MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

INTELIGÊNCIA

ICA 200-8

MEDIDAS DE SEGURANÇA PARA EQUIPAMENTOS CRIPTOTÉCNICOS E DE COMUNICAÇÕES

2019

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

INTELIGÊNCIA

ICA 200-8

MEDIDAS DE SEGURANÇA PARA EQUIPAMENTOS CRIPTOTÉCNICOS E DE COMUNICAÇÕES

2019

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

PORTARIA Nº 23/DCI, DE 9 DE MAIO DE 2019.

Aprova a reedição da instrução que dispõe sobre as Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações no âmbito do SINTAER.

O CHEFE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA, tendo em vista o disposto no Inciso III, do art. 4º do Regulamento do Centro de Inteligência da Aeronáutica, aprovado pela Portaria nº 1.546/GC3, de 3 de outubro de 2018, resolve:

Art. 1º Aprovar a reedição da ICA 200-8 "Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações", que com esta baixa.

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

Art. 3º Revoga-se a Portaria C-5/CIAER, de 19 de dezembro de 2008, publicada no Boletim do Comando da Aeronáutica Confidencial nº 1, de 15 de janeiro de 2009.

Brig Ar JÚLIO CÉSAR MAIELLO VILLELA
Chefe do CIAER

(Publicado no BCA nº 080, de 14 de maio de 2019).

SUMÁRIO

PREFÁCIO

A segurança da informação pode ser afetada por vários fatores, tais como o ambiente, as rotinas estabelecidas para manuseio dos documentos e outros meios de armazenamento dessas informações, pelas pessoas responsáveis por seu manuseio e, sem sombra de dúvida, pela infraestrutura e recursos de Tecnologia da Informação utilizados para processar, armazenar e difundir essa informação.

Por isso, a legislação que trata da proteção do conhecimento apresenta uma série de recomendações, parâmetros e determinações que devem ser observadas para a garantia de condições mínimas de segurança dos ativos que se deseja proteger. Entre essas determinações, o uso de recursos criptográficos recebe atenção especial.

A edição desta Instrução tem o objetivo de reunir, de forma prática, simples e objetiva, as medidas de segurança para os recursos criptográficos em uso no COMAER, além de fornecer referências para o uso desses recursos para o manuseio da informação classificada.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

A presente Instrução tem por finalidade estabelecer os preceitos que devem ser adotados para a utilização dos equipamentos criptográficos que irão prover a segurança das informações, padronizar os procedimentos relativos à segurança das comunicações e estabelecer os requisitos mínimos de segurança para a utilização de recursos computacionais no tratamento de Informações Classificadas no âmbito do Sistema de Inteligência da Aeronáutica (SINTAER).

1.2 FUNDAMENTAÇÃO LEGAL

1.2.1 A Lei 12.527, de 18 de novembro de 2011 (LAI) estabelece as restrições de acesso à informação, a classificação de informações quanto ao Grau de Sigilo e determina, em seu art. 25, o dever do Estado de assegurar a Proteção das Informações Sigilosas, por meio do controle do acesso e da divulgação.

1.2.2 O Decreto 7.845, de 14 de novembro de 2012, no art. 57 estabelece que "Os órgãos e entidades poderão expedir instruções complementares, no âmbito de suas competências, que detalharão os procedimentos relativos ao credenciamento de segurança e ao tratamento da informação classificada".

1.3 CONCEITUAÇÃO

Para os efeitos desta Instrução, aplicam-se as seguintes definições:

1.3.1 SINTAER

É o Sistema de Inteligência da Aeronáutica tendo como órgão central o Centro de Inteligência da Aeronáutica (CIAER).

1.3.2 ATIVOS DE INFORMAÇÃO

Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

1.3.3 ATIVOS DE REDE

Equipamentos utilizados para interconectar meios de TI. Por Exemplo, *switches,* roteadores, etc.

1.3.4 CRIPTOTÉCNICA

Emprego de técnicas destinadas a tornar ininteligível o conteúdo de mensagens, mediante o emprego de cifração, codificação e grafia dissimulada. Equivale a CRIPTOGRAFIA.

1.3.5 SEGURANÇA DAS COMUNICAÇÕES

Conjunto de medidas destinadas à proteção das fontes de comunicações, quer quanto à segurança do conteúdo (criptotécnica), quer no que tange à escolha do processo a ser utilizado, tendo em vista os fins da própria comunicação.

1.3.6 SEGURANÇA EM PROCESSAMENTO DE DADOS

Medidas voltadas à proteção dos recursos computacionais, visando a estabelecer padrões de segurança que permitam garantir a integridade do *hardware*, *software* e dos dados, no que tange aos seguintes aspectos: a manutenção do sigilo dos dados armazenados ou em trânsito; a integridade e a precisão desses dados, assim como dos programas que os gerenciam; e a garantia de que os recursos de informática, os dados e os serviços estarão disponíveis para aqueles que têm acesso permitido.

1.3.7 SEGURANÇA NOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO (TI)

A Segurança nos Meios de TI abrange a Segurança das Comunicações e a Segurança em Processamento de Dados.

1.3.8 CREDENCIAL DE SEGURANÇA

Certificado que autoriza pessoa para o tratamento de informação classificada.

1.3.9 MEIOS DE TECNOLOGIA DA INFORMAÇÃO (TI)

Equipamentos e programas (*hardware e software*) de computação e/ou de comunicação programados para processar, armazenar ou transmitir informação. Englobam aqueles localizados em instalações fixas, equipamentos móveis ou embarcados em aeronaves, navios, etc.

1.3.10 CONEXÃO LÓGICA ENTRE REDES

Conexão na qual os computadores de um circuito de rede são capazes de acessar computadores de outro circuito de rede e/ou de serem por eles acessados. Pressupõe a existência de "roteamento" entre essas redes.

1.3.11 EQUIPAMENTO MÓVEL

Meio de TI passível de ser transportado para fora do ambiente de segurança de uma OM.

1.3.12 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Conjunto de processos que permitem identificar e adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

1.3.13 INFORMAÇÃO CLASSIFICADA (IC)

Informação em poder dos órgãos e entidades públicas que, em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, é classificada como ULTRASSECRETA, SECRETA ou RESERVADA.

1.3.14 INFORMAÇÃO DE ACESSO RESTRITO

É aquela que, não sendo passível de receber classificação sigilosa, por sua utilização ou finalidade, demanda medidas especiais de proteção. Deve receber as mesmas medidas cautelares da IC equivalente.

1.3.15 INFORMAÇÃO SIGILOSA (IS)

Inclui as informações classificadas, além daquelas abrangidas pelas demais hipóteses legais de sigilo, como informações pessoais, sigilos bancários e telefônicos, etc.

1.3.16 TRATAMENTO DA INFORMAÇÃO

Conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação. Também chamado de Processamento da informação.

1.4 ÂMBITO

A presente Instrução aplica-se a todas as Organizações do Comando da Aeronáutica. Pode, também, ser utilizada para orientar procedimentos nas empresas vinculadas, ou outras empresas e órgãos com os quais o COMAER mantém contrato ou convênio com cláusula de manutenção de sigilo.

1.5 COMPETÊNCIAS

1.5.1 COMPETE AO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA (CIAER)

1.5.1.1 Acompanhar as determinações legais que possam influenciar os requisitos de segurança apresentados nesta Instrução, mantendo-a sempre atualizada.

1.5.1.2 Definir critérios e procedimentos para a utilização dos meios criptotécnicos e dos recursos computacionais no processamento de IC.

1.5.1.3 Realizar inspeções de segurança nos Elos do SINTAER, sob a forma de auditoria, no tocante ao cumprimento das instruções e procedimentos de utilização dos equipamentos criptotécnicos, de segurança das comunicações e de segurança orgânica.

1.5.1.4 Realizar estudos técnicos, criptoanálises, análises de risco, testes de invasão de redes e análises de vulnerabilidades, voltadas para a segurança das comunicações.

1.5.1.5 Especificar e gerenciar a utilização de recursos de infraestrutura de criptografia em uso no COMAER.

1.5.1.6 Especificar, desenvolver e analisar a utilização de recursos criptotécnicos, equipamentos e dispositivos voltados à segurança das comunicações.

1.5.1.7 Gerenciar o desenvolvimento e a manutenção de todos os recursos criptotécnicos do COMAER, incluindo o controle, a guarda e a distribuição das respectivas chaves de criptografia.

1.5.2 COMPETE AOS COMANDANTES, CHEFES E DIRETORES:

1.5.2.1 Garantir que toda IC sob responsabilidade de sua OM esteja protegida pelos recursos criptográficos e de TI adequados, durante as fases de produção, transmissão e armazenamento.

1.5.2.2 Verificar a necessidade de utilização de recursos de TI no âmbito de sua OM, para o tratamento de informações classificadas.

1.5.2.3 Emitir certificado, consignando a adequação de um recurso de TI para o processamento de IC, de acordo com os parâmetros estabelecidos nesta instrução. Para isso, deverá contar com assessoramento dos Chefes dos Setores de Inteligência (SI) de sua OM (ou da OM apoiadora), e do elo de Serviço do Sistema de Tecnologia da Informação (STI).

1.5.2.4 Manter os registros e o controle dos recursos de TI certificados para o processamento de IC e dos recursos criptotécnicos existentes em sua OM.

1.5.2.5 Identificar os desvios praticados quanto aos procedimentos e ao mau uso dos meios de TI usados para o processamento de IC e dos recursos criptotécnicos, aplicar as correções apropriadas e comunicar o fato ao Órgão Central do SINTAER.

2 EQUIPAMENTO CRIPTOTÉCNICO

2.1 SEGURANÇA FÍSICA

2.1.1 Enquanto não estiverem em uso, os equipamentos deverão estar armazenados em cofre.

2.1.2 Os sistemas e os materiais criptográficos devem ser guardados em locais distintos de seus manuais de utilização e de suas senhas

2.1.3 A utilização de equipamentos criptográficos deve ser realizada em área de acesso restrito, que atenda às recomendações da ICA 205-47 INSTRUÇÕES PARA SALVAGUARDA DE ASSUNTOS SIGILOSOS (ISAS) quanto à segurança das áreas e instalações.

2.1.4 SEGURANÇA NO TRANSPORTE

2.1.4.1 Os materiais criptográficos, bem como os sistemas de cifra e códigos e os seus respectivos manuais, só podem ser transportados por portador credenciado, pertencente ao SINTAER, e entregues pessoalmente ao destinatário. É proibida sua remessa por malote.

2.1.4.2 O material acima não pode ser despachado como bagagem. Deve ser transportado em mãos pelo portador.

2.2 SEGURANÇA DO MATERIAL

2.2.1 Os materiais criptográficos, bem como os sistemas de cifra e códigos e os seus respectivos manuais são, por sua natureza, considerados Materiais de Acesso Restrito.

2.2.2 Tais equipamentos são, no SINTAER, Materiais Controlados – MC e estão sujeitos a medidas adicionais de controle, de acordo com as ISAS, entre elas:

a) Deverão constar anualmente em termos de inventário; e

b) Sua transferência ou empréstimo dar-se-á mediante a lavratura de termo de custódia ou guarda.

3 RECURSOS COMPUTACIONAIS PARA O PROCESSAMENTO DE IC

Em geral, as prescrições legais são plenamente adequadas a documentos em formato digital criados, transmitidos ou armazenados em recursos de TI. Entretanto, no COMAER, utilizam-se complexos sistemas computacionais para o processamento de dados na produção de conhecimento de acesso restrito. Como exemplos, podem ser citados sistemas de análise de Inteligência de Sinais (SigInt) ou de Imagens (ImInt).

Nesse tipo de cenário, muitos sistemas são incompatíveis com os requisitos legais (ANEXO B). Apesar dessas incompatibilidades, não se pode deixar de usar um sistema crítico.

Após criteriosa análise dos riscos à segurança das informações, definiram-se as ações a seguir, que visam a permitir o processamento de IC com o mais elevado nível de segurança possível, tanto em condições ideais – com o uso de criptografia – quanto em condições especiais sem, contudo, comprometer a segurança.

3.1 CERTIFICAÇÃO DE RECURSO DE TI

3.1.1 Para que um meio de TI possa processar IC, ele deverá ser avaliado por meio de trabalho conjunto do Setor de Inteligência da OM (ou da OM apoiadora) e do Elo de Serviço de TI que apoie essa Organização.

3.1.2 O ponto de partida para a avaliação das condições de segurança cibernética de um equipamento está estabelecido pelo STI, por meio da NSCA 7-13. Por vezes os padrões estabelecidos naquela norma serão reforçados nesta Instrução em virtude da importância deles na proteção do conhecimento.

3.1.3 Uma vez que atenda aos requisitos mínimos de segurança estabelecidos nesta Instrução, o Certificado para Processamento de Informação Classificada (CPIC) deverá ser emitido pelo Comandante, Chefe ou Diretor da OM responsável pelo recurso computacional.

3.1.4 A partir da emissão desse certificado, o equipamento passa à condição de MATERIAL DE ACESSO RESTRITO, em nível compatível com o grau de sigilo das informações que irá processar, e deve passar a exibir as marcações, de acordo com a ICA 205-47.

3.1.5 O certificado deverá ser emitido de acordo com o modelo disponibilizado no Portal da Rede Criptográfica (ANEXO C), armazenado e controlado pelo SI.

3.2 REQUISITOS COMUNS

3.2.1 Os requisitos aqui apresentados devem ser atendidos por todo recurso de TI utilizado para processamento de IC. Esses são os requisitos para um recurso computacional isolado, operado no interior de uma OM.

3.2.2 SEGURANÇA FÍSICA

3.2.2.1 Devem ser fornecidas condições mínimas de segurança das instalações compatíveis com o grau de sigilo/nível de restrição de acesso das informações que se deseja processar. Por exemplo: controle de acesso ao local de instalação, existência de dispositivos de trancamento ou lacres, etc.

3.2.2.2 A adequação das condições deverá ser avaliada pelo Setor de Inteligência da OM (ou da OM apoiadora) e consignada no CPIC. A ICA 205-47 deve ser usada como referência.

3.2.3 SEGURANÇA DO *HARDWARE*

3.2.3.1 Devem ser instalados lacres que permitam detectar facilmente eventuais violações.

3.2.3.2 Antes da utilização de *hardware* que processe IC, os lacres devem ser verificados e violações prontamente reportadas ao SI. O equipamento NÃO DEVE ser utilizado se tiver sido violado.

3.2.3.3 Os equipamentos devem possuir senhas para proteger contra modificações no *setup* da BIOS, como ativação de periféricos, sequência de inicialização, etc. Essa senha deve ser de conhecimento EXCLUSIVO dos administradores do elo de serviços de TI.

3.2.3.4 A sequência de inicialização do equipamento deve incluir EXCLUSIVAMENTE o dispositivo que armazena o Sistema Operacional.

3.2.3.5 Interfaces que permitam escolher a inicialização por mídias removíveis devem ser desabilitadas.

3.2.3.6 As interfaces de rede sem fio (se existentes) devem ser desabilitadas.

3.2.3.7 As interfaces de rede *ethernet* devem ser desabilitadas.

3.2.3.8 Não deve ser permitida manutenção do equipamento por pessoal não credenciado, tampouco sua retirada da OM. Caso seja necessário esse tipo de manutenção, dispositivos de armazenamento (discos, *solid state*, etc) devem ser removidos.

3.2.3.9 Equipamentos que deixem de ser utilizados para processar IC devem ter os dispositivos de armazenamento removidos e armazenados de forma segura. Isso deve acontecer antes que os equipamentos sejam descartados, transferidos ou alienados.

3.2.3.10 Os dispositivos de armazenamento que se tornem inservíveis, uma vez que tenham sido utilizados para armazenar IC devem ser encaminhados ao SI, que deverá providenciar o descarte adequado.

3.2.3.11 Deve ser estabelecido um controle de mídias removíveis

a) Não podem ser usadas mídias particulares em equipamentos certificados;

b) Mídias utilizadas para processar IC não podem ser conectadas a equipamentos não certificados;

c) Toda mídia deve ser verificada pelo sistema antivírus antes de sua utilização;

d) Sempre que praticável a mídia deve receber marcação equivalente ao grau de sigilo/nível de restrição de acesso da informação armazenada; e

e) Enquanto não estiverem em uso, as mídias contendo IC devem receber tratamento equivalente ao grau de sigilo das informações armazenadas.

3.2.4 SEGURANÇA DO *SOFTWARE*

3.2.4.1 Todo *software* utilizado deve ser licenciado, obtido de fonte confiável e instalado pelo elo de serviço do STI que apoie a OM.

3.2.4.2 Os aplicativos instalados devem ser os mínimos necessários para a realização do serviço.

3.2.4.3 Devem ser mantidas as mídias de instalação de todos os aplicativos / sistemas operacionais.

3.2.4.4 Cópias de segurança (*back-up)* devem ser realizadas de acordo com as rotinas da OM. Um teste de recuperação deve ser realizado pelo menos uma vez ao ano. As mídias que contém o *back-up* devem ser armazenadas em local físico diferente dos dados originais, com condições de segurança compatíveis com o grau de sigilo / nível de restrição de acesso dos dados originais.

3.2.4.5 As atualizações de segurança dos aplicativos e dos sistemas operacionais devem ser instaladas ao menos mensalmente.

3.2.4.6 O *software* antivírus padronizado pelo STI deve ser utilizado. As definições de vírus devem ser atualizadas ao menos semanalmente.

3.2.4.7 Em caso de infecção do recurso computacional por vírus, o uso deve ser interrompido, as mídias removíveis em uso devem ser mantidas separadas e os setores de TI e de Inteligência devem ser prontamente notificados.

3.2.4.8 Credenciais administrativas padrão (root, Administrador, admin, etc.) não devem ser utilizadas. Os administradores devem possuir credenciais pessoais, que permitam identificar a positivamente quem está acessando o sistema com direitos administrativos.

3.2.5 SEGURANÇA DO PESSOAL

3.2.5.1 Usuários e administradores devem possuir Credencial de Segurança no grau de sigilo da informação processada.

3.2.5.2 Usuários não podem possuir direitos administrativos sobre o equipamento (direitos de instalar aplicativos e alterar configurações).

3.2.5.3 Os usuários devem firmar o termo de responsabilidade (ANEXO D) para cada equipamento que forem utilizar.

3.2.6 O equipamento ISOLADO que atenda aos requisitos acima pode processar IC sem o uso de recurso criptográfico.

3.3 REQUISITOS PARA EQUIPAMENTOS MÓVEIS

3.3.1 Atenção especial deve ser dedicada aos equipamentos móveis, uma vez que podem ser removidos do ambiente de segurança provido pelas instalações de uma OM.

3.3.2 Exemplos desse tipo de recurso computacional incluem, mas não se limitam a *notebooks* e *tablets*. Esses equipamentos apresentam alto poder de processamento, grandes capacidades de armazenamento, além de grandes recursos de conectividade como redes sem fio, conexões GSM, etc. Esses recursos que inicialmente representam vantagens traduzem-se em vulnerabilidades para o processamento de IC. Por isso, além dos REQUISITOS COMUNS, procedimentos adicionais devem ser adotados a fim de permitir o processamento de informações classificadas em equipamentos móveis.

3.3.3 Para os equipamentos móveis, o uso de recurso criptográfico homologado pelo CIAER na proteção da IC é a regra. Excepcionalmente, e mediante criteriosa avaliação do SI consignada no Termo de Responsabilidade (ANEXO D), o uso de criptografia pode ser dispensado.

3.3.4 USO DE EQUIPAMENTOS MÓVEIS PARTICULARES

3.3.4.1 É PROIBIDO o uso de equipamentos móveis particulares para o processamento de IC.

3.3.4.2 Com o objetivo de atender ao princípio da oportunidade, está autorizado o uso de aparelhos celulares pessoais para o sistema móvel de comunicações seguras (Athena). Esse software foi produzido pela Agência Brasileira de Inteligência (ABIN), e é gerenciado e distribuído pelo CIAER, no âmbito do COMAER.

3.3.5 SEGURANÇA FÍSICA

3.3.5.1 Quando os equipamentos móveis estiverem em uso no ambiente de segurança de uma OM, devem ser usados como estações isoladas ou conectadas a uma rede segura.

3.3.5.2 Os equipamentos móveis podem ser retirados da OM mediante autorização do SI consignada no Termo de Responsabilidade (ANEXO D).

3.3.5.3 É proibido o uso desses equipamentos em locais públicos, pois o usuário pode estar sendo observado e permitir a visualização não autorizada da IC.

3.3.5.4 Equipamentos contendo IC NÃO PODEM ser despachados como bagagem. Devem ser transportados em mãos pelo detentor.

3.3.5.5 Os procedimentos para transporte e armazenamento dos equipamentos móveis contendo IC dependerão diretamente da utilização ou não de recurso criptográfico homologado pelo CIAER.

3.3.5.6 Caso a IC não esteja protegida por recurso criptográfico:

a) O equipamento não pode ser retirado do território nacional;

b) O transporte deve ser realizado por portador credenciado;

c) Quando não estiver em uso, o armazenamento deve ser realizado de acordo com o grau de sigilo da informação processada, conforme previsto nas ISAS.

3.3.5.7 Caso a Informação Classificada esteja protegida por recurso criptográfico:

a) O equipamento móvel, o hardware criptográfico (se existir), as chaves e as senhas devem ser transportados e armazenados separadamente;

b) O equipamento pode deixar o território nacional;

c) O transporte deve ser realizado por portador credenciado.

3.3.6 SEGURANÇA DO *HARDWARE*

3.3.6.1 Soluções comerciais de criptografia (por exemplo, chip "Trusted Plataform Module" (TPM) ou *softwares* como o VeraCrypt e BitLocker) não são homologadas pelo CIAER como recurso de proteção de IC.

3.3.6.2 Tais soluções comerciais servem como uma barreira adicional e impossibilitam o uso do equipamento protegido por terceiros não autorizados. Dessa forma, o uso desses recursos é altamente recomendado na proteção de equipamentos móveis.

3.3.6.3 Quando retirados da OM, os equipamentos móveis devem ter todas as interfaces de rede desabilitadas.

3.4 REQUISITOS PARA REDES LOCAIS

As redes locais internas e exclusivas de uma OM podem interconectar equipamentos para o processamento de IC e receber a classificação de "Rede Segura", desde que:

3.4.1 Os equipamentos interconectados atendam às prescrições de "3.2 REQUISITOS COMUNS" naquilo que couber.

3.4.2 A rede NÃO PODE possuir conexões físicas ou lógicas à Internet, à Intraer ou a qualquer outro circuito de rede que não atenda às prescrições desta Instrução.

3.4.3 A rede só pode ser conectada a outra rede segura, por meio de canais seguros, providos pela infraestrutura de comunicação segura padronizada pelo CIAER.

3.4.4 SEGURANÇA FÍSICA

3.4.4.1 Os ativos de rede devem estar instalados em locais protegidos, de acesso restrito aos administradores da rede.

3.4.4.2 Os racks onde os ativos de rede estão instalados devem estar organizados, a fim de permitir a pronta identificação da instalação de equipamentos não autorizados.

3.4.4.3 Sempre que os ativos de rede permitam, deve ser usado recurso de controle de endereços físicos dos equipamentos conectados (*MAC-Security)*.

3.4.4.4 É PROIBIDO o uso de equipamentos para acesso sem fio a essas redes.

3.4.4.5 É PROIBIDO o uso de acessos remotos a essas redes.

3.4.5 SEGURANÇA DO *HARDWARE*

3.4.5.1 Sempre que possível, os ativos e circuitos que integram a rede segura devem ser exclusivos, ou seja, sem conexão física a outras redes não certificadas.

3.4.5.2 É possível compartilhar fisicamente os ativos e os circuitos físicos de rede, desde que sejam utilizados equipamentos gerenciáveis, capazes de isolar logicamente os tráfegos de diferentes redes, por meio da utilização de Redes Virtuais (VLAN).

3.4.5.3 Os ativos de rede gerenciáveis devem possuir as seguintes configurações:

3.4.5.3.1 Devem utilizar credenciais (usuário/senha) diferentes daquelas fornecidas pelo fabricante;

3.4.5.3.2 Devem utilizar a versão mais recente do *firmware* (verificação com periodicidade mínima semestral);

3.4.5.3.3 Devem permitir o acesso gerencial, preferencialmente, por meio de conexão direta ao console; e

3.4.5.3.4 Caso seja necessário gerenciar o equipamento remotamente:

a) O endereçamento deve ser inacessível pelos usuários da rede; e

b) A VLAN de gerenciamento deve ser acessível exclusivamente para os administradores.

4 DISPOSIÇÕES FINAIS

4.1 VISITAS TÉCNICAS

O CIAER, por ocasião das Visitas Técnicas aos órgãos do SINTAER realizará a conferência dos recursos computacionais certificados existentes na OM quanto à aderência às orientações desta Instrução.

4.2 CASOS NÃO PREVISTOS

Os casos não previstos nesta Instrução devem ser submetidos à apreciação do Exmo. Sr. Chefe do CIAER.

REFERÊNCIAS

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

BRASIL. Comando da Aeronáutica. Comando-Geral do Pessoal. Confecção, Controle e Numeração de Publicações Oficiais do Comando da Aeronáutica: NSCA 5-1. Brasília, DF, 2011.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Instruções para Salvaguarda de Assuntos Sigilosos: ICA 205-47. Brasília, DF, 2015.

BRASIL. 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. *Diário Oficial da União*, 16 nov. 2012.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Diário Oficial da União – Seção 1 – Edição Extra,* 18 nov. 2011.

ANEXO A – CONSIDERAÇÕES SOBRE SEGURANÇA ORGÂNICA

Não obstante o fato de esta Instrução tratar das medidas de segurança para equipamentos criptotécnicos e de comunicações, é importante destacar que todos os campos da Segurança Orgânica (SO) terão influência na manutenção do sigilo daquilo que se deseja proteger. Essa influência traduzir-se-á em ações que têm o objetivo de obstruir e prevenir ações adversas que possam comprometer a segurança das informações.

Dentre os ramos da SO, destacam-se a Segurança de Pessoal, a Segurança das Áreas e Instalações e, inevitavelmente, a Segurança dos meios de TI.

SEGURANÇA DO PESSOAL

A correta seleção de pessoal autorizado a conhecer informações sigilosas é fundamental para evitar o comprometimento desse conhecimento que se deseja proteger. A ferramenta disponibilizada para essa seleção é o Credenciamento de Segurança.

Por meio do processo de credenciamento avaliam-se possíveis vulnerabilidades passíveis de serem exploradas por ameaças que busquem acesso a conhecimento sigiloso.

Contudo, o Credenciamento de Segurança por si só, não garante o acesso a conhecimento Sigiloso. Para que haja o acesso, o credenciamento deve estar associado à Necessidade de Conhecer.

Tão importante quanto a correta seleção do pessoal, o acompanhamento no exercício da função começa com o fornecimento de treinamento adequado. Esse treinamento tem o objetivo de capacitar o efetivo para a correta utilização dos equipamentos associados à segurança da informação, além de aumentar a consciência situacional e a percepção de eventuais ameaças.

SEGURANÇA DE ÁREAS E INSTALAÇÕES

A Segurança das áreas utilizadas para o processamento de conhecimento Sigiloso deverá contemplar as barreiras físicas que impeçam ou dificultem o acesso não autorizado aos equipamentos utilizados para esse processamento.

A eficiência dessas barreiras é medida em função direta do tempo necessário para superá-las e do investimento exigido de um invasor para ultrapassá-las. Além disso, o administrador deverá ser capaz de detectar com precisão uma tentativa de invasão e de corrigir as falhas tempestivamente.

A segurança física mostra-se extremamente importante para sistemas baseados em redes. Nesse tipo de ambiente, a segurança de todo sistema é equivalente àquela de seu terminal mais desprotegido, pois, a partir dele, um invasor pode obter acesso total aos recursos do servidor mais bem protegido.

SEGURANÇA DOS MEIOS DE TI

Os meios de TI devem garantir que as informações por eles processadas mantenham a integridade, que garante que a informação chegue inalterada ao destinatário, a confidencialidade, para que se tenha a certeza que apenas o destinatário seja capaz de

conhecer o significado dessa mensagem. Contudo, os controles empregados não podem prejudicar a disponibilidade, pois a informação deve chegar inalterada, exclusivamente ao destinatário de forma oportuna!

Uma série de legislações, além de consagradas boas práticas orientam os gerentes, quanto a segurança do hardware, quando se busca proteger os componentes físicos de um sistema, bem como quanto a segurança do software, quando o administrador preocupa-se em utilizar aplicativos licenciados e atualizados, administrar sistemas antivírus e, quando tudo mais falhar, em possuir cópias de segurança e um plano de contingências.

ANEXO B – DISPOSITIVOS LEGAIS

As medidas cautelares dedicadas às informações CLASSIFICADAS devem ser aplicadas aos documentos e materiais de ACESSO RESTRITO de nível equivalente. Portanto, ao analisar-se a legislação que regulamenta o tratamento de informação CLASSIFICADA, deve-se compreender que o mesmo aplica-se àquela submetida a RESTRIÇÃO DE ACESSO.

LEGISLAÇÃO COMUM À ADMINISTRAÇÃO PÚBLICA FEDERAL

O Decreto nº 7.845/2012 regulamenta o tratamento de informação classificada em qualquer grau de sigilo.

O Artigo 30 desse Decreto determina que "A informação classificada em qualquer grau de sigilo será mantida ou arquivada em condições especiais de segurança."

No Artigo 38, que trata "Dos Sistemas de Informação", consta que:

> *Art. 38. No tratamento da informação classificada deverão ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade e segurança definidos pelo Poder Executivo federal. (grifo nosso)*

No âmbito do COMAER, a INTRAER é a "rede corporativa", que interliga as redes locais das OM. Para que seja possível o uso desse meio de transmissão, o parágrafo 1º estabelece a necessidade de uso de canais seguros:

> *§ 1º A transmissão de informação classificada em qualquer grau de sigilo por meio de sistemas de informação deverá ser realizada, no âmbito da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra de segurança.* (grifo nosso)

O "canal seguro" é fornecido pela infraestrutura de Rede Privada Virtual (VPN) padronizada pelo CIAER, baseada no uso do Módulo Criptográfico Interno (MCI) e algoritmo de Estado.

> *§ 4º Os sistemas de informação de que trata o caput deverão manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por prazo igual ou superior ao de restrição de acesso à informação.* (grifo nosso)

Portanto, para que um sistema possa processar informações classificadas, deverá ser ajustado para manter esses registros em função do grau de sigilo e do prazo máximo da restrição de acesso, ou seja, cinco ou quinze anos, para processar informações RESERVADAS ou SECRETAS, respectivamente.

Em complemento, o Artigo 39 apresenta duas alternativas para processamento de informações classificadas:

> *Art. 39. Os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar isolados ou ligados a canais de comunicação seguros, que estejam física ou logicamente isolados de qualquer outro, e que*

> *possuam recursos criptográficos e de segurança adequados à sua proteção. (grifo nosso)*

Para efeito desta Instrução, exemplos de *equipamentos* incluem (mas não se limitam a) servidores, estações de trabalho, computadores pessoais, computadores portáteis, *tablets*, etc. Ao passo que o conceito de *sistemas* um conjunto de recursos de TI, interconectados, com uma finalidade definida como, por exemplo uma rede local, incluindo as estações de trabalho dos usuários, os servidores, bem como os ativos dessa rede.

O ideal para o tratamento de IS é utilizar a primeira opção, ou seja, um equipamento ou sistema isolado, sem qualquer tipo de comunicação externa. Por exemplo, uma rede local, exclusiva de uma OM, dedicada ao processamento de IS, sem conexões lógicas a redes externas como a INTRAER ou à Internet.

LEGISLAÇÃO NO ÂMBITO DO COMAER

Soma-se a essa legislação, a normatização do Sistema de Tecnologia da Informação (STI) do COMAER. O STI regula, entre outros assuntos, o uso da INTRAER, os acessos à Internet e estabelece ações para aumento da segurança e da defesa cibernética dos ativos de informação da Aeronáutica.

A NSCA 7-1 USO DA REDE DE DADOS DO COMANDO DA AERONÁUTICA - INTARER, em seu item 2.2, indica a necessidade de utilização exclusiva de *software* licenciado:

> *É expressamente proibida a utilização dos recursos da INTRAER nas seguintes situações: (...)obtenção, armazenamento, instalação e utilização de programas, sem o devido licenciamento junto à Empresa ou Instituição detentora legal dos seus direitos de uso;*(grifo nosso)

A determinação justifica-se para todos os meios de TI, mesmo fora da INTRAER, ao passo que o uso de software não licenciado fragiliza a Segurança. Programas de computador não licenciados não recebem as correções e atualizações críticas.

Com o objetivo de reduzir a incidência de vírus de computador e de outros tipos de programas maliciosos que podem interferir no correto funcionamento dos sistemas e, em última instância, causar perdas ou vazamentos de informações classificadas, a NSCA 17-3 (SEGURANÇA DA INFORMAÇÃO DE DEFESA CIBERNÉTICA NAS ORGANIZAÇÕES DO COMANDO DA AERONÁUTICA) determina o uso do antivírus corporativo:

> *1.28 Instalar em todos os recursos computacionais utilizados pelos usuários um software antivírus homologado e atualizado, de preferência corporativo, conforme estabelecido na Política de Antivírus e Códigos Maliciosos (Anexo D).* (grifo nosso)

A NSCA7-13 apresenta orientações obrigatórias quanto aos princípios a serem observados para a manutenção da segurança cibernética no âmbito do COMAER.

ANEXO C – CERTIFICADO PARA PROCESSAMENTO DE INFORMAÇÕES CLASSIFICADAS

COMANDO DA AERONÁUTICA
NOME DA ORGANIZAÇÃO MILITAR

CERTIFICADO PARA PROCESSAMENTO
DE INFORMAÇÕES CLASSIFICADAS

CPIC Nº SequenciaNaOM/ANO

De acordo com a ICA 200-8, o equipamento abaixo identificado foi verificado e considerado adequado para processar Informações Classificadas ou de Acesso Restrito

Equipamento
Marca:
Modelo:
Número de Série:

Grau de Sigilo / Nível de restrição autorizado:
( )RESERVADO / Nível 1 ( )SECRETO / Nível 2

Segurança Física
Local de Instalação:
Há condições de segurança adequadas ao grau de sigilo proposto (SIM) (NÃO)

Segurança do Hardware
Senhas configurada no SETUP (SIM) (NÃO)
Adaptadores Wi-Fi desabilitados (SIM) (NÃO)
Adaptadores *ethernet* desabilitados (SIM) (NÃO)
Só pode ser conectado a redes seguras

Segurança do Software
O Sistema Operacional é licenciado (SIM) (NÃO)
Os aplicativos são licenciados (SIM) (NÃO)
O Antivírus padronizado pelo STI
está instalado (SIM) (NÃO)

Segurança do Pessoal
Administradores possuem credencial (SIM) (NÃO)
Usuários possuem direitos administrativos (SIM) (NÃO)

Local e Data

CMT, CHF, DIR

SETOR DE TI

SETOR DE INTELIGÊNCIA

ANEXO D – TERMO DE RESPONSABILIDADE

COMANDO DA AERONÁUTICA
NOME DA ORGANIZAÇÃO MILITAR

TERMO DE RESPONSABILIDADE
PARA O USO DE EQUIPAMENTOS DE ACESSO RESTRITO

De acordo com a ICA 200-8, o portador abaixo identificado está autorizado a utilizar o equipamento acesso restrito:

Identificação
Nome Completo:
Posto:
Quadro:
Identidade:
Credencial de Segurança Nº:

Equipamento
Marca:
Modelo:
Número de Série:
Número do CPIC:

( ) O equipamento POSSUI recurso criptográfico
Software instalado:
Versão:
Hardware criptográfico associado (modelo e Número de Série):

( ) O equipamento NÃO POSSUI recurso criptográfico

O usuário está autorizado a retirar o equipamento da OM ( ) SIM ( ) NÃO

Declaro que estou ciente das restrições impostas para a utilização do equipamento aqui descrito para o processamento de Informações Classificadas ou de Acesso Restrito, conforme a ICA 200-8/2019.

Assinatura do usuário:

Testemunha 1: nome, CPF e assinatura

Testemunha 2: nome, CPF e assinatura