGEM INSTANTÂNEA

Forma de comunicação que acontece via internet, por meio de uma ferramenta (aplicativo ou software). Seu objetivo é oferecer o diálogo em tempo real entre seus usuários.

1.2.41 NAVEGADOR *WEB*

Também conhecido como *web browser* ou simplesmente *browser*, é um programa que habilita seus usuários a interagirem com documentos de linguagem de marcação de hipertexto da internet ou *HyperText Markup Language* (HTML) hospedados em um servidor *Web*.

1.2.42 ÓRGÃO CENTRAL DO STI**.**

A Portaria nº 549/GC3, de 09 de agosto de 2010, reformulou o Sistema de Tecnologia da Informação do COMAER e designou a Diretoria de Tecnologia da Informação da Aeronáutica -DTI como Órgão Central do STI.

1.2.43 PADRONIZADO

Aquilo que foi estabelecido pelo STI ou que os Centros de Computação prestam suporte ou, ainda, demandado por força de Lei.

1.2.44 PROGRAMA

É um conjunto de instruções que descrevem uma tarefa a ser realizada por um computador. O termo é uma referência ao código fonte, escrito em alguma linguagem de programação, ou ao arquivo que contém a forma executável deste código fonte.

1.2.45 PROGRAMAS REGULARES

Softwares padronizados pelo Órgão Central do STI.

1.2.46 PROGRAMAS IRREGULARES

Softwares não padronizados pelo Órgão Central do STI.

1.2.47 PROVEDORES DE ACESSO À INTRAER

O provedor de internet, ou *Internet Service Provider* (ISP), é o intermediador que faz com que a internet chegue até os dispositivos. É um serviço promovido por empresas especializadas, que oferecem internet banda larga com conexões via cabo, satélite, rádio ou fibra.

1.2.48 PLUGIN

Programa / *software*, extensão ou ferramenta que pode ser adicionada no programa principal, que incrementa recursos adicionais a ele sem comprometer o seu funcionamento.

1.2.49 PROTOCOLOS DE ACESSO REMOTO

Conjunto de regras para comunicação entre computadores que permite que usuários consigam ter acesso às suas respectivas áreas de trabalho sem que seja necessário estar fisicamente próximo a seus computadores. São exemplos de protocolos de acesso remoto: RDP (*Remote Desktop Protocol*), VNC (*Virtual Network Computing*), SSH (*Secure Shell*).

1.2.50 REDE DE LONGA DISTÂNCIA

Uma rede de longa distância ou *Wide Area Network* (WAN) é uma rede de telecomunicações privada, geograficamente distribuída que interconecta várias redes locais (LANs).

1.2.51 REDES SOCIAIS

Sites e aplicativos usados por pessoas e organizações que se conectam com clientes, familiares, amigos e pessoas que compartilham seus interesses em comum.

1.2.52 RENOVAÇÃO DO CERTIFICADO

Processo modificar a emissão e instalação do Certificado digital de pessoa física ou jurídica.

1.2.53 SERVIDOR DE REDE

Computador que oferece um serviço ou que compartilha com outros computadores em uma rede, recursos na forma de arquivos, impressoras, etc.

1.2.54 SISTEMA

É um conjunto integrado de componentes regularmente inter-relacionados e interdependentes criados para realizar um objetivo definido, com relações definidas e mantidas entre seus componentes e cuja produção e operação como um todo é melhor que a simples soma de seus componentes.

1.2.55 SISTEMA OPERACIONAL

Conjunto de programas que gerenciam recursos, processadores, armazenamento, dispositivos de entrada e saída e dados da máquina e seus periféricos.

1.2.56 SISTEMA OPERACIONAL HOMOLOGADO

Garantia de que o sistema operacional desenvolvido ou adquirido atenda aos requisitos do negócio e esteja dentro dos padrões de qualidade e desempenho desejados.

1.2.57 SISTEMA REGULARES

Sistemas que passaram pelo processo de homologação no STI.

1.2.58 SISTEMAS IRREGULARES

Sistemas que não passaram pelo processo de homologação no STI.

1.2.59 SÍTIOS DE BATE-PAPO

Espaço virtual na internet que reúne pessoas, comumente identificadas por apelidos (*nicknames*), para trocar, em tempo real, mensagens escritas sobre os mais diversos assuntos.

1.2.60 SOFTWARE

Trata-se de um serviço computacional utilizado para realizar ações nos sistemas de computadores. Ou seja: Um *software* é todo programa presente nos diversos dispositivos (computadores, celulares, televisores, entre outros).

1.2.61 SOFTWARE CLIENTE

Refere-se ao software que atua do lado do dispositivo cliente, buscando como seu destino o software do lado do servidor de rede.

1.2.62 SOLUÇÕES DE TI

Solução de TI não se define apenas como um único recurso. É, basicamente, todo o conjunto de sistemas, softwares, equipamentos, máquinas, ferramentas e quaisquer aplicações utilizadas para dar suporte aos projetos e processos do dia a dia, com o objetivo de torná-los mais eficientes e enxutos.

1.2.63 SUBDOMÍNIO

Subdomínio é um endereço que faz parte do domínio, ou seja, é uma ramificação que faz referência a uma parte de um domínio na intraer/internet. Por exemplo:

Na Intraer: Para o endereço http://www.dti.intraer. ⇒ Nesse caso o domínio é Intraer e o subdomínio é "DTI".

Na internet: Para o endereço https://ilavirtual.fab.mil.br ⇒ Nesse caso o domínio é "*fab.mil.br"* e o subdomínio é "ilavirtual".

1.2.64 TERMO DE COMPROMISSO E DE MANUTENÇÃO DE SIGILO

Documento firmado entre duas ou mais partes com o objetivo de manter determinadas informações em sigilo.

1.2.65 TRABALHO REMOTO/ TELETRABALHO

Prática dos funcionários de realizarem suas tarefas em um local que não o escritório central operado pelo empregador.

1.2.66 USUÁRIO

São pessoas que fazem uso de um determinado tipo de serviço, objeto, dispositivo ou produto.

1.2.67 VIRTUAL PRIVATE NETWORK (VPN)

Conexão de rede privada entre dispositivos através da internet. Utilizadas para transmitir dados de forma segura e anônima em redes públicas.

1.3 ÂMBITO

Esta Instrução se aplica a todas as Organizações do COMAER.

2 INTRAER

2.1 ESTRUTURA DA REDE

2.1.1 A intraer é composta pela integração das redes locais (LAN) das Organizações do COMAER, por meio de infraestrutura de telecomunicações.

2.1.2 Nas diversas localidades do Brasil, existem organizações militares (OM) do COMAER que possuem uma infraestrutura de telecomunicação denominada Rede Metropolitana (MAN) que interliga as redes locais das OM existentes no Brasil.

2.1.3 Dessa forma, todas as Redes Metropolitanas estão interligadas, em nível nacional, constituindo uma Rede de Longa Distância (WAN).

2.1.4 Os Elos de Serviço que concentram os serviços de TI de uma guarnição e os Elos Especializados são considerados provedores de acesso à intraer.

2.2 SOLUÇÕES DE TI QUE UTILIZAM RECURSOS DA INTRAER

2.2.1 A utilização e o consumo da intraer como infraestrutura de comunicação de dados para suporte ao tráfego de informações oriundas ou destinadas a sistemas ou a aplicativos, desenvolvidos ou adquiridos por iniciativa própria ou por aquisição em processo licitatório, estão sujeitos aos seguintes fatores condicionantes, conforme estabelecido no anexo "J":

a) o projeto da solução de TI deve ser submetido ao Órgão Central do STI, para análise e aprovação, com antecedência mínima de 90 dias em relação à data prevista para a sua entrada em operação;

b) o processo de implantação da solução de TI deve ser acompanhado por representantes do Órgão Central do STI;

c) a solução de TI deve ser submetida a testes de comunicação, acompanhados por representantes do Órgão Central do STI, que comprovem sua capacidade de operar nas condições técnicas disponíveis na intraer;

d) a entrada em operação do aplicativo só deverá ocorrer com autorização expressa do Órgão Central do STI;

e) a implantação de soluções de TI, cujo consumo de recursos de rede esteja limitado à rede local da OM interessada, poderá ser processada, desde que preenchidos os requisitos das letras "a", "b', "c" e "d" deste item e que a solução de TI não venha a sobrecarregar a rede da OM, prejudicando de forma acentuada o acesso a soluções de TI de interesse do COMAER que são operadas naquela OM;

f) a suspensão do suporte da intraer a uma solução de TI pode ocorrer, a qualquer tempo, em caráter temporário ou permanente, caso a solução de TI em questão passe a comprometer o desempenho da intraer e, principalmente, a adequada operacionalidade de sistemas de interesse do COMAER; e

g) a depender da complexidade do sistema e disponibilização de meios para análise de segurança cibernética (e.g. ambiente de teste), o Órgão Central do STI poderá solicitar um novo prazo para aprovação.

2.2.2 Fica vedada a instalação de sistemas ou aplicativos na infraestrutura de TI da intraer das

OM se a forma de acesso ocorrer pela internet. Caso o acesso do sistema ou aplicativo seja realizado pela internet, a OM deverá proceder conforme estabelecido no item referente a “SISTEMAS APLICATIVOS NA INTERNET" desta norma.

2.3 ACESSOS REMOTOS À REDE LOCAL DE UMA OM

2.3.1 O acesso remoto à rede local de uma OM permite o acesso a serviços como servidores de arquivos, administração de servidores, administração de ativos físicos, etc. Tais serviços não estão disponíveis para o acesso remoto à rede intraer por intermédio de VPN.

2.3.2 A solicitação de acesso remoto à rede local de uma OM deve ser aprovada pelo respectivo Elo de Coordenação do STI e pelo Órgão Central do STI, conforme anexo “G”.

2.3.3 O pedido de acesso à rede local de uma OM deve ser solicitado, exclusivamente, pela equipe técnica do Elo de Serviço para realização de manutenções e ou intervenções na infraestrutura de TI.

2.3.4 Esse pedido de acesso, também, poderá ser solicitado para as situações em que as empresas terceirizadas precisem realizar manutenções e atualizações nos ativos de TI na infraestrutura de TI da intraer, via Internet, para serviços adquiridos através de contratações. Vale destacar que as empresas contratadas devem assinar o Termo de Compromisso e de manutenção de sigilo e respeito às normas de segurança vigentes no COMAER, a ser assinado pelo representante legal da contratada, conforme orientado em normas vigentes.

2.3.5 Os Centros de Computação deverão disponibilizar serviços de acesso remoto à infraestrutura de TI da intraer através da internet, conforme determinações do Órgão Central do STI.

2.3.6 Todo acesso remoto à rede intraer deverá ser realizado pelos servidores de rede hospedados nos datacenters dos Centros de computação da FAB.

2.3.7 Os Centros de computação deverão estabelecer critérios para o acesso seguro e monitorar os acessos à rede intraer via internet.

2.3.8 O acesso remoto à rede local de uma OM, por meio da internet, deve ser feito por meio da combinação da VPN com outros protocolos, como: SSH, RDP, VNC, ETC.

2.3.9 O acesso remoto à rede local de uma OM, por meio da internet, é estritamente pessoal e intransferível, com validade de 12 meses.

2.4 ACESSO REMOTO À REDE INTRAER POR INTERMÉDIO DE VPN

2.4.1 DA APLICAÇÃO

2.4.1.1 Todo acesso remoto à rede intraer deverá ser realizado pelos servidores de rede hospedados nos datacenters dos Elos de Serviço e dos Elos Especializados do STI.

2.4.1.2 O pedido de acesso à rede intraer por intermédio da VPN deve ser solicitado pelo usuário ou Elo de serviço para o trabalho remoto a fim de acessar os sistemas homologados pelo STI disponibilizados na intraer, tais como: SIGADAER, SILOMS, Portal da OM, Página *Web* hospedadas no domínio intraer, dentre outros.

2.4.2 DA INSTALAÇÃO

2.4.2.1 Para atender aos requisitos de instalação do acesso seguro, é obrigatório que o sistema operacional da estação de trabalho esteja homologado e atualizado, bem como possua um software de antivírus em iguais condições.

2.4.3 SOLICITAÇÃO DA VPN

2.4.3.1 Esse serviço deverá ser solicitado ao Comandante/Chefe/Diretor da OM pelo chefe imediato do militar/civil, conforme anexo C.

2.4.3.2 As solicitações de acessos à VPN aprovadas deverão ser encaminhadas pela OM ao Elo Especializado, via SAU.

2.4.3.3 O Chamado do SAU deverá conter uma cópia do Termo de Responsabilidade devidamente preenchido e assinado.

2.4.3.4 Elo Especializado deverá manter atualizada a lista de usuários das OM cujos os acessos à VPN estejam sob sua responsabilidade.

2.4.3.5 O Termo de Responsabilidade poderá ser assinado digitalmente ou fisicamente, sendo mandatório o mesmo padrão de assinatura por todos no documento, inclusive pela autoridade responsável pela solicitação.

2.4.3.6 Os arquivos do sistema de acesso seguro serão enviados via e-mail corporativo FAB "fab.mil.br" ao usuário e a senha para acesso será enviada via e-mail pessoal cadastrado no Portal do Militar (Portal de Pessoal/Dados pessoais/cadastro/contatos/Endereço Eletrônico).

2.4.3.7 Nos casos de civis sem vínculo com o COMAER, o Comandante/Chefe/Diretor da OM deverá solicitar, via ofício, ao Elo Especializado do STI, que lhe presta apoio de TI, com o anexo C devidamente preenchido e assinado.

2.4.4 ACESSO SEGURO

2.4.4.1 O acesso seguro à intraer, por meio da internet, é estritamente pessoal e intransferível, com validade de 12 meses.

2.4.4.2 As solicitações de novos acessos serão realizadas conforme disposto no item 2.4.3

2.4.4.3 A autenticação para utilização do acesso seguro deverá utilizar as credenciais do Login Único.

2.4.4.4 A interrupção do acesso seguro poderá ocorrer a qualquer tempo por motivo de segurança ou por expiração do acesso.

2.4.4.5 As renovações dos acessos VPN serão processadas de forma automatizada, pelo Elo Especializado responsável, desde que o usuário conste na lista atualizada de sua OM.

2.4.4.6 As OM interessadas em manter os acessos à VPN deverão encaminhar anualmente ao Órgão Central do STI, via Ofício, sua lista atualizada dos usuários autorizados a ter seu acesso renovado.

2.4.4.7 A renovação do certificado para o acesso seguro será enviada para o e-mail corporativo FAB "fab.mil.br" do usuário com as seguintes informações:

a) expiração do acesso;

b) novo prazo de validade para a renovação do acesso;

c) portal de acesso para o download dos arquivos e tutoriais necessários para acesso à VPN.

d) código de acesso para download dos arquivos (enviado para o e-mail particular cadastrado no Portal do Militar); e

e) orientações para o processo de instalação e utilização do acesso VPN.

2.4.4.8 Por medida de segurança e com o intuito de conter possível ataque cibernético, os acessos seguros que permanecerem inativos por 60 (sessenta) dias consecutivos poderão ter o fornecimento do serviço interrompido pelos Elos Especializados.

2.4.4.9 O acesso seguro é realizado com autenticação de senha, mediante utilização de cliente VPN específico instalado na estação de trabalho de cada usuário.

2.4.4.10 É terminantemente proibido aos usuários a alteração do código-fonte do cliente VPN.

2.4.4.11 Também é terminantemente proibido, por razões de segurança da intraer, acessar a intraer e a internet simultaneamente nos equipamentos cujo Cliente VPN foi configurado, sob pena de sanções administrativas e legais.

2.5 COMPARTILHAMENTO DE RECURSOS DA INTRAER COM OUTRAS REDES

2.5.1 O compartilhamento de recursos (servidores de rede, estações de trabalho, ativos de TI, etc.) utilizados na intraer com a internet ou outras redes só poderá ocorrer com autorização expressa do Órgão Central do STI.

2.5.2 A solicitação para compartilhamento desses recursos deverá ser encaminhada pela OM interessada ao Órgão Central do STI, via seu Elo de Coordenação do STI, com antecedência mínima de 180 dias.

2.5.3 A solicitação de compartilhamento de recursos da intraer com outras redes deverá seguir o modelo/desenho conforme estabelecido no anexo "I".

2.6 ENDEREÇOS IP E DNS

2.6.1 A atribuição e controle dos endereços IP é de responsabilidade do Centro de Gerenciamento Técnico do Sistema de Controle do Espaço Aéreo Brasileiro - CGTEC, conforme estabelecido na ICA 66-32 "Núcleo de Gerenciamento Técnico do SISCEAB - NUCGTEC".

2.6.2 A atribuição e o controle dos registros de DNS é de responsabilidade do Órgão Central do STI.

2.6.3 O padrão de nome de domínio a ser utilizado pela Organização é a sequência de letras minúsculas e algarismos correspondentes à sigla da OM, sem qualquer sinal gráfico (hífen, travessão, barra, espaço, sinais de pontuação, acentos gráficos, etc.), seguidos da expressão "intraer", como, por exemplo:

a) bagl.intraer;

b) comar1.intraer;

c) pamals.intraer; e

d) srpvmn.intraer.

2.6.4 As estruturas sistémicas do COMAER utilizarão o padrão de domínio letras minúsculas correspondestes à sigla do Sistema, sem qualquer sinal gráfico (hífen, travessão, barra, espaço, sinais de pontuação, acentos gráficos, etc.), seguidos da expressão "intraer", como, por exemplo:

a) sti.intraer.

2.7 ACESSO AO DOMÍNIO INTRAER

2.7.1 Todo usuário da intraer no COMAER deverá assinar um Termo de Responsabilidade e de conhecimento da Política de Segurança da Informação do COMAER e das políticas de segurança da informação definidas pelas respectivas Organizações conforme estabelecido no anexo “B”.

2.7.2 O acesso ao domínio será exclusivamente realizado por ativos de TI pertencentes ao patrimônio do COMAER. Esses equipamentos devem ser configurados pelos Elos de serviço ou especializado do STI, devendo ser inseridos no subdomínio “OM” do domínio “intraer”.

2.7.3 As contas de acesso à rede estão vinculadas à infraestrutura de TI da OM apoiadora em que o usuário está lotado. Cada conta de acesso à rede corresponde a uma única conta de autenticação na rede intraer.

2.7.4 A conta de acesso à rede protege o acesso a qualquer dado que tramite pela intraer. Essa conta deve ser criada logo que o usuário se apresenta na OM e deve ser excluída no momento de seu desligamento.

2.7.5 A conta de acesso à rede é acessada por login e senha, com validade de 2 anos, e somente poderá ser utilizada pelo usuário cadastrado. A senha é pessoal e intransferível não cabendo, em qualquer hipótese, a alegação de uso indevido após ato de compartilhamento. Ficam vedados os acessos múltiplos simultâneos, como também os funcionais que não identifiquem o usuário.

2.7.6 Para a intraer, a formação da conta de acesso à rede deve ser uma sequência de letras minúsculas que identifique o nome-de-guerra e as iniciais do nome completo do militar (no caso de civis, o nome pelo qual é conhecido o funcionário), por exemplo:

a) Maj. Av. Marco Aurélio da SILVA ⇒ silvamas.

2.7.7 Para os casos em que o usuário possua o mesmo nome de guerra e as iniciais para formação de sua conta, deve se proceder da seguinte maneira:

a) 1° Ten Av. Marco Aurélio da SILVA ⇒ silvamas.

b) Maj Av Maurício Albuquerque de SILVA⇒ silvamas1

2.7.8 Deve ser adicionado um numeral em sequência no final das iniciais da conta, levando em prioridade o momento da confecção, no caso a conta do Major foi confeccionada posteriormente à conta do Tenente.

3 INTERNET

3.1 ACESSO FUNCIONAL DAS OM DO COMAER À INTERNET

3.1.1 As organizações do COMAER deverão acessar à internet por meio dos acessos regionais autorizados pelo Órgão Central do STI.

3.1.2 Eventualmente, o Órgão Central do STI poderá autorizar a implantação, em caráter provisório, de acessos à internet em OM do COMAER, distintos dos acessos regionais, podendo a OM solicitante contratar serviço comercial de provedor da localidade, desde que instale em sua rede local os equipamentos de segurança estabelecidos pelo STI para a conexão com a internet. Se os equipamentos de segurança forem adquiridos pela própria OM, as especificações, as configurações, as conexões e a montagem devem ser aprovadas pelo Órgão Central do STI, antes de se tornar operacional a conexão com a internet.

3.1.3 O acesso à internet de caráter provisório será concedido nos casos de exercício ou operação militar conforme estabelecido no MCA 400-24 - Manual da Unidade Celular de Tecnologia da Informação - UCTI.

3.1.4 A solicitação de autorização para implantação, em OM do COMAER, de acessos provisórios à internet deverá ser feita pela Organização interessada ao seu respectivo Elo de Coordenação do STI que, caso seja de parecer favorável à implantação do acesso, a submeterá ao Órgão Central do STI, conforme estabelecido no anexo “H”.

3.1.5 Os recursos para manutenção do acesso provisório e para os equipamentos utilizados na solução de segurança implementada são de responsabilidade da OM onde será implantado o ponto de acesso àquela rede.

3.1.6 Todo acesso à internet deve ser utilizado pelo usuário cadastrado via login e senha. A senha é pessoal e intransferível, não cabendo, em qualquer hipótese, a alegação de uso indevido após ato de compartilhamento. Fica vedado os acessos múltiplos, como também os funcionais que não identifiquem os usuários.

3.1.7 O usuário para possuir o acesso à internet, com validade de 2 anos, deverá solicitar através do Sistema de Atendimento ao Usuário (SAU), mediante assinatura de termo de responsabilidade, conforme estabelecido no anexo “A”.

3.1.8 Todo usuário da internet no COMAER deverá assinar um Termo de Responsabilidade e de conhecimento da Política de Segurança da Informação do COMAER e das políticas de segurança da informação definidas pelas respectivas Organizações.

3.1.9 Todo o tráfego de dados com acesso à internet deve ser protegido por ferramentas contra *malware*.

3.1.10 O Órgão Central do STI é responsável pela padronização e fornecimento do software de antivírus corporativo.

3.1.11 As OM poderão adquirir *software* de antivírus distintos do padronizado, desde que autorizado pelo respectivo Elo de Coordenação do STI e pelo Órgão Central do STI, e com os recursos previstos no planejamento financeiro da respectiva OM e que seja integrado aos sistemas de monitoramento de vulnerabilidades padronizado no COMAER e gerenciado pelo Centro de Tratamento de Incidentes de Redes da Força Aérea Brasileira (CTIR.FAB)

3.1.12 A utilização do acesso à internet está restrita ao atendimento das necessidades de serviço da Organização do COMAER.

3.1.13 As Organizações do COMAER detentoras de acessos provisórios à internet deverão monitorar o seu uso pelo pessoal devidamente autorizado, mediante credencial de segurança (ICA 200-13), e habilitado, providenciando para que sejam corrigidas as discrepâncias observadas.

3.1.14 O monitoramento do acesso provisório à internet deverá também ser realizado pelos Elos Especializados, sendo responsabilidade da OM disponibilizar acesso à solução de segurança.

3.2 SOLUÇÕES DE TI NA INTERNET

3.2.1 A entrada em operação de soluções de TI, cujo acesso será feito a partir da internet, só poderá ser efetivada quando autorizada por meio de documento oficial emitido pelo Órgão Central do STI.

3.2.2 A solicitação de autorização para entrada em operação de soluções de TI disponibilizados na internet deverá ser feita pela Organização interessada ao seu respectivo Elo de Coordenação do STI que, caso seja de parecer favorável à entrada em operação do sistema, a submeterá ao Órgão Central do STI, para avaliação quanto ao nível de segurança da informação e quanto às necessidades de canalização de dados. conforme estabelecido no anexo “D”.

3.2.3 As soluções de TI disponibilizadas na internet deverão ser, obrigatoriamente, hospedados nos equipamentos servidores de rede dos Centros de Computação da Aeronáutica.

3.2.4 A realização de ajustes, determinados pelo Órgão Central do STI, nas soluções de TI disponibilizadas na internet, será de responsabilidade da OM interessada, mediante acompanhamento e coordenação dos Elos Especializados regionais.

3.3 ACESSOS NÃO FUNCIONAIS À INTERNET

3.3.1 CONCENTRAÇÃO REGIONAL DE TI

3.3.1.1 Com a reestruturação do COMAER houve necessidade de criação e desativação de OM, nesse sentido, houve a exclusão de alguns Grupamentos de Apoio - GAP e as suas infraestruturas de TI passaram a ser responsabilidades das novas OM. Dessa forma, a concentração de serviços de TI nos GAP conforme preconizado no Força Aérea 100 foi modificada e, atualmente, existem concentração de serviços em GAP/Bases/OM de Ensino.

3.3.1.2 Com a implementação da Concentração dos Serviços de Tecnologia da Informação, conforme previsto no MCA 11-2, enlaces de comunicação de alta velocidade foram concentrados em algumas OM para acesso à internet, os quais foram providos com ferramentas de proteção de perímetro com capacidade de mitigar riscos associados à Segurança Cibernética, de modo a atender às regulamentações em vigor.

3.3.1.3 No processo de concentração de TI, identificou-se a necessidade de padronizar os acessos NÃO funcionais das Organizações Militares do COMAER, com vistas a também adequá-los às legislações de TI vigentes no âmbito do Governo Federal, tais como o armazenamento de registros de acesso previstos pelo § 1°, 5° e 6° do Art. 13 da Lei nº 12.965 de 22 de abril de 2014 (Marco Civil da Internet), transcrito no item a seguir.

3.3.2 SITUAÇÕES AUTORIZADAS PARA ACESSO

3.3.2.1 Os procedimentos gerais para o acesso não funcional à internet provido por Organização Militar do COMAER devem ser aplicáveis as seguintes situações:

a) acesso à internet provido por Hotéis de Trânsito (cabeado ou Wi-Fi);

b) acesso Wi-Fi à internet em Elo de Serviço do STI;

c) acesso Wi-Fi à internet em Exercício ou Operação; e

d) qualquer tipo de ponto de acesso contratado e mantido por Organização da Aeronáutica.

3.3.3 IMPLANTAÇÃO E USO DE REDE SEM FIO (*WIRELESS*)

3.3.3.1 As regras e procedimentos para instalação de utilização para rede sem fio no COMAER serão tratados em norma específica.

4 INTERNET E INTRAER

4.1 MENSAGEM ELETRÔNICA

4.1.1 A mensagem eletrônica é um serviço de comunicação interna do COMAER, viabilizando as mensagens do tipo "*e-mail*". Este serviço pode ser acessado tanto pela intraer (https://mail.intraer/) quanto pela internet (https://mail.fab.mil.br/).

4.1.2 Para o funcionamento do serviço de mensagem eletrônica do COMAER (FABMail), devem ser observadas as orientações dispostas na ICA 7-51.

4.2 PUBLICAÇÕES DE PÁGINAS *WEB*

4.2.1 CONTEÚDO

4.2.1.1 O conteúdo das páginas *Web* publicadas na internet/intraer são de responsabilidade do Comandante da OM. Deve ser observado que alguns assuntos, por motivos evidentes, não devem ser divulgados nessas páginas, como por exemplo:

a) planos ou Ordens referentes a operações militares;

b) referências que facilitem a obtenção de informações classificadas; e

c) informações de cunho pessoal sobre os militares e seus familiares.

4.2.1.2 Para a divulgação de informações em páginas *web* deve ser observado também o disposto no item 3.4.6 da RCA 205-47 “Regulamento para Salvaguarda de assuntos Sigilosos da Aeronáutica”, de 7 de março de 2006.

4.2.2 PADRÕES

4.2.2.1 Além dos padrões já estabelecidos em legislação interna do COMAER, as páginas do COMAER na internet/intraer devem atender também aos Padrões Brasil e-Gov.

4.3 PÁGINAS WEB

4.3.1 A página confeccionada será um *template* padronizado já existente e a OM irá editar e preencher com as respectivas informações.

4.3.2 Cabe às OM capacitarem o seu corpo técnico e administrativo na utilização da ferramenta implementada para criação da sua página WEB.

4.3.3 PÁGINAS NA INTRAER

a) confecção: as OM da FAB solicitarão ao Elo de Serviço do STI a criação da página, via SAU.

b) registro do domínio: as OM da FAB solicitarão ao órgão central do STI, via Ofício.

c) publicação: a publicação será realizada pelo Elo de Serviço do STI em coordenação com a OM solicitante.

4.3.4 PÁGINAS NA INTERNET

4.3.4.1 As Organizações do COMAER deverão utilizar subdomínios do domínio fab.mil.br para publicar suas páginas *web* na internet.

4.3.4.2 Na eventualidade de surgirem condições especiais que requeiram o registro de domínios na internet, fora do domínio fab.mil.br, estes só poderão ser efetivados quando autorizados, por meio de documento oficial emitido ao Órgão Central do STI, conforme estabelecido no anexo "E". Uma vez autorizados, o Órgão Central do STI efetuará o registro do domínio junto ao registro.br.

4.3.4.3 No que diz respeito à avaliação e necessidades da canalização de internet, sempre que necessário, o Órgão Central do STI consultará o DECEA e solicitará o atendimento às demandas identificadas.

4.3.4.4 As páginas publicadas pelas Organizações do COMAER na internet deverão ser, obrigatoriamente, hospedadas nos equipamentos servidores de rede dos Elos Especializados do STI.

4.3.4.5 Recomenda-se que o acesso às páginas *web* das Organizações do COMAER, publicadas na internet seja realizado, a partir da página portal do COMAER na internet (portal único do COMAER - https://www.fab.mil.br/organizacoes).

4.3.4.6 O processo de criação de páginas *web* deve atender aos padrões de uniformidade definidos pelo CECOMSAER, para isso as solicitações devem seguir as orientações estabelecidas no anexo "E".

a) confecção: As OM da FAB solicitarão ao seu Elo de Coordenação do STI a criação da página. Após a aprovação destas pelo Elo de Coordenação do STI serão criadas pelo CCA-BR, mediante abertura de chamado SAU;

b) registro do domínio: O Elo de Coordenação do STI solicitará o registro do domínio ao Órgão Central do STI, via Ofício; e

c) publicação: Após aprovação do CECOMSAER, o Elo de Coordenação do STI solicitará a publicação da página ao CCA-BR, via SAU.

4.4 MÍDIAS SOCIAIS

4.4.1 A solicitação de autorização para publicação de perfis de mídia social corporativa deverá ser feita pela OM interessada ao seu respectivo Elo de Coordenação do STI.

4.4.2 O Elo de coordenação do STI submeterá as solicitações aprovadas ao Órgão Central do STI, para avaliação quanto ao nível de segurança da informação, bem como ao CECOMSAER para a avaliação da identidade digital, recomendada pelo Governo Federal.

4.4.3 O conteúdo exposto nessas mídias é de inteira responsabilidade do Comandante/Chefe/Diretor da Organização Militar (OM).

4.5 MENSAGEM INSTANTÂNEA

4.5.1 A solicitação de uso de serviços de mensagem instantânea, de sítios de bate-papo e de serviços associados às redes sociais é um procedimento que requer a devida autorização e definição de responsabilidades.

4.5.2 Esse serviço deverá ser solicitado ao Comandante/Chefe/Diretor da OM pelo chefe imediato do militar, conforme estabelecido no anexo “A”.

4.5.3 As solicitações de uso de serviços de mensagem instantânea aprovadas deverão ser encaminhadas ao Elo de Serviço do STI apoiador.

4.5.4 O Órgão Central do STI solicitará a coordenação dos Centros de Computação da Aeronáutica junto ao Elo de Serviço local para alinhar a execução das configurações necessárias na infraestrutura de TI no intuito de conceder o acesso.

4.5.5 Cabe ao Elo de Serviço realizar as configurações de acesso conforme orientações dos Centros de Computação.

5 RESTRIÇÕES RELATIVAS À SEGURANÇA DAS INFORMAÇÕES

5.1 É expressamente proibida a utilização dos recursos da intraer/internet nas seguintes situações:

a) atividades ilegais, fraudulentas e/ou maliciosas; político-partidárias; lobby ou proselitismo político ou religioso; propaganda de empresas ou instituições sem relação direta com a missão do COMAER; incitação à prática de crime ou de transgressão disciplinar;

b) causar prejuízos morais ou financeiros a terceiros;

c) explorar vulnerabilidades de outros sítios da internet, promovendo ataques do tipo daqueles realizados por hackers;

d) expressar discriminação, preconceito ou apologia ao vício ou ao emprego ou utilização de ações, procedimentos ou práticas consideradas ilegais ou contrários à moral e aos bons costumes;

e) realizar procedimentos que se configurem como crimes, tais como pirataria, pedofilia, assédio, difamação ou outros quaisquer que contrariem as leis em vigor ou a moral e os bons costumes;

f) provocar danos à imagem do COMAER e das demais instituições governamentais;

g) prejudicar a realização de atividades de interesse do COMAER;

h) atividades com o propósito de ganho pessoal ou comercial;

i) uso de recursos computacionais com o propósito de acessar ou divulgar informação inapropriada, ofensiva ou contrária aos bons costumes;

j) armazenamento ou processamento de informação classificada, sem a devida autorização;

k) obtenção, armazenamento, instalação e utilização de programas, sem o devido licenciamento junto à Empresa ou Instituição detentora legal dos seus direitos de uso;

l) liberação do acesso, por parte de indivíduos não expressamente autorizados, de recursos disponíveis na intraer, sejam estes recursos equipamentos, serviços de rede ou programas que foram licenciados para o COMAER;

m) atividades visando a modificação ou a substituição de programas padronizados pelo Órgão Central do STI para emprego nos servidores de rede ou nas estações de trabalho da intraer;

n) atividades visando a modificação ou a substituição de programas aplicativos homologados e padronizados pelos Elos de Coordenação do STI, na sua área de responsabilidade, para emprego nos servidores de rede ou nas estações de trabalho da intraer;

o) atividades visando divulgar identidade dos usuários e senhas ou, de outro modo, permitir ou capacitar qualquer indivíduo não autorizado para acessar um sistema de TI do COMAER;

p) uso não autorizado de identificação ou senha individual;

q) atividades que permitam visualizar, modificar ou remover arquivos ou qualquer outro tipo de informação de propriedade de usuários da rede, sem a devida autorização;

r) emprego de ferramentas que realizem análises nas redes locais (*LAN*), visando obter informações sobre os servidores de rede, as estações de trabalho clientes e os demais recursos das redes, exceto quando devidamente justificado e expressamente autorizado pelo Cmt/Chefe/Dir da OM, sob a supervisão do chefe do Elo de serviço que apoia a OM; e

s) emprego as redes metropolitanas e de longa distância, visando obter informações sobre os servidores de rede, as estações de trabalho clientes e os demais recursos das redes, exceto quando devidamente justificado e expressamente autorizado pelo Órgão Central do STI, via cadeia de comando, conforme estabelecido no anexo “F”.

6 CONDIÇÕES GERAIS

6.1 Os usuários da intraer devem estar cientes de que os computadores do COMAER, os seus sistemas de informação e as suas redes estão sujeitos ao monitoramento, a qualquer tempo, e que o uso dos seus recursos não requer consentimento para este monitoramento.

6.2 Os sistemas de informação e os dados que neles existem são bens do COMAER e devem ser protegidos contra a divulgação indevida e contra a perda de integridade, de disponibilidade e de confidencialidade.

6.3 Em particular, devem ser adotados adequadamente todos os procedimentos estabelecidos pelo Órgão Central do STI, quando necessário, devem ser adotadas medidas complementares, específicas de cada interessado, além daquelas preconizadas para uso geral ou recomendadas.

6.4 Em todos os níveis da rede, devem ser implementados os meios adequados de autenticação de usuários e de registro de suas atividades, de modo a possibilitar o conhecimento e a verificação de todas as ações realizadas. A autenticação e o registro são obrigatórios para qualquer que seja a modalidade de inicialização do sistema ou de acesso.

6.5 Vale destacar que a senha para qualquer acesso (intraer/internet) é pessoal e intransferível, não cabendo, em qualquer hipótese, a alegação de uso indevido após ato de compartilhamento. Fica vedado os acessos múltiplos, como também os funcionais que não identifiquem os usuários.

7 COMPETÊNCIAS

7.1 DO ÓRGÃO CENTRAL DO STI

a) a supervisão técnica e operacional da intraer;

b) o estabelecimento de normas para administração e uso da intraer, inclusive para o planejamento, a aquisição, a manutenção, a utilização, a padronização, o controle de acesso, a segurança, o gerenciamento da rede e o treinamento dos operadores e dos usuários da intraer;

c) avaliar, quanto ao nível de segurança das informações e quanto às necessidades de canalização de dados, as solicitações, encaminhadas pelos Elos de Coordenação do STI, relativas ao uso da internet pelas OM do COMAER, que tratam da instalação de acessos provisórios, da publicação de páginas, da disponibilização de sistemas ou aplicativos e do acesso a sistemas de TI da intraer;

d) autorizar a entrada em operação de soluções de TI disponibilizados na internet por OM do COMAER;

e) autorizar o acesso a sistemas de TI da intraer a partir da internet;

f) dotar os Centros de Computação da Aeronáutica da infraestrutura de rede (equipamentos, programas e canalização de dados) necessária, bem como de níveis adequados de capacitação de pessoal, adequados ao funcionamento dos seus acessos à intraer/internet; e

g) gerenciar o registro de domínios e subdomínios da intraer/internet para atender às Organizações do COMAER.

7.2 DOS ELOS DE COORDENAÇÃO DO STI

a) analisar as solicitações encaminhadas pelas OM do COMAER, no contexto sob sua área de responsabilidade funcional, relativas ao uso da internet, quando tratar de instalação de acessos provisórios, da publicação de páginas, da disponibilização de soluções de TI, do acesso a sistemas de TI da intraer e aquisição de softwares antivírus distintos do padronizado pelo Órgão Central do STI;

b) encaminhar as solicitações analisadas e consideradas adequadas ao Órgão Central do STI; e

c) fiscalizar, periodicamente, as páginas *web* já publicadas e aprovadas.

7.3 DO ELO ESPECIALIZADO DO STI EM SEGURANÇA DA INFORMAÇÃO

a) Compete a esse Elo, em coordenação com o Órgão Central do STI, orientar e controlar a utilização dos procedimentos de segurança da intraer;

b) assessorar o Órgão Central do STI na avaliação de soluções técnicas de criptografia utilizadas para garantir a segurança das comunicações em acessos à internet; e

c) produzir e disseminar conhecimentos acerca de incidentes de segurança da informação resolvidos e em andamento, objetivando prevenir ocorrências futuras.

7.4 DOS DEMAIS ELOS ESPECIALIZADOS DO STI

a) operar os acessos à internet sob sua responsabilidade garantindo os níveis de segurança da informação estabelecidos pelo Órgão Central do STI, bem como a disponibilidade dos acessos para atender às páginas *web* e aos sistemas aplicativos hospedados;

b) prover o CECOMSAER do apoio técnico necessário ao trato das suas competências referentes ao emprego da internet;

c) gerar relatórios estatísticos relativos à utilização do acesso à internet sob sua responsabilidade, por solicitação das Organizações do COMAER usuárias do acesso;

d) apoiar os Elos de Serviço na resolução de incidentes de segurança da informação;

e) cooperarem com o Órgão Central do STI na operação e no controle de utilização da intraer e, ainda, apoiar o funcionamento das redes locais das OM;

f) configurar os servidores necessários aos acessos seguros cujo atendimento técnico for a eles atribuído pelo Órgão Central do STI;

g) manter, por no mínimo 5 (cinco) anos, os registros dos acessos seguros distribuídos, para fins arquivísticos e legais, mantendo informações sobre a quantidade de acessos fornecidos por OM, os dados de identificação dos usuários que receberam os acessos, a data de início da disponibilização do acesso e há quanto tempo os acessos estão inativos;

h) deve possuir, para fins arquivísticos e legais, controle dos Termos de Responsabilidade, conforme estabelecido no anexo "A", dos usuários que utilizam o acesso seguro por ele fornecido, por igual período; e

i) prestar suporte técnico ao Elo de Serviço da OM, caso este não consiga solucionar a requisição ou o incidente reportado pelo usuário.

7.5 DO ELO DE SERVIÇO DO STI

a) prestar suporte técnico ao usuário, mediante abertura de chamado através do SAU;

b) cuidar para o contínuo funcionamento da rede local, por meio de inspeções periódicas;

c) supervisionar diariamente as operações da intraer/internet;

d) cuidar da segurança local e cooperar com a segurança geral dos sistemas, instalações, equipamentos e redes que compõem a intraer;

e) implementar, executar e controlar os procedimentos de segurança, incluindo a realização de cópias e a guarda adequada dos meios de recuperação dos sistemas;

f) preservar a confidencialidade das informações disponíveis na rede local;

g) controlar a concessão e a utilização de senhas, autenticações, contas, acessos e afins de interesse local para uso da intraer/internet;

h) providenciar para que o Comandante, Diretor ou Chefe da OM tome pronto conhecimento das irregularidades que observar no funcionamento da intraer/internet;

i) controlar o acesso físico às instalações e aos equipamentos da intraer de sua responsabilidade;

j) instalar somente programas e arquivos que tenham sido verificados previamente, quanto à existência de softwares maliciosos;

k) inspecionar para que o equipamento não contenha softwares com licenças falsas e/ou programas que possam apresentar risco à rede intraer, principalmente vírus, *worms, adware, spyware, ransomware, bot, rootkits*, cavalos de tróia e *bugs* conhecidos no código de software que possam comprometer a segurança da intraer;

l) cancelar os acessos aos sistemas de TI nos casos: transferência de OM ou reserva;

m) realizar abertura do chamado SAU sobre qualquer situação que enseje a perda ou a alteração da concessão para o uso do acesso seguro, conforme descrito nesta norma;

n) registrar a ocorrência de incidentes de segurança da informação, mediante SAU;

o) a instalação do acesso VPN;

p) a instalação de programas obtidos da internet é de responsabilidade da própria Organização, devendo respeitar as condições de licenciamento e suporte técnico a que o programa está submetido;

q) configurar os perfis de acesso definidos e controlar a manutenção dos requisitos para acesso às redes; e

r) deve possuir, para fins arquivísticos e legais, controle dos Termos de Responsabilidade físicos assinados, anexos "A" e "B", dos usuários que utilizam o acesso intraer e internet por ele fornecido, por igual período.

7.6 DO CECOMSAER

a) elaborar e manter atualizado o Portal da Força Aérea na internet;

b) padronizar as informações de Comunicação Social da Aeronáutica divulgadas pela internet;

c) fazer a triagem, selecionar e encaminhar às OM detentoras da informação solicitada as correspondências eletrônicas recebidas pela internet e endereçadas ao Comando da Aeronáutica;

d) responder as correspondências eletrônicas endereçadas ao Comandante da Aeronáutica;

e) analisar o conteúdo das propostas de páginas para a internet apresentadas pelas OM do COMAER;

f) as páginas para a internet no COMAER serão consideradas propriedades digitais, devendo ser observado o disposto no Instrução

g) Normativa SECOM-PR n° 8 de 19 de dezembro de 2014, com relação à

adequação à identidade padrão de comunicação digital;

h) as páginas para a internet no COMAER necessitam observar o Manual de operação do Portal único da Força Aérea Brasileira; e

i) estabelecer conexão ("*hiperlinks*") entre o Portal da Força Aérea e as páginas *web* cujas propostas tenham sido aprovadas pelo CECOMSAER.

7.7 DOS COMANDANTES, CHEFES OU DIRETORES DE OM

a) viabilizar o uso adequado das redes de dados no âmbito da OM;

b) solicitar a criação das páginas *web* de sua OM;

c) cooperar com o STI com a manutenção e controle do funcionamento das redes de dados, disponibilizando equipe técnica para auxílio e atendimento quando lhe for solicitado - subordinação sistêmica;

d) implementar as medidas complementares de segurança física e lógica e as demais que forem necessárias para o adequado funcionamento da rede local e dos datacenters (principais concentradores da intraer/internet);

e) promover a capacitação de técnicos e de usuários de sistemas e soluções de TI do efetivo de sua OM;

f) incluir na ficha de desimpedimento, um campo para certificação, pelo setor de Tecnologia da Informação, da efetivação de cancelamento, de remoção ou de encerramento de acessos, senhas, autorizações de acessos e afins, pertinentes ao pessoal movimentado da OM;

g) impedir a instalação de programas ou de sistemas irregulares em computadores da Organização;

h) comunicar ao seu Elo de Coordenação do STI as irregularidades e/ou as sugestões relativas ao funcionamento da intraer/internet;

i) assegurar que os equipamentos de TI da OM não contenham *softwares* com licenças falsas e/ou programas que possam apresentar risco à rede intraer, principalmente *malwares* e bugs conhecidos no código de software que possam comprometer a segurança;

j) autorizar a liberação do acesso seguro para o usuário, conforme estabelecido no anexo "C";

k) providenciar que o Elo de Serviço local realize abertura de chamado SAU para o cancelamento do acesso (acesso seguro por VPN, acesso remoto, acesso ao domínio intraer) nos casos: mudança de função, transferência, missão, entre outros;

l) informar prontamente via chamado SAU, qualquer situação que enseje a perda ou a alteração da concessão para o uso do acesso seguro, conforme descrito nesta norma; e

m) concessão do acesso ao serviço de rede, cabendo ao responsável pela rede de TI local controlar a utilização delas.

7.8 DOS USUÁRIOS

a) manter sigilo e utilizar adequadamente senhas, autenticações, acessos, equipamentos, arquivos, programas e afins, para que não haja comprometimento nem da segurança, nem do funcionamento da intraer/ internet;

b) utilizar somente programas regularizados e de uso autorizado na intraer;

c) realizar criteriosamente os procedimentos lógicos de login (conexão) e de logout (desconexão) da sua rede local;

d) responder pela utilização das estações de trabalho, programas e arquivos sob sua responsabilidade;

e) cuidar da armazenagem apropriada das cópias de mensagens que devam ser preservadas;

f) relatar qualquer irregularidade observada durante o uso da intraer/internet, a seu superior ou ao Administrador ou ao Gerente da rede local;

g) verificar a autenticidade das mensagens de correio eletrônico sempre que julgar conveniente, na dúvida consulta o Elo de serviço do STI;

h) para os casos de furto, roubo, extravio dos equipamentos com acesso seguro - VPN implica imediata notificação através do SAU;

i) realizar abertura de chamado SAU para o fornecimento dos acessos aos sistemas de TI; e

j) realizar a boa utilização de programas instalados nas máquinas funcionais da Organização. Havendo necessidade de programas adicionais, o usuário deverá acionar a Elo de serviço local, via SAU.

8 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

8.1 Os incidentes de segurança da informação devem ser reportados tão logo sejam observados pelo Elo do STI ao Sistema de Atendimento ao Usuário (SAU), ou ao STI (**DTI** - Diretoria de Tecnologia da Informação da Aeronáutica/**CTIR** - Centro de Tratamento de Incidentes de Rede.

8.2 O Elo que reportar o incidente deverá preservar, tanto quanto possível, as evidências do incidente observado, conforme orientações a serem dadas pelo Órgão Central do STI, visando a possibilitar procedimentos específicos de análise ligados ao fato, a fim de garantir a legitimidade do procedimento e das evidências coletadas.

8.3 O atendimento aos incidentes de segurança da informação caberá a um dos Elos Especializados, conforme orientações do Órgão Central do STI, o qual coordenará, operacionalmente, a estrutura do CTIR.FAB.

8.4 O Órgão Central do STI elaborará e manterá atualizadas as regulamentações específicas, estabelecendo os processos de atendimento aos incidentes de segurança da informação e de prática forense computacional, em auxílio à coleta de evidências no âmbito do STI.

8.5 O Órgão Central do STI produzirá e divulgará conhecimentos baseados 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.

9 DISPOSIÇÕES GERAIS

A Norma de Sistema que tem por finalidade orientar a reestruturação da infraestrutura de provimento de acesso à intraer/internet para as Organizações Militares do Comando da Aeronáutica.

10 DISPOSIÇÕES FINAIS

Esta publicação substitui as ICA 7-5, NSCA 7-1, NSCA 7-15 e OTCA 009/DTI/2019.

Os casos não previstos serão submetidos à apreciação do Diretor de Tecnologia da Informação da Aeronáutica.

REFERÊNCIAS

BRASIL. Presidência da República. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 de agosto de 2018.

BRASIL. Presidência da República. Lei n° 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 de abril de 2014.

BRASIL. Conselho de Defesa Nacional. Portaria nº 22, de 15 de julho de 2014. Homologa a Revisão 01 da Norma Complementar nº 07/IN01/DSIC/GSIPR. Diário Oficial da União: seção 1, Brasília, DF, 16 de julho de 2014.

BRASIL. Ministério da Defesa. Portaria Normativa n° 4.034 GM/MD, de 01 de outubro de 2021. Aprova o manual de abreviaturas, siglas, símbolos e convenções cartográficas das Forças Armadas – MD33-M-02. Manual de abreviaturas, siglas, símbolos e convenções cartográficas das Forças Armadas. 4.ed. Brasília, DF, 2021.

BRASIL. Comando da Aeronáutica. Portaria n° 549/GC3, de 09 de agosto de 2010. Reformular o Sistema de Tecnologia da Informação do Comando da Aeronáutica (STI), com finalidade de organizar, disciplinar e controlar as atividades de Tecnologia da Informação (TI). Boletim do Comando da Aeronáutica. Brasília, DF, 24 AGO 2010, fl. 6.368-6.370.

BRASIL. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. Disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta, e dá outras providências.

BRASIL. Instrução Normativa SECOM-PR nº 8, de 19 de dezembro de 2014. Disciplina a implantação e a gestão da Identidade Padrão de Comunicação Digital das propriedades digitais dos órgãos e entidades do Poder Executivo Federal e dá outras providências.

BRASIL. Instrução Normativa SECOM-PR nº 8, de 19 de dezembro de 2014. Disciplina a implantação e a gestão da Identidade Padrão de Comunicação Digital das propriedades digitais dos órgãos e entidades do Poder Executivo Federal e dá outras providências.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 27001. Sistema de Gestão de segurança da informação: índice: apresentação. Rio de Janeiro, RJ, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 27002. Código de Práticas para a Gestão da Segurança da Informação: índice: apresentação. Rio de Janeiro, RJ, 2005.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Núcleo de Gerenciamento Técnico do SISCEAB – NUCGTEC: ICA 66-32. Rio de Janeiro, RJ, 2015.

BRASIL. Comando da Aeronáutica. Diretoria de Tecnologia da Informação da Aeronáutica. Manual de Unidade Celular de Tecnologia da Informação: MCA 400-24. São Paulo, SP, 2019.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica: NSCA 7-13. São Paulo, SP, 2022.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Credenciamento de Segurança: ICA 200-13. Brasília, DF, 2022.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Concepção Estratégica Força Aérea 100: DCA 11-45. Brasília, DF, 2018.

BRASIL. Comando da Aeronáutica. Diretoria de Tecnologia da Informação da Aeronáutica. Manual de Procedimentos para Concentração de Serviços de Tecnologia da Informação nos Grupamentos de Apoio: MCA 11-2. Rio de Janeiro, RJ, 2016.

BRASIL. Comando da Aeronáutica. Diretoria de Tecnologia da Informação da Aeronáutica. Manual de Procedimentos para Concentração de Serviços de Tecnologia da Informação nos Grupamentos de Apoio: MCA 11-2. Rio de Janeiro, RJ, 2016.

BRASIL. Comando da Aeronáutica. Diretoria de Tecnologia da Informação da Aeronáutica. Funcionamento do Serviço de Correio Eletrônico do COMAER (FABMail): ICA 7-51. São Paulo, SP, 2021.

Anexo A – Termo de Responsabilidade para uso de internet e mídias sociais

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

Nome Completo:	
Posto/Grad:	**OM:**
CPF:	**E-mail:**

Acessos solicitados	**Justificativa:**
☐ **COM** acesso às mídias sociais	☐ **SEM** acesso às mídias sociais
☐ Acesso **PROVISÓRIO**	☐ Acesso **DEFINITIVO**
Preencha com o tipo de solicitação ((I) Inclusão; (A) Alteração; (E) Exclusão): ☐	

AVISO DE PRIVACIDADE

O Comando da Aeronáutica coletará e tratará seus dados de acordo com a Lei 13.709 de agosto de 2018 (LGPD), com a ***finalidade*** *de ceder acesso aos seus militares possuidores de larga experiência profissional e reconhecida competência técnico-administrativa,* ***limitando-se ao mínimo de dados*** *para a realização do acesso ao referido serviço. Os dados* ***não serão compartilhados*** *por terceiros e nem utilizados fora da finalidade da coleta. Os* ***dados pessoais coletados ficarão constante em nossa base de dados e ao fim da vigência, as informações serão tratadas conforme o previsto nas leis arquivísticas vigentes.***
O requerente ao serviço, titular dos dados pessoais, concorda com o tratamento de seus dados pessoais para a finalidade determinada de forma livre e inequívoca.

Cláusula 1 - Declaro ter recebido do Elo do STI responsável, os acessos solicitados para meu usuário do *proxy*, sendo responsável por quaisquer ações que venham a infringir as legislações em vigor e as cláusulas descritas neste termo.

Cláusula 2 - Declaro, sob as penas de lei vigente, ter conhecimento dos normativos de Segurança da Informaçãovigentes no âmbito da Administração Pública Federal.

Cláusula 3 - Declaro estar ciente de todo o conteúdo da **NSCA 7-13,** de 02 maio 2022, **SEGURANÇA DA INFORMAÇÃO E DEFESA CIBERNÉTICA NAS ORGANIZAÇÕES DO COMANDO DA AERONÁUTICA,** a fim de contribuir para a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações armazenadas, processadas ou em trânsito nos sistemas do COMAER.

Cláusula 4 - Declaro estar ciente das determinações contidas no Termo de Uso das Mídias Sociais do COMAER e suas atualizações, bem como das demais normas castrenses vigentes.

Continuação do Anexo A – Termo de Responsabilidade para uso de internet e mídias sociais

Cláusula 5 - Comprometo-me ser responsável pelos acessos a mim confiados, como também observar as cláusulas presentes neste instrumento.

Cláusula 6 - Comprometo-me a respeitar o grau de sigilo atribuído às informações a mim confiadas ou que venha a ter conhecimento em função da execução de atividades por mim desenvolvidas, para atendimento dos objetivos do COMAER.

Cláusula 7 - Estou ciente que a utilização da internet deve ser exclusivamente para apoiar as atividades de interesse do COMAER, sendo vedada a sua utilização que, direta ou indiretamente, não esteja voltada para o atendimento dos objetivos do COMAER.

Cláusula 8– Estou ciente de que o *login* e senha são únicos e intransferíveis, sendo vedado compartilhamento. Também estou ciente que o acesso é monitorado e passível de penalidades previstas na legislação em vigor.

Cláusula 9 – Comprometo-me a colaborar, no que couber, para que a Subdivisão de Suporte do CCA-BR mantenha o Sistema Operacional e o *software* antivírus corporativo, padronizado pelo Órgão Central do STI, atualizados no computador onde está sendo utilizado o acesso, sob pena de ter o acesso revogado, caso seja detectada alguma ação maliciosa proveniente de atividade de *malware*.

Cláusula 10 – Estou ciente de que as senhas de acesso têm caráter sigiloso, **sendo minha responsabilidade zelar pelo seu sigilo**, evitando:

a) Revelar a senha a quem quer que seja ou sob qualquer justificativa; e

b) Anotá-la ou registrá-la em qualquer meio visível por terceiros.

Cláusula 11 – Declaro que devo informar imediatamente ao CTIR.FAB caso seja detectado algum evento relacionado ao acesso à internet que possa comprometer a segurança da Informação.

Cláusula 12 – Declaro que tenho o conhecimento de que todas as minhas ações nos sistemas do COMAER podem ser registradas e posteriormente averiguadas pelo órgão competente, **sem prejuízo das ações disciplinares e/ou criminais** que possam ser tomadas.

Cláusula 13 – Comprometo-me responder por possíveis fugas de dados e aumento de vulnerabilidades causados por ações inerentes ao acesso disponibilizado.

Cláusula 14 – Comprometo-me responder por ações cibernéticas maliciosas por uso indevido do acesso disponibilizado.

Cláusula 15 – Declaro, finalmente, estar ciente da obrigação de preservar os recursos tecnológicos a mim confiados e que o descumprimento dos itens constantes neste instrumento e das normas de segurança do COMAER serão tratados como atos de transgressão disciplinar, podendo acarretar ainda, no que couber, processos administrativos e judiciais na esfera criminal.

Continuação do Anexo A – Termo de Responsabilidade para uso de internet e mídias sociais

TABELA DE TEMPORALIDADE (TT)

Título	Descrição	Corrente	Destinação
Dados pessoais	Compreende os dados necessários para a inclusão deacesso ao **Proxy corporativo**	Prazo de vigência (1 ano)	Eliminação

_____, _____ de _____ de _____

_____
Assinatura do solicitante

_____
Assinatura do Comandante/Chefe/Diretor OM

Nome de guerra: _____Setor: _____

Anexo B – Termo de Responsabilidade para usuários da rede INTRAER

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

Nome Completo:	
Posto/Graduação:	**OM:**
CPF:	**E-mail:**

AVISO DE PRIVACIDADE

O Comando da Aeronáutica coletará e tratará seus dados de acordo com a Lei 13.709 de agosto de 2018 (LGPD), com a ***finalidade*** *de ceder acesso aos seus militares possuidores de larga experiência profissional e reconhecida competência técnico-administrativa,* ***limitando-se ao mínimo de dados*** *para a realização do acesso ao referido serviço. Os dados* ***não serão compartilhados*** *por terceiros e nem utilizados fora da finalidade da coleta. Os* ***dados pessoais coletados ficarão constante em nossa base de dados e ao fim da vigência, as informações serão tratadas conforme o previsto nas leis arquivísticas vigentes.***
O requerente ao serviço, titular dos dados pessoais, concorda com o tratamento de seus dados pessoais para a finalidade determinada de forma livre e inequívoca.

1. Finalidade

1.1. Este Termo de Responsabilidade estabelece os direitos, responsabilidades e obrigações relacionadas ao tratamento de dados pessoais e ao uso adequado da rede intraer no COMAER. Ao utilizar a rede intraer, você está concordando com os termos e condições estabelecidos neste normativo.

2. Responsabilidades

Cláusula 1 - Reconheço que é proibido o uso da rede intraer para fins não autorizados, incluindo, mas não se limitando a: acesso a informações confidenciais sem autorização, disseminação de conteúdo ilegal ou prejudicial, violação de direitos autorais, envio de spam ou realização de atividades fraudulentas.

Cláusula 2 - Reconheço que sou responsável por manter minhas credenciais de acesso à rede intraer em sigilo e não as compartilhar. Qualquer atividade realizada por meio de minhas credenciais será de minha inteira responsabilidade.

Cláusula 3 – Estou ciente de que as senhas de acesso têm caráter sigiloso, **sendo minha responsabilidade zelar pelo seu sigilo**, evitando:

a) Revelar a senha a quem quer que seja ou sob qualquer justificativa;
b) Anotá-la ou registrá-la em qualquer meio visível por terceiros.

Cláusula 4 - Declaro estar ciente de que o órgão competente pode monitorar a utilização da rede intraer para fins de segurança, conformidade com as políticas estabelecidas e investigações internas, passível de penalidades previstas na legislação em vigor.

Continuação do Anexo B – Termo de Responsabilidade para usuários da rede INTRAER

Cláusula 5 – Declaro que tenho o conhecimento de que todas as minhas ações na rede intraer do COMAER podem ser registradas e posteriormente averiguadas pelo órgão competente, **sem prejuízo das ações disciplinares e/ou criminais** que possam ser tomadas.

Cláusula 6 - Reconheço que o uso indevido da rede intraer, em violação às políticas e diretrizes estabelecidas, poderá resultar em medidas disciplinares, conforme os regulamentos internos do COMAER.

Cláusula 7 - Comprometo-me a respeitar o grau de sigilo atribuído às informações a mim confiadas ou que venha a terconhecimento em função da execução de atividades por mim desenvolvidas, para atendimento dos objetivos do COMAER.

Cláusula 8 - Estou ciente que a utilização da intraer deve ser exclusivamente para apoiar as atividades de interesse do COMAER, sendo vedada a sua utilização que, direta ou indiretamente, não esteja voltada para o atendimento dos objetivos do COMAER.

Cláusula 9 - Comprometo-me a não divulgar, compartilhar ou utilizar indevidamente os dados pessoais de outros usuários da rede intraer.

Cláusula 10 - Comprometo-me a cumprir as políticas e diretrizes estabelecidas por este normativo, bem como as leis e regulamentos em vigor

Cláusula 11 - Comprometo-me ser responsável pelos acessos a mim confiados, como também observar as cláusulas presentes neste instrumento.

Cláusula 12 - Declaro estar ciente de todo o conteúdo da **NSCA 7-13,** de 02 maio 2022, **SEGURANÇA DAINFORMAÇÃO E DEFESA CIBERNÉTICA NAS ORGANIZAÇÕES DO COMANDO DA AERONÁUTICA,** a fim de contribuir para a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações armazenadas, processadas ou em trânsito na rede intraer do COMAER.

Cláusula 13 – Declaro, finalmente, estar ciente da obrigação de preservar os recursos tecnológicos a mim confiados e que o descumprimento dos itens constantes neste instrumento e das normas de segurança do COMAER serão tratados como atos de transgressão disciplinar, podendo acarretar ainda, no que couber, processos administrativos e judiciais na esfera criminal.

Continuação do Anexo B – Termo de Responsabilidade para usuários da rede INTRAER

TABELA DE TEMPORALIDADE (TT)

Título	Descrição	Corrente	Destinação
Dados pessoais	Compreende os dados necessários para a inclusão de acesso à **rede INTRAER do COMAER**	Prazo de vigência(1 ano)	Eliminação

_____, _____ de _____ de _____

_____
Assinatura do solicitante

_____
Assinatura do Comandante/Chefe/Diretor OM

Nome de guerra: _____Setor: _____

Anexo C – Termo de Responsabilidade para usuário de Sistemas Criptográficos remotos (VPN)

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

Nome Completo:		
Posto/Graduação:	**SARAM:**	**CPF:**
E-mail:		**OM:**

AVISO DE PRIVACIDADE

O Comando da Aeronáutica coletará e tratará seus dados de acordo com a Lei 13.709 de agosto de 2018 (LGPD), com a ***finalidade*** *de ceder acesso aos seus militares possuidores de larga experiência profissional e reconhecida competência técnico-administrativa,* ***limitando-se ao mínimo de dados*** *para a realização da contratação do referido serviço. Os dados* ***não serão compartilhados*** *por terceiros e nem utilizados fora da finalidade da coleta. Os* ***dados pessoais coletados ficarão constante em nossa base de dados e ao fim da vigência, as informações serão tratadas conforme o previsto nas leis arquivísticas vigentes.***
O requerente ao serviço, titular dos dados pessoais, concorda com o tratamento de seus dados pessoais para a finalidade determinada de forma livre e inequívoca.

Eu declaro ter ciência e estar de acordo com os procedimentos e regras abaixo discriminadas, comprometendo-me a respeita-las e cumpri-las:

a) a VPN institucional é pessoal e intransferível, não sendo permitido o acesso de terceiros, nem mesmo outro servidor, ainda que habilitado;
b) VPN deverá ser implementada em um DISPOSITIVO seguro, isto é:
   i. Com Sistema operacional dentro do seu ciclo de vida;
   ii. Com Sistema operacional atualizado e com todos os *patches* de segurança aplicados; e
   iii. Com antivírus atualizado.
c) o acesso à aplicação da VPN deverá ser feito com usuário de perfil limitado (não pode ser administrador ou *root*), no DISPOSITIVO.

Tenho ciência de que:

a) devo comunicar imediatamente eventual furto ou extravio do DISPOSITIVO à equipe de TI da OM onde trabalho;
b) a VPN será vinculada ao primeiro DISPOSITIVO em que ela for utilizada;
c) o DISPOSITIVO vinculado à VPN será o único em que ela poderá ser utilizada;
d) as informações de acesso à VPN serão de minha total responsabilidade; e
e) todos os meus acessos serão monitorados.

Continuação do Anexo C – Termo de Responsabilidade para usuário de Sistemas Criptográficos remotos (VPN)

Responsabilizo-me por todo e qualquer acesso e utilização da VPN.

TABELA DE TEMPORALIDADE (TT)

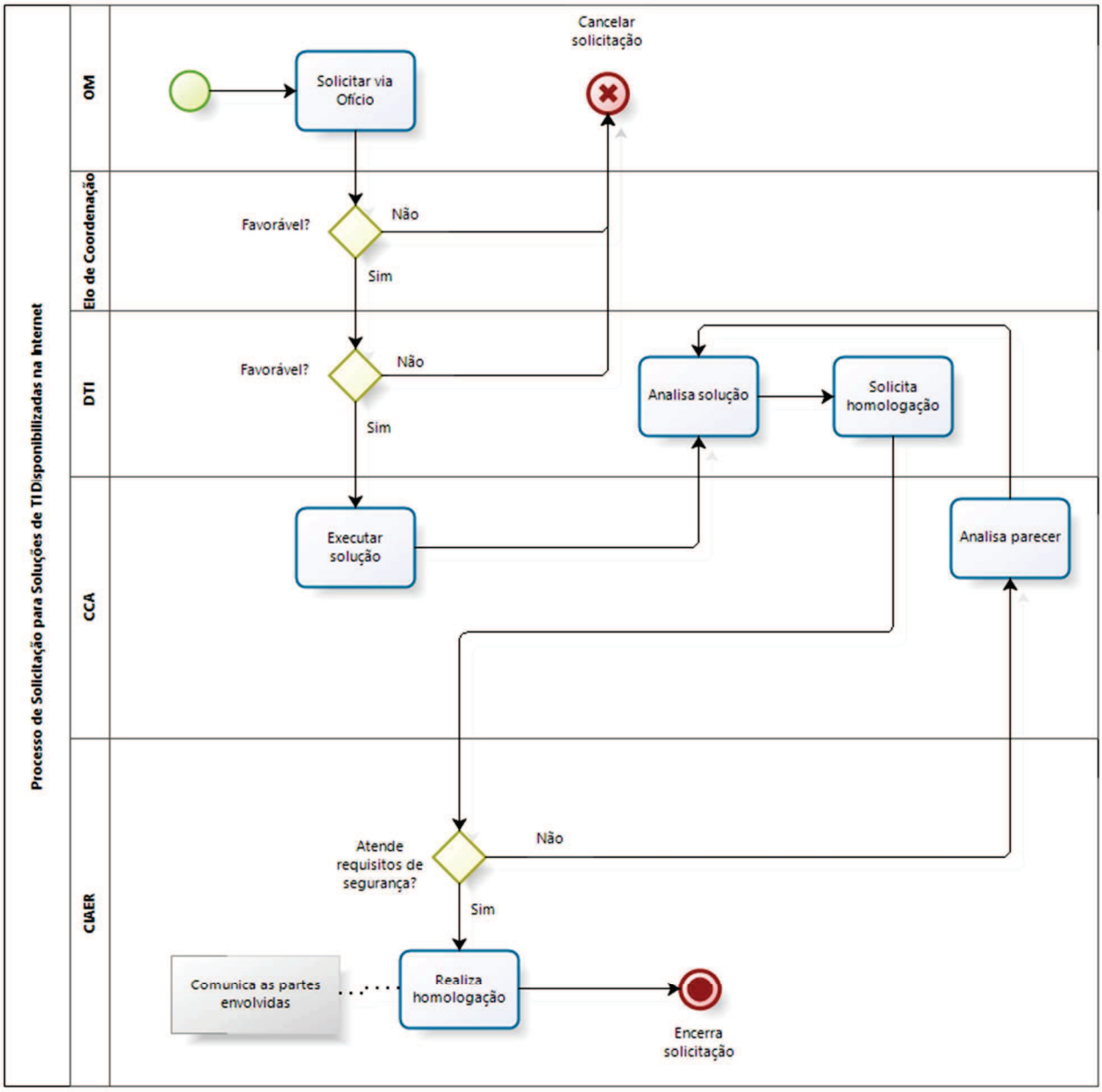
Título	Descrição	Corrente	Destinação
Dados pessoais	Compreende os dados necessários para a inclusão de acesso a **VPN**	Prazo de vigência (1 ano)	Eliminação

_____, _____ de _____ de _____

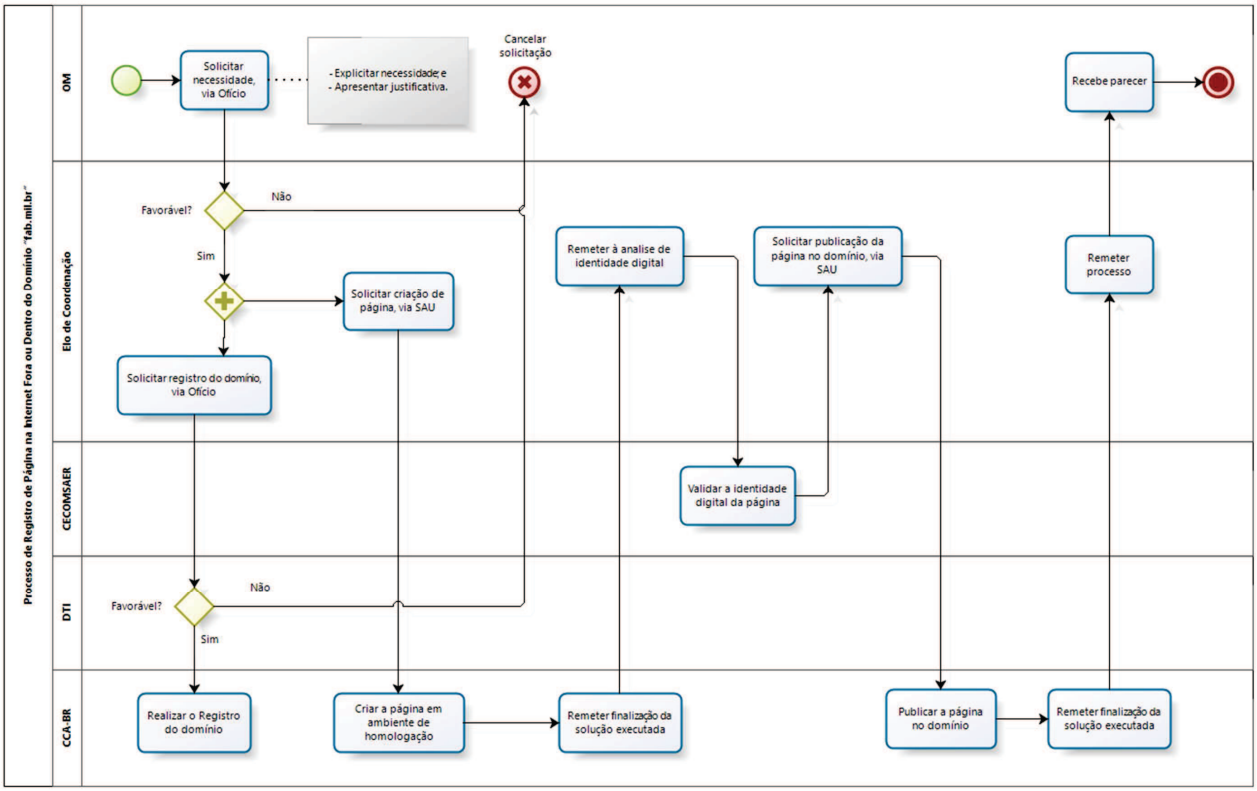
_____
Usuário da VPN

_____
Comandante/Chefe/Diretor OM

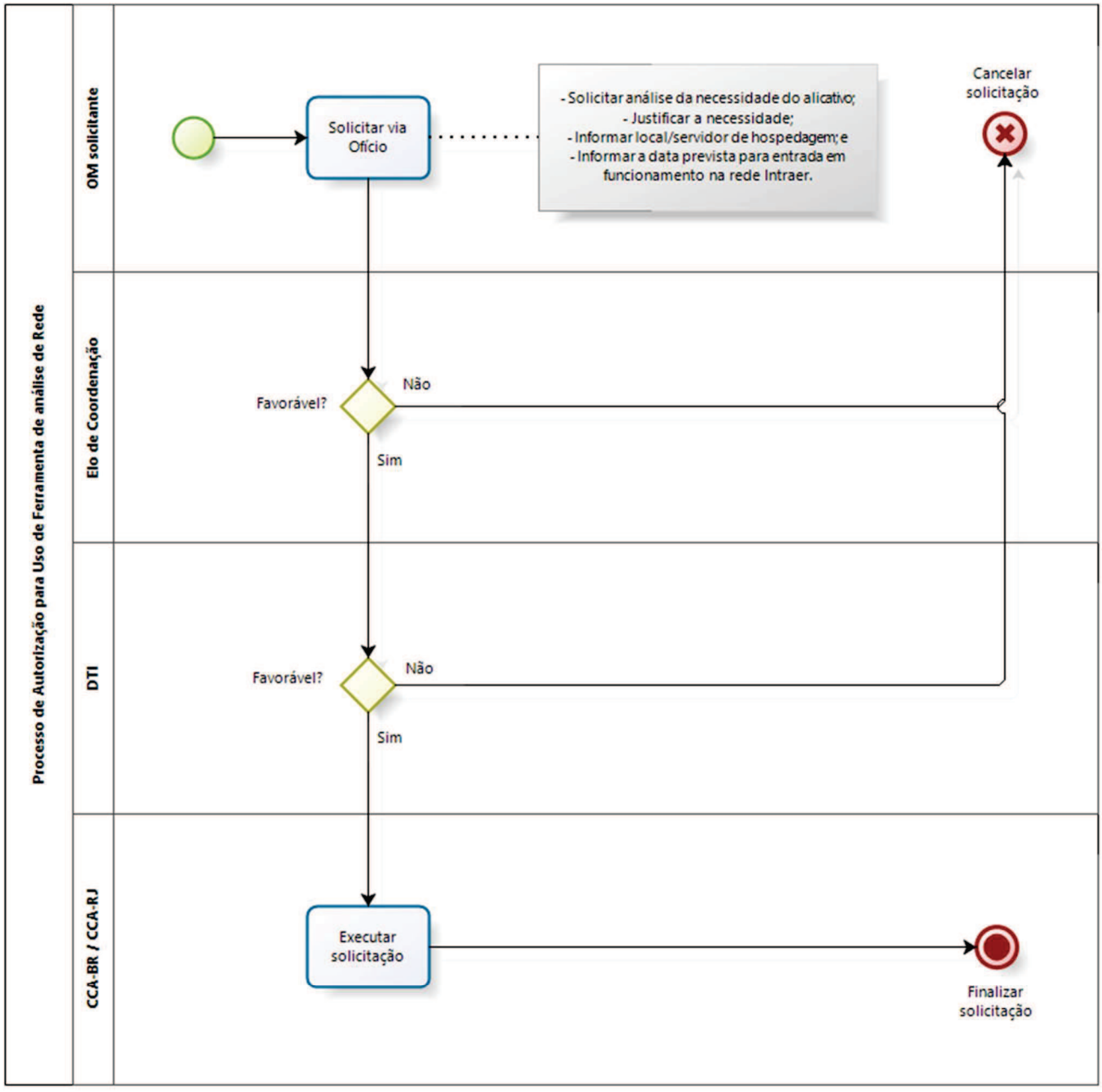
Anexo D – Processo de Solicitação para Soluções de TI Disponibilizadas na Internet



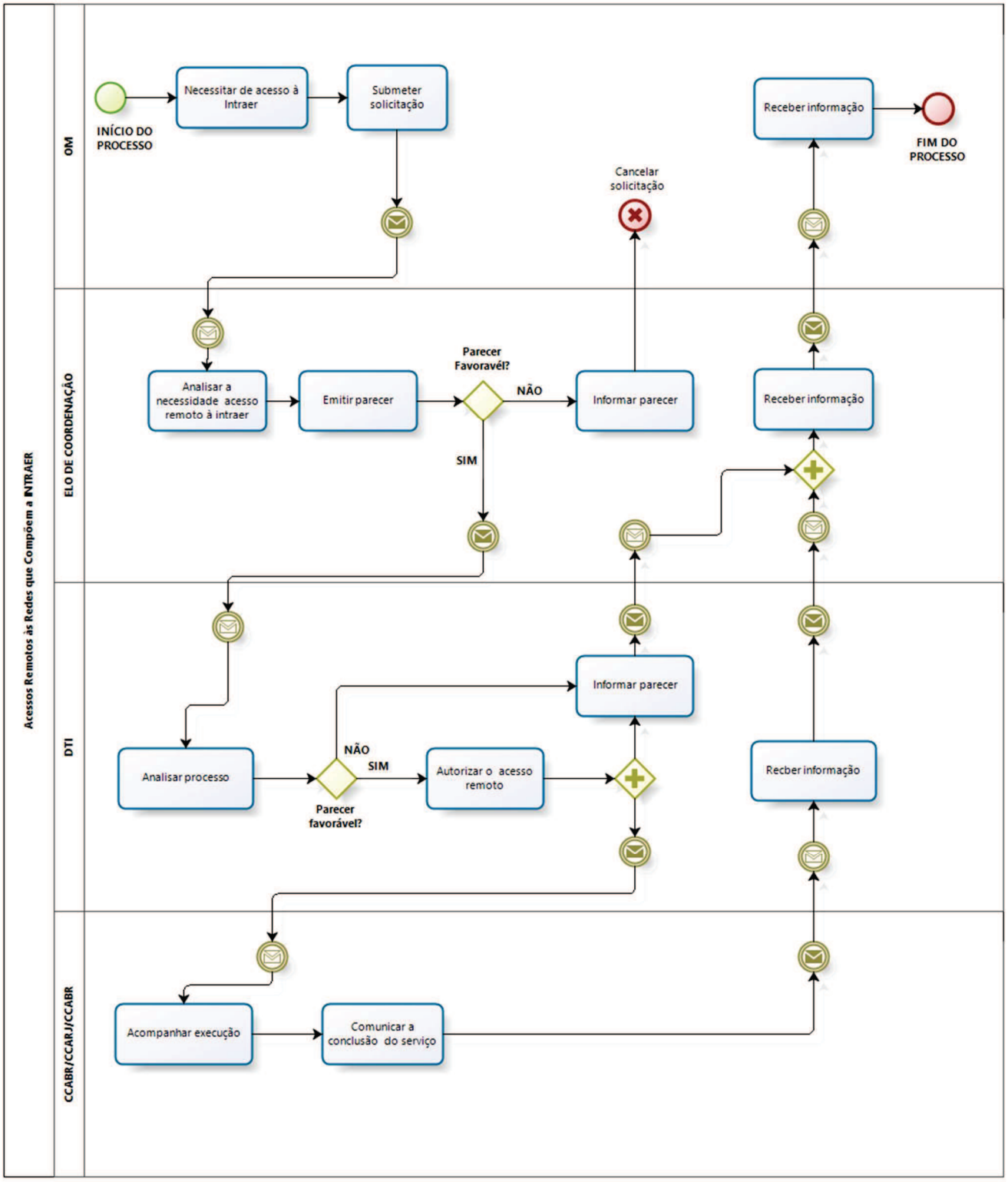
Anexo E – Processo de Registro de Página na Internet Fora ou Dentro do Domínio “fab.mil.br”



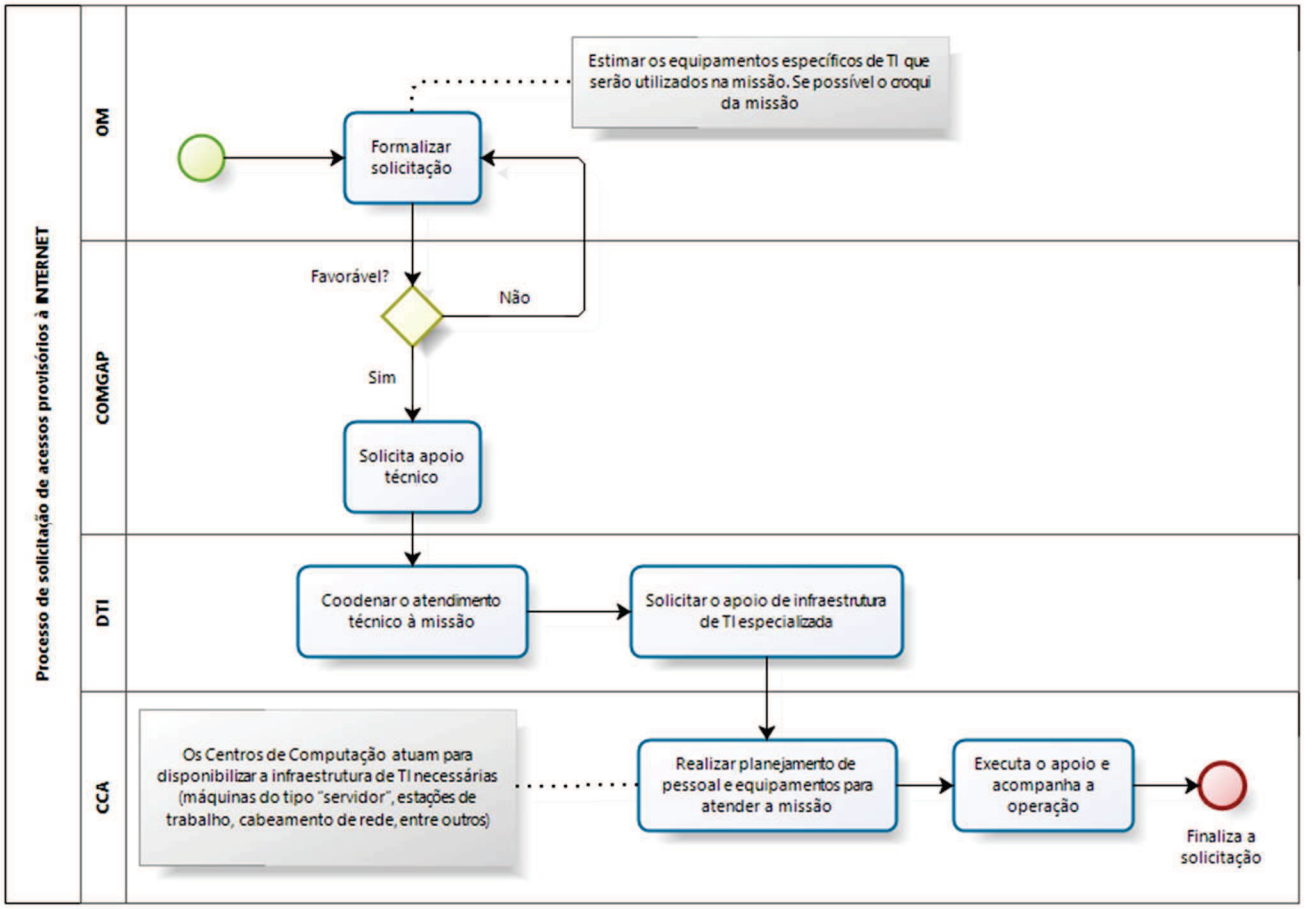
Anexo F – Processo de autorização para uso de ferramenta de análise de rede



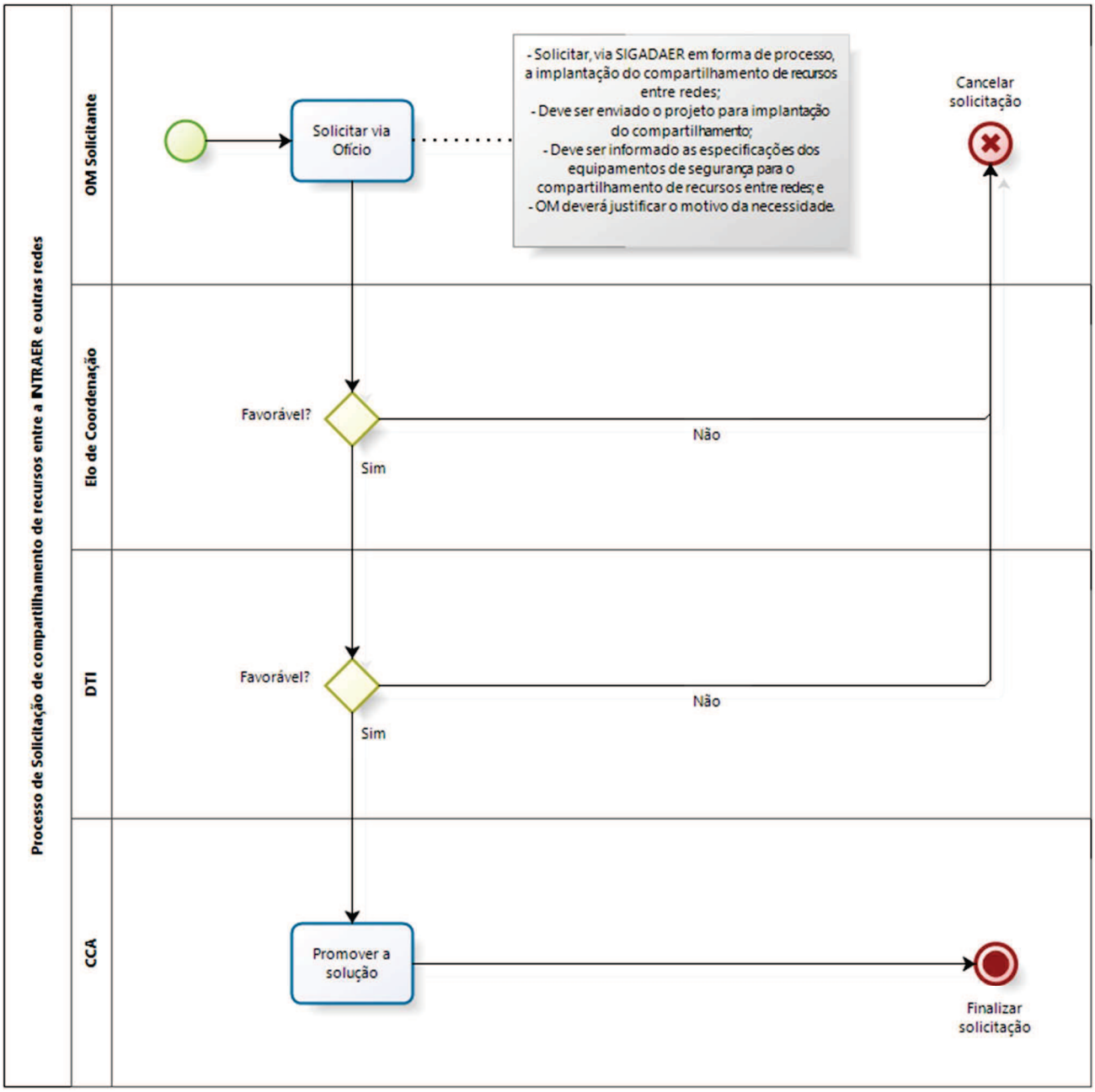
Anexo G – Acesso remoto às redes que compõem a INTRAER



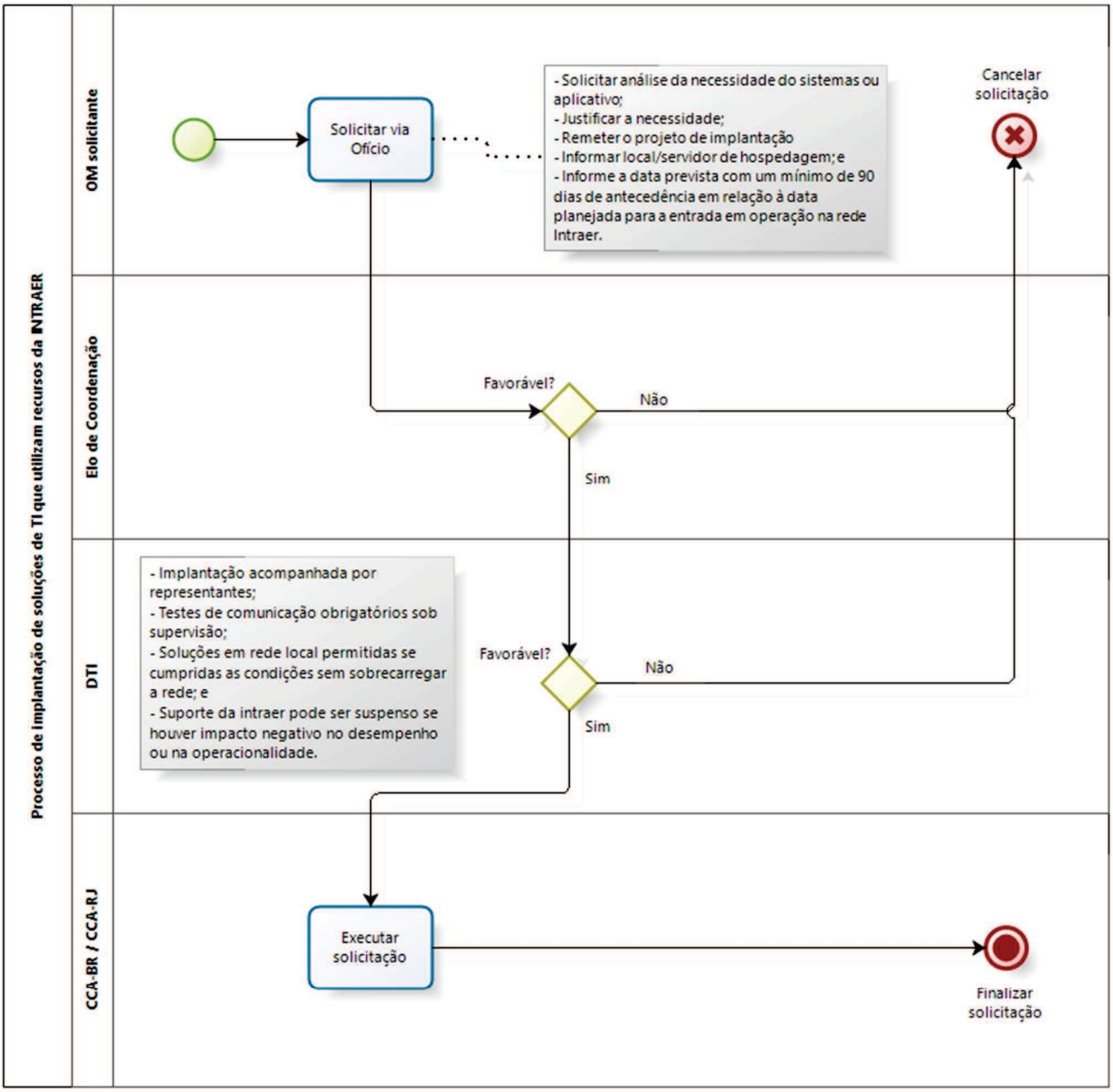
Anexo H – Processo de solicitação de acessos provisórios à INTERNET



Anexo I – Processo de Solicitação de compartilhamento de recursos entre a INTRAER e outras redes



Anexo J – Processo de implantação de soluções de TI que utilizam recursos da INTRAER



MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

NSCA 7-13

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

2013

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

2013

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
COMANDO-GERAL DE APOIO

PORTARIA COMGAP Nº 31/3EM, DE 06 DE MAIO DE 2013.

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

O COMANDANTE-GERAL DE APOIO, no uso de suas atribuições, que lhe conferem o Inciso IX do Art. 5º e o Inciso XI do Art. 9º do Regulamento do Comando-Geral de Apoio, aprovado pela Portaria n° 643/GC3, de 8 de setembro de 2010 e tendo em vista o disposto no item 3.3 da ICA 700-1/2006 "Implantação e Gerenciamento de Sistemas no Comando da Aeronáutica", resolve:

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

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

Ten Brig Ar HÉLIO PAES DE BARROS JÚNIOR
Comandante-Geral de Apoio

(Publicado no BCA nº 088, de 9 de maio de 2013)

SUMÁRIO

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.

Alem 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 "*hacker*s" 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 administrar a rede local de computadores de uma Organização Militar.

1.2.5 *ADWARE*

Do inglês *Advertising Software*. *Softwar*e especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do usuário, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas. (Fonte: Cartilha de Segurança para Internet – Glossário; Comitê Gestor da Internet no Brasil – gci.br, versão 3.1, 2006).

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 irrecuperáveis.

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 de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. (Fonte: Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008).

1.2.10 *BACKDOOR*

Programa que permite a um usuário invasor ganhar acesso a um Recurso Computacional. Normalmente este programa é colocado de forma a não ser notado. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

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*

Redes formadas por diversos computadores infectados com *bots* e que podem ser usadas em atividades de negação de serviço, esquema de fraude, envio de spam e outros. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.13 *BOTS*

Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas de configuração dos *software*s instalados em um computador, dispõe de mecanismo de comunicação com o usuário invasor, permitindo que o programa seja controlado remotamente. O usuário invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar spam e outros. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.14 CAVALO-DE-TRÓIA (*TROJANS*)

Programas recebidos normalmente como anexos de e-mail, que, além de executarem funções para os quais foram aparentemente projetados, também executam outras funções, geralmente maliciosas e sem o conhecimento do usuário. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.15 CONFIDENCIALIDADE

Propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado. (Fonte: Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008).

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

Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. (Fonte: NBR ISO/IEC 27002 – Código de Práticas para Gestão de Segurança da Informação).

1.2.18 CONTROLE DE ACESSO

Conjunto de procedimentos de segurança estabelecido para o acesso do usuário aos Recursos Computacionais. (Fonte: NBR ISO/IEC 27002 – Código de Práticas para Gestão de Segurança da Informação).

1.2.19 CRIPTOGRAFIA

É a ciência ou arte de escrever mensagens em forma cifrada ou em código. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.20 CTIR.AER (CENTRO DE TRATAMENTO DE INCIDENTES EM REDES)

Sigla designativa para a equipe de resposta a incidentes de Segurança da Informação, a ser implantada e mantida pelo Centro de Computação da Aeronáutica de Brasília, cuja finalidade é a de prover as ações necessárias no trato dos incidentes de segurança da informação no âmbito do Comando da Aeronáutica. (Fonte: Norma Complementar 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009).

1.2.21 DISPONIBILIDADE

Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade. (Fonte: Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008).

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 DA INFORMAÇÃO 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 de dados, 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 do negócio e ameaçar a segurança da informação.

1.2.30 INTEGRIDADE

Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. (Fonte: Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008).

1.2.31 IRRETRATABILIDADE / NÃO REPÚDIO

Impossibilidade de negar o fato de ser o autor ou a fonte de determinada informação em ambiente digital (Fonte: DCA 14-8 – Política de Segurança da Informação do COMAER).

1.2.32 *KEYLOGGERS*

Programas capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação

prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet *Banking*, para captura de senhas bancárias ou números de cartão de crédito. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.33 *LOG*

Um arquivo contendo um registro de eventos em um Recurso Computacional. (Fonte: NBR ISO/IEC 27002 – Código de Práticas para Gestão de Segurança da Informação).

1.2.34 *LOGON*

Ato de se conectar a um sistema de TI. (Fonte: NBR ISO/IEC 27002 – Código de Práticas para Gestão de Segurança da Informação).

1.2.35 *LOGOFF*

Ato de se desconectar de um sistema de TI. (Fonte: NBR ISO/IEC 27002 – Código de Práticas para Gestão de Segurança da Informação).

1.2.36 *MALWARE*

Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.37 MODEM

Dispositivo periférico que estabelece conexão entre computadores para envio de informações através de linhas telefônicas ou cabos. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.38 *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).

1.2.39 PLANO DE CONTINUIDADE DE NEGÓCIOS

Documento associado a um sistema de TI considerado crítico pelo COMAER e que institui os procedimentos a serem seguidos, com a finalidade de atingir os seguintes objetivos principais:

a) manter a operacionalidade do sistema, independentemente da ocorrência de falhas;

b) restaurar ou substituir os componentes necessários para sustentar a operação do sistema, após a ocorrência de um desastre; e

c) evitar o agravamento das situações de crise envolvendo o sistema. (Fonte:

Norma Complementar nº 06/IN01/DSIC/GSIPR de 14 de agosto de 2009).

1.2.40 *PORT-SCAN*

O ato de sistematicamente fazer varreduras de portas (local onde informações entram e saem) de Recursos Computacionais. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.41 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).

1.2.42 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*.

1.2.43 RECURSOS COMPUTACIONAIS CORPORATIVOS

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

1.2.44 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.

1.2.45 *ROOTKITS*

Conjunto de programas que tem como finalidade esconder e assegurar a presença de um usuário invasor em um computador comprometido. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.46 SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS)

É um programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas. (Fonte: Norma Complementar nº 08/IN01/DSIC/GSIPR de 14 de agosto de 2009).

1.2.47 SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (Fonte: Instrução Normativa GSI nº 1, de 13 de junho de 2008).

1.2.48 SENHA

Senha é uma palavra ou frase secreta que deve ser fornecida sozinha ou precedida de uma identificação do seu proprietário ou usuário, com a finalidade de ter acesso liberado a um programa ou sistema de TI. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.49 SERVIDOR

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

1.2.50 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.

1.2.51 *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, determinado pelo titular.

1.2.52 *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).

1.2.53 *SPYWARE*

Termo usado para se referir a uma grande categoria de *software*s que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.54 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).

1.2.55 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 Eletronics Engineers*) e suas variantes. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.56 *TOKEN*

É um *hardware* portátil com a mesma funcionalidade dos *smart cards*.

1.2.57 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*).

1.2.58 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

1.2.59 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.

1.2.60 *VIRTUAL PRIVATE NETWORK* (VPN)

Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública. (Fonte: Cartilha de Segurança para Internet do Comitê Gestor da Internet no Brasil).

1.2.61 VULNERABILIDADES

Fragilidade de um alvo ou grupo de ativos, que pode ser explorada por uma ou mais ameaças. (Fonte: DCA 14-8 – Política de Segurança da Informação do COMAER).

1.2.62 *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 *software*s 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 interesse do 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 às 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 do Brasil (ICP-Brasil), a fim de garantir a autenticidade e a irretratabilidade 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, ou 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 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, porém, os setores de TI das Organizações Militares poderão adquirir produtos distintos do padronizado, desde que autorizado pelo Órgão Central e com os recursos previstos no planejamento financeiro da respectiva OM.

3.3.3 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.

3.3.4 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.

3.3.5 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.

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

3.3.7 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.

3.3.8 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 27002:2008, 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:

a) administração e manutenção dos ambientes operacionais dos sistemas servidores;

b) administração e manutenção de sistemas de redes locais, metropolitanas e de longa distância; e

c) 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:

3.7.3.1 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.

3.7.3.2 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.

3.7.3.3 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.

3.7.4 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.

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

3.7.6 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.

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

3.7.8 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 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 no item 2.1.4, da ICA 200-8/2008 – Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações.

3.9.3 O CTIR.AER 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.AER é operado pelo Centro de Computação da Aeronáutica de Brasília.

3.9.5 O CTIR.AER 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.

3.9.6 Compete ao Órgão Central do STI definir as regras do funcionamento do CTIR.AER em instrução específica.

3.9.7 O CTIR.AER deverá enviar relatórios trimestrais 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 ao SAUTI, quando for o caso, ou diretamente ao CTIR.AER.

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 O Órgão Central do STI definirá o processo de atendimento aos incidentes de Segurança da Informação e a prática forense computacional necessária na etapa de coleta de evidências, na ICA que irá estabelecer os parâmetros do CTIR.AER.

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

3.11.1 Cada um dos sistemas de TI considerados críticos pelo COMAER deve estar protegido por um Plano de Continuidade de Negócios. A competência para a elaboração e a implantação desse Plano pertence ao Elo de Coordenação ou ao Elo Especializado do STI, que se constituir como gestor do sistema.

3.11.2 Os critérios utilizados para a confecção de Planos de Continuidade de Negócio 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 entre 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 ao DECEA, Órgão Central de Telecomunicações, 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 pelo DECEA, Órgão Central de Telecomunicações do COMAER.

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.AER; 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 – 3ª edição, 2008" ou versão mais atualizada, disponível no *site* do Tribunal de Contas da União (www.tcu.gov.br), e verificar seus procedimentos de segurança conforme a ICA 200-5 "Gerenciamento do 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, 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.AER 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 27001:2006, 27002:2005, 27005:2008 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 7-13/2006, aprovada pela Portaria DECEA nº 108/DGCEA, de 19 de outubro de 2006.

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.

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*. Rio de Janeiro, RJ, 2006.

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

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

Brasil. Tribunal de Contas da União. *Boas Práticas em Segurança da Informação*, 3. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008. Disponível em <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/biblioteca_tcu/biblioteca_digital/Boas_praticas_em_seguranca_da_informacao_3a_edicao.pdf >. Acesso em 22/06/2009.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Ciclo de Vida de Sistemas e Materiais da Aeronáutica*: **DCA 400-6.** Brasília, DF, 2007.

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

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. *Funcionamento do Serviço de Atendimento aos Usuários de Tecnologia da Informação (SAUTI)*: **NSCA 7-8**. Rio de Janeiro, RJ, 2011.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Gerenciamento do Ciclo de Vida de Sistemas de Tecnologia da Informação da Aeronáutica*: **NSCA 7-4**. Brasília, DF, 2006.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Gerenciamento do Plano de Segurança Orgânica do Comando da Aeronáutica*: **ICA 200-5**. Brasília, DF, 2009.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações*: **ICA 200-8**. Brasília, DF, 2008.

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

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

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Processo de Concessão de Credencial de Segurança de Pessoa Jurídica*: **ICA 200-4**. Brasília, DF, 2007.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Política Militar Aeronáutica*: **DCA 14-5**. [Brasília, DF], 2008.

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

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Uso da Rede Mundial de Computadores - INTERNET – No Comando da Aeronáutica*: **ICA 7-5**. Brasília, DF, 2001.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio.*Uso da Rede de Dados do Comando da Aeronáutica -INTRAER*: **NSCA 7-1** Rio de Janeiro, RJ, 2012.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. *Visita de Assessoria em Tecnologia da Informação – VATI:* **ICA 7-2**. **1** Rio de Janeiro, RJ, 2012.

BRASIL. Comando da Aeronáutica. Comando-Geral de Tecnologia Aeroespacial. *Política de Segurança em Tecnologia da Informação e de Uso dos Recursos Computacionais do CTA:* **DTA 08**, São José dos Campos, SP, 2007.

BRASIL. Instrução Normativa GSI Nº 1, de 13 de junho de 2008.

BRASIL. Instrução Normativa Nº 4 - SLTI/MPOG, de 12 de novembro de 2010.

BRASIL. Norma Complementar nº 01/IN01/DSIC/GSIPR, Atividade de Normatização. (Publicada no DOU Nº 200, de 15 Out 2008 - Seção 1).

BRASIL. Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da informação e Comunicações. (Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1).

BRASIL. Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. (Publicada no DOU Nº 125, de 03 Jul 2009 - Seção 1).

BRASIL. Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1).

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. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1).

BRASIL. Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 223, de 23 Nov 2009 - Seção 1).

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, direta e indireta – APF. (Publicada no DOU Nº 86, de 7 Maio 2010 - Seção 1)

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. (Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1).

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, direta e indireta. (Publicada no DOU Nº 222, de 22 Nov 2010 - Seção 1).Comando da Aeronáutica.

BRASIL. Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)

BRASIL. Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)

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. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)

BRASIL. Norma Complementar nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)

BRASIL. Norma Complementar nº 14/IN01/DSIC/GSIPR, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1)

BRASIL. Norma Complementar nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 119, de 21 Jun 2012 - Seção 1)

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. (Publicada no DOU Nº 224, de 21 Nov 2012 - Seção 1)

BRASIL. Acórdão - AC-1233-19/12-P, que trata de relatório consolidado das ações do TMS 6/2010, cujo objeto foi avaliar se a gestão e o uso da tecnologia da informação estão de

acordo com a legislação e aderentes às boas práticas de governança de TI, agregando os resultados de todas as fiscalizações previstas, de modo a sintetizar os achados e conclusões sobre a gestão e uso de TI na Administração Pública Federal (APF), nos moldes apresentados pela equipe coordenadora da Secretaria de Fiscalização de Tecnologia da Informação. (Publicado no DOU na ATA 19 - Plenário, de 23/05/2012).

Glossário Completo ICP-Brasil: Disponível em:
https://www.icpbrasil.gov.br/duvidas/glossario_iti.pdf/view; Acessado em: 22.04.2009.

Portaria nº 38, de 11 de junho de 2012, do Conselho de Defesa Nacional, que estabelece as diretrizes para o uso seguro das redes sociais na Administração Pública Federal.

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 No que tange ao uso da Internet no COMAER, os usuários também devem observar as normas 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 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.

3.5 Para a abertura de Contas de usuários nos recursos computacionais corporativos, o solicitante deverá justificar ao Chefe da Equipe de TI da OM o motivo pelo qual a conta deverá ser aberta nos mesmos e não nos recursos computacionais locais, sendo que esta justificativa deverá ser avalizada pelo responsável.

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 (contendo letras maiúsculas e minúsculas, números, sinais de pontuação e símbolos).

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.AER 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 portáveis 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) interceptar ou tentar interceptar transmissão de dados não destinados ao seu 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*, *rootkits* 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), por estes serem, comprovadamente, grande difusores de programas maliciosos;

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 *software*s do COMAER em atividades particulares;

d) explorar, sem autorização, aplicações e sistemas corporativos para obter dados ou alterar dados;

e) realizar qualquer outro procedimento de uso de *software* não previsto nesta 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.

1.2 Abrir, administrar e encerrar contas de usuários.

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 periódica de senha em intervalos de até 60 (sessenta) dias. Findo este prazo, a troca de senha deverá ser realizada. Nestes casos, 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 impedir a utilização de mensagem instantânea ou de bate-papo disponíveis na INTERNET, aqueles hospedados e mantidos por entidades externas ao COMAER, por estes serem, comprovadamente, grandes difusores de programas maliciosos.

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.

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 Pesquisar, obter e aplicar os pacotes de correção e atualização disponibilizados pelos fabricantes 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.

1.15 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 Trocar suas senhas periodicamente segundo o grau de segurança necessário à sua OM, em um período nunca superior a 60 (sessenta) dias.

1.23 Envidar esforços para evitar o acesso simultâneo de um usuário a um mesmo recurso computacional.

1.24 Executar programas, de forma sistemática, para quebra de códigos e senhas. Quando essas quebras ocorrerem, os usuários deverão ser notificados para providenciarem a troca imediata.

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

1.26 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.

1.27 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.

1.28 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).

1.29 Desabilitar a opção de execução automática de arquivos anexados dos *software*s clientes de correio eletrônico.

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

1.31 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.

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

1.33 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.

1.34 Dar ciência aos usuários que todas as atividades relacionadas ao uso dos recursos computacionais do COMAER são passíveis de registro, monitoramento e Inspeção.

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

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

1.37 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 não devem ser disponibilizados, tampouco transmitidos através da INTRAER/INTERNET e deverão observar o preconizado no Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica: RCA 205-1.

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 no Regulamento para Salvaguarda de Assunto Sigilosos (RSAS) – RCA 205-1/2006.

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 decriptação 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.

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 deve emitir alerta para os Administradores de Rede quando da detecção de vírus, sendo também notificado, pelo Elo de Serviço, o CTIR.AER.

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.

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

As Organizações do COMAER deverão configurar um servidor de *firewall* entre as suas respectivas Redes de Comunicação de Dados Locais e a rede corporativa de comunicação de dados, de forma a atender ao que se segue:

a) deverá ser o ponto de entrada e saída da rede filtrando todo o tráfego de informações entre as Redes Locais das OM e outra rede de forma a minimizar os incidentes de segurança e o seu uso abusivo;

b) deverá ser controlado e monitorado pelos Administradores de Rede, através de detecção de intrusão, inspeção interna e outros *software*s específicos;

c) 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.

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, observando-se o disposto no RCA 205-1.

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, contendo recursos, que não os membros das equipes locais de TI, ela deverá ser sempre 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.

e) serviços ou protocolos inseguros devem ser substituídos por equivalentes mais seguros, sempre que existirem, antes de serem disponibilizados na rede local da OM. Necessidades específicas serão tratadas pelo Chefe da Equipe de TI da OM ou pelo respectivo Elo Especializado do STI.

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.AER.

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 de um Servidor, este deverá ser imediatamente desconectado da rede, não podendo ser desligado, e o incidente investigado para as providências cabíveis, inclusive criminais, se for o caso.

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, bem como dos sistemas operacionais dos Servidores, devem ser mantidos por um mínimo de 6 (seis) meses. Qualquer atividade suspeita deve ser analisada e, constatando-se um incidente de segurança, a Equipe de Segurança em TI da OM e/ou o CTIR.AER deverá ser imediatamente comunicado.

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) os serviços não poderão sofrer manutenções remotas, devendo sua manutenção preventiva ser efetuada no console local do recurso computacional, por pessoa habilitada e autorizada para tal, ou pelo Administrador da Rede Local.

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.

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) Usuários não devem ter acesso físico ao Servidor via console. O acesso lógico de usuários ao Servidor deverá ser somente através da rede.

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 (*logon*s/*logoff*s), 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 *software*s 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 Segurança em TI da OM e/ou ao CTIR.AER que revisará os *logs* e gerará relatório de incidentes. 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.

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 será permitido 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 Anexo 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, bem como o acesso à INTRAER, por intermédio do uso da INTERNET somente poderá ser realizado mediante uso de solução desenvolvida pelo CIAER.

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) As inspeções serão coordenadas e realizadas pelos Elos de Coordenação de TI, nas Organizações Militares das respectivas áreas de subordinação, com suas respectivas Equipes de Segurança em TI e/ou em conjunto com o CTIR.AER.

c) Quando necessário, ou com o propósito de ser executada a inspeção, os membros da Equipe de Segurança em TI da OM e do CTIR.AER 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) O CTIR.AER, com a anuência do Exmo. Sr. Chefe do EMAER, poderá manter um monitoramento remoto constante da INTRAER em qualquer ponto do *backbone*, incluindo Redes Locais, sem necessidade de prévio aviso a qualquer usuário, desde que o Chefe ou Comandante ou Diretor do ODGSA tenha conhecimento desta ação e a tenha autorizado.

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, sem qualquer aviso prévio ao usuário, e quando estas atividades forem realizadas em Organizações subordinadas a outro ODGSA após conhecimento e autorização por parte do respectivo Chefe ou Comandante ou Diretor.

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.

ÍNDICE

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

POLÍTICA

DCA 14 -8

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA

2013

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO-MAIOR DA AERONÁUTICA

POLÍTICA

DCA 14 -8

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA

2013

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO-MAIOR DA AERONÁUTICA

PORTARIA Nº 1.966/GC3, DE 30 DE OUTUBRO DE 2013.

Aprova a reedição da Diretriz que estabelece a Política de Segurança da Informação do Comando da Aeronáutica.

O COMANDANTE DA AERONÁUTICA, , de conformidade com o previsto no inciso XIV do art. 23 da Estrutura Regimental do Comando da Aeronáutica, aprovada pelo Decreto nº 6.834, de 30 de abril de 2009, e considerando o que consta do Processo nº 67050.011908/2013-57, resolve::

Art. 1º Aprovar a reedição da DCA 14-8 "Política de Segurança da Informação do Comando da Aeronáutica", que com esta baixa.

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

Art. 3º Revoga-se a Portaria EMAER nº R-11/6SC, de 20 de outubro de 2006, publicada no Boletim do Comando da Aeronáutica Reservado nº 23, de 31 de outubro de 2006.

Ten Brig Ar JUNITI SAITO
Comandante da Aeronáutica

(Publicado no BCA nº 210, de 1º de novembro de 2013)

S U M Á R I O

PREFÁCIO

Na era da informação em que vivemos não há dúvida de que o conteúdo informacional de uma organização - considerado um de seus principais patrimônios - está sob constante risco. Dessa maneira, a Segurança da Informação e do Conhecimento tornou-se um ponto crucial para a sobrevivência das instituições públicas e privadas e, em particular, para o cumprimento da missão institucional do Comando da Aeronáutica (COMAER).

Na época em que informação era armazenada apenas em papel, a segurança aplicada à sua proteção era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com o incremento tecnológico de meios e o uso de computadores de grande porte, os processos voltados para a Segurança da Informação, em prática nas organizações, tornaram-se mais sofisticados, englobando controles lógicos, porém ainda centralizados.

Com o advento dos computadores pessoais, conectando virtualmente as Organizações Militares (OM) do COMAER e essas com a Internet, os aspectos relativos à Segurança da Informação atingiram um nível de complexidade elevado. É fato que o uso da Tecnologia da Informação (TI) já adquiriu uma importância vital para a sobrevivência dessas, pois é viabilizadora da automatização dos seus processos gerenciais e operacionais.

Em um contexto mundial, as informações contidas em sistemas computacionais são consideradas ativos críticos - tanto para a concretização dos negócios de uma empresa como para a tomada de decisão em questões governamentais, sociais, educativas e outras - necessitando, dessa maneira, que a segurança seja gerida de forma absoluta. Tal realidade não é diferente no âmbito do COMAER, onde cada vez mais se projetam sistemas corporativos sob o enfoque gerencial ou transacional, com vistas a auxiliar o processo de tomada de decisão sem, no entanto, ser deixada de lado a segurança dos sistemas de informação manuais.

As facilidades no acesso a ferramentas de ataque disponíveis na rede mundial de computadores (Internet) aumentam significativamente a exposição dos ativos informacionais a novas ameaças. Diante disso, faz-se necessário cuidado contra ações ofensivas aos sistemas do COMAER. Essas ações sempre visarão comprometer pessoas, processos, infraestruturas de comunicação e, consequentemente, os requisitos de confidencialidade, de integridade e de disponibilidade da informação e do conhecimento. Ademais, as ações ofensivas adquirem uma maior expectativa de êxito quando da ausência de uma gestão de riscos integrada a um modelo de gestão definido para o gerenciamento da Segurança da Informação.

Outrossim, enquanto os usuários de TI estão mais rígidos quanto a requisitos de sigilo, de integridade e de disponibilidade da informação - assim como quanto à qualidade do serviço prestado pelo seu computador pessoal ou pelos sistemas de informação disponíveis - os setores responsáveis em manter o ambiente de TI, por sua vez, esperam que seus sistemas sejam eficientes, atendam às necessidades dos usuários e estejam protegidos contra qualquer ameaça que possa comprometer seu funcionamento, impactando no negócio organizacional.

Diante do exposto, um sistema de informação focado no uso da TI, para operar de forma adequada e prover a Segurança da Informação e do Conhecimento, disponível em formato digital, necessita de ambientes controlados e protegidos contra desastres naturais (incêndio, terremoto e enchente), falhas estruturais (interrupção do fornecimento de energia

elétrica, sobrecargas elétricas e outros), sabotagem, fraudes, acessos não autorizados (*hackers*, espionagem industrial, venda de informações confidenciais) e outros tipos de ameaças que gerem riscos não aceitáveis e que, consequentemente, necessitam ser tratados e monitorados constantemente.

Portanto, ações defensivas e proativas devem ser encaradas como proteção ao patrimônio da organização e aos investimentos feitos em equipamentos, processos e capital humano, considerados nesta Política como ativos, de forma a assegurar o cumprimento da missão institucional do COMAER.

Por fim, esta Política possibilita a adoção, ao longo de toda a cadeia hierárquica, de atitude favorável no tocante à Segurança da Informação quanto ao uso de recursos computacionais no COMAER, incrementando a conscientização a respeito da importância do assunto.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Os objetivos e as diretrizes desta Política têm por finalidade orientar o planejamento e a execução das ações relacionadas com a Segurança da Informação no âmbito do COMAER.

1.2 CONCEITUAÇÃO

1.2.1 AMEAÇA

Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

1.2.2 ANÁLISE DE RISCO

Uso sistemático de informações para identificar fontes de risco e estimá-los.

1.2.3 ATIVO

Qualquer coisa que tenha valor para a organização.

1.2.4 ATIVOS FÍSICOS

Patrimônio composto de equipamentos computacionais (processadores, monitores, *laptops e modems*), equipamentos de comunicação (roteadores, *switchs*, *hubs*, PABX, fax e secretárias eletrônicas), mídias removíveis (fitas, discos, *pendrives*) e outros recursos tecnológicos (impressoras, *no-breaks e* estabilizadores).

1.2.5 ATIVOS DE INFORMAÇÃO

Patrimônio composto de bases de dados e arquivos, documentação de sistemas, informações sobre pesquisas, manuais de usuários, material de treinamento, procedimentos de suporte e operação, planos de continuidade, procedimentos de recuperação de sistemas, trilhas de auditoria e informações armazenadas.

1.2.6 ATIVOS DE SOFTWARE

Patrimônio composto de aplicativos, sistemas operacionais, ferramentas de desenvolvimento e utilitários.

1.2.7 AUTENTICIDADE

É a garantia de que o conteúdo da informação seja verdadeiro, como também a fonte geradora da informação e o seu destinatário sejam realmente quem alegam ser.

1.2.8 AVALIAÇÃO DE RISCO

Processo de comparar o risco estimado com critérios predefinidos para determinar a sua importância.

1.2.9 CERTIFICADO DE CONFORMIDADE

Garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal.

1.2.10 CONFIDENCIALIDADE

Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

1.2.11 CONTROLE

Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

1.2.12 DISPONIBILIDADE

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

1.2.13 ELOS DE COORDENAÇÃO

São os setores pertencentes aos Órgãos de Direção-Geral e de Direção Setorial (ODGS) e ao Gabinete do Comandante da Aeronáutica, responsáveis pela coordenação de suas atividades de TI junto ao órgão central do Sistema de Tecnologia da Informação (STI).

1.2.14 ELOS ESPECIALIZADOS

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.

1.2.15 ELOS DE SERVIÇOS

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.

1.2.16 GERENCIAMENTO DE RISCOS

Atividades coordenadas para direcionar e controlar uma organização ou Sistema no que se refere a riscos, incluindo os processos de análise de riscos, a avaliação de riscos, o tratamento dos riscos e a sua comunicação.

1.2.17 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 do negócio e ameaçar a segurança da informação.

1.2.18 INTEGRIDADE

Propriedade de salvaguarda da exatidão e completeza da informação.

1.2.19 IRRETRATABILIDADE/ NÃO REPÚDIO

Impossibilidade de negar o fato de ser o autor ou a fonte de determinada informação em ambiente digital.

1.2.20 RISCO

Combinação da propabilidade de um evento e de suas consequências.

1.2.21 SEGURANÇA DA INFORMAÇÃO

Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como a intrusão e a modificação desautorizada de dados ou informações armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacionais.

1.2.22 SISTEMA

É o conjunto de elementos integrantes e interdependentes que tem por finalidade realizar uma tarefa de apoio em proveito da missão principal de uma organização. A vinculação desses elementos, entre si, ocorre por interesse de coordenação, orientação técnica e normativa, não implicando subordinação hierárquica, conforme definido na ICA 700-1.

1.2.23 SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMAER (STI)

Sistema que tem a finalidade de organizar, disciplinar e controlar as atividades de Tecnologia da Informação (TI), em consonância com as políticas específicas do Governo Federal e com a Política da Aeronáutica para a Tecnologia da Informação.

1.2.24 TECNOLOGIA DA INFORMAÇÃO (TI)

Conjunto formado por pessoal técnico especializado, processos, serviços e bens de natureza financeira e tecnológica, incluindo equipamentos (computadores, roteadores, *switches* e outros) e programas, que são empregados na geração, armazenamento, veiculação, processamento, reprodução e uso da informação.

1.2.25 TRATAMENTO DO RISCO

Processo de seleção e implementação de controles para modificar o grau de um risco.

1.2.26 VULNERABILIDADES

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

1.3 ÂMBITO

Esta Diretriz se aplica a todas as OM do COMAER.

2 CONCEPÇÃO

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

2.2 A Segurança da Informação no COMAER compreende um conjunto de objetivos, diretrizes, normativas gerenciais e técnicas, e demais controles destinados a garantir a confidencialidade, a disponibilidade, a integridade, a irretratabilidade e a autenticidade da informação em todo o seu ciclo de vida, disponibilizada ou em trânsito em ambiente digital.

2.3 As ameaças e vulnerabilidades associadas a ativos, no que tange ao emprego e ao acesso às informações em ambiente digital, devem ser adequadamente consideradas no contexto de uma crescente automação de atividades e processos.

2.4 A eficiência no emprego seguro dos recursos de TI constitui fator primordial para a eficácia do COMAER.

2.5 O sucesso das ações nos assuntos de Segurança da Informação está diretamente associado à capacitação científico-tecnológica do capital humano envolvido, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

2.6 Todo ativo de informação produzido ou processado no STI e demais ativos considerados críticos no Sistema devem ser claramente identificados, inventariados e submetidos a procedimentos de segurança, baseados em uma metodologia formalizada que identifique as ameaças a que estão expostos e os níveis de probabilidade e de impacto diante de um incidente de segurança, a fim de mensurar qualitativamente os riscos e selecionar os controles necessários à garantia da confidencialidade, da integridade e da disponibilidade da informação.

2.7 Toda documentação normativa relacionada à Segurança da Informação, a ser elaborada ou revisada no âmbito do COMAER, deve estar em consonância com esta Política e suas referências bibliográficas e demais instrumentos de teor legal afetos ao tema, a fim de garantir o alinhamento com a legislação superior vigente.

2.8 A exploração pelo COMAER de tecnologias consagradas pelo uso, tais como a Internet, a Intranet, o correio eletrônico, a infraestrutura de chaves públicas, dentre outras, deve ser disciplinada em documentos normativos gerenciais e técnicos, respeitando as diretrizes de segurança traçadas por esta Política.

2.9 O cumprimento das regras previstas nos documentos normativos de Segurança da Informação vigentes é de responsabilidade de cada integrante da Aeronáutica, seja militar ou civil, dentro de seu nível de acesso e de sua esfera de atribuições.

2.10 Os usuários do STI em função de comando ou equivalente devem estar comprometidos com o tema em foco e adotar medidas necessárias para que seus subordinados conheçam e cumpram as regras contidas nos documentos normativos gerenciais e técnicos de Segurança da Informação, nos seus níveis de atribuições.

3 OBJETIVOS

3.1 Os objetivos e as diretrizes descritas nesta Política representam tacitamente o comprometimento do COMAER com o tema Segurança da Informação, bem como estabelece o enfoque a ser dado por todas as suas organizações quanto ao assunto em questão.

3.2 As diretrizes desta Política visam definir responsabilidades para o planejamento, a execução, a manutenção e o controle das atividades relativas à Segurança da Informação, assim como para a atualização da documentação pertinente.

3.3 Em consonância com as políticas específicas do Governo Federal, as atividades envolvidas na Segurança da Informação, sob o enfoque do STI, devem garantir a aderência às diretrizes específicas estabelecidas na Política do COMAER para a TI, em todo o âmbito da Instituição, bem como o seu alinhamento ao negócio institucional deste Comando.

3.4 A Política de Segurança da Informação do COMAER identifica cinco objetivos principais a serem perseguidos.

3.4.1 PRIMEIRO OBJETIVO

Dotar as organizações do COMAER de instrumentos normativos e organizacionais que as capacitem científica, tecnológica e administrativamente, visando à garantia de requisitos de confidencialidade, de integridade, de disponibilidade, de autenticidade e não repúdio dos serviços e dos ativos físicos, dos ativos de informação e dos ativos de *software*.

3.4.2 SEGUNDO OBJETIVO

Promover a capacitação do capital humano do COMAER para o desenvolvimento de competência científico-tecnológica, visando à condução proficiente e confiável das atividades inerentes à segurança dos serviços, dos ativos físicos, dos ativos de informação e dos ativos de *software*.

3.4.3 TERCEIRO OBJETIVO

Promover as ações necessárias ao desenvolvimento, à implementação e ao gerenciamento da segurança dos serviços e dos ativos físicos, dos ativos de informação e dos ativos de *software*, com vistas à garantia da operacionalidade da Força.

3.4.4 QUARTO OBJETIVO

Promover o intercâmbio científico-tecnológico entre o COMAER e os órgãos da Administração Pública, da iniciativa privada e demais Forças singulares, nacionais e estrangeiras, com vistas a garantir o uso das melhores práticas existentes na gestão da Segurança da Informação e o seu alinhamento às legislações em vigor.

3.4.5 QUINTO OBJETIVO

Garantir a interoperabilidade entre soluções direcionadas para a Segurança da Informação, no âmbito do COMAER, e deste com as demais Forças singulares e órgãos da Administração Pública, assegurando, dessa maneira, a otimização dos recursos aplicados na

proteção da informação e do conhecimento disponível em ambiente digital, assim como a eficácia dos processos envolvidos na manutenção segura dos meios de comunicação.

4 DIRETRIZES ESTRATÉGICAS

4.1 O STI deve possuir normativas gerenciais e técnicas inerentes à implementação, ao controle e à emissão de certificados digitais, no âmbito do COMAER, utilizando-se da infraestrutura de chaves públicas da Autoridade Certificadora de Defesa (AC-Defesa), baseada em padrões e diretrizes emanados pelo Governo Federal, visando à sua utilização em sistemas de informação e em recursos computacionais.

4.2 O Sistema de Inteligência do COMAER deve possuir normativas gerenciais que definam padrões, níveis, tipos e demais aspectos relacionados com o emprego de produtos que incorporem recursos criptográficos, de modo a assegurar a autenticidade, a confidencialidade, a integridade e o não repúdio, atentando para a garantia da interoperabilidade entre os ativos físicos, de informação e de *software*.

4.3 O Sistema de Inteligência do COMAER deve possuir normativas gerenciais inerentes aos processos necessários à emissão de certificados de conformidade, no tocante aos produtos que incorporem recursos criptográficos, com base nas orientações emitidas pelo Ministério da Defesa e pela Secretaria-Geral do Conselho de Defesa Nacional.

4.4 O STI deve possuir normativas técnicas, bem como requisitos operacionais e técnicos, a serem considerados no gerenciamento do ciclo de vida de sistemas de informação, promovendo a incorporação de funcionalidades que façam uso de certificados digitais, no transporte e no armazenamento de dados e de informações em meio digital, garantindo requisitos de identificação, de autenticação, de controle de acesso e de não repúdio, assim como da integridade de documentos digitais e da confidencialidade nas transações eletrônicas realizadas através de redes de computadores no COMAER.

4.5 O STI deve possuir normativas gerenciais que promovam as atividades de gerenciamento de riscos em todas as OM do COMAER, por meio da definição de uma metodologia simplificada, com vistas ao levantamento do nível de criticidade e de vulnerabilidade dos ativos físicos, ativos de informação e ativos de *software*, bem como a identificação das ameaças associadas a esses ativos em uso nos diversos Sistemas, a fim de que possam ser mensurados os níveis de riscos e selecionados os controles necessários ao seu tratamento.

4.6 O STI deve possuir normativas gerenciais que propiciem a auditoria nos serviços e nos ativos físicos, ativos de informação e ativos de software disponíveis e em operação no COMAER.

4.7 O STI deve possuir programas educativos destinados à conscientização e à capacitação do capital humano, no contexto da Segurança da Informação, quanto ao adequado uso dos sistemas de informação e dos recursos computacionais associados aos ativos disponíveis e em uso no STI.

4.8 O STI deve estimular a participação do capital humano em cursos e estágios realizados em organizações militares e civis, no Brasil e no exterior, cujos temas estejam afetos à Segurança da Informação.

4.9 O Sistema de Ensino deve fomentar o desenvolvimento de teses e trabalhos científicos em instituições de ensino superior do País, de interesse do COMAER, os quais estejam voltados para o tema Segurança da Informação.

4.10 O Sistema de Ensino deve incluir nos programas dos cursos de formação, de adaptação, de aperfeiçoamento militar e de especialização do COMAER, conteúdos didáticos que visem a disseminar o tema Segurança da Informação.

4.11 O STI deve prever auditorias periódicas nos seus diversos Elos, sob a coordenação do Órgão Central, com o intuito de aferir o nível de segurança quanto à utilização, ao armazenamento e ao controle dos serviços e dos ativos físicos, de informação e de *software*, bem como o alinhamento dos processos às normas e instruções voltadas para a Segurança da Informação em vigor no COMAER.

4.12 O STI deve conceber, implementar e manter um grupo técnico-especializado, no âmbito do COMAER, sob coordenação do Órgão Central, dedicado ao tratamento, controle, monitoramento, análise forense e resposta a incidentes de segurança, no ambiente cibernético, com vistas a manter a operacionalidade dos serviços e dos ativos físicos, de informação e de *software* disponíveis no Sistema.

4.13 Os sistemas implantados no COMAER devem conceber, implementar e manter programas de orientação para a divulgação da Política, das Normas e das Instruções existentes, que versam sobre o tema Segurança da Informação e uso seguro dos recursos computacionais.

4.14 Os sistemas implantados no COMAER devem evitar o uso de sistemas criptográficos de origem estrangeira, devendo ser buscado o desenvolvimento e a adoção de padrões criptográficos conforme normas e demais instruções emitidas pelo Sistema de Inteligência, respeitando a necessidade de interoperabilidade com os sistemas criptográficos adotados pelo Ministério da Defesa, Forças singulares e demais órgãos da Administração Pública Federal, quando pertinente.

4.15 O STI deve fomentar a criação de um núcleo de excelência, no âmbito do COMAER, voltado para a pesquisa e o desenvolvimento de soluções no campo da criptologia.

4.16 O STI deve acompanhar, em âmbitos nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à Segurança da Informação.

4.17 O STI deve possuir Fóruns e Comitês Temáticos, presenciais ou à distância, no âmbito do COMAER, envolvidos com a evolução doutrinária e tecnológica das atividades inerentes à Segurança da Informação, cujos resultados promovam uma atualização contínua das capacidades técnico-operacionais associadas aos ativos físicos, ativos de informação e ativos de *software*.

4.18 O STI deve manter um canal entre o COMAER e as demais Forças singulares, de modo a facilitar o compartilhamento dos conhecimentos relativos à Segurança da Informação.

4.19 O STI deve manter padrões de procedimentos e, quando aplicável, de equipamentos, nas soluções de segurança em sistemas de informação, os quais promovam a interoperabilidade dos mesmos, bem como a otimização dos recursos investidos.

4.20 O STI deve elaborar e implantar um Modelo de Gestão da Segurança da Informação (MGSI), a ser homologado por meio de publicação complementar a esta Política, contendo diretivas que regulem o gerenciamento sistêmico da segurança da informação no âmbito do COMAER.

5 DISPOSIÇÕES TRANSITÓRIAS

5.1 Esta Política de Segurança da Informação deverá estar completamente implementada e operacionalizada, em um prazo inferior a vinte e quatro meses, a partir de sua entrada em vigor.

5.2 As diretrizes traçadas nesta Política deverão ser reavaliadas, assim como este instrumento regulatório atualizado, depois de completado trinta e seis meses de sua entrada em vigor.

6 DISPOSIÇÕES FINAIS

Os casos não previstos serão submetidos à apreciação do Comandante da Aeronáutica.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. *Política Militar da Aeronáutica*: **DCA 14-5**. [Brasília, DF], 2008.

_____. Comando da Aeronáutica. *Política do Comando da Aeronáutica para a Tecnologia da Informação*: **DCA 14-7**. [Brasília, DF], ___ dez. 2004.

_____. Governo Federal. *Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências*: **Lei nº 8.159**. [Brasília, DF], 08 jan. 1991.

_____. Governo Federal. *Política Nacional de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*: **Decreto nº 3.505**. [Brasília, DF], 13 jun. 2000.

_____. Governo Federal. *Altera o Decreto-Lei Nr. 2.848, de 7 de dezembro de 1940 – Código Penal - dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública Federal*: **Lei nº. 9.983**. [Brasília, DF], 14 jul. 2000.

_____. Governo Federal. *Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal*: **Decreto nº 3.996**. [Brasília, DF], 31 out. 2001.

_____. Governo Federal. *Estabelece requisito para contratação de serviços de certificação digital pelos órgãos Públicos Federais e dá outras providências*: **Decreto nº 3.865**. [Brasília, DF], 13 jul. 2001.

_____. Governo Federal. *Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP Brasil e dá outras providências*: **Medida Provisória nº 2.200-2**. [Brasília, DF], 25 ago. 2001.

_____. Governo Federal. *Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências*: **Decreto nº 4.553**. [Brasília, DF], 27 dez. 2002.

_____. Governo Federal. *Regulamentada Medida Provisória nº 228, de 9 de dezembro de 2004, e institui a Comissão de Averiguação e Análise de Informações Sigilosas*: **Decreto nº 5.301**. [Brasília, DF], 09 dez. 2004.

_____. *Gestão de Riscos – Vocabulário – Recomendação para uso em normas*: **ABNT NBR ISO/IEC GUIA73**. 31 ago. 2005.

_____. *Código de prática para a gestão da segurança da informação*: **ABNT NBR ISO/IEC 17799**. 30 set. 2005.

_____. *Tecnologia da Informação - Sistemas de gestão de segurança da informação - Requisitos*: **ABNT NBR ISO/IEC 27001**. 30 abr. 2006.

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

CONTROLE DE ASSINATURAS ELETRÔNICAS DO DOCUMENTO

Documento:	23. ANEXO I_TR
Data/Hora de Criação:	30/04/2026 18:28:44
Páginas do Documento:	190
Páginas Totais (Doc. + Ass.)	191
Hash MD5:	8407a55154738b890bebf0543b4e2366
Verificação de Autenticidade:	https://autenticidade-documento.sti.fab.mil.br/assinatura

Este documento foi assinado e conferido eletronicamente com fundamento no artigo 6º, do Decreto nº 8.539 de 08/10/2015 da Presidência da República pelos assinantes abaixo:

Assinado via ASSINATURA CADASTRAL por 1º Ten NATHALIE LIMA ZUCCHERELLI no dia 30/04/2026 às 15:43:09 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Cap ROMULO DOS SANTOS FARIAS no dia 30/04/2026 às 15:43:36 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Terceiro Sargento ANDRÉSIA PEREIRA DE OLIVEIRA no dia 30/04/2026 às 15:47:15 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Soldado 2a. Classe JOAO PEDRO PEREIRA BARBOSA no dia 30/04/2026 às 15:48:07 no horário oficial de Brasília.

CONTROLE DE ASSINATURAS ELETRÔNICAS DO DOCUMENTO