

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



INTELIGÊNCIA

MCA 200-23

**AÇÕES DE CONTRAINTELIGÊNCIA NO
COMANDO DA AERONÁUTICA**

2017

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA**



INTELIGÊNCIA

MCA 200-23

**AÇÕES DE CONTRAINTELIGÊNCIA NO
COMANDO DA AERONÁUTICA**

2017



MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

PORTARIA CIAER Nº 22/SED-DPL, DE 19 DE JUNHO DE 2017.

Aprova a edição do Manual que dispõe sobre as Ações de Contraineligência no Comando da Aeronáutica.

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 463/GC3, de 03 de abril de 2017, resolve:

Art. 1º Aprovar a edição da MCA 200-23 “Ações de Contraineligência no Comando da Aeronáutica”, que com esta baixa.

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

Brig Ar AUGUSTO CESAR ABREU DOS SANTOS
Chefe do CIAER

(Publicada no BCA nº 109, de 28 de junho de 2017)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES	5
1.1 <u>OBJETIVO</u>	7
1.2 <u>FINALIDADE</u>	7
1.3 <u>ÂMBITO</u>	7
1.4 <u>CONCEITOS</u>	7
 2 CONTRAINTELIGÊNCIA NO COMAER	10
2.1 <u>CONSIDERAÇÕES INICIAIS</u>	10
2.2 <u>NOÇÕES FUNDAMENTAIS</u>	10
2.3 <u>SEGMENTOS DA CONTRAINTELIGÊNCIA</u>	12
 3 DIRETRIZES	16
3.1 <u>PREVENIR AÇÕES DE ESPIONAGEM NO COMAER</u>	16
3.2 <u>AMPLIAR A CAPACIDADE DE DETECTAR, ACOMPANHAR E INFORMAR</u> <u>SOBRE AÇÕES ADVERSAS AOS INTERESSES DO COMAER</u>	16
3.3 <u>PREVENIR AÇÕES DE SABOTAGEM</u>	16
3.4 <u>FORTALECER A CULTURA DE PROTEÇÃO DE CONHECIMENTOS</u>	16
3.5 <u>COOPERAR NA PROTEÇÃO DE INSTALAÇÕES DAS OM DO COMAER</u>	17
 4 DISPOSIÇÕES FINAIS	18
4.1 <u>CONDUTA ÉTICA</u>	18
4.2 <u>ABRANGÊNCIA</u>	18
 REFERÊNCIAS	19

1 DISPOSIÇÕES PRELIMINARES

1.1 OBJETIVO

Desenvolver uma mentalidade de Contraineligência com vistas ao preparo e ao emprego da Força Aérea Brasileira e promover e manter a salvaguarda das fontes cujo sigilo seja de interesse do COMAER.

1.2 FINALIDADE

Estabelecer as ações de Contraineligência a serem implementadas por todas Organizações Militares (OM) do Comando da Aeronáutica (COMAER).

1.3 ÂMBITO

A presente Norma tem sua aplicação no âmbito do Sistema de Inteligência da Aeronáutica (SINTAER).

1.4 CONCEITOS

Para efeito desta Norma são estabelecidos alguns conceitos e definições.

1.4.1 ACESSO

É a possibilidade ou oportunidade de se obter conhecimento ou dado classificado ou de acesso restrito. Depende, necessariamente, de uma autorização oficial expedida por autoridade competente, materializada por uma Credencial de Segurança, que levará em conta se a pessoa tem necessidade de conhecer o dado classificado ou de acesso restrito.

1.4.2 AUTENTICIDADE

Qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema e que tenha sua origem e destinos comprovados.

1.4.3 CLASSIFICAÇÃO

É o ato de se atribuir grau de sigilo a dado, informação, documento, material e área que requeiram medidas especiais de salvaguarda e, por consequência, ao documento, material ou área que a contenha, utilize ou veicule.

1.4.4 COMPARTIMENTAÇÃO

É a restrição do acesso com base na necessidade de conhecer.

1.4.5 COMPROMETIMENTO

É a perda de segurança resultante de acesso não autorizado a dados, informações e conhecimentos que devam ser protegidos. Abrange, também, a inutilização, mesmo parcial, de conhecimentos e/ou dados, por meio de adulteração, sabotagem, destruição ou extravio, que possam proporcionar prejuízo aos interesses do COMAER.

É o certificado que autoriza uma pessoa para o tratamento de informação

classificada ou sob restrição de acesso.

1.4.6 CREDENCIAMENTO DE SEGURANÇA

É o processo utilizado para habilitar órgão ou entidade pública ou privada e, ainda, para credenciar pessoa visando ao tratamento de informação classificada ou sob restrição de acesso.

1.4.7 DESCLASSIFICAÇÃO

É o ato pelo qual a autoridade responsável pela classificação de documento ou material classificado o torna ostensivo.

1.4.8 DISPONIBILIDADE

Qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados.

1.4.9 DISPOSITIVO MÓVEL

É o equipamento portátil dotado de capacidade computacional ou dispositivo de memória para armazenamento passível de remoção, entre os quais se incluem, não se limitando a estes: *notebooks, netbooks, smartphones, smartwatches, tablets, pendrives, USB drives, HD* externo e cartões de memória.

1.4.10 GRAU DE SIGILO

É a gradação atribuída à informação classificada.

1.4.11 INTEGRIDADE

Qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino.

1.4.12 MEDIDA DE SEGURANÇA

É a ação destinada a garantir o sigilo, a inviolabilidade, a integridade, a autenticidade e a disponibilidade da informação classificada ou sob restrição de acesso.

1.4.13 NECESSIDADE DE CONHECER

É a condição indispensável, inerente ao exercício funcional, para que uma pessoa, possuidora de credencial de segurança, tenha acesso a conhecimento ou dado sigiloso específico, compatível com seu credenciamento. Dessa maneira, a **inexistência** da Necessidade de Conhecer constitui fator restritivo do acesso, independentemente do grau hierárquico ou do nível da função exercida pela pessoa.

1.4.14 VAZAMENTO

Divulgação não autorizada de informação classificada ou sob restrição de acesso.

1.4.15 VISITANTE

É a pessoa não credenciada, cuja entrada foi admitida, em caráter excepcional e sob condições específicas, em área sob restrição de acesso.

2 CONTRAINTELIGÊNCIA NO COMAER

2.1 CONSIDERAÇÕES INICIAIS

2.1.1 As ações de Contrainteligência têm por objetivo salvaguardar dados, conhecimentos e seus suportes (documentos, áreas e instalações, pessoal, material e meios de tecnologia da informação) de interesse do COMAER preservar, face à possibilidade de ação por parte de organizações de Inteligência adversa ou órgãos e pessoas a elas vinculadas, assim como de ações de qualquer natureza que se constituam em ameaça.

2.1.2 A Contrainteligência é implementada pela adoção de medidas eminentemente defensivas e, mesmo quando empregando medidas ofensivas, prevalece sua finalidade de contínua proteção do conhecimento contra as ações adversas.

2.1.3 A Contrainteligência projeta suas ações para além dos limites dos Órgãos de Inteligência (OI), alcançando, por conseguinte, o conhecimento e/ou dado a salvaguardar, onde quer que ele se encontre: no âmbito das OM do COMAER dentro do País; nas representações do COMAER no exterior (Adidâncias, CAB, outros); ou no ambiente do Teatro de Operações.

2.1.4 Deve-se ressaltar que, fora dos OI, a proteção dos conhecimentos e/ou dados sigilosos é da responsabilidade dos respectivos custodiantes, cabendo, nesse caso, aos OI, a responsabilidade de assessorá-los.

2.1.5 No caso das empresas que mantêm contratos com o COMAER com cláusulas de manutenção de sigilo receberão do CIAER assessoria de Proteção do Conhecimento por ocasião das visitas técnicas de habilitação dos Postos de Controle e credenciamento dos Gestores de Segurança.

2.1.6 A Contrainteligência tem por objetivos:

- a) a identificação das ameaças efetivas ou potenciais à salvaguarda dos conhecimentos de interesse do COMAER e seus suportes, representadas pelas ações de Inteligência adversa e ações de qualquer natureza;
- b) a identificação das deficiências e vulnerabilidades na salvaguarda dos conhecimentos de interesse do COMAER e seus suportes;
- c) a propositura e/ou adoção de medidas que resultem no estabelecimento do nível desejável de salvaguarda dos conhecimentos de interesse do COMAER e seus suportes;
- d) a propositura e/ou adoção de medidas e ações a serem empregadas com a finalidade de influir no processo decisório adverso; e
- e) a produção de conhecimentos, em cumprimento ao Plano de Inteligência da Aeronáutica e aos Planos de Inteligência Setoriais.

2.2 NOÇÕES FUNDAMENTAIS

2.2.1 A Contrainteligência envolve ações voltadas para a detecção, identificação, neutralização, obstrução e prevenção da atuação da Inteligência adversa e das ações de

qualquer natureza que constituam ameaças à salvaguarda de dados, conhecimentos de interesse do COMAER preservar. Pressupõe a adoção de medidas que se contraponham, entre outras, às ameaças abaixo discriminadas:

2.2.1.1 Espionagem

É a ação realizada por pessoal adverso, vinculado ou não a Serviço de Inteligência, visando à obtenção de conhecimento, dado sigiloso, documento ou material para beneficiar Estados, grupos, organizações, facções, empresas ou indivíduos.

2.2.1.2 Sabotagem

É o ato deliberado, de efeitos físicos e/ou psicológicos, executado por agentes adversos, vinculados ou não a serviço de Inteligência, com o objetivo de destruir, inutilizar, adulterar, total ou parcialmente, definitiva ou temporariamente, conhecimento, dado, material, equipamento e instalação. Pode ser, ainda, empregada para a destruição de ideias ou da reputação de instituições e de pessoas.

Normalmente, os alvos constituem meios de comunicação ou de transporte, portos, aeroportos, estações ferroviárias ou rodoviárias, instalações públicas ou estabelecimentos destinados ao abastecimento de água, luz, combustíveis ou alimentos, ou à satisfação de necessidades gerais e imprescindíveis à sociedade, com a finalidade de coagir o Estado ou a sociedade visando a destituir a ordem constitucional ou o Estado Democrático de Direito.

2.2.1.3 Terrorismo

Usar ou ameaçar usar, de forma ilícita e premeditada, violência contra pessoas ou bens, nacionais ou estrangeiros, com a finalidade de coagir o Estado ou a sociedade visando destituir a ordem constitucional e o Estado Democrático de Direito. Observar, ainda, o disposto na Lei nº 13.260, de 16 de março de 2016. Regulamenta o dispositivo no inciso XLIII do Art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista.

2.2.1.4 Propaganda adversa

Configura-se pela manipulação planejada de quaisquer informações, idéias ou doutrinas para influenciar grupos e indivíduos, com vistas a obter comportamentos pré-determinados que resultem em benefício ao seu patrocinador.

2.2.1.5 Desinformação

Ação especializada utilizada pra iludir ou confundir um decisor, visando, intencionalmente, a induzi-lo a erro de avaliação.

2.2.1.6 Ataque cibernético

Compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente.

2.2.1.7 Criminalidade organizada

É ameaça a todos os Estados e merece atenção especial dos órgãos de Inteligência e de repressões nacionais e internacionais. A incidência desse fenômeno, notadamente em sua vertente transnacional, reforça a necessidade de aprofundar a cooperação. Apesar dos esforços individuais e coletivos das nações, não se projetam resultados que apontem para a sua redução em curto e médio prazo.

A Convenção das Nações Unidas contra o Crime Organizado Transnacional define “Grupo criminoso organizado” como “grupo estruturado de três ou mais pessoas, existente há algum tempo e atuando concertadamente com o propósito de cometer uma ou mais infrações graves ou enunciadas na presente Convenção, com a intenção de obter, direta ou indiretamente, um benefício econômico ou outro benefício material”.

2.3 SEGMENTOS DA CONTRAINTELIGÊNCIA

2.3.1 Para racionalização dos trabalhos de Contrainteligência, as ações a serem executadas agrupam-se em dois segmentos:

- a) Segurança Orgânica: de caráter preventivo; e
- b) Segurança Ativa: de caráter proativo.

2.3.2 Esses segmentos são implementados por meio de medidas voltadas para detecção, identificação, neutralização, obstrução e prevenção da atuação da Inteligência adversa e das ações de qualquer natureza que constituam ameaças à salvaguarda de dados, conhecimentos e seus suportes (documentos, áreas e instalações, pessoal, material e meios de Tecnologia da Informação e de Comunicações) de interesse do COMAER.

2.3.3 SEGURANÇA ORGÂNICA

2.3.3.1 É o segmento da Contrainteligência que visa a obter um grau de proteção ideal, por meio da adoção eficaz e consciente de um conjunto de medidas destinadas a prevenir e obstruir as ações de qualquer natureza que ameacem a salvaguarda de dados, conhecimentos e seus suportes de interesse do COMAER.

2.3.3.2 A adoção dessas medidas pressupõe, dentre outras, a implementação de:

- a) Programas de conscientização, destinados a criar mentalidade, motivar e comprometer o efetivo do COMAER com a salvaguarda de dados, conhecimentos e seus suportes;
- b) Documentos destinados a formalizar as medidas de proteção a serem adotadas;
- c) Programa de treinamento continuado sobre os fundamentos, as medidas de Segurança Orgânica e outros julgados necessários;
- d) Sistemática para o credenciamento do pessoal e das empresas, de interesse do COMAER, que necessitem ter acesso a dados, conhecimentos ou materiais classificados ou sob restrição de acesso e áreas e instalações de acesso restrito;
- e) Estruturas para gerência, auditoria e validação da SegOrg de um sistema ou de parte dele;
- f) Serviços e mecanismos de SegOrg necessários para dar eficácia às medidas

estabelecidas; e

g) Medidas de contingência e de controle de danos.

Entende-se por medidas de contingência aquelas a serem tomadas por uma OM o mais rápido possível, em uma situação de emergência, para garantir a proteção do conhecimento de dados, materiais e documentos que tratam de assuntos sensíveis, bem como das áreas e instalações onde tramitam, evitando, assim, que em uma condição de anormalidade prolongada haja o comprometimento ou vazamento da informação que seja de interesse do COMAER preservar. Os incidentes mais comuns que causam a contingência na área de sistemas são enchentes, incêndios, interrupção no fornecimento de energia, ataques de hackers internos ou externos, vírus de computador, sabotagem, acidentes e erros humanos.

Medidas de controle de danos são procedimentos reativos que deverão ser adotados após a ocorrência de uma situação anormal ou emergencial, visando minimizar ou neutralizar os prejuízos à proteção do conhecimento advindos dela, ou seja, o comprometimento e o vazamento da informação sensível ou sigilosa.

2.3.3.3 A Segurança Orgânica dedica-se à proteção direta das informações e atua, objetivamente, sobre seus suportes. Desdobra-se, didaticamente, nos seguintes grupos de medidas:

- a) Proteção no Pessoal;
- b) Proteção na Documentação;
- c) Proteção no Material;
- d) Proteção nos meios de Tecnologia da Informação e Comunicações (TIC); e
- e) Proteção nas Áreas e Instalações.

2.3.3.4 Compreende, dentre outras, as seguintes atividades:

- a) Proteção no Pessoal: compreende um conjunto de medidas destinadas a assegurar comportamentos adequados à proteção de qualquer dado e conhecimento;
- b) Proteção na Documentação: compreende o conjunto de medidas voltadas para evitar o comprometimento de documentos, salvaguardando dados e/ou conhecimentos que devam ser protegidos, sigilosos ou não, neles contidos. Os documentos, por constituírem o suporte mais comum de dados e conhecimentos, tornam-se alvos permanentes das ações hostis, em particular da espionagem.
- c) Proteção no Material: compreende o conjunto de medidas voltadas para proteger dados e conhecimentos contidos em um determinado material. “Material” é entendido como toda matéria, substância ou artefato que contenha, utilize e/ou veicule dados e conhecimentos, que de posse de elemento(s) e/ou grupo(s) de natureza adversa, possa beneficiá-lo(s) ou atentar contra qualquer segmento de um sistema, de forma direta ou indireta. Os materiais que, por sua utilização ou finalidade, demandarem proteção terão acesso restrito às pessoas autorizadas pelo órgão ou entidade.
- d) Proteção nos meios de TIC: consiste no conjunto de medidas destinadas a

preservar o sigilo das atividades de processamento, armazenamento, transmissão de dados digitais e comunicações, bem como a integridade dos sistemas, materiais e programas de TIC, no sentido de salvaguardar dados e conhecimentos. Proteção nas Áreas e Instalações: compreende um conjunto de medidas voltadas para preservar as informações contidas em áreas e instalações.

2.3.3.5 Para efeito desta Norma, deve ser considerado **material de acesso restrito** qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule informação classificada, informação pessoal, informação econômica ou informação científico-tecnológica, cuja divulgação implique risco ou dano aos interesses da sociedade ou do Estado, tais como:

- a) Equipamentos, máquina, modelo, molde, maquete, protótipo, artefato, aparelho, dispositivo, instrumento, representação cartográfica, sistema, suprimento;
- b) Veículo terrestre, aquaviário e aéreo, suas partes, peças e componentes;
- c) Armamento e seus acessórios, munição, aparelho, equipamento, suprimento e insumo correlato;
- d) Aparelho, equipamento, suprimento e programa relacionado à tecnologia da informação e comunicações, inclusive à Inteligência de Sinais, de Imagens e Cibernética;
- e) Recurso criptográfico;
- f) Explosivo, líquido e gás;
- g) Manuais, planos, diretrizes, normas, folhetos, tabelas e demais documentos de instrução;
- h) Planos de segurança;
- i) Pesquisas e trabalhos de aperfeiçoamento ou de elaboração de projeto de acesso restrito;
- j) Meio de armazenamento de dados ou informação sigilosa, tais como disco sonoro e óptico (*CD-ROM* e *DVD*), fita e disco magnético, *pendrive*, *HD* externos, cartão de memória e demais meios de armazenamento de dados (*smartphone*, etc);
- k) Plano de coleta;
- l) Credencial de segurança; e
- m) Boletim de Acesso Restrito.

2.3.4 SEGURANÇA ATIVA

2.3.4.1 É o segmento da Contraineligência que preconiza a adoção de medidas de caráter proativo destinado a detectar, identificar, avaliar e neutralizar as ações da Inteligência adversa e outras ações de qualquer natureza, dirigidas contra os interesses do COMAER.

2.3.4.2 É exercida dentro e fora da esfera de competência da Segurança Orgânica. Requer o emprego de pessoal especializado e, na sua condução, poderá ser utilizado o segmento operacional para a obtenção de dados ou conhecimentos negados. A Segurança Ativa desdobra-se, didaticamente, dentre outras, nos seguintes grupos de medidas:

- a) **Contraespionagem** – é o conjunto de medidas destinado a se contrapor às ações de espionagem. As medidas de contraespionagem se contrapõem ao trabalho deliberado de pessoas e organizações, vinculados ou não à Inteligência adversa, que venham a ameaçar os interesses do COMAER. As ações adversas objetivam beneficiar Estados, grupos de países, organizações, facções, empresas, personalidades ou indivíduos. Assim, as medidas de contraespionagem visam a se contrapor às ações adversas que visem à obtenção de conhecimentos ou dados sigilosos referentes a projetos estratégicos, de inovação e tecnologia, bem como planejamentos institucionais e de preparo e emprego nos níveis estratégico, operacional e tático do COMAER;
- b) **Contrassabotagem** – conjunto de medidas voltado a detectar, identificar, avaliar e neutralizar atos de sabotagem contra instituições, pessoas, documentos, materiais, áreas e instalações que o COMAER tem interesse em preservar.
- c) **Contraterrorismo** – conjunto de medidas voltado a contribuir para detectar, identificar, avaliar e neutralizar atos e ameaças terroristas que ponham em risco a Defesa Nacional.
- d) **Contra-ações psicológicas** – conjunto de medidas destinado a se contrapor às ações de influência psicológica, em especial à propaganda adversa, que possam causar prejuízos e danos ao Sistema de Defesa.

2.3.4.3 A Desinformação é uma técnica especializada de Contraineligência destinada a desorientar e a induzir o oponente ao erro, gerando uma análise da situação consistente, porém, equivocada. Permeia todo o segmento de Segurança Ativa.

3 DIRETRIZES

3.1 PREVENIR AÇÕES DE ESPIONAGEM NO COMAER

3.1.1 O desenvolvimento de ações destinadas à obtenção de dados protegidos é fato usual e consolidado nas relações internacionais.

3.1.2 A diversidade de interesses e iniciativas com impacto regional e global vem aumentando continuamente.

3.1.3 Segredos militares, de inovação e tecnologia, operacionais e de projetos estratégicos do COMAER são alvos preferenciais da espionagem estrangeira. Portanto, faz-se necessário identificar, avaliar e interpretar posturas externas, elencando aquelas que representam ameaças, prejuízos e comprometimento das políticas e planos do COMAER.

3.2 AMPLIAR A CAPACIDADE DE DETECTAR, ACOMPANHAR E INFORMAR SOBRE AÇÕES ADVERSAS AOS INTERESSES DO COMAER

3.2.1 O Brasil é detentor de conhecimentos que despertam interesses internacionais. Na tentativa de obtê-los, podem ser realizadas ações ilícitas sobre alvos nacionais, sejam eles materiais ou humanos. Instalações, sistemas informatizados ou pessoas com acesso ou possibilidade de acesso a conhecimentos sensíveis e sigilosos podem ser alvos dessas ações.

3.2.2 O COMAER vem ampliando a sua atuação nos cenários nacional e internacional e, não raro, ações de interesse estratégico para o País são executadas e desenvolvidas com projetos vinculados na área de Ciência e Tecnologia.

3.2.3 Nesse cenário, torna-se imprescindível para a Contraineligência conhecer as principais ameaças e vulnerabilidades a que estão sujeitos os interesses do COMAER, como forma de bem assessorar Comandantes, Chefes e Diretores responsáveis pela consecução dos objetivos da instituição.

3.3 PREVENIR AÇÕES DE SABOTAGEM

3.3.1 A projeção mais relevante do País no cenário internacional aumenta o risco de se tornar alvo de ações de sabotagem, que visam a impedir ou a dificultar a consecução de seus interesses estratégicos.

3.3.2 As consequências de atos de sabotagem podem situar-se em pontos distintos de uma ampla escala, que vão da suspensão temporária até a paralisação total de atividades e serviços essenciais do COMAER.

3.3.3 Dessa forma, é necessário mapear potenciais alvos sujeitos à sabotagem, com o intuito de identificar eventuais ações, em seus estágios iniciais, a fim de neutralizá-las.

3.4 FORTALECER A CULTURA DE PROTEÇÃO DE CONHECIMENTOS

3.4.1 O acesso não autorizado a técnicas, processos de inovação, pesquisas, planos operacionais e a conhecimentos tradicionais a eles associados, pode comprometer a consecução de objetivos estratégicos e resultar em prejuízos expressivos ao preparo e emprego da Força Aérea Brasileira. A proteção dos conhecimentos sensíveis constitui fator essencial para o desenvolvimento do País e das instituições como um todo. Os importantes

resultados advindos de pesquisas científicas e tecnológicas requerem contínuo aperfeiçoamento de mecanismos de proteção nas diversas OM do COMAER.

3.4.2 Torna-se, portanto, imprescindível e urgente fortalecer, no âmbito do COMAER, a cultura de proteção, visando ao estabelecimento de práticas para a salvaguarda de conhecimentos por parte daqueles que os detém. A Contraineligência deve concorrer para a disseminação dessa cultura como forma de evitar ou minimizar prejuízos advindos de um vazamento.

3.5 COOPERAR NA PROTEÇÃO DE INSTALAÇÕES DAS OM DO COMAER

3.5.1 Ameaças como terrorismo, organizações criminosas transnacionais e grupos de diferentes origens e com distintos interesses ligados a atos de sabotagem devem ser identificados e monitorados, como forma de minimizar as possibilidades de sucesso das ações que visem a interromper ou mesmo comprometer o funcionamento das diversas OM do COMAER.

3.5.2 Nesse cenário, a Contraineligência deve participar do processo de avaliação de riscos e vulnerabilidades relativos a alvos potenciais daquelas ameaças, visando a concorrer para a consecução de um Plano de Segurança Orgânica eficiente.

4 DISPOSIÇÕES FINAIS

4.1 CONDUTA ÉTICA

4.1.1 A Contrainteligência pauta-se pela conduta ética, que pressupõe um conjunto de princípios orientadores do comportamento humano em sociedade. A sua observância é requisito fundamental a profissionais de qualquer campo da atividade humana. No que concerne ao comportamento dos profissionais de Inteligência, representa o cuidado com a preservação dos valores que determinam a primazia da verdade, sem conotações relativas, da honra e da conduta pessoal ilibada, de forma clara e sem subterfúgios.

4.1.2 Na atividade de Contrainteligência, os valores éticos devem balizar tanto os limites de ação de seus profissionais quanto os de seus usuários.

4.2 ABRANGÊNCIA

4.2.1 A atividade de Contrainteligência deve possuir abrangência tal que lhe possibilite identificar ameaças, riscos e oportunidades em todos os níveis da estrutura organizacional do COMAER.

4.2.2 É importante que as capacidades individuais e coletivas, de todo o efetivo do COMAER, colaborem com o SINTAER, potencializando a atuação da Contrainteligência e contribuindo com a instituição na persecução de seus objetivos.

4.3 Sugestões para o aperfeiçoamento desta norma deverão ser encaminhadas ao CIAER por meio de documento circunstanciado via cadeia de comando.

4.4 Os casos não previstos nesta Norma serão submetidos à apreciação do Chefe do Centro de Inteligência da Aeronáutica.

REFERÊNCIAS

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações: ICA 200-8*. Brasília, 2008.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Mentalidade de Segurança: FCA 200-2*. Brasília, 2008.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Prevenção de Escuta Clandestina: FCA 200-1*. Brasília, 2008.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Gerenciamento de Plano de Segurança Orgânica do Comando da Aeronáutica: ICA 200-5*. Brasília, 2009.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Prevenção à Engenharia Social: FCA 200-3*. Brasília, 2009.

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

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Instrução para Salvaguarda de Assuntos Sigilosos da Aeronáutica (ISAS). ICA 205-47*. Brasília, 2015.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Visita às Organizações Militares do Comando da Aeronáutica: ICA 205-22*. Brasília, 2015.

BRASIL. **Lei Nº 9.883, de 7 de dezembro de 1999**. *Dispõe sobre o Sistema Brasileiro de Inteligência – SISBIN e cria a Agência Brasileira de Inteligência – ABIN e dá outras providências*. Brasília, 1999.

BRASIL. **Lei nº 13.260, de 16 de março de 2016**. *Regulamenta o dispositivo no inciso XLIII do Art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nº 7.960, de 21 de dezembro de 1989, e nº 12.850, de 2 de agosto de 2013*. Brasília, 2016.

BRASIL. **Decreto Nº 5.015, de 12 de março de 2004**. *Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional*. Brasília, 2004.

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*. Brasília, 2012.

BRASIL. **Portaria Nº 5/GSIPR, de 31 de março de 2005**. *Dispõe sobre o Manual de Inteligência – Doutrina Nacional de Inteligência – Bases Comuns, homologado pelos membros do Conselho Consultivo do Sistema Brasileiro de Inteligência – SISBIN*. Brasília, 2005.

BRASIL. Ministério da Defesa. *Doutrina Militar de Defesa Cibernética*: **MD 31-M-07**. Brasília, 2014. BRASIL. Ministério da Defesa. *Doutrina de Inteligência de Defesa*: DID. Brasília, 2016.