MINISTÉRIO DA DEFESA

COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-53

SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E USO DOS RECURSOS COMPUTACIONAIS DO COMAE

2022

MINISTÉRIO DA DEFESA

COMANDO DA AERONÁUTICA

COMANDO DE OPERAÇÕES AEROESPACIAIS

TECNOLOGIA DA INFORMAÇÃO

ICA 7-53

SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E USO DOS RECURSOS COMPUTACIONAIS DO COMAE

2022

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
COMANDO DE OPERAÇÕES AEROESPACIAIS

PORTARIA Nº 8/DIVCSI, DE 18 DE FEVEREIRO DE 2022.

Aprova a edição da instrução que dispõe sobre a segurança em tecnologia da informação e uso dos recursos computacionais do Comando de Operações Aeroespaciais.

O COMANDANTE DE OPERAÇÕES AEROESPACIAIS, no uso das atribuições que lhe conferem os incisos I e VI do art. 8º do Regulamento do Comando de Operações Aeroespaciais (ROCA 20-12), aprovado pela Portaria nº 1.238/GC3, de 12 de novembro de 2020, resolve:

Art. 1º Aprovar a edição da ICA 7-53 "Segurança em Tecnologia da Informação e Uso dos Recursos Computacionais do COMAE".

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

No Imp Ten Brig Ar SÉRGIO ROBERTO DE ALMEIDA
Cmt de Operações Aeroespaciais

Maj Brig Ar ALCIDES TEIXEIRA BARBACOVI

(Publicada no BCA nº 045, de 8 de março de 2022)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES 9
1.1 FINALIDADE 9
1.2 OBJETIVO 9
1.3 CONCEITUAÇÕES 9
1.3.1 ACESSO REMOTO 9
1.3.2 ADMINISTRADOR DE REDE 9
1.3.3 ANTIVÍRUS 9
1.3.4 BLUETOOTH 9
1.3.5 CONTA DE USUÁRIO 9
1.3.6 CONHECIMENTO 9
1.3.7 DADO 9
1.3.8 DMZ 10
1.3.9 FIREWALL 10
1.3.10 PHISHING 10
1.3.11 REDE SEM FIO 10
1.3.12 SENHA 10
1.3.13 USUÁRIO 10
1.3.14 VPN 10
1.4 ÂMBITO E GRAU DE SIGILO 10
2 SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E USO DOS RECURSOS COMPUTACIONAIS 11
2.1 PREMISSAS 11
2.2 RECURSOS COMPUTACIONAIS E REGRAS DE UTILIZAÇÃO 11
2.2.1 CONTAS DE ACESSO À REDE 11
2.2.2 ESTAÇÃO DE TRABALHO 11
2.2.3 E-MAIL CORPORATIVO 12
2.2.4 INTERNET, INTRAER E REDES LOCAIS DO COMAE 12
2.2.5 REDE SEM FIO DO COMAE 13
2.2.6 INTERNET DEDICADA AOS SERVIÇOS OPERACIONAIS 13
2.2.7 SOFTWARE E SISTEMAS 13
2.2.8 ANTIVÍRUS E CÓDIGOS MALICIOSOS. 14
2.2.9 ACESSO REMOTO 14
2.2.10 DISPOSITIVOS MÓVEIS 14
2.2.11 ARMAZENAMENTO DE ARQUIVOS 14
2.2.12 EXERCÍCIOS OPERACIONAIS 14
2.2.13 FIREWALL E RECURSOS COMPUTACIONAIS NA DMZ 14
2.2.14 INFRAESTRUTURA FÍSICA 15
2.2.15 AUDITORIA 15
2.2.16 TRATAMENTO DE INCIDENTES DE SEGURANÇA 15
2.3 RECURSOS HUMANOS DE ADM DA INFRAESTRUTURA DE TI 15
2.4 RESPONSABILIDADES 16
2.4.1 DA EQUIPE DE ADMINISTRAÇÃO E SUPORTE DE REDE 16
2.4.2 DA EQUIPE DE SEGURANÇA CIBERNÉTICA 17
2.4.3 DA EQUIPE DE SUPORTE AO USUÁRIO 17
2.4.4 DOS CHEFES DE DIVISÃO, SEÇÃO E ASSESSORIA 17
2.4.5 DOS USUÁRIOS 17
2.5 RESTRIÇÕES 18
2.5.1 AOS USUÁRIOS SERÁ VEDADO 18

2.5.2 AOS ADMINISTRADORES E TÉCNICOS DE TI É VEDADO 20
3 DISPOSIÇÕES FINAIS 21
REFERÊNCIAS 22

PREFÁCIO

O Comando de Operações Aeroespaciais (COMAE), Organização do Comando da Aeronáutica (COMAER) prevista pelo Decreto nº 6.834, de 30 de abril de 2009, alterado pelo Decreto nº 9.077, de 8 de junho de 2017, é o órgão central de Sistema de Defesa Aeroespacial Brasileiro (SISDABRA), subordinado diretamente ao Comandante da Aeronáutica em tempo de paz e, quando em situação de conflito, ao Presidente da República. É um Comando Operacional Conjunto, permanentemente ativado, ao qual compete realizar a defesa aeroespacial do território nacional contra todas as formas de ameaça, a fim de assegurar o exercício da soberania no espaço aéreo brasileiro, sintetizado na missão: "Empregar o poder aeroespacial brasileiro com vistas a garantir a soberania do espaço aéreo e a integração do Território Nacional".

Como qualquer outra Organização do mundo contemporâneo, o COMAE faz uso da Tecnologia da Informação (TI) como ferramenta imprescindível para o suporte ao cumprimento de sua missão. Para tanto, a OM dispõe de uma estrutura de rede de computadores que interliga os Centros que lhe são subordinados, integrando e compartilhando recursos tecnológicos essenciais à execução de suas atividades administrativas e operacionais.

Considerando a sua importância no contexto da Defesa Nacional e o uso intenso dos recursos de TI, torna-se importante considerar os aspectos relacionados ao Espaço Cibernético, uma região sem fronteiras definidas, formada por diversas camadas, com a presença de ameaças virtuais. Essa dimensão operacional passou a servir de suporte à espionagem para as mais diversas finalidades, sendo inclusive explorada como campo de batalha das guerras contemporâneas, principalmente pelo fato de possuir características singulares, como possibilidade do anonimato, ação em velocidade, precisão dos ataques e o alto poder de causar danos com um efeito colateral extremamente reduzido.

Vale salientar que os crimes virtuais estão se tornando comuns e que as Organizações Governamentais estão entre os principais alvos dos criminosos digitais. Nesse cenário, a vulnerabilidade cibernética, muitas vezes, ocorre pela falha ou fragilidade humana, sendo potencializada pelo simples descuido, pela omissão, pela preguiça e pela vaidade, entre outras.

Diante dessa conjuntura, é necessário que o COMAE aprimore a Segurança Cibernética para fazer frente a todas as ameaças potenciais que estão atreladas ao uso da Tecnologia da Informação. Para tanto, diversas ações devem ser adotadas em busca de um ambiente digital mais seguro, ressaltando-se a adoção de medidas para reforçar o "elo mais fraco da corrente", o ser humano.

Sendo assim, o propósito desta instrução é estabelecer regras de segurança em tecnologia da informação no COMAE, além de contribuir para reforçar a segurança da Organização, reduzindo suas vulnerabilidades sob o ponto de vista do uso do Espaço Cibernético. O documento estabelece regras e orientações que visam não só, o aperfeiçoamento da proteção da estrutura composta por todos os recursos computacionais do COMAE, como também, adotar boas práticas no uso desses recursos e, principalmente, gerar no efetivo uma mudança de hábitos que certamente irá retroalimentar todo o processo de forma positiva.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Apresentar as regras de segurança em Tecnologia da Informação (TI) e uso dos recursos computacionais do Comando de Operações Aeroespaciais (COMAE).

1.2 OBJETIVO

Estabelecer as diretivas para a implementação e manutenção dos mecanismos de segurança lógica e física dos recursos computacionais existentes no COMAE, dos papéis e responsabilidades da Equipe de TI e de Administração da Rede e a conduta dos usuários e Centros subordinados no uso dos recursos de TI da Organização.

1.3 CONCEITUAÇÕES

A interpretação de significado da terminologia empregada deve ser feita de acordo com o consagrado no vernáculo, nos documentos normativos em vigor no Ministério da Defesa (MD) e no Comando da Aeronáutica (COMAER) ou conforme explicitado a seguir.

1.3.1 ACESSO REMOTO

Acesso a qualquer recurso disponibilizado na rede do COMAE, bem como na INTRAER, por intermédio de outra rede, dispositivo, ou meio estranho ao ambiente controlado pela equipe de TI deste Comando.

1.3.2 ADMINISTRADOR DE REDE

Membro da equipe de TI designado para administrar a rede de comunicação de dados local da OM.

1.3.3 ANTIVÍRUS

Sistema de proteção do computador que detecta e elimina programas maliciosos.

1.3.4 BLUETOOTH

Bluetooth é uma tecnologia de comunicação sem fio que permite que computadores, celulares, *tablets*, TVs e afins troquem dados entre si e se conectem a mouses, teclados, fones de ouvido, caixas de som, impressoras e outros dispositivos por meio de ondas eletromagnéticas.

1.3.5 CONTA DE USUÁRIO

Identificação individual, constituída por um código e uma senha, que permite o acesso do usuário à rede e aos recursos nela compartilhados.

1.3.6 CONHECIMENTO

É o produto resultante do processamento do(s) dado(s) de interesse para o processo decisório, com vistas ao cumprimento da missão da Aeronáutica.

1.3.7 DADO

É o elemento ou a base para a formação do juízo, a ser utilizado na produção do conhecimento.

1.3.8 DMZ

Desmilitarized Zone (DMZ) é uma subrede que fica situada entre uma rede confiável e outra não confiável, garantindo a segurança por meio do isolamento.

1.3.9 FIREWALL

Dispositivo de rede que monitora e controla o tráfego de borda por meio da utilização de regras específicas.

1.3.10 PHISHING

O termo *phishing* faz alusão à palavra em inglês *fishing*, que significa "pescaria", em tradução livre. O *phishing scam* é uma tentativa de fraude pela internet que utiliza "iscas", isto é, artifícios para atrair a atenção de uma pessoa e fazê-la realizar alguma ação. Mensagens consideradas *phishing* (ou *phishing scam*) estão entre os maiores perigos da internet. Essas tentativas de fraudes podem chegar por e-mail e resultar em consequências graves às vítimas, principalmente prejuízo financeiro.

1.3.11 REDE SEM FIO

Solução técnica de rede comumente utilizada para acesso à INTERNET, cujo objetivo é estabelecer conectividade entre equipamentos e um determinado ambiente de rede sem a utilização de conexão física por meio de cabos.

1.3.12 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.

1.3.13 USUÁRIO

Pessoa física com algum vínculo direto ou indireto com o COMAE, que esteja autorizada a utilizar, de alguma forma, mesmo que eventual, os Recursos Computacionais existentes.

1.3.14 VPN

Do inglês *Virtual Private Network*, 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 deve ser interceptado enquanto estiver passando pela rede pública.

1.4 ÂMBITO E GRAU DE SIGILO

Esta Instrução se aplica a todos os servidores militares ou civis, prestadores de serviços e fornecedores que venham a desempenhar atividades no âmbito do COMAE ou dos seus Centros subordinados.

Este documento é classificado como Ostensivo.

2 SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E USO DOS RECURSOS COMPUTACIONAIS

2.1 PREMISSAS

A presente Instrução define as principais regras de acesso, utilização e controle dos recursos computacionais do COMAE. Portanto, é o documento que contém as diretivas gerais no que diz respeito à segurança cibernética no âmbito deste Comando. Trata-se de uma Instrução com efeitos obrigacionais, a qual todos os Usuários, civis ou militares, de todos os setores e Centros da Organização, são responsáveis por sua observância.

Os detalhamentos operacionais e as medidas de implementação serão estabelecidas por intermédio dos processos internos, fazendo-os constar em suas respectivas Normas Padrão de Ação (NPA).

A equipe de Segurança Cibernética do COMAE representa o braço operacional desse Comando para fins de auditoria em todo o ambiente computacional da Organização, bem como para verificação de conformidade do emprego dos recursos computacionais com esta Instrução e demais normas de Tecnologia da Informação do COMAER. As ações de auditoria poderão ocorrer de forma inopinada, devendo desta maneira, receber a colaboração e cooperação dos demais setores da Organização.

2.2 RECURSOS COMPUTACIONAIS E REGRAS DE UTILIZAÇÃO

Os recursos computacionais do COMAE têm por finalidade servir às atividades técnicas, administrativas e operacionais que dão o devido suporte às Operações Aeroespaciais da Força Aérea Brasileira. Tais recursos devem ser utilizados exclusivamente para esse fim.

O uso dos recursos computacionais do COMAE está sujeito às leis federais, às normas e regulamentos do COMAER e às diretivas internas deste Comando.

A permissão de acesso aos recursos computacionais somente poderá ser concedida após análise de solicitação formal de abertura de Contas de Usuário direcionada à equipe de administração e suporte de rede da OM.

O acesso aos recursos computacionais do COMAE somente será autorizado para usuário devidamente autenticado pelo administrador de domínio da rede.

2.2.1 CONTAS DE ACESSO À REDE

Recurso por meio do qual o usuário tem acesso ao ambiente de rede.

A conta de acesso e a respectiva senha serão atribuídas com exclusividade para cada usuário, são intransferíveis, não devem ser compartilhadas com outras pessoas, tampouco ser armazenadas em arquivos eletrônicos, escritas em papel, inseridas em mensagens de e-mail ou qualquer outra forma de comunicação eletrônica.

2.2.2 ESTAÇÃO DE TRABALHO

Recurso por meio do qual cada usuário se conecta à rede para executar as tarefas relacionadas com as suas funções.

Todos os equipamentos conectados à rede devem ser obrigatoriamente integrados ao seu respectivo domínio.

Todas as estações de trabalho do COMAE devem ingressar no Servidor de Domínio da Organização e serem monitoradas via software de gestão de ativos de TI.

As entradas do tipo USB terão o recurso de acesso aos dispositivos portáteis de armazenamento restrito mediante mecanismos técnicos ou operacionais a serem implementados pela equipe de TI.

Concessões específicas a setores, usuários e/ou estações de trabalho para possibilitar o acesso a dispositivos de armazenamento portátil, após análise da equipe de TI, serão submetidas à apreciação do Chefe do Estado-Maior Conjunto do COMAE.

2.2.3 E-MAIL CORPORATIVO

Recurso de correio eletrônico disponibilizado pelo Comando da Aeronáutica para seu efetivo, devendo ser utilizado apenas para o tráfego de mensagens relacionadas com as atividades administrativas e funcionais em consonância com os interesses do Ministério da Defesa e das Forças Armadas.

As caixas postais do e-mail corporativo e seus conteúdos são de propriedade do Comando da Aeronáutica, sendo passíveis de monitoramento e não havendo expectativa de privacidade por parte dos usuários.

2.2.4 INTERNET, INTRAER E REDES LOCAIS DO COMAE

Os serviços de acesso à INTERNET e INTRAER estão disponíveis para os usuários como ferramenta de trabalho, devendo sua utilização guardar estrita relação com as atividades desenvolvidas no âmbito do COMAER, de acordo com a NSCA 7-1 e a ICA 7-5.

O acesso à INTERNET a partir dos equipamentos conectados à rede do COMAE será realizado, obrigatoriamente, via INTRAER, por meio do serviço oferecido pelo CCA-BR, mediante os critérios estabelecidos por aquele Centro de Computação e a utilização das credenciais de acesso ao Portal do Militar.

O acesso a qualquer serviço oferecido na INTERNET, que porventura não seja atendido pelos parâmetros estabelecidos no parágrafo anterior, deverá ser solicitado pelo interessado ao CCA-BR, seguindo as orientações divulgadas na página daquele Centro.

Em caso de resposta negativa ao pleito citado no parágrafo anterior, o Chefe do setor interessado deverá encaminhar a referida solicitação devidamente justificada e fundamentada para apreciação do CHEMC.

Caso a solicitação citada no parágrafo anterior seja aprovada pelo CHEMC, a equipe de administração e suporte de rede estudará a possibilidade técnica de atender ao pleito a partir de um ponto de acesso em rede segregada.

O acesso de dispositivos móveis à INTERNET por meio da rede sem fio do COMAE poderá ser realizado, desde que seja expressamente autorizado pelo CHEMC.

As redes locais devem ser segregadas física ou logicamente, utilizando-se para tal, o critério de níveis de segurança. Para designar o tipo de segregação, esse critério deve considerar os dados e os ativos presentes em cada rede.

Em conformidade com o item anterior, as redes e os ativos que se comunicam com a Rede Operacional de Defesa (ROD), a Sala de Guerra e outros meios de acesso à INTERNET que não sejam providos pelo Proxy Brasília, devem ser fisicamente segregados desde a sua borda.

A Rede de Área de Armazenamento (SAN) do COMAE deve permanecer fisicamente segregada.

Os ativos de DMZ que compõem os serviços SPA-GE, SISTRASAG e HF Militar não podem enviar requisições às demais redes do COMAE.

Nenhum equipamento do COMAE, desde a borda, quer sejam ativos de rede ou *endpoints*, que se comunique com a INTRAER, terá acesso à INTERNET, salvo àquela provida pelo Centro de Computação de Aeronáutica de Brasília (CCA-BR).

O tráfego entre as VLANS de usuários do COMAE e a sua DMZ poderá ser segregado logicamente, desde que o tráfego entre essas redes tenha ao menos dois ativos de segurança entre elas.

Regras de controle de acesso em equipamentos que realizam a função de roteamento entre as VLANS de usuários do COMAE devem garantir o isolamento entre elas, excetuando-se dessa premissa apenas a VLAN de serviços internos e a VLAN de serviços externos, para as quais serão aplicadas regras de acesso de acordo com a necessidade.

2.2.5 REDE SEM FIO DO COMAE

A rede sem fio do COMAE deverá, no mínimo, possuir a arquitetura preconizada na OTCA 009/DTI/2019 e obedecer aos critérios de segurança existentes nas demais normas do COMAER.

Em hipótese alguma, a rede sem fio do COMAE poderá ter comunicação com as demais redes locais da Organização.

O ingresso de dispositivos móveis na rede sem fio do COMAE, após a aprovação do CHEMC, deverá ser controlado via registro do endereço MAC do dispositivo e autenticação do usuário.

Todos os logs de acesso do usuário, na rede sem fio do COMAE, devem ser gerados e armazenados, conforme requisitos da Leis 12.965, de 23 de abril de 2014 e 13.709. de 14 de agosto de 2018.

2.2.6 INTERNET DEDICADA AOS SERVIÇOS OPERACIONAIS

Os serviços operacionais que exigirem acesso à internet dedicada, como o download de imagens satelitais, serão suportados por uma rede segregada fisicamente da INTRAER e de todas as outras redes da organização.

2.2.7 SOFTWARE E SISTEMAS

Somente a Equipe de TI do COMAE terá permissão e privilégios de sistema para proceder a instalação de Softwares nas Estações de Trabalho. Os perfis dos integrantes da equipe serão estabelecidos em NPA específica,

Todos os softwares a serem instalados no COMAE devem ser devidamente licenciados. É vedada a instalação/utilização de qualquer software nas estações de trabalho da OM, sem prévia homologação pela DTI ou pela equipe de segurança cibernética.

De acordo com o item 3.6.2 (NSCA 7-13), os processos de desenvolvimento e manutenção de sistemas e aplicativos devem ser acompanhados pela equipe de segurança cibernética que realizará os testes necessários para detectar as possíveis vulnerabilidades.

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

2.2.8 ANTIVÍRUS E CÓDIGOS MALICIOSOS.

Todas as estações de trabalho do COMAE devem contar com um software Antivírus, padronizado pela DTI e administrado pelas equipes de TI da OM.

2.2.9 ACESSO REMOTO

O acesso à INTRAER, via internet (VPN), poderá ser fornecido pelo CCA-BR mediante solicitação, seguindo as orientações divulgadas na página daquele Centro.

2.2.10 DISPOSITIVOS MÓVEIS

É vedada a conexão de dispositivos particulares às estações de trabalho e às redes locais do COMAE.

É vedado o uso de dispositivos móveis em salas de reunião, operação, exercício e demais ambientes classificados como sensíveis.

2.2.11 ARMAZENAMENTO DE ARQUIVOS

Os arquivos, relacionados às atividades dos setores do COMAE, devem ser armazenados em pastas específicas disponíveis na rede administrativa da OM.

As pastas devem ser segregadas de acordo com as credenciais de acesso e a necessidade de conhecer de cada usuário da rede.

O acesso, a manipulação e o armazenamento de arquivos sigilosos ou de acesso restrito devem ser realizados com obediência total às normas do COMAER, bem como a legislação pertinente à matéria.

Os arquivos armazenados localmente nas estações de trabalho não farão parte dos procedimentos de backup da OM.

O usuário é o único responsável pelos arquivos pessoais que possam existir localmente nas estações de trabalho do COMAE. Esses equipamentos, bem como o conteúdo neles armazenados, para todos os efeitos, não estão sujeitos a qualquer regime de privacidade e são passíveis de monitoramento e inspeção, sem prévio aviso, pela equipe de segurança da rede, em consonância com as normas e legislação vigente.

2.2.12 EXERCÍCIOS OPERACIONAIS

Os Exercícios Operacionais realizados no âmbito do COMAE deverão contar com uma infraestrutura de TI específica, totalmente segregada das redes locais da Organização.

Os recursos computacionais disponibilizados para um determinado Exercício Operacional poderão ser customizados, no intuito de atender às suas necessidades específicas, desde que todos os requisitos estejam listados no respectivo Plano de Operação e sejam comunicados em tempo hábil às equipes de TI responsáveis.

Em nenhuma hipótese, os recursos computacionais dedicados aos Exercícios Operacionais poderão ser compartilhados com aqueles utilizados nas redes locais do COMAE.

2.2.13 FIREWALL E RECURSOS COMPUTACIONAIS NA DMZ

A rede administrativa do COMAE deve contar com uma infraestrutura de FIREWALL de modo que o mesmo seja o único ponto de entrada e saída, filtrando todo o

tráfego de informações entre a rede local e outras redes de forma a minimizar os incidentes de segurança.

Deve ser adotada a posição de negação padrão bloqueando todo e qualquer tráfego entre as redes, exceto aqueles serviços necessários para as atividades funcionais.

Sempre que for necessária a liberação de algum serviço para acesso externo, este deve ser disponibilizado em uma zona desmilitarizada (DMZ) onde devem ser feitos os controles necessários para a proteção e o monitoramento de tentativas de invasão, negação de serviços, dentre outros.

2.2.14 INFRAESTRUTURA FÍSICA

Servidores, roteadores, switches e demais equipamentos utilizados na manutenção e administração dos recursos computacionais do COMAE, deverão estar em salas exclusivas e com acesso restrito às equipes de TI.

2.2.15 AUDITORIA

Além do monitoramento diário, bem como das intervenções necessárias para eliminar eventuais vulnerabilidades encontradas na rede, a Célula de Defesa Cibernética do COMAE deve realizar auditorias regulares, preferencialmente semestrais nos recursos computacionais da Organização, emitindo parecer técnico e orientando aos demais setores sobre a necessidade de correções e aplicação de boas práticas de defesa cibernética.

2.2.16 TRATAMENTO DE INCIDENTES DE SEGURANÇA

O tratamento de incidentes de segurança será regulamentado em NPA específica e será atribuição exclusiva da equipe de segurança cibernética.

2.3 RECURSOS HUMANOS DE ADMINISTRAÇÃO DA INFRAESTRUTURA DE TI

O componente humano exerce papel específico e possui perfis de interação com os recursos computacionais da Organização.

Para efeito desta ICA, os papeis definidos para interação com os recursos computacionais estão estabelecidos no Regimento Interno do Comando de Operações Aeroespaciais (RICA 20-39), bem como regulamentados em Normas Padrão de Ação (NPA) específicas dos setores envolvidos.

Os recursos humanos responsáveis pela administração da infraestrutura de TI, cujas responsabilidades estão estabelecidas no item 2.4 deste documento, são aqueles pertencentes ao efetivo dos seguintes setores previsto no RICA 20-39: Célula de Tecnologia da Informação (CTI), aqui definida com Equipe de administração e Suporte de Rede; Célula de Defesa Cibernética (CDC), aqui definida como Equipe de Segurança Cibernética; e Seção de Infraestrutura (SIE), aqui definida como Equipe de Suporte ao Usuário.

Todos os recursos humanos responsáveis pela administração da infraestrutura de TI devem assinar Termo de Responsabilidade e Sigilo previsto em NPA específica confeccionada pela Célula de Defesa Cibernética (CDC).

Tanto a mobilização como a desmobilização de recursos humanos responsáveis pela administração da infraestrutura de TI serão regulamentadas em NPA específica e obedecerão aos critérios exigidos pelo Centro de Inteligência da Aeronáutica (CIAER) para a emissão, controle e manutenção de credenciais de segurança.

2.4 RESPONSABILIDADES

2.4.1 DA EQUIPE DE ADMINISTRAÇÃO E SUPORTE DE REDE

2.4.1.1 Adotar as medidas necessárias para garantir elevado nível de segurança no que diz respeito aos critérios de criação e manutenção das senhas utilizadas para acesso à rede.

2.4.1.2 Manter as contas de usuário em um único sistema de cadastro, o qual deverá conter informações cadastrais de todas as contas existentes no COMAE.

2.4.1.3 Providenciar a validação periódica e o bloqueio ou a exclusão das contas de usuário inativas.

2.4.1.4 Suspender, temporariamente, o acesso de qualquer conta de usuário, a todo e qualquer recurso computacional, nos casos de suspeita de violação das regras estabelecidas neste documento ou qualquer ato que atente contra a segurança cibernética.

2.4.1.5 Manter as credenciais de administrador de rede, bem como administrador local apenas para o grupo reduzido de técnicos, cuja execução das tarefas diárias exija tal privilégio.

2.4.1.6 Atualizar periodicamente as credenciais de administração dos recursos de rede.

2.4.1.7 Efetuar a troca completa das credencias conhecidas por determinado membro da equipe que seja desligado de suas funções.

2.4.1.8 Garantir que o acesso às informações corresponda exatamente às credenciais de segurança de cada usuário.

2.4.1.9 Evitar a manutenção de sessão aberta para estações de trabalho inativas.

2.4.1.10 Manter rigoroso controle para garantir que o acesso aos recursos computacionais seja permitido apenas para pessoas pertencentes ao efetivo da OM, que estejam no exercício normal de suas funções.

2.4.1.11 Manter atualizada, acessível, integra e funcional a cópia de segurança (backup) dos arquivos e pastas armazenados na rede administrativa do COMAE, bem como de todos os sistemas em uso, seus respectivos bancos de dados e código fonte.

2.4.1.12 Manter desabilitadas as funções de montagem de dispositivos de armazenamento removíveis em todas as estações de trabalho, salvo exceções expressamente autorizadas pelo CHEMC.

2.4.1.13 Manter desabilitadas em todas as estações de trabalho os recursos, porventura existentes, de acesso à rede sem fio e de comunicação do tipo Bluetooth.

2.4.1.14 Garantir a segregação entre as redes existentes na OM.

2.4.1.15 Garantir a confidencialidade e o sigilo das informações cujo acesso seja viabilizado pelos privilégios concedidos aos administradores da infraestrutura computacional.

2.4.1.16 Cumprir fielmente as normas de segurança, principalmente quando em uso dos perfis privilegiados de administração da infraestrutura computacional.

2.4.1.17 Atuar de forma a preservar a privacidade funcional de todos os usuários da infraestrutura computacional.

2.4.1.18 Utilizar-se dos meios e perfis com acessos privilegiados exclusivamente para fins do serviço e no uso de suas prerrogativas funcionais.

2.4.2 DA EQUIPE DE SEGURANÇA CIBERNÉTICA

2.4.2.1 Validar todos os ativos a serem instalados na rede do COMAE, tais como switches, servidores, máquinas físicas ou virtuais, software, sistemas, etc.

2.4.2.2 Impedir que as máquinas conectadas à rede do COMAE acessem a INTERNET por qualquer meio diferente do previsto, qual seja, autenticação via CCA-BR.

2.4.2.3 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.

2.4.2.4 Impedir o compartilhamento de recursos e ativos de tecnologia da informação entre a rede administrativa do COMAE e qualquer outra rede externa ao COMAER.

2.4.2.5 Manter as normas de segurança de rede do COMAE sempre fundamentadas nas boas práticas, tais como NBR 27000, biblioteca ITIL e IEEE e alinhadas com a legislaçõe de TI no âmbito do COMAER.

2.4.2.6 Realizar testes para detectar vulnerabilidades nos processos de desenvolvimento, implantação e manutenção de sistemas e aplicativos, considerando, dentre outros, os controles de segurança previstos na Norma NBR ABNT ISO/IEC 27002:2013.

2.4.2.7 Visualizar e monitorar as estações de trabalho da rede do COMAE no que diz respeito à solução de Antivírus adotada pelo COMAER.

2.4.2.8 Fiscalizar e exigir que software antivírus seja mantido atualizado e seja executado periodicamente.

2.4.2.9 Controlar e monitorar a segurança da rede por meio da utilização de softwares de detecção de intrusão, auditoria interna e outros softwares específicos.

2.4.3 DA EQUIPE DE SUPORTE AO USUÁRIO

2.4.3.1 Garantir a segurança e o sigilo das credenciais de acesso direto às estações de trabalho, inclusive no que se refere à área de configuração do BIOS.

2.4.3.2 Manter as estações de trabalho configuradas de forma tal que a inicialização seja realizada somente pelo disco rígido.

2.4.3.3 Manter as estações de trabalho do COMAE com Sistema Operacional padronizado, licenciado e atualizado.

2.4.3.4 Manter as estações de trabalho do COMAE com software de Antivírus, definido pela DTI, instalado, configurado e atualizado.

2.4.4 DOS CHEFES DE DIVISÃO, SEÇÃO E ASSESSORIA

2.4.4.1 Manter, rotinas regulares, preferencialmente a cada três meses, de verificação dos arquivos armazenados na rede, na área reservada ao seu setor de trabalho, eliminando as duplicações e os arquivos não mais utilizados.

2.4.5 DOS USUÁRIOS

2.4.5.1 Responder individualmente por todas as atividades desenvolvidas por meio da utilização de suas credenciais de acesso aos recursos computacionais que lhe forem disponibilizados.

2.4.5.2 Zelar pelos recursos computacionais que lhe forem disponibilizados.

2.4.5.3 Tomar medidas para evitar o acesso não autorizado à sua estação de trabalho, efetuar o LOGOUT da sua Conta, bloquear ou desligar o equipamento sempre que se afastar do seu local de trabalho.

2.4.5.4 Desligar sua estação de trabalho ao final do expediente, possibilitando assim, a aplicação de atualizações no Sistema Operacional.

2.4.5.5 Efetuar a troca de sua senha sempre que houver a suspeita de que ela tenha sido descoberta.

2.4.5.6 Solicitar o cancelamento de suas credenciais em caso de afastamento definitivo de suas atribuições no COMAE.

2.4.5.7 Usar os recursos que lhe forem disponibilizados apenas para efetuar atividades diretamente relacionadas com suas obrigações funcionais.

2.4.5.8 Comunicar, imediatamente, ao Setor de Defesa Cibernética sobre o recebimento de mensagens de e-mail do tipo PHISHING. O usuário deverá relatar o problema e fornecer cópia do material suspeito para que sejam realizados os procedimentos de coleta e envio ao CTIR.FAB.

2.4.5.9 Comunicar, imediatamente, a inexistência ou desatualização de Antivírus em sua estação de trabalho.

2.4.5.10 Reportar, imediatamente, a observância de mau funcionamento de sua estação de trabalho, comportamentos anômalos dos sistemas utilizados e/ou suspeita de infecção por vírus ou códigos maliciosos.

2.4.5.11 Entregar à equipe de segurança cibernética qualquer dispositivo móvel de armazenamento (pendrives, cartões de memória, mídias SSD, Cds/DVDs, etc.) encontrado sem um responsável. Tais dispositivos não devem ser conectados a quaisquer recursos computacionais do COMAE.

2.5 RESTRIÇÕES

2.5.1 AOS USUÁRIOS SERÁ VEDADO

2.5.1.1 Efetuar instalação, manutenção, realocação ou qualquer tipo de configuração nos equipamentos utilizados na rede da OM.

2.5.1.2 Conectar qualquer tipo de equipamento, acessório ou dispositivo, seja este particular ou não, à rede da OM.

2.5.1.3 Utilizar quaisquer softwares de análise de rede/pacotes/vulnerabilidades ou qualquer tipo de exploração em qualquer rede de computadores no âmbito do COMAE.

2.5.1.4 Usar sua conta de e-mail corporativo do COMAER para fins particulares, como efetuar compras ou realizar cadastro de qualquer natureza.

2.5.1.5 É vedado ao usuário de e-mail corporativo:

a) tentar acesso não autorizado à caixa postal de terceiros;

b) enviar materiais obscenos, ofensivos, ilegais, não éticos, propagandas, ameaças, difamação, injúria, racismo, de pedofilia ou hebefilia, mensagens do tipo corrente, spam ou outros que venham a causar molestamento, tormento ou danos ao destinatário ou a terceiros;

c) enviar qualquer informação que viole a legislação em vigor no Brasil;

d) enviar intencionalmente mensagens que contenham vírus ou qualquer espécie de programação de computador prejudicial ou danosa;

e) utilizar as listas públicas de endereços eletrônicos do COMAE para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida autorização dos responsáveis pelas listas;

f) abrir e enviar quaisquer arquivos anexados a mensagens de correio eletrônico, sem antes passá-los pelo software antivírus;

g) enviar mensagens em resposta a qualquer assunto, na qualidade de representante legal do COMAE, sem autorização formal da autoridade competente;

h) executar qualquer arquivo recebido de terceiros, sejam eles pertencentes ao Comando da Aeronáutica ou não, os quais possuam extensões do tipo .EXE, .COM, .SCR, .MSI ou outros que possam comprometer o sistema através da execução de comandos maliciosos, vírus e similares;

i) cadastrar o endereço de e-mail corporativo em listas de distribuição externas ao COMAER, excetuando-se aquelas pertencentes às demais Forças Armadas (MB e EB) e ao Ministério da Defesa;

j) realizar qualquer outro procedimento de uso do correio eletrônico que possa afetar de forma negativa a Força Aérea Brasileira ou COMAE e seus usuários; e

k) clicar em links de acesso, recebidos por remetentes desconhecidos.

2.5.1.6 Ativar redes sem fio a partir de qualquer dispositivo que possua a capacidade de prover tal recurso.

2.5.1.7 Acessar a rede a partir de equipamentos que não tenham sido previamente integrados ao respectivo domínio da rede.

2.5.1.8 Possuir ou utilizar, ainda que de outrem, credenciais de administrador local das estações de trabalho, tampouco da rede ou de qualquer um de seus ativos.

2.5.1.9 Instalar softwares ou aplicativos em sua estação de trabalho.

2.5.1.10 Desabilitar os serviços previamente configurados e ativos no Antivírus.

2.5.1.11 Acessar ou permitir o acesso remoto à rede local do COMAE. Exceção feita apenas para os acessos aos serviços publicados na INTRAER, realizados por meio de VPN fornecida por qualquer um dos Centros de Computação da Aeronáutica.

2.5.1.12 Usar a área de armazenamento da rede para guardar arquivos de natureza particular.

2.5.1.13 Armazenar arquivos de mídia (vídeos, imagens, etc) nas pastas da rede administrativa do COMAE, exceto aqueles estritamente necessários para atividades do seu setor de trabalho.

2.5.1.14 Usar dispositivos móveis funcionais conectados em redes do tipo Wi-Fi fora do ambiente militar, tais como hotéis, aeroportos, shopping centers ou qualquer tipo de ambiente compartilhado e liberado para acesso público. Nessas ocasiões, deverá utilizar o acesso disponível no pacote de dados contratado pelo COMAE no serviço de telefonia móvel.

2.5.1.15 Instalar qualquer tipo de software nos laptops funcionais.

2.5.1.16 Utilizar WhatsApp Web bem como qualquer serviço de mensagem instantânea ou de bate-papo disponível na Internet e mantido por entidades externas ao COMAER.

2.5.2 AOS ADMINISTRADORES E TÉCNICOS DE TI É VEDADO

2.5.2.1 Os administradores e técnicos de TI estão sujeitos a todas as proibições aplicadas aos usuários, excetuando-se as previstas nos itens 2.5.1.1; 2.5.1.3; 2.5.1.6; 2.5.1.7; e 2.5.1.8.

2.5.2.2 Usar suas credenciais para criar qualquer tipo de facilidade ou configuração de exceção, atendendo ao interesse particular, nem tampouco a um pedido direto de qualquer usuário.

2.5.2.3 Criar ou utilizar qualquer tipo de mecanismo para acessar os ativos de rede a partir de ambiente alheio à rede de gerência ou de interface diferente da console de acesso de cada equipamento.

2.5.2.4 Utilizar os perfis ou privilégios de acesso aos meios computacionais para obter informações ou dados restritos ou privativos funcionais para objetivos diversos que não sejam exclusivamente do interesse do serviço e com o devido amparo legal.

3 DISPOSIÇÕES FINAIS

As determinações e orientações contidas nesta instrução terão efeito a partir da data de sua publicação e serão, quando houver necessidade, regulamentadas em normas (NPA) específicas para cada caso.

A não observância ao previsto nesta instrução será apurada e poderá ter efeitos na esfera administrativa e, se for o caso, criminal.

Os casos não previstos serão submetidos à apreciação do Comandante de Operações Aeroespaciais.

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, 2013.

_____. ABNT NBR ISO/IEC 27002 - *Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação*. Rio de Janeiro, RJ, 2013.

_____. ABNT NBR ISO/IEC 27003 - *Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Orientações.* Rio de Janeiro, RJ, 2020.

_____.ABNT NBR ISO/IEC 27004 -*Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Monitoramento, medição, análise e avaliação.*Rio de Janeiro, RJ,2017.

_____. ABNT NBR ISO/IEC 27005 - *Tecnologia da informação - Técnicas de segurança - Gestão de Riscos de Segurança da Informação*. Rio de Janeiro, RJ, 2019.

_____.ABNT NBR ISO/IEC 27007 - *Segurança da informação, segurança cibernética e proteção da privacidade - Diretrizes para auditoria de sistemas de gestão da segurança da informação*. Rio de Janeiro, RJ, 2021.

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.

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

_____. Padronização de Acesso à INTERNET no COMAER - Acesso não Funcional: **OTCA 009/DTI/2019**. São Paulo, SP, 2019.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Plano de Tecnologia da Informação da Aeronáutica*: **PCA 11-319**. Brasília, DF, 2020.

_____.*Uso da Rede Mundial de Computadores - INTERNET – No Comando da Aeronáutica*: **ICA 7-5**. Brasília, DF, 2015.

_____.*Gerenciamento de Incidentes de Segurança em Redes de Computadores no Comando da Aeronáutica*: **ICA 7-42**. Brasília, DF, 2016.