

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



TECNOLOGIA DA INFORMAÇÃO

ICA 7-34

**POLÍTICA DE SEGURANÇA EM TECNOLOGIA DA
INFORMAÇÃO E USO DOS RECURSOS
COMPUTACIONAIS DO DCTA**

2023

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA AEROESPACIAL



TECNOLOGIA DA INFORMAÇÃO

ICA 7-34

**POLÍTICA DE SEGURANÇA EM TECNOLOGIA DA
INFORMAÇÃO E USO DOS RECURSOS
COMPUTACIONAIS DO DCTA**

2023



MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA AEROESPACIAL

PORTARIA DCTA Nº 183/DTIC, DE 4 DE OUTUBRO DE 2023.

Aprova a reedição da Instrução que dispõe sobre a Política de Segurança em Tecnologia da Informação e Uso dos Recursos Computacionais do DCTA.

O DIRETOR-GERAL DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA AEROESPACIAL, no uso das atribuições que lhe confere o inciso IV do art. 10 do Regulamento do Departamento de Ciência e Tecnologia Aeroespacial, aprovado pela Portaria GABAER nº 411/GC3, de 25 de novembro de 2022, resolve:

Art. 1º Aprovar a reedição da ICA 7-34 “Política de Segurança em Tecnologia da Informação e Uso dos Recursos Computacionais do DCTA”, que com esta baixa.

Art. 2º Esta Portaria entra em vigor em 1º de novembro de 2023.

Art. 3º Revoga-se a Portaria DCTA Nº 272/DTI, de 11 de agosto de 2014, publicada no Boletim do Comando da Aeronáutica nº 168, de 5 de setembro de 2014.

Ten Brig Ar MAURÍCIO AUGUSTO SILVEIRA DE MEDEIROS
Diretor-Geral do DCTA

(Publicada no BCA nº 189, de 16 de outubro de 2023)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES	9
1.1 <u>FINALIDADE</u>	9
1.2 <u>CONCEITUAÇÃO</u>	9
1.3 <u>ÂMBITO</u>	18
2 POLÍTICA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E DE USO DOS RECURSOS COMPUTACIONAIS.....	19
2.1 <u>PREMISSAS</u>	19
2.2 <u>RESPONSABILIDADES</u>	20
2.3 <u>POLÍTICAS</u>	23
2.4 <u>PENALIDADES</u>	24
3 DISPOSIÇÕES GERAIS	25
4 DISPOSIÇÕES FINAIS.....	26
REFERÊNCIAS	27
Anexo A – Política de Uso dos Recursos Computacionais.....	31
Anexo B – Política de Administração de Recursos Computacionais.....	40
Anexo C – Política de Manipulação de Informações Classificadas.....	44
Anexo D – Política de Antivírus e Códigos Maliciosos	46
Anexo E – Política de Firewall e Recursos Computacionais Localizados na Zona Desmilitarizada (DMZ) da RCD/DCTA	47
Anexo F – Política de Segurança Física	48
Anexo G – Política de Segurança Lógica	51
Anexo H – Política de Segurança dos Serviços de Rede.....	53
Anexo I – Política de Segurança em Servidores	55
Anexo J – Política de Acesso Remoto	57
Anexo K – Política de Auditoria	58
Anexo L – Plano de Continuidade de Negócio	59
Anexo M – Ficha de Cadastro de Usuário	60

PREFÁCIO

O conhecimento, cada vez mais, é a mola propulsora do desenvolvimento de um país, trazendo melhores condições econômicas e sociais para a sua sociedade.

Por sua vez, a Tecnologia da Informação (TI) perpassa e capilariza toda organização, tornando-se, assim, estratégica na consecução de sua missão.

Portanto, a utilização da Tecnologia da Informação para gerar, armazenar e proteger esse conhecimento, bem como para zelar, apropriadamente, pelas informações trafegadas de uma organização, com segurança, é uma atividade de suma importância para a Aeronáutica e para o País.

No mundo atual, essa utilização gera novas informações, em um processo contínuo e, dependendo de suas aplicações, pode fazer parte de um processo mais amplo, recentemente denominado de poder cibernético, que possui uma linha divisória tênue com a chamada defesa cibernética.

A guerra moderna, na maioria dos casos, sem soldados, tende a utilizar maciçamente a TI e seus procedimentos de segurança, para explorar as vulnerabilidades de segurança dos oponentes aos objetivos definidos, quer sejam bélicos, materiais, econômicos, logísticos, estratégicos e outros.

Desta forma, é essencial aperfeiçoar e aplicar esses procedimentos de segurança para mitigar as vulnerabilidades dos recursos computacionais de uma organização contra ataques cibernéticos de toda ordem.

O Departamento de Ciência e Tecnologia Aeroespacial (DCTA), no desenvolvimento de suas atividades de ensino, pesquisa, desenvolvimento, inovação e de serviços técnicos especializados, no campo aeroespacial, foi, e é, um polo de excelência na geração e disseminação de conhecimento, o qual se desdobra em outras áreas de aplicação, além da área aeroespacial, em prol do bem comum do País.

Neste contexto, a utilização de recursos computacionais e de infraestrutura tecnológica é importante para o compartilhamento da informação no ambiente do DCTA, bem como no seu relacionamento com o ambiente externo. No entanto, é necessário que este compartilhamento seja realizado com segurança, e sob a égide e vigência de normas e diretrizes, tanto internas como externas, visando a garantir a proteção da informação, bem como dos equipamentos da infraestrutura tecnológica do DCTA e, também, orientar seus usuários na sua utilização.

Assim, o objetivo desta Instrução é resguardar e proteger o DCTA, considerando suas informações geradas, armazenadas e trafegadas, seus recursos computacionais e outros equipamentos operacionais pertinentes, bem como orientar seus usuários, não só em relação à segurança da informação, mas também em relação à segurança moral, patrimonial e legal, estabelecendo, ainda, uma política de segurança em tecnologia da informação efetiva, que permita a detecção de erros e falhas em toda cadeia sistêmica, causadas com ou sem a vontade humana.

Em adição, a presente Instrução permite, ainda, um entendimento das diretivas e princípios adotados pelo DCTA no tocante à segurança em tecnologia da informação e do uso de seus recursos computacionais, e define os direitos e deveres e as principais

responsabilidades legais dos usuários, em consonância com as legislações do Governo Federal e do Comando da Aeronáutica.

Por fim, para efeito de registro, esta Instrução reflete as atualizações realizadas na ICA 7-34, de 2014, que por sua vez, substituiu a Diretriz de Tecnologia Aeroespacial DTA 08/2007 (Política de Segurança em Tecnologia da Informação e de Uso dos Recursos Computacionais) do então Comando-Geral de Tecnologia Aeroespacial (CTA).

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

A presente Instrução tem por finalidade estabelecer as diretrizes para a implementação e manutenção dos mecanismos de segurança lógica e física dos recursos computacionais em uso no Departamento de Ciência e Tecnologia Aeroespacial (DCTA) e em suas Organizações Militares (OM) subordinadas, bem como normatizar o uso destes recursos computacionais pelos usuários do DCTA e suas OM subordinadas.

1.2 CONCEITUAÇÃO

1.2.1 ACESSO REMOTO

Qualquer acesso à Rede de Comunicação de Dados do DCTA (RCD/DCTA), bem como à Rede Intraer, através de uma rede, dispositivo, ou meio não controlado por este Departamento.

1.2.2 ADMINISTRADOR DE REDE

É o militar ou servidor designado no DCTA e OM subordinadas ao DCTA para administrar a rede de comunicação de dados local, sendo membro integrante da Equipe de Tecnologia da Informação local.

1.2.3 ADWARE

Do inglês *Advertising Software*. Programa 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.

1.2.4 ANALISTA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO

É o militar ou servidor designado no DCTA e OM subordinadas ao DCTA para desempenhar as atividades inerentes à Segurança em Tecnologia da Informação local, sendo membro integrante da Equipe de Tecnologia da Informação local.

1.2.5 APAGAMENTO SEGURO

Processo de apagamento e escrita, repetidas vezes, de espaços em disco anteriormente ocupados por dados, os quais precisam ser apagados.

1.2.6 ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

Patrimônio composto de ativos físicos, ativos de informação, ativos de *software* e outros recursos tecnológicos utilizados na tecnologia da informação do DCTA.

1.2.7 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.

1.2.8 BACKBONE

Espinha dorsal de uma rede de dados. Designação dada a um meio físico que interconecta outras redes de dados.

1.2.9 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.

1.2.10 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.

1.2.11 BOTNETS

Redes formadas por diversos computadores infectados com *bots*. Podem ser usados em atividades de negação de serviço, esquemas de fraude, envio de *spam* e outros.

1.2.12 BOTS

Programas que, além de incluir funcionalidades de *worms*, sendo capazes de se propagarem automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõem de mecanismos de comunicação com o usuário invasor, permitindo que os programas sejam controlados 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.

1.2.13 CAVALOS-DE-TRÓIA

Também conhecidos como *trojans*, são programas normalmente recebidos como anexos de *correio eletrônico*, que além de executarem funções para as quais foram aparentemente projetados, também executam outras funções, geralmente maliciosas e sem o conhecimento do usuário.

1.2.14 COMISSÃO DE COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO DO DCTA (CCTI)

Comissão assessora da Divisão de Tecnologia da Informação e Comunicação (DTIC) do Subdepartamento Técnico do DCTA (SDT/DCTA), prevista no Regimento Interno do DCTA (RICA 20-3), composta pelos Coordenadores de TI do DCTA e das OM subordinadas ao DCTA indicados pelo respectivo Diretor/Reitor/Prefeito/Presidente/Chefe/Comandante da OM, com competência para representar suas respectivas OM no assessoramento à DTIC/DCTA na condução da Política de TI do Departamento.

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.

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 DCTA.

1.2.17 CONTROLE

Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas e estrutura organizacional.

1.2.18 CONTROLE DE ACESSO

Conjunto de procedimentos de segurança estabelecidos para o acesso do usuário à rede e aos recursos computacionais.

1.2.19 COORDENADOR DE TECNOLOGIA DA INFORMAÇÃO DAS OM SUBORDINADAS

Militar ou servidor responsável, em cada OM subordinada ao DCTA, pela condução das atividades de TI, sendo o elo sistêmico de ligação da OM de origem com a DTIC/DCTA e, também, o Coordenador da Equipe de TI local.

1.2.20 DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO DCTA (DTIC/DCTA)

Divisão do Subdepartamento Técnico do DCTA, prevista no Regimento Interno do DCTA (RICA 20-3), responsável pela gestão estratégica de Tecnologia da Informação e pelas atividades de planejamento, organização, controle, orientação e coordenação relativas à TIC no âmbito do DCTA e de suas OM subordinadas, bem como dos recursos computacionais de Processamento e de Comunicação de Dados do DCTA. A DTIC atua como Elo de Coordenação de TIC do DCTA junto ao Órgão Central de TI do COMAER.

1.2.21 CRIPTOGRAFIA

Conjunto de técnicas utilizadas para conversão de dados de um formato legível para um formato codificado. Os dados criptografados só podem ser lidos após decodificados.

1.2.22 DISPONIBILIDADE

Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

1.2.23 ELOS DE COORDENAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO COMAER – STI

São os setores pertencentes aos Órgãos de Direção-Geral, Órgãos de Direção Setorial 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 EQUIPE DE TI

Equipe de Tecnologia da Informação (TI) existente em cada OM do DCTA, prevista na Governança de Tecnologia da Informação do DCTA (ICA 7-33), responsável pela execução das atividades de TI. Essas equipes são chefiadas pelo Coordenador de TI da OM e devem conter, pelo menos, um membro capacitado na área de Segurança em TI e um membro capacitado em Administração de Redes.

1.2.25 ERISC

Designa a Equipe de Resposta a Incidentes de Segurança em Computadores do DCTA, constituída por pelo menos 5 (cinco) militares ou servidores dedicados, preferivelmente de forma exclusiva, às atividades de segurança computacional no âmbito da RCD/DCTA, provendo as ações necessárias no trato dos incidentes de segurança da informação, conforme preconizado na ICA 7-42 e na ICA 7-46. A ERISC/DCTA vincula-se funcionalmente à DTIC/DCTA, conforme previsto no Regimento Interno do DCTA (RICA 20-3), e atua como ETIR, vinculada sistemicamente ao Centro de Tratamento de Incidentes da FAB (CTIR-FAB).

1.2.26 ESTAÇÃO DE TRABALHO

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

1.2.27 FIREWALL

Sistema ou combinação de sistemas que filtram o tráfego de dados e protegem a fronteira entre duas ou mais redes.

1.2.28 FIREWALL DE APLICAÇÃO WEB (WAF)

Sistema que protege as aplicações *web* com filtragem e monitoramento do tráfego entre a aplicação e a Internet.

1.2.29 FRAÇÃO FUNCIONAL

Setor funcional presente no organograma do Departamento e OM subordinadas ao DCTA, em nível igual ou superior à divisão funcional, coordenadoria ou equivalente.

1.2.30 FRAME RELAY

Protocolo de chaveamento de pacotes para conexão de dispositivos em uma rede WAN (*Wide Area Network*).

1.2.31 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.

1.2.32 INCIDENTES DE SEGURANÇA

Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos recursos computacionais, que tenham a grande probabilidade de comprometer as operações e ameaçar a segurança da informação.

1.2.33 INFRAESTRUTURA COMO SERVIÇO (IaaS)

Serviço de computação em nuvem onde o provedor de serviço de nuvem oferece a infraestrutura ao cliente para o uso de recursos fundamentais de computação, armazenamento e rede sob demanda.

1.2.34 INTEGRIDADE

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

1.2.35 IRRETRATABILIDADE / NÃO REPÚDIO

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

1.2.36 ISDN

Do inglês *Integrated Services Digital Network*, um padrão internacional de comunicação para transmissão de voz, vídeo e dados em uma linha telefônica digital ou analógica.

1.2.37 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 a captura de senhas bancárias ou números de cartões de crédito.

1.2.38 LACRE ANTIVIOLAÇÃO

Tipo de lacre que deixa evidências visíveis em caso de tentativa de remoção, violação, alteração ou substituição.

1.2.39 LOG

Um arquivo contendo um registro de eventos em um Recurso Computacional.

1.2.40 LOGON

Ato de se estabelecer uma conexão com um sistema de TI, mediante autenticação do usuário.

1.2.41 LOGOFF

Ato de desconectar um usuário de um sistema de TI.

1.2.42 MAIL BOMBS

É o envio de uma grande quantidade de *correio eletrônico* para uma pessoa ou sistema.

1.2.43 MODEM

Dispositivo periférico que estabelece conexão entre computadores para envio de informações através de linhas telefônicas ou cabos.

1.2.44 NÚCLEO CORPORATIVO DE TECNOLOGIA DA INFORMAÇÃO (NCTI)

O Núcleo Corporativo de TI, previsto no Regimento Interno do DCTA (RICA 20-3), é responsável pelo gerenciamento executivo das atividades de TI, relativas às redes corporativas de comunicação de dados (RCD/DCTA e Intraer) e sistemas corporativos para o âmbito do DCTA e OM subordinadas, disponibilizando sua Infraestrutura como Serviço (IaaS). Este Núcleo é subordinado à DTIC/DCTA e se encontra fisicamente nas dependências da Direção do DCTA, sendo constituído por dois *datacenters*, sendo um principal e um de recuperação de desastres.

1.2.45 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 sistema operacional.

1.2.46 PLANO DE CONTINUIDADE DE NEGÓCIO

Plano que tem o objetivo de descrever antecipadamente as medidas a serem tomadas para fazer com que processos e sistemas de TI críticos permaneçam operacionais ou voltem a funcionar, após a ocorrência de um desastre, plenamente ou num estado minimamente aceitável, o mais rápido possível, evitando assim, uma paralisação prolongada que possa gerar maiores prejuízos à organização, como perda de informações, adiamento de tomada de decisões, problemas jurídicos, abordagens maliciosas da imprensa e outros.

1.2.47 PORT-SCAN

O ato de sistematicamente fazer a varredura de portas (canais para receber conexões) de recursos computacionais.

1.2.48 PROGRAMA MALICIOSO (MALWARE)

O termo refere-se a qualquer código ou programa mal-intencionado, tais como vírus, *worms*, cavalos-de-troia (*trojans*), *adware*, *spywares*, *mail bombs*, *backdoor*, *keyloggers*, *bots*, *botnets*, *rootkits* e assemelhados, 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.

1.2.49 RECURSOS COMPUTACIONAIS

São os equipamentos, as instalações, os programas de computador e os bancos de dados administrados, mantidos ou operados pelo DCTA e OM subordinadas, sendo, também, conhecidos como ativos de TI:

- a) computadores e similares, bem como terminais de qualquer espécie;
- b) impressoras e demais periféricos usados com computadores;
- c) redes e seus dispositivos;
- d) dispositivos de comunicação de dados e equipamentos afins, móveis ou não;
- e) bancos de dados e documentos residentes em disco, fita ou outros meios de armazenamento;
- f) salas de computadores e laboratórios;
- g) sistemas operacionais, aplicativos e *software* de rede ou qualquer arquivo residente em disco que contenha um conjunto de instruções que possam ser interpretadas e/ou executadas em computador;
- h) outros recursos tecnológicos utilizados na tecnologia da informação do DCTA e OM subordinadas.

1.2.50 RECURSOS COMPUTACIONAIS CORPORATIVOS

Recursos computacionais existentes no âmbito do DCTA, utilizados pelas OM do DCTA e administrados pelo Departamento.

1.2.51 RECURSOS COMPUTACIONAIS LOCAIS

Recursos computacionais existentes, utilizados e administrados no âmbito de cada OM do DCTA.

1.2.52 REDE DE COMUNICAÇÃO DE DADOS DO DCTA (RCD/DCTA)

Rede de comunicação de dados do DCTA que interliga as redes locais das OM do DCTA, através de uma rede central (*backbone*).

1.2.53 REDE DE COMUNICAÇÃO DE DADOS LOCAL/REDE LOCAL

Rede de comunicação de dados localizada no Departamento e suas OM subordinadas que interliga seus respectivos recursos computacionais.

1.2.54 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.

1.2.55 ROOTKIT

Conjunto de programas que tem como finalidade esconder e assegurar a presença de um usuário invasor em um computador comprometido.

1.2.56 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.

1.2.57 SERVIÇOS DE REDE

Aplicações de *software* que realizam operações utilizando conexão com a RCD/DCTA e/ou com as Redes Locais das OM.

1.2.58 SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS)

É um programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

1.2.59 SISTEMA DE PREVENÇÃO DE INTRUSÃO (IPS)

É um programa, ou um conjunto de programas, cuja função é proteger contra ameaças identificadas.

1.2.60 SEGURANÇA DA INFORMAÇÃO

Preservação da confidencialidade, da integridade e da disponibilidade da informação, envolvendo ainda autenticidade, responsabilidade, não repúdio de autoria e confiabilidade.

1.2.61 SERVIDOR

Recurso Computacional que desempenha alguma função de prestação de serviços de rede na RCD/DCTA e sub-redes a ela conectadas, tais como processamento e armazenamento de dados, impressão, acesso para usuários e outros.

1.2.62 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.

1.2.63 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 seu usuário.

1.2.64 SPAM

Termo usado para se referir aos correios eletrônicos não solicitados, que geralmente são enviados para um grande número de pessoas.

1.2.65 SPYWARE

Termo utilizado para se referir a uma grande categoria de *softwares* 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.

1.2.66 SSH

Do inglês *Secure Shell*, protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos e outros.

1.2.67 SWITCH

Equipamento de conectividade de rede, com capacidade de comutação em alta velocidade entre as portas, possibilitando a utilização de toda a banda disponível para a comunicação entre dois equipamentos.

1.2.68 TECNOLOGIA DA INFORMAÇÃO

Conjunto formado por recurso humano técnico especializado, processos, serviços, infraestrutura tecnológica e recursos computacionais, que é empregado na geração, armazenamento, veiculação, processamento, reprodução e uso da informação pelo DCTA e OM subordinadas.

1.2.69 TOKEN

É um *hardware* portátil com a mesma funcionalidade do *smart card*.

1.2.70 USUÁRIO

Militar ou servidor do DCTA ou de suas OM subordinadas, ou pessoa física ou jurídica com algum vínculo direto ou indireto com essas organizações, que esteja autorizada a utilizar, de alguma forma, mesmo que eventual, os recursos computacionais existentes.

1.2.71 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*).

1.2.72 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.

1.2.73 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.

1.2.74 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.

1.2.75 VULNERABILIDADES

Fragilidade de um alvo ou grupo de ativos, que pode ser explorada por uma ou mais ameaças.

1.2.76 WORMS

Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferentemente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

1.2.77 ZONA DESMILITARIZADA (DMZ)

Do inglês, *Demilitarized Zone*. É a área de rede que permanece entre a rede interna de uma organização e uma rede externa, em geral a rede Internet. Comumente, uma DMZ contém equipamentos apropriados para o acesso à rede Internet, como Servidores para *web* (HTTP), Servidores FTP, Servidores para correio eletrônico (SMTP) e Servidores DNS.

1.3 ÂMBITO

Esta Instrução aplica-se ao DCTA e suas OM Subordinadas.

2 POLÍTICA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E DE USO DOS RECURSOS COMPUTACIONAIS

A utilização de recursos computacionais e de infraestrutura tecnológica é importante para o compartilhamento da informação no ambiente do DCTA, bem como no seu relacionamento com o ambiente externo. No entanto, é necessário que este compartilhamento seja realizado com segurança, e sob a égide e vigência de normas e diretrizes, tanto internas como externas, visando garantir a proteção da informação, bem como dos equipamentos da infraestrutura tecnológica do DCTA e, também, orientar seus usuários na sua utilização.

Assim, o objetivo desta Instrução é resguardar e proteger o DCTA, considerando suas informações geradas e trafegadas, seus recursos computacionais e outros equipamentos operacionais pertinentes, bem como orientar seus usuários, não só em relação à segurança da informação, mas também em relação à segurança moral, patrimonial e legal, estabelecendo, ainda, uma política de segurança em tecnologia da informação efetiva, que permita a detecção de erros e falhas em toda cadeia sistêmica, causadas com ou sem a vontade humana.

Em adição, a presente Instrução permite, ainda, um entendimento das diretivas e princípios adotados pelo DCTA no tocante à segurança em tecnologia da informação e do uso de seus recursos computacionais, e define os direitos e deveres e as principais responsabilidades legais dos usuários.

2.1 PREMISSAS

2.1.1 As redes de comunicação de dados locais devem ter uma configuração que permita o controle de acesso de usuários.

2.1.2 Os Servidores não podem ser utilizados como estações de trabalho.

2.1.3 Todos os usuários são responsáveis pela observância do disposto nesta Instrução.

2.1.4 Os dados trafegados na RCD/DCTA e/ou armazenados em seus recursos computacionais são classificados como dados ostensivos, na falta de uma classificação formal de sensibilidade da informação. Em consequência, não será possível garantir a confidencialidade dos mesmos sem o uso das adequadas medidas de segurança indicadas na Política de Manipulação de Informações Classificadas, descrita no Anexo C.

2.1.5 Para os propósitos de segurança, manutenção da RCD/DCTA e verificação do cumprimento desta Instrução, Administradores de Rede autorizados podem monitorar os equipamentos, sistemas e tráfego de rede a qualquer instante, de acordo com a Política de Auditoria, descrita no Anexo K.

2.1.6 A atribuição de responsabilidades, bem como todos os procedimentos adotados para viabilizar a segurança da informação devem ser detalhadamente documentados por escrito.

2.1.7 A presente Instrução traz efeitos obrigacionais, nos termos das legislações pertinentes aos casos apurados.

2.2 RESPONSABILIDADES

2.2.1 DCTA E OM SUBORDINADAS

2.2.1.1 Fazer cumprir esta Instrução em seu âmbito de atuação.

2.2.1.2 Analisar e autorizar, quando aplicável, as solicitações de veiculação de *home page* nas suas respectivas redes de comunicação de dados.

2.2.1.3 Zelar pela observância dos dispositivos legais aplicáveis aos direitos de propriedade intelectual, em particular aos que se referem à lei em vigor que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País.

2.2.1.4 Aplicar as providências cabíveis quando da ocorrência de infrações a esta Instrução.

2.2.1.5 Submeter à DTIC/DCTA as solicitações de conexões internas e externas à RCD/DCTA.

2.2.1.6 Submeter à DTIC/DCTA as solicitações de acesso às redes Intraer e Internet, quando houver necessidade de um acesso de caráter excepcional e que não seja possível o acesso por meio da RCD/DCTA.

2.2.1.7 Examinar, a seu critério, toda e qualquer informação armazenada em seus recursos computacionais ou que circule nas suas redes de comunicação de dados.

2.2.1.8 Incluir o setor de TI na Ficha de Desimpedimento de militar ou servidor.

2.2.2 DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO DCTA (DTIC/DCTA)

2.2.2.1 Analisar e, quando aplicável, submeter à aprovação do DCTA, as solicitações institucionais das OM subordinadas, de conexões à RCD/DCTA, bem como de acesso às redes Intraer e Internet.

2.2.2.2 Analisar, assessorada pela Comissão de Coordenação de TI do DCTA (CCTI), bem como pelo NCTI, as requisições de novas instalações ou alterações nas redes internas de comunicações de dados do DCTA e OM subordinadas, bem como as solicitações institucionais de conexões à RCD/DCTA, quando julgado aplicável, aprovando, ou não, sua efetivação.

2.2.2.3 Propor a adequação da estrutura organizacional das Equipes de TI das OM Subordinadas, de modo a contemplar um setor responsável pela segurança da informação dos sistemas de TI sob suas responsabilidades.

2.2.3 EQUIPE DE TECNOLOGIA DA INFORMAÇÃO

2.2.3.1 Instalar, alterar, configurar e excluir recursos computacionais, tanto de *hardware* quanto de *software* existentes na rede de comunicação de dados local.

2.2.3.2 Estabelecer e difundir as normas e os procedimentos específicos pertinentes a esta Instrução.

2.2.3.3 Apurar e investigar falhas e tentativas de quebra de segurança nos recursos computacionais locais, por meio de seu Administrador de Rede e Analista de Segurança.

2.2.3.4 Manter um cadastro atualizado dos recursos de *hardware* e *software* da rede local. Cabe a cada OM definir a melhor maneira de criar e manter este cadastro, observando o disposto no Anexo F.

2.2.3.5 Solicitar ao Órgão Central de TI, por meio da DTIC/DCTA, autorização para uso de redes sem fio, bem como de acesso às redes Intraer e Internet, quando este acesso for de caráter excepcional e não puder ser realizado por meio da RCD/DCTA.

2.2.3.6 Submeter à DTIC/DCTA projeto para implantação de solução de videoconferência ou *VoIP*, o qual deve ser analisado de acordo com as orientações emanadas pelo Órgão Central de TI.

2.2.3.7 Estabelecer critérios para o tempo de validade das contas de usuário.

2.2.3.8 Estabelecer tempo máximo de inatividade das contas de usuário, o qual não deve ser superior a 45 dias.

2.2.3.9 Prestar suporte somente aos *softwares* licenciados e por ela instalados nos recursos computacionais.

2.2.3.10 No desligamento de militar ou servidor de sua OM, solicitar a devolução de bens de TI de propriedade da organização registradas em cautelas, e diligenciar pelos arquivos funcionais digitalizados do usuário, transferindo-os para quem de direito, quando aplicável.

2.2.3.11 Demais responsabilidades descritas no Anexo B.

2.2.4 ADMINISTRADOR DE REDE

2.2.4.1 Implementar os procedimentos e mecanismos de segurança estabelecidos.

2.2.4.2 Apurar e investigar falhas e tentativas de quebra de segurança nos recursos computacionais locais.

2.2.4.3 Demais responsabilidades descritas no Anexo B.

2.2.5 ANALISTA DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO

2.2.5.1 Zelar pela disponibilidade, confiabilidade e confidencialidade das informações que trafegam e/ou encontram-se armazenadas nos recursos computacionais locais.

2.2.5.2 Implementar e difundir normas e procedimentos específicos desta Instrução em sua OM, bem como os procedimentos locais aprovados por seu respectivo Diretor/Reitor/Presidente/Prefeito/Chefe/Comandante.

2.2.5.3 Zelar pela proteção dos usuários e da Instituição contra riscos e vulnerabilidades de segurança, bem como contra o uso indevido que possa resultar em medidas legais provenientes de terceiros.

2.2.5.4 Realizar monitoramento e auditoria na utilização dos recursos computacionais locais, com conhecimento prévio do Diretor/Reitor/Presidente/Prefeito/Chefe/Comandante da respectiva OM, visando preservar a integridade das informações institucionais e a imagem do DCTA e da OM, podendo fiscalizar:

- a) conteúdo de mensagens transmitidas e recebidas;
- b) arquivos armazenados em disco;
- c) programas de computador instalados;
- d) fluxo de pacotes na rede local;
- e) arquivos específicos de controle (*logs*);
- f) programas de computador em execução;
- g) outros recursos computacionais, no que for indicado pela DTIC/DCTA.

2.2.6 EQUIPE DE RESPOSTA A INCIDENTES DE SEGURANÇA EM COMPUTADORES (ERISC)

2.2.6.1 Apurar e investigar falhas e tentativas de quebra de segurança nos recursos computacionais locais, com conhecimento prévio do Diretor/Reitor/Presidente/Prefeito/Chefe/Comandante da respectiva OM.

2.2.6.2 Apurar e investigar falhas e/ou tentativas de quebra de segurança no âmbito do DCTA e OM subordinadas, em especial nas ações pertinentes à RCD/DCTA, atuando de forma proativa e corretiva na análise de riscos e vulnerabilidades de segurança.

2.2.6.3 Monitorar e auditar a utilização dos recursos computacionais do DCTA e OM subordinadas, com conhecimento prévio do Diretor/Reitor/Presidente/Prefeito/Chefe/Comandante da respectiva OM, visando preservar a integridade das informações institucionais e a imagem do DCTA e OM subordinadas, podendo fiscalizar:

- a) conteúdo de mensagens transmitidas e recebidas;
- b) arquivos armazenados em disco;
- c) programas de computador instalados;
- d) fluxo de pacotes na rede local;
- e) arquivos específicos de controle (*logs*);
- f) programas de computador em execução;
- g) histórico de acesso à Internet e execução de programas; e
- h) outros recursos computacionais, no que for indicado pela DTIC/DCTA.

2.2.6.4 A ERISC atua no trato de incidentes de segurança da informação, conforme preconizado na ICA 7-46 e na ICA na 7-42, sendo a Equipe de Tratamento de Incidentes de Redes (ETIR) no DCTA.

2.2.7 CHEFE DE FRAÇÃO FUNCIONAL

2.2.7.1 Solicitar a abertura de conta de usuário em recursos computacionais locais, preenchendo a Ficha de Cadastro de Usuário (Anexo M), a qual deve ser assinada pelo usuário e por esta chefia.

2.2.7.2 Comunicar à Equipe de TI local toda alteração no quadro de pessoal (entrada e saída) para atualização do sistema de cadastro de contas de usuário.

2.3 POLÍTICAS

2.3.1 POLÍTICA DE USO DOS RECURSOS COMPUTACIONAIS

Esta Política estabelece normas e procedimentos para o uso aceitável dos recursos computacionais do DCTA e OM subordinadas, e está explicitada no Anexo A.

2.3.2 POLÍTICA DE ADMINISTRAÇÃO DE RECURSOS COMPUTACIONAIS

Esta Política estabelece normas, procedimentos e responsabilidades para a administração dos recursos computacionais do DCTA e OM subordinadas, e está explicitada no Anexo B.

2.3.3 POLÍTICA DE MANIPULAÇÃO DE INFORMAÇÕES CLASSIFICADAS

Esta Política estabelece diretivas para o armazenamento e tramitação seguros de informações classificadas (sensíveis), e está explicitada no Anexo C.

2.3.4 POLÍTICA DE ANTIVÍRUS E CÓDIGOS MALICIOSOS

Esta Política estabelece os requisitos a serem implementados nos recursos computacionais no que se refere à prevenção, detecção e erradicação de vírus, contaminações e códigos maliciosos nesses recursos. Esta Política está explicitada no Anexo D.

2.3.5 POLÍTICA DE *FIREWALL* E RECURSOS COMPUTACIONAIS LOCALIZADOS NA ZONA DESMILITARIZADA (DMZ) DA RCD/DCTA

Esta Política estabelece as diretivas para a criação de *firewall* e de zona de rede desmilitarizada (DMZ). Esta Política está explicitada no Anexo E.

2.3.6 POLÍTICA DE SEGURANÇA FÍSICA

Esta Política estabelece os procedimentos mínimos de segurança para salvaguardar fisicamente os recursos computacionais do DCTA e OM subordinadas. Esta Política está explicitada no Anexo F.

2.3.7 POLÍTICA DE SEGURANÇA LÓGICA

Esta Política estabelece os procedimentos mínimos de segurança lógica para salvaguardar os recursos computacionais do DCTA e OM subordinadas. Esta Política está explicitada no Anexo G.

2.3.8 POLÍTICA DE SEGURANÇA DOS SERVIÇOS DE REDE

Esta Política estabelece os padrões mínimos de segurança para os serviços de rede disponibilizados na RCD/DCTA e nas redes locais conectadas à mesma, além de padronizar quais serviços podem ser disponibilizados na RCD/DCTA e em suas respectivas sub-redes. Esta Política está explicitada no Anexo H.

2.3.9 POLÍTICA DE SEGURANÇA EM SERVIDORES

Esta Política estabelece padrões para a configuração básica de qualquer equipamento Servidor, de propriedade ou não deste Departamento e OM subordinadas. A implementação efetiva desta Política visa minimizar acesso não autorizado à informação sigilosa e à tecnologia desenvolvida neste Departamento e OM subordinadas. Esta Política está explicitada no Anexo I.

2.3.10 POLÍTICA DE ACESSO REMOTO

A Política de acesso remoto prevê as medidas de segurança a serem tomadas na disponibilização de serviços de acesso remoto a algum Recurso Computacional da RCD/DCTA e de suas respectivas sub-redes, definindo padrões para conexão de qualquer equipamento à RCD/DCTA. Esta Política está explicitada no Anexo J.

2.3.11 POLÍTICA DE AUDITORIA

Esta Política estabelece critérios para se conduzir uma auditoria de segurança em qualquer sistema informatizado no âmbito do DCTA e OM subordinadas, de forma a assegurar a integridade, confidencialidade e disponibilidade da informação e dos recursos computacionais, investigar possíveis incidentes de segurança e monitorar as atividades dos usuários e dos recursos computacionais da RCD/DCTA e das Redes Locais, quando isto for apropriado. Esta Política está explicitada no Anexo K.

2.3.12 PLANO DE CONTINUIDADE DE NEGÓCIO

Este plano estabelece diretrizes para a elaboração do Plano de Continuidade de Negócio (PCN) do DCTA e OM subordinadas, de forma a possibilitar a recuperação segura de qualquer Recurso Computacional do DCTA e OM subordinadas, no menor tempo possível. Este Plano está explicitado no Anexo L.

2.4 PENALIDADES

Após processo disciplinar formal, às transgressões a esta Instrução devem ser aplicadas punições previstas na legislação em vigor e também as definidas a seguir.

2.4.1 O usuário que infringir as normas previstas nesta Instrução está sujeito a penalidades administrativas, o que não impede e tampouco elide outras penalidades de natureza civil e penal previstas na legislação em vigor e às quais o usuário tiver dado causa em razão da gravidade do ato praticado.

2.4.2 Sempre que julgar necessário para a preservação da integridade dos recursos computacionais do DCTA e OM subordinadas, dos serviços aos usuários ou dos dados, em função da natureza das atividades tecnológicas desenvolvidas, a ERISC pode suspender temporariamente qualquer conta de usuário, independentemente de violação cometida.

2.4.3 Compete ao Administrador de Rede do DCTA e de cada OM subordinada, no seu âmbito de atuação, identificar e apresentar soluções que possam dirimir dúvidas relacionadas à ocorrência de infrações, permitindo assim, evitar sua reincidência.

2.4.4 Compete ao Diretor-Geral do Departamento de Ciência e Tecnologia Aeroespacial e ao Diretor/Reitor/Presidente/Prefeito/Chefe/Comandante das OM subordinadas ao DCTA, a quem se encontra vinculado o usuário infrator ou no qual ele desenvolve sua atividade, fazer aplicar as providências cabíveis quando da ocorrência de infrações a esta Instrução.

3 DISPOSIÇÕES GERAIS

3.1 Cada OM conectada à RCD/DCTA deve obrigatoriamente operacionalizar esta Instrução, sendo que, qualquer alteração que se faça necessária, em função de peculiaridades e necessidades da rede de comunicação de dados local, deve estar em consonância com esta Instrução e ser submetida à apreciação da Equipe de TI para verificação, validação e posterior homologação pela DTIC/DCTA.

3.2 Os procedimentos complementares contidos na NSCA 7-13 também devem ser observados pelo DCTA e suas OM subordinadas.

3.3 A fim de promover o melhor uso dos recursos computacionais, os usuários que participarem de evento de capacitação e reciclagem de conhecimentos em Tecnologia da Informação, com recursos de sua OM origem, ficam previamente compromissados a repassar, a critério do Chefe da respectiva Fração Funcional, as informações e conhecimentos recebidos aos demais militares e servidores de sua OM de origem e/ou do Departamento, através de palestra ou reunião agendada, com o prévio conhecimento da DTIC/DCTA.

3.4 O DCTA e OM subordinadas não devem renunciar a nenhuma pendência que possa porventura existir quanto à propriedade ou controle de quaisquer *softwares* e *hardwares* e dos dados criados ou armazenados em seus sistemas ou transmitidos através de suas redes.

3.5 O NCTI e a ERISC podem submeter à DTIC/DCTA sugestão de outras normas de utilização dos recursos computacionais.

4 DISPOSIÇÕES FINAIS

4.1 O Comandante da OM deve garantir o cumprimento dos procedimentos desta ICA, dos demais procedimentos relativos à TI do DCTA e das diretrizes do Comando da Aeronáutica, por meio da sua Equipe de TI, bem como garantir a capacitação dos usuários e do efetivo das Equipes de TI, fazendo uso dos recursos financeiros devidamente planejados em instrumentos de planejamento, tais como o Plano Diretor de Tecnologia da Informação e Comunicação do COMAER e o Programa de Trabalho.

4.2 O Subdepartamento Técnico do DCTA (SDT), por intermédio da Divisão de Tecnologia da Informação e Comunicação (DTIC), é responsável pela atualização desta Instrução.

4.3 Os casos não previstos nesta Instrução devem ser submetidos ao Chefe do SDT que os analisará, assessorado pela DTIC e, quando necessário, os encaminhará para decisão do Diretor-Geral do DCTA.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001 - *Segurança da Informação, Segurança Cibernética e Proteção à Privacidade – Sistemas de Gestão da Segurança da Informação - Requisitos*. Rio de Janeiro, RJ, 2022.

_____. ABNT NBR ISO/IEC 27002 – *Segurança da Informação, Segurança Cibernética e Proteção à Privacidade – Controles de Segurança da Informação*. Rio de Janeiro, RJ, 2022.

_____. ABNT NBR ISO/IEC 27005 - *Segurança da Informação, Segurança Cibernética e Proteção à Privacidade - Orientações para Gestão de Riscos de Segurança da Informação*. Rio de Janeiro, RJ, 2023.

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.

_____. *Guia Prático de Execução das Medidas do Decreto de Tratamento das Informações Classificadas no Comando da Aeronáutica: FCA 200-6*. Brasília, DF, 2013

_____. *Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações: ICA 200-8*. Brasília, DF, 2019.

_____. *Processo de Concessão de Credencial de Segurança de Pessoa Jurídica: ICA 200-4*. Brasília, DF, 2007.

_____. *Instrução para Salvaguarda de Assuntos Sigilosos da Aeronáutica (ISAS): ICA 205-47*. Brasília, DF, 2015.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. *Funcionamento do Serviço de Atendimento aos Usuários de Tecnologia da Informação do Comando da Aeronáutica (SAUTI): NSCA 7-8*. Rio de Janeiro, RJ, 2022.

_____. *Gerenciamento de Incidentes de Segurança em Redes de Computadores no Comando da Aeronáutica. ICA 7-42*. Rio de Janeiro, RJ, 2016.

_____. *Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica: NSCA 7-13*. Rio de Janeiro, RJ, 2022.

_____. *TI Verde no Sistema de Tecnologia da Informação da Aeronáutica: NSCA 7-17*. São Paulo, SP, 2020.

_____. *Uso da Rede de Dados do Comando da Aeronáutica – INTRAER: NSCA 7-1*. Rio de Janeiro, RJ, 2012.

BRASIL. Comando da Aeronáutica. Departamento de Ciência e Tecnologia Aeroespacial. *Governança de Tecnologia da Informação do DCTA: ICA 7-33*. São José dos Campos, SP, 2023.

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, 2022.

_____. *Governança da Proteção de Dados Pessoais do Comando da Aeronáutica: DCA 16-6*. Rio de Janeiro, RJ, 2022.

_____. *Plano de Tecnologia da Informação da Aeronáutica: PCA 11-319* - Brasília, DF, 2020.

_____. *Política de Segurança da Informação do Comando da Aeronáutica: DCA 14-8*. Brasília, DF, 2022.

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

BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. Secretaria de Governo Digital. *Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022*. Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. *Decreto nº 4.829, de 3 de setembro de 2003*. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Brasília, 2003.

_____. *Decreto nº 7.845, de 14 de novembro de 2012*. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Brasília, 2012.

_____. *Lei nº 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, 1996.

_____. *Lei nº 9.609, de 19 de fevereiro de 1998*. Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no País e dá outras providências. Brasília, 1998.

_____. *Lei nº 9.610, de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, 1998.

_____. *Lei nº 9.983, de 14 de julho de 2000*. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Brasília, 2000.

_____. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Instrução Normativa nº 1, de 27 de maio de 2020*. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

_____. *Instrução Normativa nº 2, de 5 de fevereiro de 2013*. Dispõe sobre o Credenciamento de Segurança para o Tratamento de Informação Classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

_____. *Instrução Normativa nº 3, de 6 de março de 2013*. Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

_____. *Instrução Normativa nº 3, de 28 de maio de 2021*. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

_____. *Instrução Normativa nº 4, de 26 de março de 2020*. Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.

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

_____. *Instrução Normativa nº 6, de 23 de dezembro de 2021*. Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.

_____. *Norma Complementar nº 01/IN02/NSC/GSI/PR de 27 de junho de 2013*. Disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas.

_____. *Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009*. Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR.

_____. *Norma Complementar nº 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010*. Gestão de ETIR: Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal.

_____. *Norma Complementar nº 09/IN01/DSIC/GSIPR, Revisão 02, de 15 de julho de 2014*. Orientações Específicas para o Uso de Recursos Criptográficos em Segurança da Informação e Comunicações.

_____. *Norma Complementar nº 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012*. Uso de Dispositivos Móveis nos Aspectos Relativos à Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

BRASIL Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. *Decreto nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, 2016.

_____. *Decreto nº 9.637, de 26 de dezembro de 2018*. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, 2018.

_____. *Lei nº 13.709 de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018.

_____. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, 2014.

BRASIL. Tribunal de Contas da União. *Boas Práticas em Segurança da Informação*. 4. ed. Brasília: TCU, 2012. Disponível em:

<http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/biblioteca_tcu/biblioteca_digital/BOAS_PRATICAS_EM_SEGURANCA_DA_INFORMACAO_0.pdf>. Acesso em: 29 de junho de 2023.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. *Cartilha de Segurança para Internet*. Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em:

<<https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>>. Acesso em: 29 de junho de 2023.

COMITÊ GESTOR DA INTERNET NO BRASIL. *Resolução nº 1/2005, de 21 de outubro de 2005*. Dispõe sobre a execução do registro de nomes de domínio, a alocação de endereços IP (Internet Protocol) e a administração relativa ao Domínio de Primeiro Nível, atribuídas ao Núcleo de Informação e Coordenação do Ponto BR – NIC.br e dá outras providências. São Paulo, 2005. Disponível em: <<http://www.cgi.br/resolucoes/documento/2005/001>>. Acesso em: 29 de junho de 2023.

REDE NACIONAL DE ENSINO E PESQUISA. *Política de segurança da informação do Sistema RNP*, de 02 julho 2020. Disponível em: <https://www.rnp.br/arquivos/documents/SEG.P.002.Polit_Seguranca_Sistema_v1_0_0.pdf?B_e3IwmOYHplr4JB4Zu5TEHzh6vYUxlX=>>. Acesso em: 29 de junho de 2023.

Anexo A – Política de Uso dos Recursos Computacionais

Para o uso dos recursos computacionais do DCTA e OM subordinadas deve ser observado o que se segue.

1 RECURSOS COMPUTACIONAIS

1.1 Os recursos computacionais do Departamento e OM subordinadas têm por finalidade servir à pesquisa, ao desenvolvimento, ao ensino, à inovação e aos serviços técnicos especializados, do setor aeroespacial, e às atividades técnicas, administrativas e operacionais do Departamento e OM subordinadas.

1.2 O uso dos recursos computacionais do Departamento e das OM subordinadas está sujeito às leis federais, às normas e regulamentos do COMAER, e às diretivas internas do DCTA, bem como às normas estabelecidas pela DTIC/DCTA, assessorada pela CCTI.

1.3 No que tange ao uso da Internet no Departamento e OM subordinadas, o qual é destinado para fins estritamente de ensino, pesquisa, desenvolvimento, inovação e serviços técnicos especializados, do setor aeroespacial, e sem finalidade comercial, os usuários devem observar as normas do Comitê Gestor da Internet no Brasil (CGI.BR) e da Rede Nacional de Ensino e Pesquisa (RNP) do Ministério de Ciência, Tecnologia e Inovação.

2 AUTORIZAÇÃO DE USO

2.1 O usuário, para utilizar os recursos computacionais do Departamento e OM subordinadas, deve solicitar, ao seu responsável imediato, a abertura de uma conta de usuário, a qual o identifica univocamente.

2.2 A permissão de acessos aos recursos computacionais do Departamento e OM subordinadas, a partir de pontos externos aos mesmos, encontra-se regulamentada na Governança de Tecnologia da Informação do DCTA (ICA 7-33) e no Anexo J desta Instrução.

2.3 Todo acesso a recursos computacionais do DCTA deve ser feito mediante autenticação (usuário e senha).

2.4 Cada usuário deve possuir o nível de acesso adequado para exercer sua função.

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 definido no Anexo M, que deve ser assinada pelo usuário solicitante e por seu responsável.

3.1.1 O responsável é o Chefe da Fração Funcional onde o usuário está desempenhando suas atividades.

3.2 O responsável pela solicitação da conta de usuário deve providenciar a abertura desta conta encaminhando a Ficha de Cadastro de Usuário (Anexo M) à Equipe de TI da OM.

3.3 As Fichas de Cadastro de Usuário ficam arquivadas junto à Equipe de TI da respectiva OM.

3.4 Para a abertura de contas de usuário em recursos computacionais locais, a OM responsável pode definir procedimentos adicionais, além dos previstos nesta Instrução.

3.5 Para abertura de contas de usuário nos recursos computacionais corporativos, o solicitante deve justificar, ao Coordenador da Equipe de TI da OM, o motivo pelo qual a conta deve ser

Continuação do Anexo A – Política de Uso dos Recursos Computacionais

aberta nos mesmos e não nos recursos computacionais locais, sendo que esta justificativa deve ser avaliada pelo responsável.

3.6 A Equipe de TI da OM é responsável por segmentar e limitar os acessos dos usuários de acordo com seus setores e necessidade de serviço, sendo vedado, a qualquer usuário que não pertença à equipe de TI, possuir conta com privilégios de administrador da rede.

4 RESPONSABILIDADES DOS USUÁRIOS

4.1 USO DAS CONTAS DE USUÁRIOS

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

4.1.2 As senhas devem ser tratadas como informação classificada do Departamento e OM subordinadas.

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 Departamento e OM subordinadas.

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, datas e outras informações pessoais;
- b) não devem conter palavras que façam parte de dicionários, ou seja, nomes de músicas, filmes e outros;
- c) ter no mínimo 14 (quatorze) caracteres, contendo, pelo menos, 1 letra minúscula, 1 letra maiúscula, 1 número e 1 caractere especial.

4.1.5 As contas de usuário e senhas não devem ser inseridas em mensagens de correio eletrônico ou qualquer outra forma de comunicação eletrônica, bem como armazenadas em arquivos eletrônicos, escritas em papel, bilhetes colados nos recursos computacionais ou guardadas em qualquer local.

4.1.6 Não deve ser usada a mesma senha para contas de usuário diferentes e para sistemas 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 devem ser imediatamente trocadas.

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

4.1.11 Todas as senhas de contas de acesso de usuário devem ser trocadas, no máximo, a cada 60 (sessenta) dias, não sendo permitida a reutilização das 6 (seis) últimas senhas.

Continuação do Anexo A – Política de Uso dos Recursos Computacionais**4.2 USO DOS RECURSOS COMPUTACIONAIS**

4.2.1 O usuário é responsável pelos eventuais arquivos e informações de cunho pessoal ou particular que possam existir nos recursos computacionais do DCTA e OM subordinadas, sendo que os mesmos, para todos os efeitos, não estão sujeitos a qualquer regime de privacidade e são passíveis de monitoramento e auditoria pelo NCTI, pela ERISC, pelo Administrador de Rede e pelo Analista de Segurança em TI da respectiva OM, em consonância com as normas e legislações vigentes.

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 através das redes de comunicação de dados do Departamento e das OM subordinadas deve ser tratada e considerada como pertencente à respectiva OM.

4.2.4 Os serviços de transmissão de informação em redes do Departamento e OM subordinadas não fornecem mecanismos automáticos de encriptação. Portanto, nenhuma responsabilidade deve ser assumida por revelação de informações transmitidas através destas redes.

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

4.2.6 Durante a utilização dos recursos computacionais, sempre que for solicitado, o usuário deve apresentar crachá funcional da OM ou autorização escrita do Responsável pela Fração Funcional pertinente, aos integrantes da Equipe de TI local, sob pena de imediata suspensão de acesso aos mesmos.

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

4.2.8 O usuário deve informar, imediatamente, qualquer violação a esta Instrução e prejuízos causados por terceiros a eles próprios e aos recursos computacionais do Departamento e OM subordinadas, ao seu chefe imediato e ao Coordenador de TI local.

4.2.9 Os Analistas de Segurança de TI das OM ou, na sua ausência, os Administradores de Rede das OM, preferencialmente, devem possuir telefones celulares funcionais cujos números devem ser divulgados.

4.2.10 Qualquer mau funcionamento de um sistema deve ser imediatamente reportado ao Administrador de Rede, pois a demora neste ato pode levar a sérios danos aos sistemas, e até mesmo a indisponibilidade dos recursos computacionais envolvidos.

4.2.11 Informações a respeito de medidas de segurança são sigilosas e não devem ser reveladas para pessoas não autorizadas.

4.2.12 Os recursos computacionais somente podem se conectar fisicamente às redes de comunicação de dados existentes no Departamento e OM subordinadas.

4.2.13 Todas as mídias removíveis, independente da fonte, devem ser verificadas com o programa antivírus antes de serem utilizadas.

Continuação do Anexo A – Política de Uso dos Recursos Computacionais

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

4.2.15 O usuário deve observar o estabelecido na política para recebimento (*download*) de arquivos, por correio eletrônico ou qualquer outro meio eletrônico, disposta na Política de Antivírus e Códigos Maliciosos (Anexo D).

4.2.16 É vedado ao usuário de recursos computacionais:

- a) utilizar os recursos computacionais para fins diversos dos funcionais ou institucionais, em desacordo com esta política e demais normas do DCTA e OM subordinadas;
- b) efetuar acesso não autorizado, atacar ou monitorar os recursos computacionais ou redes externas, utilizando recursos da RCD/DCTA, das redes locais ou outros meios;
- c) tentar ou efetuar acesso não autorizado a arquivos confidenciais do DCTA e OM subordinadas;
- d) interceptar ou tentar interceptar transmissão de dados não destinados ao seu próprio acesso, seja monitorando barramentos de dados, seja através das redes existentes no DCTA e OM subordinadas;
- e) utilizar produtos de *hardware* e *software* de uso exclusivo das Equipes de Tecnologia da Informação, dos Administradores de Rede, dos Analistas de Segurança e da Equipe ERISC;
- f) tentar ou efetuar a interferência em serviços de outros usuários ou o seu bloqueio, utilizando recursos da RCD/DCTA ou outros meios;
- g) violar ou tentar violar os sistemas de segurança dos recursos computacionais do DCTA e OM subordinadas, como quebrar ou tentar adivinhar contas de usuário ou senhas de terceiros;
- h) utilizar *softwares* em desacordo com o item 4.7 desta Política;
- i) instalar ou manter programas maliciosos (*malwares*) dentro da rede ou de Servidores;
- j) utilizar serviços 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. Está autorizado o uso de serviços de mensagem instantânea 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 sejam utilizados *softwares* homologados divulgados na página Intraer do Órgão Central do STI;
- k) interromper processos de rastreamento de vírus;
- l) utilizar, armazenar ou distribuir, nas redes de comunicação e nos recursos computacionais do DCTA e OM subordinadas, informações indesejadas, tais como, correntes de cartas, circulares e similares, materiais obscenos, ofensivos, ilegais, não éticos, comercial privado, propagandas, ameaças,

Continuação do Anexo A – Política de Uso dos Recursos Computacionais

- difamação, injúria, racismo, *spam* ou outros que venham a causar molestamento, tormento ou danos a terceiros;
- m) utilizar, armazenar ou distribuir material com conteúdo que incentive ou instrua a invasão de recursos computacionais ou redes de computadores;
 - n) instalar, alterar, configurar ou excluir os recursos computacionais, tanto de *hardware* como de *software*, existentes tanto nas redes locais como na RCD/DCTA;
 - o) remanejar recursos computacionais locais sem a prévia autorização do Responsável por sua Fração Funcional e sem o prévio conhecimento da Equipe de TI local, ou remanejar recursos computacionais corporativos sem a prévia autorização da DTIC/DCTA;
 - p) fazer má utilização dos recursos computacionais, expondo-os a choques elétricos, interferências elétricas ou magnéticas, líquidos e outros fatores que possam provocar danos aos mesmos;
 - q) realizar a transferência de qualquer informação ou documento não ostensivos existentes nos recursos computacionais do DCTA e OM subordinadas, sem a prévia autorização do Responsável pela Fração Funcional, sem a devida proteção criptográfica e sem a utilização da Rede de Comunicações de Dados Sigilosos (Rede Mercúrio), mantida e normatizada pelo CIAER;
 - r) utilizar processo criptográfico em arquivos contendo informação ou documento não ostensivos residentes nos recursos computacionais, diferente do padrão definido, sem conhecimento do Administrador de Rede local ou de quem por ele tenha sido investido nesse poder;
 - s) impedir ou dificultar, de alguma forma, a realização das atividades de monitoramento e auditoria dos recursos computacionais do DCTA e OM subordinadas; e
 - t) realizar qualquer outro procedimento de uso dos recursos computacionais não previsto nesta Política, que possa afetar de forma negativa o DCTA e OM subordinadas, outras organizações e seus usuários.

4.3 USO DO CORREIO ELETRÔNICO

4.3.1 O sistema de correio eletrônico é disponibilizado aos usuários de acordo com os objetivos e interesses do DCTA e suas Organizações subordinadas.

4.3.2 As caixas postais de correio eletrônico e seus conteúdos são de propriedade do DCTA e OM subordinadas, sendo passíveis de monitoramento e não havendo expectativa de privacidade dos usuários.

4.3.3 O serviço não é protegido por mecanismos de encriptação, de forma que todas as mensagens que circulam estão em texto claro e são, portanto, passíveis de serem lidas.

4.3.4 Para a transmissão de mensagens com informações não ostensivas deve ser observado o disposto na Política de Manipulação de Informações Classificadas (Anexo C).

4.3.5 O espaço de armazenamento reservado aos usuários no Servidor de correio eletrônico é limitado, havendo um prazo máximo para a manutenção das mensagens, definidos pela OM.

Continuação do Anexo A – Política de Uso dos Recursos Computacionais

4.3.6 Caixas postais não acessadas para verificação por um período de mais de 60 (sessenta) dias devem ser desativadas.

4.3.7 Havendo desconfiança com relação à origem e conteúdo da mensagem, antes de abri-la o usuário deve confirmar o seu envio junto ao remetente.

4.3.8 O *backup* das mensagens que foram baixadas nos recursos computacionais através de *softwares* de correio eletrônico, são de responsabilidade do usuário.

4.3.9 É recomendável que todo e qualquer correio eletrônico enviado por usuário da rede, contenha no final da mensagem, uma assinatura padrão contendo: nome completo, cargo ou função e organização.

4.3.10 Visando preservar a confidencialidade do conteúdo dos correios eletrônicos enviados por usuários, todas as mensagens devem conter ao final o seguinte aviso de confidencialidade: “As informações contidas nesta mensagem e seus anexos são classificadas, para uso restrito, sendo seu sigilo protegido por lei. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização do emissor. Caso V. Sa. não seja o destinatário, preposto, ou a pessoa responsável pelo recebimento desta mensagem, fica, desde já, notificado que qualquer divulgação, distribuição ou reprodução é estritamente proibida, sujeitando-se o infrator às sanções legais. Caso esta comunicação tenha sido recebida por engano, favor nos avisar imediatamente, respondendo esta mensagem. *“The information contained in this message and in the attached files is classified for a restrict use. If the reader of this transmittal is not the intended recipient or an agent responsible for receiving it, you are hereby notified that you have received this communication in error, and that any dissemination, distribution, retention or copy of this communication is strictly prohibited. In this case, please immediately reply this message to the e-mail address above”*.”

4.3.11 O monitoramento descrito nesta Política tem por objetivo verificar o respeito do usuário, às regras estabelecidas no presente instrumento, bem como produzir prova de eventual violação das condições constantes no presente e na legislação em vigor, uma vez que todos os atos praticados através do correio eletrônico, bem como dos *sites* navegados na Internet são exercidos estritamente para as atividades laborativas, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, o que o usuário, declara, expressamente estar ciente.

4.3.12 É vedado ao usuário de correio eletrônico:

- a) tentar acesso não autorizado à caixa postal de terceiros;
- b) enviar materiais obscenos, ofensivos, ilegais, não éticos, comercial privado, 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 DCTA e OM subordinadas e de seus usuários, para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida autorização dos responsáveis pelas listas;
- f) transmitir e retransmitir mensagens com finalidade comercial de interesse particular ou para obtenção de ganhos financeiros pessoais;

Continuação do Anexo A – Política de Uso dos Recursos Computacionais

- g) abrir e enviar quaisquer arquivos anexados a mensagens de correio eletrônico, sem antes passá-los pelo programa antivírus;
- h) redirecionar as caixas de correio eletrônico do DCTA e OM subordinadas, da qual o usuário é o titular, para correios de provedores externos;
- i) executar ou participar de atividades de interceptação e/ou revelação de informações que trafegam nas redes de comunicação de dados, exceto na qualidade de integrante da ERISC, ou de Administrador de Rede local, ou de Analista de Segurança local, sempre que as circunstâncias exigirem, de acordo com o disposto nesta Instrução;
- j) enviar mensagens em resposta a qualquer assunto na qualidade de representante legal da OM, sem autorização formal da autoridade competente;
- k) realizar qualquer outro procedimento de uso do correio eletrônico não previsto nesta Política, que possa afetar de forma negativa o DCTA e OM subordinadas, outras organizações e seus usuários; e
- l) utilizar correio eletrônico particular para o trato de assuntos institucionais e laborativos.

4.4 CONEXÃO A REDES EXTERNAS

4.4.1 O usuário, ao se conectar logicamente às redes de comunicação de dados externas, por meio da RCD/DCTA, deve observar rigorosamente as normas, os procedimentos e as diretrizes daquelas Redes, bem como utilizá-las estritamente para fins funcionais.

4.4.2 São autorizadas conexões lógicas a instituições bancárias e mercantis, em volume razoável, necessárias ao atendimento de necessidades pessoais do usuário, com o objetivo de proporcionar-lhe maior comodidade e agilidade.

4.4.3 É vedado ao usuário realizar qualquer outro procedimento de uso das redes externas não previsto nesta Política, que possa afetar de forma negativa o DCTA e OM subordinadas, outras organizações e seus usuários.

4.4.4 Qualquer saída para a rede externa (como a Internet) deve passar pelo *firewall* que permita o controle de segurança de perímetro gerenciado pelo NCTI/DCTA, e possibilite a gestão de segurança pela ERISC/DCTA, sendo que essa saída deve ser previamente autorizada pela DTIC/DCTA.

4.5 CONEXÃO À RCD/DCTA e Redes Locais

4.5.1 É vedado ao usuário realizar qualquer tipo de ligação física à RCD/DCTA e Redes Locais.

4.5.2 É vedado ao usuário conectar nas redes locais, na RCD/DCTA ou nos recursos computacionais do DCTA e OM subordinadas, equipamentos de qualquer natureza, funcional ou pessoal, sem o conhecimento e autorização explícita dos responsáveis por essas redes e por esses recursos.

4.5.3 A utilização de rede sem fio, ou uso de tecnologias baseadas em propagação de ondas eletromagnéticas em rede, deve observar o disposto na Política de Acesso Remoto, Anexo J.

Continuação do Anexo A – Política de Uso dos Recursos Computacionais

4.6 DISPONIBILIZAÇÃO DE HOME PAGE (PÁGINA ELETRÔNICA)

4.6.1 É vedada a veiculação de *home page* com conteúdo não institucional ou não funcional nas redes de comunicação de dados do DCTA e OM subordinadas.

4.6.2 Nenhuma informação sigilosa deve constar das *home pages* veiculadas nas redes de comunicação de dados do DCTA e OM subordinadas.

4.6.3 O conteúdo das *home pages* do DCTA e OM subordinadas deve ser submetido à apreciação de suas respectivas Assessorias de Comunicação Social, sendo que, onde elas não existirem, o conteúdo deve ser, preferivelmente, submetido à apreciação da Assessoria de Comunicação Social do DCTA.

4.6.4 É vedada ao usuário a veiculação de *home page* nas redes de comunicação de dados do DCTA e OM subordinadas sem a autorização formal da Direção/Reitoria/Presidência/Prefeitura/Chefia/Comando da respectiva OM.

4.7 USO DE SOFTWARE

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

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

4.7.3 Os *softwares* cedidos por produtores ou seus representantes legais, a título de demonstração ou teste, devem estar acompanhados de contratos específicos formalizados.

4.7.4 O *software* de propriedade do usuário ou por ele contratado de terceiros, deve estar acompanhado do seu contrato específico formalizado ou seu termo de responsabilidade, junto ao comprovante de registro do produto, com licença compatível para o uso corporativo, quando da utilização do mesmo no âmbito do DCTA e OM subordinadas e sua utilização só pode ser realizada com a autorização da Equipe de TI local.

4.7.5 Os *softwares* classificados como de domínio público *freeware* devem seguir orientação específica do Coordenador de TI do DCTA e das OM subordinadas; e

4.7.6 Os *softwares* utilizados devem estar alinhados às necessidades da Organização, e utilizados somente para o desenvolvimento das atividades funcionais do usuário.

4.7.7 É vedado ao usuário de qualquer *software*:

- a) escrever, gerar, compilar, copiar, propagar, executar ou tentar introduzir nos recursos computacionais do DCTA e OM subordinadas, códigos ou *softwares* contendo processos destrutivos;
- b) invadir recursos computacionais do DCTA e OM subordinadas, com exceção daqueles usuários cuja função esteja relacionada com a utilização destas ferramentas para os fins de monitoramento e auditoria, na forma prevista nesta Política;
- c) utilizar os *softwares* do DCTA e OM subordinadas em atividades particulares, exceto naquelas previstas no item 4.4.2;

Continuação do Anexo A – Política de Uso dos Recursos Computacionais

- d) explorar, sem autorização, aplicações e sistemas corporativos para obter ou alterar dados;
- e) realizar qualquer outro procedimento de uso de *software* não previsto nesta Política, que possa afetar de forma negativa o DCTA e OM subordinadas, outras organizações e seus usuários;
- f) possuir senha de administrador de estação de trabalho, a fim de que não efetuem instalação de *software*; e
- g) utilizar softwares não regularizados nos recursos computacionais da organização e em seus recursos computacionais particulares, quando esses sejam autorizados a se conectarem às redes de comunicação de dados locais das OM e na RCD/DCTA.

4.8 USO DE VIDEOCONFERÊNCIA E VOIP

4.8.1 Os projetos que visam à implantação de soluções de videoconferência diferentes daquelas padronizadas para o COMAER, deverão ser submetidos à DTIC/DCTA para análise e posterior encaminhamento da proposta para análise e aprovação do Órgão Central do STI, com antecedência mínima de 120 (cento e vinte) dias antes da data prevista de entrada em operação.

4.8.2 Para assuntos de caráter geral, via Internet, deverão ser utilizados os sistemas de videoconferência ou VoIP padronizados pela DTI para o COMAER, tanto no âmbito interno da Organização (rede local) quanto entre Organizações.

4.8.3 Para assuntos sigilosos, deverão ser utilizados os sistemas de videoconferência ou VoIP padronizados pela DTI para o COMAER, mediante o uso de solução corporativa que possibilite a comunicação segura via Intraer.

4.9 COMPUTAÇÃO MÓVEL

4.9.1 A utilização de dispositivos portáteis (*notebooks, tablets, smartphones* e similares) deve ser precedida de medidas que visem à orientação dos usuários dos equipamentos e, se necessário, do emprego de soluções de criptografia de dados, respeitando normas gerenciais e técnicas existentes no COMAER, sendo vedado o uso dos referidos dispositivos portáteis pessoais para o trato de informação classificada ou sob restrição de acesso de cunho funcional, conforme item 6.5.38 da ICA 205-47/2015 - Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ISAS).

4.9.2 É vedada a utilização de computadores pessoais (particulares) na RCD/DCTA e nas Redes Locais das OM subordinadas. Excepcionalmente, em situações particulares, pode ser autorizado o uso, desde que solicitado e expressamente autorizado pelo Diretor/Reitor/Presidente/Prefeito/Chefe/Comandante da respectiva OM.

Anexo B – Política de Administração de Recursos Computacionais

Na administração dos recursos computacionais do DCTA e OM subordinadas, deve ser observado o que se segue.

1 ADMINISTRADOR DE REDE

1.1 Administrar e manter a rede local de acordo com os procedimentos definidos nesta Instrução e nas demais normas pertinentes.

1.2 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.

1.3 Abrir, administrar e encerrar contas de usuários.

1.4 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.

1.5 Controlar a validade da assinatura do Responsável por contas de usuários.

1.6 Controlar o tempo de validade das contas de usuário, segundo o critério estabelecido pela Equipe de TI de sua OM.

1.7 Controlar o tempo máximo de inatividade das contas de usuário, bloqueando-as findo o prazo definido pela Equipe de TI de sua OM, o qual deve atender o definido no item 2.2.3.8 desta Instrução.

1.8 Quando informado sobre a transferência de usuário entre Frações Funcionais da OM, solicitar o preenchimento de uma nova Ficha de Cadastro de Usuário (Anexo M), mantendo a conta original.

1.9 Quando informado sobre o desligamento de usuário, providenciar o encerramento da respectiva conta de usuário.

1.10 Recadastrar periodicamente as contas de usuário na sua rede local.

1.11 A cada 6 (seis) meses enviar, aos responsáveis por contas de usuários, informações atualizadas sobre as contas pelas quais se responsabilizaram, para efeito de manutenção das referidas informações no sistema local de cadastro de conta de usuários.

1.12 Implementar e manter mecanismos para exigir dos usuários a mudança periódica de senhas em intervalos de até 60 (sessenta) dias. Findo este prazo, realizar a troca de senha. Em ambos os casos, cada OM deve definir mecanismos próprios para a troca de senha.

1.13 Manter mecanismos para impedir a repetição de senhas considerando as 6 (seis) últimas senhas utilizadas.

1.14 Prover mecanismos para bloquear a conta de usuário após 3 (três) tentativas de acesso a um recurso computacional por erros de senha.

1.15 Prover meios para suspender as sessões de uma estação de trabalho, após um período de inatividade, e para encerrar as sessões, após um período de suspensão.

1.16 Prover a segurança e a integridade dos recursos computacionais disponíveis, dos serviços aos usuários e dos dados armazenados nas máquinas Servidoras da rede sob sua responsabilidade.

1.17 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.

Continuação do Anexo B – Política de Administração de Recursos Computacionais

1.18 Suspender temporariamente serviços da rede local em caso de violação ou suspeita de violação dos recursos computacionais locais, informando o fato à Direção/Reitoria/Chefia/Comando/Prefeito/Presidente da OM envolvida.

1.19 Analisar a rede local sob 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 sua responsabilidade ou da RCD/DCTA.

1.20 Configurar o Servidor de correio eletrônico para gerar automaticamente estatísticas de uso de cada usuário, sempre que possível.

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

1.22 Realizar monitoramento e auditoria na utilização dos recursos computacionais locais, com conhecimento prévio do Diretor/Reitor/Chefe/Comandante/Prefeito/Presidente da respectiva OM, visando preservar a integridade das informações institucionais e a imagem do DCTA e da OM subordinada, podendo fiscalizar:

- a) conteúdo de mensagens transmitidas e recebidas;
- b) arquivos armazenados em disco;
- c) programas de computador instalados;
- d) fluxo de pacotes na rede local;
- e) arquivos específicos de controle (*logs*);
- f) programas de computador em execução; e
- g) outros recursos computacionais, no que for indicado pela DTIC/DCTA.

1.23 Limitar o espaço de armazenamento reservado aos usuários no Servidor de correio eletrônico.

1.24 Desativar caixas postais não acessadas por um período de mais de 60 (sessenta) dias.

1.25 Configurar o *software* de correio eletrônico para pedir senha ao entrar na conta de correio.

1.26 Trocar as senhas de acesso aos servidores de administração da equipe de TI, periodicamente, segundo o grau de segurança necessário à sua OM, em um período nunca superior a 60 (sessenta) dias.

1.27 Enviar esforços para evitar o acesso simultâneo de um usuário a um mesmo recurso computacional.

1.28 Executar programas, de forma sistemática, para verificação de vulnerabilidades em senhas de usuários. Bloquear as contas de usuário que não estiverem seguindo os padrões estabelecidos por esta Instrução, notificando os usuários envolvidos.

1.29 Responsabilizar-se por outras tarefas inerentes a sua função que forem determinadas pela Direção/Reitoria/Chefia/Comando/Prefeito/Presidente de sua OM de origem.

Continuação do Anexo B – Política de Administração de Recursos Computacionais

2 EQUIPE DE TECNOLOGIA DA INFORMAÇÃO

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

2.2 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.

2.3 Instalar os softwares necessários ao desenvolvimento das atividades dos usuários e, em especial no que concerne a software de propriedade particular, observar o disposto no item 4.7 da Política de Uso dos Recursos Computacionais (Anexo A).

2.4 Instalar e manter atualizado, em todos os recursos computacionais utilizados pelos usuários, o *software* antivírus corporativo, homologado e fornecido pelo COMAER, conforme estabelecido na Política de Antivírus e Códigos Maliciosos (Anexo D).

2.5 Desabilitar a opção de execução automática de arquivos anexados dos *softwares* clientes de correio eletrônico.

2.6 Verificar a existência de dispositivos não autorizados de conexão remota à rede, desabilitando e removendo esses dispositivos.

2.7 Encaminhar à Divisão de Tecnologia da Informação e Comunicação do DCTA (DTIC/DCTA) requisições de novas instalações ou alterações nas redes internas de comunicações de dados locais de sua OM.

2.8 Zelar para que os sistemas multiusuários ou sistemas de comunicação 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.

2.9 Zelar para que desenvolvedores de aplicativos garantam que seus programas suportem a autenticação de usuários individuais, e não de grupos.

2.10 Prover meios para que os arquivos com registros de eventos (*logs*) sejam mantidos por, pelo menos, 2 (dois) anos. Durante este período, estes *logs* 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 continuamente. As informações relevantes devem ser mantidas armazenadas *off-line* até que sejam necessárias. Estas informações incluem: registros de acesso aos arquivos, registros de execução de aplicativos, assim como cópias de todos os arquivos potencialmente envolvidos.

2.11 Dar ciência aos usuários que todas as atividades relacionadas ao uso dos recursos computacionais do DCTA e OM subordinadas são passíveis de registro, monitoramento e auditoria.

2.12 Notificar, individualmente, os usuários a respeito dos atos específicos que constituem violações de redes e recursos computacionais.

2.13 Ajustar o tamanho máximo permitido para envio e/ou recepção de mensagens e/ou arquivos segundo as necessidades de sua OM.

2.14 Excepcionalmente, por solicitação do Diretor/Reitor/Presidente/Prefeito/Chefe/Comandante, poderá ser autorizado o uso de computadores pessoais no âmbito do DCTA e OM subordinadas, desde que expressamente autorizado pela Direção do DCTA (item 3.5.2.1

Continuação do Anexo B – Política de Administração de Recursos Computacionais

da NSCA 7-13). Antes da autorização, deve-se validar a autenticidade dos softwares existentes nesses computadores, observando o disposto no item 4.7 desta ICA.

2.15 Dar ciência a todo usuário 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.

2.16 Procurar implantar o conteúdo da cartilha “Boas Práticas em Segurança da Informação”, disponível no site do Tribunal de Contas da União, e verificar seus procedimentos de segurança conforme ICA 200-5 – Gerenciamento de Plano de Segurança Orgânica do Comando da Aeronáutica.

2.17 Prover meios para moderar a utilização de serviços de mensagem instantânea ou de bate-papo disponíveis na Internet, aqueles hospedados e mantidos por entidades externas ao COMAER, por estes serem, comprovadamente, difusores de programas maliciosos. Em casos especiais, e mediante autorização especial da Diretoria de TI do COMAER, serviços de mensagens instantâneas poderão ser utilizados para fins institucionais/corporativos.

2.18 Agendar e realizar o processo de execução de cópias de segurança (*backup*) de servidores e armazenar as mídias correspondentes conforme procedimento definido nesta Instrução.

2.19 Pesquisar, obter e aplicar os pacotes de correção e atualização disponibilizados pelos fabricantes dos recursos computacionais utilizados na rede local. Preferivelmente, esses dados devem ser obtidos nos servidores disponibilizados no NCTI para essa finalidade, garantindo a padronização e uniformidade das atualizações nos recursos computacionais da organização.

2.20 Formalizar à Direção/Reitoria/Chefia/Comando/Prefeito/Presidente da OM, observando a cadeia de comando, se comprovada qualquer violação dos recursos computacionais, pelo usuário, para que sejam tomadas as medidas cabíveis, observando, onde aplicável, o disposto na NSCA 7-13/2022.

2.21 Implantar controle de entrada e saída, da OM, de seus recursos computacionais.

2.22 Difundir constantemente as normas e procedimentos para o uso de recursos computacionais, estabelecidos no Anexo A.

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.

- 1.** Os acessos às informações classificadas devem ser registrados e exigir a autenticação do usuário, do Recurso Computacional e do ponto de acesso.
- 2.** Sendo possível, o sistema deve emitir avisos para o Administrador de Rede no caso de tentativas de acesso não autorizado aos dados classificados.
- 3.** A transmissão de dados classificados por meio eletrônico somente pode ocorrer com a utilização de um mecanismo de criptografia, utilizando-se de um programa de encriptação de dados, com algoritmo de estado, observando-se o disposto na ICA 205-47, bem como no Decreto nº 7.845, de 14 de novembro de 2012 e na Instrução Normativa GSI/PR nº 3, de 6 de março de 2013.
- 4.** Dados classificados e mantidos nos recursos computacionais do DCTA e OM subordinadas devem estar criptografados através do programa de criptografia, a qual observa o disposto na ICA 205-47, bem como no Decreto nº 7.845, de 14 de novembro de 2012 e na Instrução Normativa GSI/PR nº 3, de 6 de março de 2013.
- 5.** As cópias de segurança (*backup*) devem ser mantidas de acordo com a Política de Segurança Lógica (Anexo G).
- 6.** Informações classificadas não devem ser repassadas ou enviadas para fora do DCTA e OM subordinadas sem a devida autorização formal da autoridade competente.
- 7.** Toda exclusão de informações classificadas deve ser executada através de um processo de apagamento seguro.
- 8.** Quando os recursos computacionais não estiverem sendo utilizados e as informações neles contidas forem classificadas, estas devem ser apagadas, conforme item anterior. Caso seja necessário que estas informações permaneçam no recurso computacional, o mesmo deve ser armazenado em um local seguro, com acesso restrito ao pessoal responsável.
- 9.** Em caso de extravio de recursos computacionais contendo informações classificadas, o Setor de Inteligência da OM deve ser imediatamente comunicado pelo Diretor/Reitor/Chefe/Comandante/Prefeito/Presidente da respectiva OM, via parte reservada, e todas as chaves/senhas compartilhadas em outros recursos devem ser trocadas.
- 10.** A critério do Diretor/Reitor/Chefe/Comandante/Prefeito/Presidente da OM, deve ser aberto processo de sindicância para apuração do extravio de recursos computacionais. Caso o mesmo tenha ocorrido externamente às dependências da OM, também deve ser aberto, em sendo possível, Boletim de Ocorrência na Delegacia mais próxima da ocorrência do fato.
- 11.** Deve existir uma ferramenta para a verificação regular e automática da integridade e autenticidade dos dados classificados em uso para alertar os Administradores de Rede sobre toda e qualquer alteração.
- 12.** Sempre que a encriptação for usada, a versão original do documento somente deve ser apagada após o processo de deciptação ser executado e verificado o correto restabelecimento da versão original.
- 13.** Chaves de encriptação usadas pelo Departamento e OM subordinadas são sempre classificadas como informação sigilosa 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.

Continuação do Anexo C – Política de Manipulação de Informações Classificadas

14. Não deve ser feita a impressão de informações classificadas em dispositivos de impressão de rede. Excepcionalmente, em caso de inexistência de dispositivo de impressão dedicado a uma fração funcional, poder-se-á utilizar uma impressora de rede mediante o uso de senha no processo de impressão.

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

16. Prover informações para que seja elaborado o Relatório de Impacto de Proteção de Dados (RIPD) nos processos, projetos e serviços que utilizarem informações classificadas contendo dados pessoais para fins de defesa nacional, segurança do Estado, que poderão ou deverão ser solicitados pela Autoridade Nacional de Proteção de Dados (ANPD) nos casos previstos na Lei Geral de Proteção de Dados Pessoais (LGPD).

17. Não podem ser utilizadas soluções de assinatura eletrônica baseadas em nuvem (como o Gov.br) para assinaturas de documentos de acesso restrito e de documentos classificados (RESERVADO, SECRETO ou ULTRASSECRETO).

Anexo D – Política de Manipulação de Informações Classificadas

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

1. Todos os computadores deste Departamento e OM subordinadas devem ter instalados o *software* antivírus corporativo e outros utilitários de *software* determinados pelo Órgão Central do STI, que previnam ou mitiguem ataques gerados por programas maliciosos.
2. O Órgão Central do STI é responsável pela padronização e fornecimento do *software* de antivírus corporativo, porém, as equipes de TI deste Departamento e OM subordinadas podem adquirir produtos distintos do padronizado, desde que autorizado pelo Órgão Central, e com recursos próprios.
3. Preferencialmente, o Servidor que executa o antivírus corporativo no DCTA e OM subordinadas deve ser dedicado.
4. Os computadores infectados devem ser fisicamente desconectados da rede até que seja garantida a sua descontaminação.
5. O *software* antivírus deve ser configurado para que seja periodicamente atualizado e executado em intervalos regulares, de preferência de maneira automática.
6. O *software* antivírus deve emitir alerta para os Administradores de Rede quando da detecção de vírus, bem como a ERISC deve ser notificada pela Equipe de TI local.
7. Habilitar no recurso computacional a opção de verificação automática de vírus nas mídias removíveis.
8. Fica estabelecida a seguinte política para *download* (recebimento) de arquivos, por correio eletrônico ou qualquer outro meio eletrônico:
 - a) excepcionalmente, e quando estritamente necessário ao exercício das atividades funcionais do usuário, é permitido o recebimento de arquivos comerciais, tais como imagens, textos e outros, que devem ser sempre rastreados (“escaneados”) por antivírus antes de serem abertos. Atentar para o fato que alguns vírus usam de fontes conhecidas para se propagarem;
 - b) é estritamente proibido o carregamento de qualquer arquivo executável recebido pelos usuários, colaboradores ou prestadores de serviço com terminações como .EXE, .COM, .SCR, ou outras que possam comprometer o sistema através da execução de comandos maliciosos, vírus, *trojans* e outros similares;
 - c) quando se tratar de atualização de *software*, que envolva arquivos dos tipos citados no item anterior, a Equipe de TI local é a responsável por executar o serviço.
9. Quando da utilização de correio eletrônico, evitar clicar em *links* desconhecidos contidos nas mensagens recebidas, pois eles podem ser *links* para códigos maliciosos.

Anexo E – Política de *Firewall* e Recursos Computacionais Localizados na Zona Desmilitarizada da RDC/DCTA

O DCTA e OM subordinadas devem configurar Servidores de *Firewall*, Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS) e *Firewall* de Aplicação Web (WAF) entre suas respectivas redes de comunicação de dados locais e outra rede de comunicação de dados corporativa de forma a atender as recomendações a seguir.

1. O *firewall* deve 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 uso abusivo, de modo que:

1.1 Deve ser controlado e monitorado pelos Administradores de Rede, através da utilização de *softwares* de detecção de intrusão, auditoria interna e outros *softwares* específicos.

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

1.3. Deve adotar medidas de defesa em profundidade utilizando-se de mecanismos diversos de proteção contra falhas de nível de defesa.

1.4 Todas as OM subordinadas devem gerenciar seu próprio firewall para acessos Internet e Intraer sob responsabilidade de suas respectivas equipes de TI.

2. O ponto de entrada e saída das Redes Locais das OM deverá ser controlado e monitorado por IDS e IPS, com configuração condizente com os serviços de TI prestados pela organização;

3. Todo serviço disponibilizado para a Internet deve ser alocado em uma zona desmilitarizada (DMZ), onde devem ser feitos os controles necessários para a proteção e monitoração de tentativas de invasão, negação de serviços, dentre outros;

4. A solução de IDS/IPS pode estar inclusa em uma solução de *Firewall*;

5. Sempre que o *firewall*, IDS, IPS ou WAF possuir registro que indique a possibilidade de um incidente de segurança, o Administrador de Rede deverá notificar a ERISC pelo correio eletrônico abuse@cta.br, com as evidências do evento suspeito; e

6. Sempre que tomar conhecimento de alguma ameaça cibernética, a ERISC e o NCTI poderão propor a implementação de bloqueios e criação de assinaturas nas soluções de *Firewall*, IDS/IPS e WAF.

Anexo F – Política de Segurança Física

Para todos os recursos computacionais utilizados no DCTA e OM subordinadas, pertencentes ao DCTA e OM subordinadas, ou a terceiros, conectados ou não à RCD/DCTA, que mantenham ou não dados importantes e/ou classificados, devem ser observados os procedimentos descritos a seguir.

1. Os equipamentos de conectividade (Roteadores, *Switches*, Servidores e outros dispositivos de interconexão) devem estar em salas exclusivas e com acesso restrito à Equipe de TI da respectiva rede de comunicação de dados, conforme normas e legislações vigentes.
2. Estes equipamentos devem possuir, sempre que possível, quadros de alimentação exclusivos que devem permanecer trancados e com acesso restrito a pessoas habilitadas e com a devida ciência do Administrador de Rede Local.
3. As salas onde estes equipamentos estão localizados devem:
 - 3.1 Ser providas de mecanismos de tranca e controle de acesso baseadas no uso de biometria e de circuito fechado de câmeras, devendo os registros dos acessos permanecerem arquivados por, no mínimo, 90 dias;
 - 3.2 Ser providas de mecanismos de monitoramento e de controle ambiental, de forma a minimizar ameaças potenciais como roubo, fogo, explosivos, fumaça, poeira, vibração, efeitos químicos, temperatura, umidade, dentre outras; e
 - 3.3 Ser mantidas limpas, organizadas e conservadas, sendo proibido o consumo de alimentos, bebidas, cigarros e similares nestes locais.
4. Usuários não autorizados não podem ter acesso a esses recursos computacionais.
5. Para a conexão de computadores ao *backbone* sempre adotar *switches* ou equipamentos equivalentes que possibilitem o controle de portas.
6. Os recursos computacionais devem passar por processo de manutenção preventiva periódica para evitar falhas de *hardware*. Todas as manutenções preventivas ou corretivas devem ser documentadas para que haja um histórico dos problemas ocorridos e das respectivas soluções.
7. Caso haja necessidade da entrada de outra pessoa em salas de acesso restrito, contendo recursos computacionais, que não os membros da Equipe de TI local, ela deve ser sempre acompanhada por pelo menos um dos membros da referida Equipe.
8. A alimentação elétrica para os recursos computacionais deve ser exclusiva, constante e em níveis adequados ao funcionamento desses recursos, bem como possuir aterramento apropriado e proteção contra surtos e sobretensões, seguindo-se as recomendações fornecidas pelo fabricante de cada equipamento.
9. Os equipamentos de interconexão da Rede Local de cada OM à RCD/DCTA, devem estar alimentados por *no-break* com autonomia mínima de 20 minutos a plena carga.
10. O cabeamento interno das Redes Locais, assim como o de interconexão destas redes, devem estar encapsulados em conduítes e/ou calhas que os protejam de interrupções acidentais, e devem estar adequadamente identificados para que não sejam expostos indevidamente. O acesso a estes cabeamentos somente deve ser permitido a pessoa autorizada e qualificada para tal.
11. Nenhum recurso computacional pode ser movimentado sem o expresse consentimento do detentor local do material carga e com o conhecimento e aval do Administrador de Rede Local, 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

Continuação do Anexo F – Política de Segurança Física

Política. Deve-se, ainda, manter um registro de entrada e saída contendo horário, data e nome do responsável pela movimentação deste recurso.

12. A manutenção dos equipamentos da rede de comunicação de dados local das OM do DCTA e da RCD/DCTA, deve ser feita, preferencialmente, nas dependências da OM à qual pertence o equipamento, com a supervisão de algum membro da Equipe de TI Local.

12.1 Quando a manutenção se referir a equipamentos do *backbone* da RCD/DCTA, a supervisão deve ser realizada por um integrante do NCTI ou da ERISC do DCTA, no que for indicado por aquele Núcleo.

13. 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 deve ter todos os arquivos (de configuração e/ou de dados) apagados de forma segura, quer estejam em discos (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 deve ser executada quantas vezes forem necessárias, de forma a impossibilitar a recuperação de informações anteriormente armazenadas.

14. Cada Equipe de TI local deve 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.

15. Cada Equipe de TI local deve manter um inventário atualizado dos recursos computacionais com no mínimo as informações abaixo:

- a) local e usuário para contato;
- b) detalhamento do hardware e sistema operacional utilizados;
- c) principais funções e aplicativos.

16. Todos os recursos computacionais pertencentes à RCD/DCTA devem estar com seus respectivos gabinetes lacrados com lacres plásticos numerados ou com lacres antiviolação, permitindo, assim, constatar se o mesmo foi violado. Estes equipamentos somente podem ser abertos pela Equipe de TI de cada OM.

17. Em caso de violação do lacre, a Equipe de TI Local deve 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 Local, implica na sua responsabilização.

18. As cópias de segurança e mídias de backup devem ser armazenadas em compartimentos à prova de fogo e água, devendo ser separadas fisicamente do local do sistema copiado, em outro prédio.

19. Todos os equipamentos pertencentes à rede do Departamento e OM subordinadas devem ser protegidos com dispositivos antirroubo, se localizados em ambientes abertos.

20. No desligamento de militar ou servidor de sua OM, solicitar a devolução dos recursos computacionais de propriedade da organização, a qual é condição para o desimpedimento de sua ficha pela Equipe de TI de sua respectiva OM.

21. Todos os recursos computacionais devem ser desligados no final do expediente de trabalho, quando não houver previsão de utilização dos mesmos.

22. Os Servidores de rede, *switches* e outros equipamentos de conectividade existentes nas OM, devem permanecer ligados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

Continuação do Anexo F – Política de Segurança Física

Caso sejam desligados por motivo de manutenção programada ou força maior, os usuários devem ser comunicados previamente.

23. Equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo classificados somente poderão estar ligados a redes de computadores seguras e que sejam fisicamente e logicamente isoladas de qualquer outra, observando-se o disposto na ICA 205-47.

Anexo G – Política de Segurança Lógica

Para todos os recursos computacionais utilizados no DCTA e OM subordinadas, pertencentes ao DCTA e OM subordinadas, ou a terceiros, conectados ou não à RCD/DCTA, que mantenham ou não dados importantes e/ou classificados, devem ser observados os procedimentos descritos a seguir.

1. Para ter acesso ao serviço disponibilizado pelas redes de comunicação de dados locais e pela RCD/DCTA, bem como a um sistema de TI ou outro recurso computacional, o usuário necessita ser cadastrado e a partir de então, identificar-se através de uma Conta de usuário e uma senha ou, quando necessário, de dispositivos de segurança adicionais, tais como *smart cards*, *tokens* e interfaces com biometria.
2. A necessidade de utilização de dispositivos de segurança adicionais, tais como *smart cards*, *tokens* e interfaces com biometria, fica sujeita à avaliação por parte do CIAER, mediante solicitação direta do Diretor/Reitor/Chefe/Comandante/Prefeito/Presidente da OM.
3. 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.
4. O acesso aos recursos computacionais somente deve ser feito pelo usuário quando necessário e expressamente autorizado pelo Chefe da Fração Funcional do usuário e pelo Administrador de Rede local.
5. A permissão de acesso total ou equivalente deve ser removida dos diretórios compartilhados nos recursos computacionais utilizados como Servidores, salvo aqueles que devem ser disponibilizados ao público externo nos Servidores alocados na Zona Desmilitarizada (DMZ), com a permissão única de leitura.
6. 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.
7. Cada Equipe de TI local deve providenciar as cópias de segurança das informações armazenadas em cada Servidor sob sua responsabilidade, com o intuito de prover uma recuperação rápida dos dados armazenados em caso de falha ou interrupção de algum serviço.
8. A periodicidade e o tempo de armazenamento das cópias de segurança devem ser baseados no seu grau de criticidade para operações do dia a dia, sendo exigidas periodicidades diária, semanal, mensal ou anual, observando o disposto no Anexo L (Política de Backup) da NSCA 7-13.
9. O agendamento do processo de execução das cópias de segurança deve ser feito, obrigatoriamente, pelo Administrador de Rede Local.
10. A disponibilidade da rede deve ser mantida fazendo-se cópias de segurança programadas e regulares. Todos os recursos de segurança, atributos de arquivos e diretórios, devem ser respeitados e mantidos pelo procedimento de cópias de segurança.
11. Tanto as cópias quanto as funções de recuperação devem ser testadas regularmente.
12. Se um sistema de controle de acesso falhar, este deve negar todos os privilégios aos usuários até a eliminação da falha.
13. Para os sistemas isolados, o usuário é o responsável pelo processo de execução das cópias de segurança, enquanto que para sistemas multiusuários, o Administrador de Rede é o responsável.

Continuação do Anexo G – Política de Segurança Lógica

14. Todas as informações classificadas (sensíveis), valiosas ou críticas armazenadas nos recursos computacionais e em uma rede devem ser periodicamente copiadas, baseando-se no seu grau de criticidade para operações do dia a dia, podendo exigir, periodicidade diária, semanal ou mensal.

15. O armazenamento do conjunto de mídias de *backup* de Servidores é de responsabilidade do Administrador de Rede local, assim como o das estações de trabalho é de responsabilidade do usuário.

Anexo H – Política de Segurança dos Serviços de Rede

Na disponibilização dos serviços de rede da RCD/DCTA, e das Redes Locais a ela conectadas, deve ser observado o que se segue.

1. Os Servidores conectados à RCD/DCTA, a princípio, são privativos para uso da comunidade de usuários interna, devendo estar protegidos contra acessos indevidos.
2. Os Servidores que disponibilizam serviços para a comunidade de usuários externa devem estar na zona desmilitarizada (DMZ), e sempre ser monitorados contra tentativas de invasão e negação de serviços.
3. Cada serviço deve ser disponibilizado em um ou mais Servidores dedicados, sendo que este deverá, sempre que possível, comportar apenas um serviço.
4. A responsabilidade pela manutenção dos serviços na RCD/DCTA é do Chefe do Núcleo Corporativo de TI (NCTI) e nas Redes Locais é do Coordenador da Equipe de TI da OM.
5. Serviços ou protocolos inseguros devem ser substituídos por equivalentes mais seguros, sempre que existirem, antes de serem disponibilizados na RCD/DCTA e suas sub-redes. Necessidades específicas devem ser tratadas pelo Administrador de Rede local, com a anuência do NCTI e validação pela ERISC do DCTA.
6. Os protocolos de monitoramento e gerenciamento (*SNMP e similares*) são de uso exclusivo dos Administradores de Rede, dos membros do NCTI e da ERISC/DCTA. No caso do *backbone* da RCD/DCTA, o monitoramento e gerenciamento será feito exclusivamente pelo NCTI e pela ERISC do DCTA.
7. O acesso ao serviço *DNS* deve ser limitado à consulta para a resolução de nomes. A transferência de zonas de domínio internas deve ser somente para Servidores secundários.
8. Deve-se isolar o Servidor *DNS* de Rede Local do Servidor *DNS* de Internet, protegendo-o contra acessos externos à RCD/DCTA.
9. O serviço de banco de dados deve ter uma política específica, em conformidade com a Política de Manipulação de Informações Classificadas.
10. O serviço de sincronização de relógios (*NTP – Network Time Protocol*) deve ser mantido e provido pelo Núcleo Corporativo de TI, através de Servidores disponibilizados no *backbone* da RCD/DCTA, os quais devem ser os únicos autorizados a se conectar com o serviço *NTP* externo. Cada sub-rede da RCD/DCTA deve possuir um Servidor ou serviço conectado ao Servidor *NTP* central do DCTA, responsável pela sincronização de tempo em seus respectivos subdomínios. Todos os recursos computacionais do DCTA e OM subordinadas devem estar configurados para serem sincronizados por este serviço na sua Rede Local.
11. Repositórios de software de interesse corporativo devem ser mantidos e providos pelo Núcleo Corporativo de TI, a partir de onde as OM subordinadas ao DCTA habilitadas podem obter pacotes de softwares e instalá-los em seus recursos computacionais.
12. Em caso de comprometimento da segurança de um servidor, este deve ser imediatamente desconectado da rede, ser mantido ligado, e o incidente deve ser imediatamente reportado à ERISC pela Equipe de TI Local.
13. Todos os *softwares* dos recursos computacionais devem estar atualizados com os *patches* mais recentes previamente testados em um ambiente isolado.
14. Os *logs* de serviços, bem como dos sistemas operacionais dos servidores e de acessos a *switches* e roteadores, devem ser mantidos por um período mínimo de 6 (seis) meses. Qualquer atividade suspeita deve ser analisada e, constatando-se um incidente de segurança, a ERISC deve ser imediatamente comunicada.

Continuação do Anexo H – Política de Segurança dos Serviços de Rede

15. A responsabilidade da manutenção, monitoramento de funcionamento e segurança, bem como da aplicação dos *patches* dos sistemas é do Chefe da Equipe de TI da OM, no âmbito de suas respectivas sub-redes e subdomínios.

16. Os serviços não podem receber acessos ou sofrer manutenções remotas, devendo ser efetuado o acesso no console local do recurso computacional, por pessoa habilitada e autorizada para tal. Caso haja a necessidade de acessos ou manutenções remotas, a possibilidade deve ser avaliada pela Equipe de TI local responsável para cada caso, considerando os riscos envolvidos e as medidas de segurança disponíveis, devendo, neste caso, o acesso ser feito exclusivamente através da RCD/DCTA, por intermédio de um protocolo seguro utilizando criptografia forte.

17. Outros serviços que vierem a ser necessários na RCD/DCTA devem ser submetidos à apreciação da Divisão de Tecnologia da Informação e Comunicação do DCTA (DTIC/DCTA) que, assessorada pelo NCTI e ERISC, aprovará, ou não, a implementação do serviço, bem como a normatização do uso e dos procedimentos de segurança a serem implementados.

Anexo I – Política de Segurança em Servidores

Todos os Servidores de rede utilizados no DCTA e OM subordinadas, pertencentes ao Departamento e OM subordinadas ou a terceiros, e que não sejam acessados externamente à RCD/DCTA devem observar os procedimentos descritos a seguir.

1. 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.
2. 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 Administrador de Rede local.
3. Não devem existir múltiplas contas de acesso ao Servidor para um mesmo usuário, com exceção dos Administradores de Rede locais.
4. 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.
5. As sessões de conexão a um servidor devem ser encerradas após um período pré-determinado pelo Administrador de Rede Local.
6. Todas as funções de segurança e as alterações e inclusão de *software* devem ser feitas a partir do Servidor e apenas pelo Administrador de Rede local.
7. Usuários não devem ter acesso físico ao Servidor via console. O acesso lógico de usuários ao Servidor deve ser feito somente através da rede.
8. 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 classificados.
9. Todas as transações devem ser registradas, tais como as tentativas de entrada mal sucedidas no sistema, operação/acesso não autorizado, suspensão e encerramento de sessão (acidental ou deliberada), mudanças na atribuição de *software* e de segurança, entradas/saídas do sistema (*logons/logoffs*), outras atividades designadas (por exemplo, acessos aos arquivos classificados) e, opcionalmente, todas as atividades, por um período de 6 (seis) meses.
10. Os usuários devem possuir acessos a áreas específicas e restritas para armazenamento de arquivos da sua fração funcional ou grupo de trabalho.
11. Não devem ser transferidos programas e arquivos para as áreas públicas; o mesmo vale para as macros e as bibliotecas de macros, salvo necessidade de divulgação pública e o referido programa ou arquivo não venha a comprometer a segurança do Servidor ou da RCD/DCTA.
12. 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 deve ser bloqueada. A reativação desta conta deve ser solicitada, pelo usuário, à Equipe de TI da OM.
13. Todos os acessos para administração de equipamentos e serviços deverão ser realizados utilizando credenciais com permissões adequadas e com autenticação que permita identificar o usuário de forma nominal (individual).
14. Caso seja necessário, um procedimento adicional de identificação de usuários pode ser usado, dependendo das informações a serem acessadas.

Continuação do Anexo I – Política de Segurança em Servidores

15. Os Servidores corporativos devem estar registrados em um documento mantido com os Administradores de Rede locais e Coordenadores das Equipes de TI locais, com no mínimo as seguintes informações:

- a) localização do Servidor e o contato do Administrador de Rede local;
- b) hardware do Servidor, versão do sistema operacional e *softwares* instalados;
- c) função principal e aplicação a que se destina.

16. Alterações de configurações de Servidores em operação devem seguir os procedimentos padronizados e documentados de acordo com o planejamento prévio estabelecido pela Equipe de TI local.

17. Serviços e aplicações que não são usados devem ser desabilitados ou desinstalados do Servidor sempre que possível.

18. Acessos aos serviços devem ser registrados e protegidos.

19. Relações de confiança entre sistemas oferecem riscos à segurança e, portanto, devem ser, sempre que possível, substituídas por outro método mais seguro de comunicação.

20. Os Servidores de rede devem estar fisicamente localizados em ambiente de acesso controlado, conforme definido na Política de Segurança Física (Anexo F).

21. Quando da instalação de um novo Servidor, as senhas originais utilizadas pelo sistema operacional devem ser substituídas, assim como as contas padrões devem ser renomeadas ou desativadas.

22. Os eventos relacionados à segurança devem ser reportados à ERISC que deve revisar os *logs* e gerar relatórios de incidentes. Medidas corretivas devem ser prescritas conforme necessidade. Eventos relacionados à segurança incluem, mas não se limitam a:

- a) ataques de *port-scan*;
- b) evidência de acesso não autorizado a contas privilegiadas;
- c) ocorrências anômalas que não são relacionadas a aplicações específicas do recurso computacional.

23. Auditorias periódicas podem ser executadas pela ERISC.

Anexo J – Política de Acesso Remoto

Todos os usuários que necessitem utilizar acessos remotos devem observar os procedimentos descritos a seguir.

1. As implementações de acesso remoto coberto por esta Política incluem, mas não se limitam a serviços, tais como, *modems*, *ISDN*, *frame relay*, *VPN* e *SSH*.
2. Somente são permitidos acessos remotos à RCD/DCTA através de conexões passando pelos *firewalls* corporativos e locais, devendo ser obrigatoriamente registrados e mantidos os registros por, no mínimo, 6 (seis) meses.
3. Não é permitido que, a partir de equipamentos da RCD/DCTA e das redes locais das OM, originem-se conexões a outras redes que não sejam aquelas controladas pelos *firewalls* do DCTA e OM subordinadas, tais como acesso discado, *wireless* e equivalentes.
4. O acesso remoto à RCD/DCTA deve ser, obrigatoriamente, controlado através de um esquema de autenticação de usuário e senha em conformidade com o padrão determinado no item 4.1.4 desta Instrução ou chaves públicas.
5. Não são permitidos os acessos remotos provenientes de redes externas à RCD/DCTA, bem como aos recursos computacionais do DCTA e OM subordinadas, através de contas com privilégios de Administrador, Supervisor ou Superusuário. O acesso como Administrador, Supervisor ou Superusuário só pode ser feito via console ou através da RCD/DCTA por intermédio de um protocolo seguro utilizando criptografia forte.
6. Para a devida proteção de informações e detalhes de uso aceitável quando acessando a RCD/DCTA, deve-se observar o previsto nas seguintes Políticas:
 - a) Política de Manipulação de Informações Classificadas (Anexo C);
 - b) Política de Uso dos Recursos Computacionais (Anexo A).
7. Todo acesso remoto deve utilizar-se de algoritmos criptográficos, de acordo com as orientações emanadas pelo Centro de Inteligência do COMAER (CIAER), e de códigos de autenticação, assinaturas digitais ou outro sistema que permita a identificação do usuário no acesso à RCD/DCTA.
8. Não é permitido realizar acesso remoto a sistemas internos e externos, exceto quando, para atender uma necessidade excepcional e temporária, esse acesso seja justificado e devidamente autorizado pela DTIC/DCTA, observados os requisitos emanados pelo Órgão Central do STI; bem como o acesso à Intraer, por intermédio do uso da Internet, somente pode ser realizado mediante uso de solução desenvolvida pelo CIAER. Caso não haja a possibilidade de uso de solução desenvolvida pelo CIAER, o Órgão Central do STI poderá autorizar o uso de soluções distintas.
9. O uso de tecnologias baseadas em propagação de ondas eletromagnéticas deve ser autorizado pela DTIC/DCTA, observadas as regras emanadas pelo Órgão Central do STI.
10. O dispositivo utilizado para o acesso remoto deve ter antivírus instalado e atualizado e estar em conformidade com a política de uso de software, descrita no item 4.7 desta Instrução, sendo de responsabilidade do usuário a observação da legalidade de todos os softwares instalados em seu dispositivo e o cumprimento deste item.

Anexo K – Política de Auditoria

Na condução de auditoria de segurança em recursos computacionais do DCTA e OM subordinadas devem ser observados os critérios descritos a seguir.

- 1.** Todos os recursos computacionais pertencentes à RCD/DCTA e os recursos computacionais locais do DCTA e OM subordinadas devem sofrer auditorias para verificação da implementação e cumprimento desta Política de Segurança, com a ciência prévia da respectiva Direção/Reitoria/Chefia/Comando/Prefeito/Presidente da organização onde eles estejam localizados.
- 2.** As auditorias devem ser realizadas pela Equipe de Resposta a Incidentes de Segurança em Computadores (ERISC).
- 3.** Quando necessário, ou com o propósito de ser executada a auditoria, os membros da ERISC ou os membros designados pela DTIC devem ter acesso irrestrito aos recursos computacionais de onde será realizada a auditoria, com a ciência da Direção/Reitoria/Chefia/Comando/Prefeito/Presidente da organização auditada.
- 4.** A auditoria deve ter 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 auditada, devendo ser levada em consideração a credencial de segurança dos auditores.
- 5.** A auditoria deve ter acesso a todas as áreas de trabalho onde se encontram os recursos computacionais, tais como laboratórios, salas diversas, manutenção e outras.
- 6.** A auditoria deve ter acesso físico e lógico aos sistemas que monitoram e armazenam os *logs* da rede.
- 7.** A auditoria deve ser feita com aviso prévio ao Coordenador da Equipe de TI Local e este, além de manter sigilo sobre o processo, deve acompanhar os auditores em todos os procedimentos executados.
- 8.** A ERISC, com a anuência do DCTA, pode manter um monitoramento remoto constante da RCD/DCTA em qualquer ponto do *Backbone* da RCD/DCTA, incluindo as Redes Locais das OM, sem necessidade de prévio aviso a qualquer usuário.
- 9.** Todo esforço deve ser feito para impedir que as auditorias causem falhas operacionais ou interrupção dos serviços.
- 10.** Conforme preconizado na Política de Uso dos Recursos Computacionais (Anexo A), todo Recurso Computacional existente no DCTA e organizações subordinadas é passível de monitoramento e auditoria, sem qualquer aviso prévio ao usuário. Considerando que os recursos computacionais pertencem ao DCTA e OM subordinadas ou são utilizados em atividades desenvolvidas nestas organizações, fica entendido que o exercício do monitoramento e da auditoria não constitui violação à intimidade, vida privada, honra e imagem do usuário.


Anexo L – Plano de Continuidade de Negócio

Todos os recursos computacionais utilizados na prestação de serviço corporativo, seja no âmbito das organizações subordinadas do DCTA, seja no âmbito do Departamento, devem possuir um plano de continuidade de negócio apropriado preparado pelos responsáveis pela sua administração, observando as peculiaridades referentes à aplicação operacionalizada nesses recursos e os procedimentos descritos a seguir.

1. Realizar uma análise de risco, impacto e vulnerabilidade formal e completa para todos os recursos das redes locais do DCTA e OM subordinadas, consubstanciando-a em um documento.
2. Preparar um planejamento formal, baseado no documento gerado no item 1, completo e testado, de recuperação de desastres para todos os recursos das Redes Locais, chamado de Plano de Continuidade de Negócio, de acordo com as respectivas particularidades.
3. A elaboração dos documentos citados nos itens 1 e 2 e a execução do plano de continuidade de negócio são de responsabilidade das Equipes de TI locais e do Núcleo Corporativo de TI, observando as suas respectivas atribuições.
4. Os documentos citados acima devem contemplar, pelo menos, as ações descritas a seguir:
 - a) definição das responsabilidades de recuperação e das responsabilidades dos fornecedores;
 - b) descrição das instruções detalhadas de recuperação;
 - c) definição das instalações alternativas (local, capacidade de processamento e disponibilidade) e o local externo de armazenamento do *backup* em outro prédio;
 - d) identificação de recursos computacionais críticos;
 - e) distribuição do Plano às pessoas apropriadas;
 - f) previsão do pessoal substituto;
 - g) manutenção de, pelo menos, duas cópias impressas da documentação, armazenadas em locais distintos;
 - h) reavaliação periódica com simulações;
 - i) atualização periódica da documentação;
 - j) aprovação pelos grupos afetados;
 - k) relação de documentos, dados e arquivos a serem copiados (*backup*);
 - l) definição dos procedimentos para vários níveis de interrupções e emergências;
 - m) configuração de forma que a ocorrência de uma falha em um de seus pontos não provoque a queda de toda a rede.

Anexo M – Ficha de Cadastro de Usuário

(frente)

	<p align="center">(Nome da OM) (Nome da Fração Funcional de tecnologia da informação responsável)</p> <p align="center">Ficha de Cadastro de Usuário na RCD / (Sigla da OM)</p>	<p align="center">(Logotipo da OM)</p>
--	--	--

Nome do Usuário:

Fone:

Para uso do Chefe da Fração Funcional

Recursos Computacionais Necessários:

☐

Servidor de Arquivos

☐

VPN

☐

Conta de Correio eletrônico Internet

☐☐

Acesso à Internet

☐

Justificativa para acesso à Internet e para conta de correio eletrônico Internet:

____/____/____
Data_____
Ass. Usuário_____
Ass. Chefe da Fração Funcional
Solicitante

Termo de Responsabilidade

Eu, _____ (Nome do Usuário), assumo inteira responsabilidade pela utilização individual dos recursos computacionais da RCD/(sigla da OM), assumindo o compromisso de somente utilizá-los para fins profissionais, no meu setor funcional, tendo conhecimento de todas as normas e procedimentos de tecnologia da informação vigentes na Organização, em especial a ICA 7-34 referente à Política de Segurança em Tecnologia da Informação e Uso dos Recursos Computacionais do DCTA, as quais encontram-se disponíveis na página Intraer do DCTA.

Informo, ainda, estar ciente da legislação aplicável à utilização de Programa de Computador através da Lei nº 9.609, de 19 Fev 98, especialmente as disposições constantes do parágrafo 1º, art. 12 e inciso I do art. 6º, bem como do disposto no verso deste documento.

Concordo que todos os recursos computacionais que utilizar sejam monitorados e auditados pela Organização, sem qualquer aviso prévio, não constituindo violação à intimidade, vida privada, honra e imagem de minha pessoa.

____/____/____
Data_____
Assinatura do Usuário

Para uso da (Nome da fração funcional responsável pela tecnologia da informação na OM)

Conta aberta em ____/____/____ por _____ Encerrada em ____/____/____ por _____

Continuação do Anexo M – Ficha de Cadastro de Usuário**(verso)****Utilização de Software no DCTA**

1. O DCTA e OM subordinadas possuem licenças oficiais de uso de *software* provenientes de uma série de fornecedores. Exceto quando autorizado pelos autores do *software*, nenhum militar, servidor, aluno, visitante ou contratado do DCTA e das OM subordinadas tem o direito de reproduzi-lo.
2. Os militares, servidores, alunos, visitantes e contratados do DCTA e das OM subordinadas devem utilizar *software* apenas de acordo com os contratos de licença de uso, não podendo alegar desconhecimento desta licença em caso de eventuais sanções.
3. De acordo com a Lei de Software, as pessoas envolvidas em reprodução ilegal de programas ficam sujeitas ao pagamento das respectivas indenizações por perdas e danos, além de sanções penais previstas. Com a aplicação da Lei de Software em conjunto com a Lei de Direitos Autorais, este valor pode chegar a milhares de vezes o valor da licença para cada cópia ilegal.
4. Os militares, servidores, alunos, visitantes e contratados do DCTA e das OM subordinadas que fizerem, adquirirem ou usarem cópias de software ilegais e não autorizadas, devem sofrer penalidades de acordo com as circunstâncias, sendo inteiramente responsáveis pela reparação dos danos resultantes de tais atos.
5. As legislações pertinentes ao uso legal de software e a ICA 7-34 (Política de Segurança em Tecnologia da Informação e Uso dos Recursos Computacionais do DCTA) encontram-se disponibilizadas na página Intraer do DCTA.
6. A instalação de qualquer produto irregular de hardware e de software nos recursos computacionais do DCTA e OM subordinadas é de inteira responsabilidade de quem o instalou, e o mesmo deve ser responsabilizado por isso na forma da lei.
7. Caso ocorra a instalação de algum produto irregular, ou não licenciado, o mesmo deve ser eliminado pela Equipe de TI da respectiva OM.
8. Todo recurso computacional tem um responsável pela sua carga, cadastrado no Setor de Carga, cabendo a ele, em última análise, a corresponsabilidade por qualquer irregularidade constatada no mesmo.
9. Conforme preconizado na ICA 7-34 referente à Política de Segurança em Tecnologia da Informação e Uso dos Recursos Computacionais do DCTA, todo recurso computacional existente na Organização é passível de monitoramento e auditoria, sem qualquer aviso prévio ao usuário. Considerando que os recursos computacionais pertencem ao DCTA e suas OM subordinadas ou são utilizados em atividades desenvolvidas nessas OM, fica entendido que o exercício do monitoramento e da auditoria não constitui violação à intimidade, vida privada, honra e imagem do usuário.
10. O monitoramento e auditoria têm por objetivo verificar o respeito do usuário às regras estabelecidas na ICA 7-34 de Política de Segurança em Tecnologia da Informação e Uso dos Recursos Computacionais do DCTA, e na legislação em vigor.
11. Para o uso de VPN, deve-se observar, em especial, o disposto no Anexo J da ICA 7-34.