MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

NSCA 7-13

SEGURANÇA DE SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO NO COMANDO DA AERONÁUTICA

2006

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

TECNOLOGIA DA INFORMAÇÃO

NSCA 7-13

SEGURANÇA DE SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO NO COMANDO DA AERONÁUTICA

2006

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

PORTARIA DECEA Nº 108/DGCEA, DE 19 DE OUTUBRO DE 2006.

Aprova a Norma de Sistema que trata da Segurança de Sistemas de Tecnologia da Informação no Comando da Aeronáutica.

O DIRETOR-GERAL DO DECEA, tendo em vista o disposto no item 3.3 da IMA 700-1, de 19 de outubro de 1998, e o que consta no Processo 35-01/613/2001,

RESOLVE:

Art. 1º Aprovar a NSCA 7-13 "Segurança de Sistemas de Tecnologia da Informação no Comando da Aeronáutica", elaborada pelo Departamento de Controle do Espaço Aéreo.

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

Ten Brig Ar PAULO ROBERTO CARDOSO VILARINHO
Diretor-Geral do DECEA

(Publicado no BCA nº 205, de 7 de novembro de 2006)

S U M Á R I O

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.

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

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

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

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Orientar as Organizações do COMAER quanto aos princípios de segurança da informação que devem ser seguidos durante os processos de contratação, de desenvolvimento, de operação e de manutenção de sistemas de tecnologia da informação (TI), a fim de garantir a confidencialidade, a integridade e a disponibilidade das informações armazenadas e tratadas por esses sistemas.

1.2 CONCEITUAÇÕES

1.2.1 ACESSO DEDICADO À INTERNET

Canal de comunicação contratado junto a uma empresa provedora de acesso físico à Internet.

1.2.2 ACESSO REMOTO 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 ATIVOS DE INFORMAÇÃO

Patrimônio composto de bases de dados e arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte e operação, planos de continuidade e procedimentos de recuperação de sistemas.

1.2.4 AUTENTICIDADE

Garantia de que uma informação provém da fonte anunciada.

1.2.5 CONFIDENCIALIDADE

Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

1.2.6 DISPONIBILIDADE

Garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário.

1.2.7 ELOS DE COORDENAÇÃO DO STI

São os setores pertencentes aos Órgãos de Direção-Geral e de Direção Setorial (ODGS) e ao GABAER, responsáveis pela coordenação de suas atividades de TI junto ao DECEA, Órgão Central do STI.

1.2.8 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.

1.2.9 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.

1.2.10 ELOS USUÁRIOS

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.

1.2.11 INCIDENTE DE SEGURANÇA

Qualquer evento ou ocorrência que promova uma ou mais ações que comprometem ou possam vir a comprometer a confidencialidade, a integridade ou a disponibilidade de qualquer ativo de informação.

1.2.12 INTEGRIDADE

Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

1.2.13 INTERFACE COM BIOMETRIA

É o tipo de interface para controle de acesso a instalações físicas ou a recursos de TI, cujo funcionamento é baseado no 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.

1.2.14 IRRETRATABILIDADE

Impossibilidade de negar o fato de ser o autor ou a fonte de determinada informação.

1.2.15 PLANO DE CONTINUIDADE DE SISTEMAS

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:

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

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

- evitar o agravamento das situações de crise envolvendo o sistema.

1.2.16 PROGRAMA MALICIOSO

O termo refere-se a qualquer código ou programa inesperado ou mal-intencionado, cujo objetivo é causar danos ao computador em que for executado. Estes danos podem atingir os componentes físicos da máquina ou os dados nela armazenados. Nem todos os programas ou códigos maliciosos são do tipo conhecido como vírus.

1.2.17 SEGURANÇA DA INFORMAÇÃO

Conjunto de normas, procedimentos técnico-administrativos e soluções tecnológicas que, aplicados de maneira integrada, visam estabelecer níveis aceitáveis de proteção dos ativos de informação de interesse da instituição, estejam eles armazenados em meio digital, em documentação impressa ou trafegando em redes de comunicação de dados, garantindo a sua confidencialidade, integridade e disponibilidade.

1.2.18 SENHA SEGURA

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. Nos padrões atuais, uma senha é considerada segura quando possui, no mínimo, 8 caracteres alfanuméricos, sendo pelo menos um deles não-alfabético. Uma senha segura não deve estar associada a qualquer característica de cunho pessoal do seu detentor, tal como: placa de veículo, data natalícia, etc.

1.2.19 SERVIÇOS DE REDE

São serviços ou funcionalidades, tais como: correio eletrônico, acesso a páginas web, transferência de arquivos, acesso a INTERNET etc.

1.2.20 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.

1.2.21 SMART CARD

É um cartão semelhante a um cartão de crédito 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 uma senha pessoal, determinada pelo titular. Para sua utilização o smart card depende de um dispositivo de hardware adicional instalado no computador: a leitora de smart cards.

1.2.22 REDES SEM-FIO

Soluções técnicas de rede, cujo objetivo é estabelecer conectividade entre estações em uma rede local ou entre segmentos de redes locais. Estas soluções técnicas aquelas baseadas nas diversas variações do padrão IEEE 802.11.

1.2.23 TOKEN

É um hardware portátil com a mesma funcionalidade dos smart cards. No entanto, seu formato não é o de um cartão e não necessita de leitoras específicas, sendo normalmente acessado a partir de sua conexão a uma interface USB comum.

1.2.24 VIDEOCONFERÊNCIA

Solução técnica baseada em recursos de rede de dados que permite o contato visual e sonoro entre pessoas ou grupos de pessoas que estão em lugares diferentes, dando a sensação de que os interlocutores encontram-se no mesmo local.

1.2.25 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.

1.3 ÂMBITO

Esta Norma se aplica a todas as Organizações do COMAER.

2 OBJETIVOS

2.1 A garantia dos níveis adequados de confidencialidade, disponibilidade e integridade dos ativos de informação de interesse do COMAER que tramitam em redes de comunicação de dados ou sejam armazenados em mídia gerenciada por Sistemas de Informação ou por Sistemas Gerenciadores de Bancos de Dados.

2.2 A garantia da autenticidade e da irretratabilidade das transações que manipulam os ativos de informação de interesse do COMAER

2.3 A conscientização do efetivo de pessoal do COMAER e dos colaboradores terceirizados, sobre a importância de conhecer e aplicar as normas e os procedimentos de segurança da informação.

2.4 O apoio à operacionalização dos procedimentos de classificação, de processamento, de envio, de armazenamento e de descarte das informações sensíveis que integram os sistemas de TI.

2.5 O apoio ao emprego adequado de certificados digitais, em conformidade com a Infra-estrutura de Chaves Públicas do Brasil (ICP-Brasil).

2.6 A implantação de requisitos de segurança da informação nas atividades de contratação, de desenvolvimento, de operação e de manutenção de sistemas aplicativos de TI.

3 PROCEDIMENTOS DE SEGURANÇA

Estabelecem as condições necessárias, que devem ser respeitadas por todos os Elos do STI, a fim de garantir um nível adequado de segurança para as informações que compõem os Sistemas de TI do COMAER.

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 e a disponibilidade dos sistemas.

3.2 CONTROLE DE ACESSO LÓGICO

3.2.1 O acesso lógico aos sistemas de TI deve ser protegido por meio do emprego de senhas seguras e, 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.

3.3 PROGRAMAS MALICIOSOS

3.3.1 Deverão ser instalados e configurados, nos equipamentos servidores e nas estações de trabalho de TI, programas antivírus e outros utilitários de software que previnam ou mitiguem ataques gerados por programas maliciosos.

3.3.2 É vedada a utilização de serviços de mensagem instantânea ou de bate-papo disponíveis na Internet, por estes serem, comprovadamente, grandes difusores de programas maliciosos.

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.

3.4.2 O acesso aos serviços de rede da INTRAER e da Internet deverá ser negado quando envolver procedimentos 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 DECEA, Órgão Central do STI.

3.4.4 É vedada 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 a INTRAER, qualquer que seja o local da implantação, só poderá ocorrer a partir de aprovação prévia do DECEA.

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 DECEA.

3.5 COMPUTAÇÃO MÓVEL

3.5.1 A utilização de equipamentos do tipo "lap top", "notebook", "palm top" e etc deverá ser precedida de medidas visando à orientação dos usuários dos equipamentos e, se necessário, do emprego de soluções de criptografia de dados. Deve ser evitado, sempre que possível, o armazenamento de informações sensíveis em equipamentos de computação móvel.

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.

3.7 AUDITORIA DE SISTEMAS

3.7.1 Devem ser estabelecidos registros em mídia que permitam, posteriormente, a realização de auditorias 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.

3.8 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 no contrato entre as partes.

3.9 MONITORAÇÃO DE ATIVIDADES

3.9.1 Devem ser estabelecidos procedimentos de monitoração 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.

3.10 PLANO DE CONTINUIDADE DE SISTEMAS

3.10.1 Cada um dos sistemas de TI considerados críticos pelo COMAER deve estar protegido por um Plano de Continuidade de Sistemas. 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 SOLUÇÕES TÉCNICAS BASEADAS EM REDES SEM-FIO

3.11.1 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 DECEA.

3.11.2 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 DECEA, mesmo que estas atividades ou sistemas estejam isolados da INTRAER e que sua operação tenha caráter temporário.

3.12 EMPREGO DE VOIP

3.12.1 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 180 dias de sua data prevista de entrada em operação.

3.13 EMPREGO DE VIDEOCONFERÊNCIA

3.13.1 Os projetos que visam à implantação de soluções de videoconferência para atender a necessidades de Organizações do COMAER deverão ser submetidos ao DECEA para análise e aprovação, com antecedência mínima de 180 dias de sua data prevista de entrada em operação.

4 COMPETÊNCIAS

4.1 DO DECEA

São competências do DECEA:

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) Estabelecer normas, padrões e metodologias que regularizem o emprego de criptografia e certificados digitais nos sistemas de TI de interesse do COMAER; e
c) 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.

4.2 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;
b) Encaminhar ao DECEA 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;
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.

4.3 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;
b) Estabelecer um plano de resposta a incidentes envolvendo a segurança dos sistemas de TI sob sua responsabilidade; e
c) 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.

4.4 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.

5 ATRIBUIÇÕES

Aos Comandantes, Chefes e Diretores incumbe garantir, no âmbito de suas Organizações, o cumprimento dos procedimentos de segurança descritos nesta Norma. No caso específico da constituição de Grupos de Trabalho que atuam como Elos Especializados do STI, a incumbência será do Presidente do GT.

6 DISPOSIÇÕES FINAIS

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

6.2 Os casos não previstos nesta Norma serão submetidos à apreciação do Diretor-Geral do DECEA.

7 REFERÊNCIAS

BRASIL. Ministério da Aeronáutica. *Política da Aeronáutica*: **DMA 14-5**. [Brasília, DF], 23 mar. 1998.

BRASIL. Comando da Aeronáutica. *Política do Comando da Aeronáutica para a Tecnologia da Informação*: **DCA 14-7**. [Brasília, DF], ___ dez. 2004.

BRASIL. 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.

BRASIL. Governo Federal. *Altera o Decreto-Lei Nr. 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências*: **Lei Nº. 9.983**. [Brasília, DF], 14 jul. 2000.

_____. *Código de prática para a gestão da segurança da informação*: **NBR ISO/IEC 17799**. set. 2005.

_____. Evaluation Criteria for IT Security – Part 3: Security Assurance Requirements: **ISO/IEC 15408**. out. 2005.