MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-35

MODELO DE ESTAÇÃO DE TRABALHO SEGURA DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2015

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

TECNOLOGIA DA INFORMAÇÃO

ICA 7-35

MODELO DE ESTAÇÃO DE TRABALHO SEGURA DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2015

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

PORTARIA DECEA Nº 68/DGCEA, DE 20 DE MARÇO DE 2015.

Aprova a edição da Instrução que estabelece o Modelo de Estação de Trabalho Segura do Departamento de Controle do Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe conferem o art. 195, inciso IV, do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1049/GC3, de 11 de novembro de 2009, e o art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 1.668/GC3, de 16 de setembro de 2013, resolve:

Art. 1º Aprovar a edição da ICA 7-35 "Modelo de Estação de Trabalho Segura do Departamento de Controle do Espaço Aéreo", que com esta baixa.

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

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

(Publicada no BCA nº 067, de 10 de abril de 2015)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar o Modelo de Estação de Trabalho Segura do Departamento de Controle do Espaço Aéreo e suas Organizações Militares Subordinadas, orientando os chefes dos Elos de Serviço de TI, subordinados ao DECEA, acerca das ações e recomendações de segurança da informação para estações de trabalho.

1.2 ÂMBITO E GRAU DE SIGILO

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

1.3 ABRANGÊNCIA

Todos os usuários de TI que utilizam estações de trabalho do Departamento de Controle do Espaço Aéreo e OM Subordinadas.

1.4 SIGLAS

BIOS - *Basic Input / Output System* (Sistema Básico de entrada e saída)
COMAER - Comando da Aeronáutica
DECEA - Departamento de Controle do Espaço Aéreo
DLP - *Data Loss Protection* (Proteção de perda de dados)
EPO - McAfee ePolicy Orchestrator
GABAER - Gabinete do Comandante da Aeronáutica
HD - *Hard Disk* (Disco Rígido)
ICA - Instrução do Comando da Aeronáutica
ODGS - Órgãos de Direção-Geral e de Direção Setorial
OM - Organização Militar
SDTE - Subdepartamento Técnico do DECEA
SI - Segurança da Informação
SSSI - Seção de Segurança de Sistemas da Informação
STI - Sistema de Tecnologia da Informação do Comando da Aeronáutica
TI - Tecnologia da Informação
USB - *Universal Serial Bus* (Barramento Serial Universal)

1.5 DEFINIÇÕES

1.5.1 APLICATIVOS

São programas de computador que têm por objetivo ajudar o seu usuário a desempenhar uma tarefa específica, em geral relacionada à criação e ao processamento de dados.

1.5.2 CONTA DE USUÁRIO ADMINISTRADOR

É a credencial de acesso especial, com nível de acesso e permissões que possibilitam a execução de tarefas administrativas em uma estação de trabalho, tais como a instalação de aplicativos e a modificação de configurações do sistema operacional.

1.5.3 CONTA DE USUÁRIO PADRÃO

É a credencial de acesso de um usuário em uma estação de trabalho, com nível de acesso e permissões limitados ao mínimo necessário para desempenhar suas atividades na OM, e padronizada para todos os usuários.

1.5.4 CRIPTOGRAFIA

São princípios e técnicas pelas quais a informação se transforma de uma forma inteligível para uma impossível de ser compreendida, e apenas o usuário detentor da chave de criptografia correta consegue recuperar a informação original.

1.5.5 ELOS DE COORDENAÇÃO DO STI

São os setores pertencentes aos Órgãos de Direção-Geral e de Direção Setorial (ODGS) e ao GABAER, responsáveis pela coordenação de suas atividades de TI junto ao Órgão Central. Esses setores terão a sua constituição estabelecida nos Regulamentos e/ou Regimentos Internos das OM a que estão subordinados.

1.5.6 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.

1.5.7 ELOS USUÁRIOS DO STI

São todos os militares e servidores civis e funcionários de empresas contratadas pelo COMAER 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.

1.5.8 ESTAÇÃO DE TRABALHO

Computador fornecido pelo DECEA para que o usuário desempenhe suas funções diárias.

1.5.9 *FIREWALL* DO SISTEMA OPERACIONAL

É um *software* pré-instalado em alguns sistemas operacionais. Possui filtro de pacotes que restringe o fluxo dos dados recebidos e enviados pelo seu computador.

1.5.10 IMAGEM DE DISCO PADRÃO

É uma cópia do disco rígido de uma estação de trabalho, que pode ser utilizada para replicar uma configuração padrão a várias estações de forma mais eficiente. É geralmente criada a partir de uma estação de trabalho configurada seguindo todas as normas vigentes e com as versões homologadas de aplicativos necessários à rotina dos usuários.

1.5.11 *PATCH*

Atualização de *software* ou sistema operacional, disponibilizada pelo fabricante deste, com a finalidade de corrigir vulnerabilidades e erros constatados durante o seu ciclo de vida.

1.5.12 *SERVICE PACK*

É uma coleção de atualizações de *software* ou sistema operacional, disponibilizada pelo fabricante deste em um único pacote. Em geral, os fabricantes utilizam este método de atualização quando o número de correções atinge um limite arbitrário.

1.5.13 SISTEMA OPERACIONAL

É um *software* responsável pela criação do ambiente de trabalho da estação de trabalho. Consiste na camada intermediária entre o aplicativo e o *hardware*. Além de interpretador básico de comandos, é a interface pela qual o usuário tem acesso aos recursos que o *hardware* oferece.

1.5.14 VÍRUS

É um *software* malicioso desenvolvido por programadores. Tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios.

1.5.15 VULNERABILIDADE

É definida como uma falha no projeto ou implementação de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança

de um computador.

2 RESPONSABILIDADES

2.1 ELO DE COORDENAÇÃO DO STI NO DECEA

2.1.1 O Órgão de Coordenação de TI no DECEA é o Subdepartamento Técnico, que tem por responsabilidade estabelecer normas, padrões e metodologias relativas ao Modelo de Estação de Trabalho Segura, e realizar, a seu critério, auditorias nas OM subordinadas, verificando a aderência às orientações desta Instrução.

2.2 ELOS DE SERVIÇOS DO STI NO DECEA E OM SUBORDINADAS

2.2.1 Os Elos de Serviços do STI no DECEA e OM subordinadas são as Seções de TI destas OM, que têm por responsabilidade:

2.2.1.1 Coordenar a execução das instruções presentes nesta Norma, bem como propor ao SDTE ações de melhoria para o processo.

2.2.1.2 Homologar as estações de trabalho da OM e realizar as suas manutenções, quando necessário.

2.2.1.3 Atender às solicitações dos usuários de informática quanto à instalação e manutenção de *hardware* e *software* das estações de trabalho.

2.3 ELOS USUÁRIOS DO STI NO DECEA E OM SUBORDINADAS

2.3.1 Os Elos Usuários do STI no DECEA e OM subordinadas têm por responsabilidade:

2.3.1.1 Zelar pelo bom uso das estações de trabalho.

2.3.1.2 Informar qualquer suspeita de uso indevido das estações de trabalho e possíveis violações aos recursos de informática ao Elo de Serviço de TI de sua OM.

2.3.1.3 Informar incidentes de segurança à Sessão de Segurança da Informação da SSSI, utilizando as normativas em vigor, padronizadas pelo SDTE.

2.4 SEÇÕES DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO

2.4.1 As Seções de Segurança de Sistemas da Informação das OM Subordinadas têm por responsabilidade:

2.4.1.1 Orientar os usuários da OM acerca das boas práticas de segurança da informação.

2.4.1.2 Analisar os incidentes e recomendar ações corretivas e preventivas aos usuários da OM.

2.4.1.3 Realizar auditorias de segurança.

3 RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO E BOAS PRÁTICAS

3.1 INSTALAÇÃO E CONFIGURAÇÃO DO SISTEMA OPERACIONAL

3.1.1 Para evitar que pessoas não autorizadas obtenham privilégios administrativos e tenham acesso a arquivos confidenciais, os Elos de Serviços devem proteger com senha o Gerenciamento de *Boot*.

3.1.2 Os Elos de Serviços devem configurar todas as estações de trabalho para que solicitem autenticação por senha ao entrar no *Setup* da BIOS.

3.1.3 A senha para acesso ao *Setup* deve ser única para todas as estações de trabalho que estão sob a responsabilidade dos Elos de Serviços.

3.1.4 A senha de acesso ao *Setup* das estações de trabalho deve ser mantida sob sigilo, devendo o seu conhecimento ser restrito aos técnicos que atuam nos Elos de Serviços.

3.1.5 Todas as estações de trabalho devem ter o disco rígido como sua inicialização de *boot* primário.

3.1.6 Os Elos de Serviços devem desabilitar o *boot* por dispositivos USB, CD/DVD ou rede em todas as estações de trabalho.

3.1.7 Recomenda-se que nas estações de trabalho os discos rígidos sejam divididos em, pelo menos, duas partes, separando-se os arquivos de sistemas e os dados locais.

3.1.8 Recomenda-se o uso de criptografia nos discos rígidos de *notebooks*, para reduzir o risco de vazamento de informações sensíveis. A opção pela criptografia do disco é geralmente feita durante a instalação do sistema operacional.

3.1.9 Recomenda-se que os serviços de sistema que não serão utilizados sejam desabilitados, para otimizar o desempenho e a segurança da estação de trabalho.

3.2 ATUALIZAÇÕES E CORREÇÕES

3.2.1 Depois de o sistema operacional ter sido devidamente instalado e configurado, é necessário verificar se não existem correções (*patch ou service pack*) para vulnerabilidades conhecidas nos componentes instalados.

3.2.2 Os Elos de Serviços devem possuir um mecanismo de distribuição automatizada de correções, verificar diariamente o lançamento de novas correções, além de gerenciar a eficácia da distribuição das correções nas estações de trabalho.

3.2.3 Os Elos de Serviços devem aplicar apenas as correções que já foram homologadas em ambiente de teste.

3.2.4 Os Elos de Serviços devem restringir-se às correções publicadas que solucionem problemas em componentes que estejam efetivamente instalados no seu sistema.

3.2.5 Antes de atualizar a versão de um sistema operacional, os Elos de Serviços devem fazer

uma análise da nova versão para avaliar se os aplicativos que serão instalados na estação de trabalho funcionarão sem conflitos.

3.3 ADMINISTRAÇÃO DE CONTAS DE USUÁRIOS

3.3.1 Contas de usuário administrador não devem ser concedidas a nenhum usuário, independentemente do nível hierárquico que ele ocupa na OM.

3.3.2 As credenciais de contas de usuários administradores devem ser mantidas sob sigilo, devendo o seu conhecimento ser restrito aos técnicos que atuam nos Elos de Serviços.

3.3.3 Não é permitido aos usuários conhecer ou possuir as credenciais de acesso a contas de usuário administrador.

3.3.4 A senha para contas de usuário administrador deve cumprir, no mínimo, as exigências estabelecidas pelo Elo Central do STI na Política de Uso de Recursos Computacionais (Anexo A da NSCA 7-13).

3.3.5 A senha para contas de usuário administrador deve ser modificada, no mínimo, segundo as exigências estabelecidas pelo Elo Central do STI na Política de Uso de Recursos Computacionais (Anexo A da NSCA 7-13).

3.3.6 Recomenda-se que a senha para contas de usuário administrador sejam modificadas quando um técnico, que atua no respectivo Elo de Serviço, saia da equipe técnica.

3.3.7 As contas de usuário administrador devem ser usadas apenas em situações nas quais uma conta padrão não tenha privilégios suficientes para realizar uma operação.

3.3.8 Recomenda-se que as contas de usuário administrador não sejam mantidas com identificadores padrão já conhecidos, tais como “administrador” e “admin”.

3.3.9 Recomenda-se que as estações de trabalho possuam apenas uma conta de usuário administrador.

3.3.10 Não utilizar conta de usuário administrador nas atividades cotidianas, pois arquivos essenciais para o funcionamento do sistema operacional podem ser acidentalmente apagados ou ser instalado inadvertidamente um código malicioso, levando ao acesso irrestrito à estação de trabalho.

3.3.11 A conta de usuário padrão deve ser a usada para todo o efetivo, pois contém privilégios que a maioria dos usuários necessita para realizar tarefas rotineiras.

3.3.12 A conta de usuário padrão deve permitir ao usuário alterar configurações pessoais, acessar a internet, ler *e-mails*, redigir documentos, planilhas, apresentações e acessar os sistemas internos.

3.4 PROTEÇÃO DE *MALWARE*

3.4.1 Os Elos de Serviços devem instalar o antivírus padrão, disponibilizado pelo Órgão Central de TI do COMAER, em todas as estações de trabalho. O antivírus deve ser inserido

no EPO, independentemente do sistema operacional em uso.

3.4.2 Todas as estações devem ter instalados o módulo de Antivírus e o módulo de DLP.

3.4.3 As estações de trabalho devem possuir a última versão atualizada do antivírus quando forem disponibilizadas ao usuário final.

3.4.4 Os *softwares* de antivírus devem ser configurados de forma a permitir o gerenciamento de modo centralizado pelo EPO.

3.5 CRIAÇÃO DE IMAGEM DE DISCO PADRÃO

3.5.1 O Elo de Serviço deve, após a instalação, configuração e implementação dos itens de segurança da informação da estação de trabalho padrão, criar uma imagem de disco padrão para que seja replicada para outras estações de trabalho que venham a ser distribuídas.

3.5.2 A imagem de disco padrão deve ser atualizada mensalmente, para conter as atualizações do sistema e aplicativos.

3.6 SEGURANÇA FÍSICA

3.6.1 Os Elos de Serviços devem disponibilizar cabo de proteção contra furtos junto com os *notebooks* e orientar o usuário para que o mesmo seja usado.

3.6.2 Os equipamentos devem ser entregues com lacre de segurança, independentemente de haver ou não lacre do fabricante. Os Elos de Serviços devem providenciar lacre que somente possa ser rompido ou substituído por pessoal técnico autorizado pela Seção.

3.6.3 O equipamento da OM que possuir trava da tampa pelo *Setup* deve ter esse recurso utilizado de maneira que a tampa seja aberta apenas pelos Elos de Serviços.

3.7 MELHORES PRÁTICAS

3.7.1 Nenhum tipo de *software* ou *hardware* deve ser instalado sem autorização da equipe técnica ou de segurança.

3.7.2 Não é permitido alterar a configuração de *hardware* e de *software* da estação de trabalho sem autorização dos Elos de Serviços.

3.7.3 O usuário não pode conectar qualquer recurso de informática não autorizado pelos Elos de Serviços. Exemplo: Dispositivo para acesso a redes sem fio (3G, 4G, Wi-fi), *notebook*, roteador *wireless*, *tablet*, impressora etc.

4 DISPOSIÇÕES FINAIS

4.1 O Modelo de Estação de Trabalho Segura apresentado neste documento é de caráter geral, devendo ser revisado periodicamente a cada trinta e seis meses, ou quando fato relevante demandar atualização extemporânea.

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

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

REFERÊNCIAS

BRASIL. Associação Brasileira de Normas Técnicas. *Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação*: **NBR ISO/IEC 27002**. Rio de Janeiro, RJ, 2013.

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

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. *Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica:* **NSCA 7-13**. Rio de Janeiro, RJ, 2013.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Gerência de Configuração de Tecnologia da Informação no Âmbito do DECEA:* **DCA 7-4**. Rio de Janeiro, RJ, 2013.

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

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

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Processo de Controle de Acesso à Rede Interna do DECEA:* **ICA 7-30**. Rio de Janeiro, RJ, 2013.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Processo de Gestão de Mudanças de Ativos de Tecnologia da Informação do DECEA:* **ICA 7-24**. Rio de Janeiro, RJ, 2013.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Estrutura e Competências do Sistema de Tecnologia da Informação do Comando da Aeronáutica:* **NSCA 7-7**. Rio de Janeiro, RJ, 2004.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Glossário da Aeronáutica:* **MCA 10-4**. Rio de Janeiro, RJ, 2001.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Manual de Abreviaturas, Siglas e Símbolos da Aeronáutica:* **MCA 10-3**. Rio de Janeiro, RJ, 2003.