

**MINISTÉRIO DA DEFESA  
COMANDO DA AERONÁUTICA**



**SEGURANÇA**

**ICA 205-47**

**INSTRUÇÃO PARA A SALVAGUARDA DE  
ASSUNTOS SIGILOSOS DA AERONÁUTICA  
(ISAS)**

**2015**

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



**SEGURANÇA**

**ICA 205-47**

**INSTRUÇÃO PARA A SALVAGUARDA DE  
ASSUNTOS SIGILOSOS DA AERONÁUTICA  
(ISAS)**

**2015**



**MINISTÉRIO DA DEFESA  
COMANDO DA AERONÁUTICA**

PORTARIA Nº 1869/GC3, DE 15 DE DEZEMBRO DE 2015.

Aprova a Edição da Instrução para  
a Salvaguarda de Assuntos  
Sigilosos da Aeronáutica (ISAS).

**O COMANDANTE DA AERONÁUTICA**, em conformidade com os incisos I e XIV do art. 23, da Estrutura Regimental do Comando da Aeronáutica, aprovada pelo Decreto nº 6.834, de 30 de abril de 2009, tendo em vista o disposto na Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação, e os Decretos nº 7.724, de 16 de maio de 2012, e nº 7.845, de 14 de novembro de 2012, que a regulamentam, e considerando o que consta do Processo nº 67002.004317/2015-61, resolve:

Art. 1º Aprovar a “Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ISAS)”, que com esta baixa.

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

Art. 3º Revoga-se a Portaria nº 250/GC3, de 7 de março de 2006, publicada no Diário Oficial da União nº 47, de 09 de março de 2006.

Ten Brig Ar NIVALDO LUIZ ROSSATO  
Comandante da Aeronáutica

(Republicado por haver saído com incorreção no BCA nº 232, de 17 de dezembro de 2015)

(Publicado no BCA nº 237, de 28 de dezembro de 2015)

## SUMÁRIO

<b>1 DISPOSIÇÕES PRELIMINARES .....</b>	<b>09</b>
1.1 <u>FINALIDADE</u> .....	09
1.2 <u>CONCEITUAÇÃO</u> .....	09
1.3 <u>COMPETÊNCIA</u> .....	13
1.4 <u>ÂMBITO</u> .....	14
<b>2 DAS RESTRIÇÕES DE ACESSO .....</b>	<b>15</b>
<b>3 DAS INFORMAÇÕES CLASSIFICADAS .....</b>	<b>16</b>
3.1 <u>DAS CONDICIONANTES PARA A CLASSIFICAÇÃO DA INFORMAÇÃO</u> .....	16
3.2 <u>DA COMPETÊNCIA PARA A CLASSIFICAÇÃO DA INFORMAÇÃO</u> .....	18
3.3 <u>DOS PROCEDIMENTOS PARA CLASSIFICAÇÃO, DESCLASSIFICAÇÃO E PRORROGAÇÃO DO PRAZO DE SIGILO DA INFORMAÇÃO</u> .....	18
3.4 <u>DA PUBLICAÇÃO DE INFORMAÇÕES CLASSIFICADAS EM BOLETIM SIGILOSO DO COMANDO DA AERONÁUTICA</u> .....	21
<b>4 DAS DEMAIS SITUAÇÕES COM RESTRIÇÃO DE ACESSO .....</b>	<b>22</b>
4.1 <u>DAS INFORMAÇÕES PESSOAIS</u> .....	22
4.2 <u>DAS INFORMAÇÕES REFERENTES A PROJETOS DE PESQUISA E DESENVOLVIMENTO CIENTÍFICO OU TECNOLÓGICO</u> .....	22
4.3 <u>DAS INFORMAÇÕES CONTIDAS EM DOCUMENTOS PREPARATÓRIOS</u> .....	22
4.4 <u>DAS ÁREAS E INSTALAÇÕES DE ACESSO RESTRITO</u> .....	23
4.5 <u>DOS MATERIAIS DE ACESSO RESTRITO</u> .....	23
<b>5 DAS MEDIDAS DE CONTROLE .....</b>	<b>25</b>
5.6 <u>DO ACESSO</u> .....	25
5.7 <u>DOS DOCUMENTOS E MATERIAIS CONTROLADOS</u> .....	26
5.8 <u>DAS MARCAÇÕES DE SIGILO</u> .....	27
<b>6 DA SEGURANÇA DA INFORMAÇÃO .....</b>	<b>29</b>
6.1 <u>DA SEGURANÇA DO PESSOAL</u> .....	29
6.2 <u>DA SEGURANÇA DA DOCUMENTAÇÃO</u> .....	30
6.3 <u>DA SEGURANÇA DO MATERIAL</u> .....	36
6.4 <u>DA SEGURANÇA DAS ÁREAS E INSTALAÇÕES</u> .....	38
6.5 <u>DA SEGURANÇA NOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO</u> .....	38
<b>7 DA CELEBRAÇÃO DE CONTRATOS .....</b>	<b>44</b>
<b>8 DAS DISPOSIÇÕES FINAIS .....</b>	<b>45</b>
<b>REFERÊNCIAS .....</b>	<b>46</b>
<b>Anexo A - Modelos de Marcação para Informações, Materiais e Áreas Sigilosas .....</b>	<b>49</b>
<b>Anexo B - Modelo de Termo de Eliminação de Cópia(S) de Documento Controlado .....</b>	<b>50</b>
<b>Anexo C - Modelo de Termo de Compromisso de Manutenção de Sigilo .....</b>	<b>51</b>
<b>Anexo D - Modelo de Termo de Classificação de Informação .....</b>	<b>52</b>
<b>Anexo E - Modelo de Identificação de Cópia de Documento Sigiloso .....</b>	<b>55</b>
<b>Anexo F - Modelo de Termo de Eliminação de Material Controlado .....</b>	<b>56</b>
<b>Anexo G - Modelo de Declaração de Responsabilidade no Desligamento .....</b>	<b>57</b>

## **PREFÁCIO**

A salvaguarda de assuntos sigilosos requer, além de uma efetiva mentalidade de segurança, procedimentos e normas cautelares, que devem ser conhecidos por todos aqueles que tratam dos referidos assuntos.

A elaboração da presente Instrução tomou como referência a Lei nº 12.527 de 18 de novembro de 2011, Lei de Acesso à Informação, e os Decretos nº 7.724, de 16 de maio de 2012, e nº 7.845, de 14 de novembro de 2012.

É dever do Comando da Aeronáutica (COMAER) proteger a informação classificada ou sob restrição de acesso, sob sua custódia, que possa comprometer a segurança da sociedade ou do Estado ou que esteja amparada por dispositivos legais em vigor.

## **1 DISPOSIÇÕES PRELIMINARES**

### **1.1 FINALIDADE**

A presente Instrução, elaborada em observância ao prescrito na Lei nº 12.527, de 18 de novembro de 2011, e nos Decretos nº 7.724, de 16 de maio de 2012, e nº 7.845, de 14 de novembro de 2012, tem por finalidade regular o acesso e a divulgação de informações sigilosas e o tratamento de informação classificada ou sob restrição de acesso, no âmbito do Comando da Aeronáutica (COMAER).

### **1.2 CONCEITUAÇÃO**

#### **1.2.1 ACESSO**

É a possibilidade de tomar contato com uma informação, por intermédio da consulta a documento, ou com material que contenha dados, podendo ocorrer a entrada em área ou instalação que a contenha.

#### **1.2.2 ALGORITMO DE ESTADO**

É a função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgão ou entidade do Poder Executivo Federal.

#### **1.2.3 ÁREA OU INSTALAÇÃO DE ACESSO RESTRITO**

É a área ou instalação que contenha documento ou material classificado ou sob restrição de acesso, ou que, por sua utilização ou finalidade, demande proteção.

#### **1.2.4 ARQUIVO PÚBLICO**

É o conjunto de documentos produzidos e recebidos por órgão público, de todas as esferas da administração pública, ou por agentes do Poder Público, no exercício de seu cargo ou função, ou deles decorrente.

#### **1.2.5 CIFRA**

É o sistema criptográfico no qual as letras de cada palavra de um texto em claro são substituídas por outras letras, símbolos ou algarismos, segundo regra ou convenção predeterminada, para se obter um texto criptografado.

#### **1.2.6 CIFRAÇÃO**

É ato de cifrar informação, mediante uso de algoritmo simétrico ou assimétrico, com uso de recurso criptográfico, para substituir sinal de linguagem clara por outro ininteligível, protegendo-a de pessoa que não tenha a necessidade de conhecer o seu conteúdo.

### **1.2.7 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.

### **1.2.8 CÓDIGO DE INDEXAÇÃO**

É o código alfanumérico que indexa documento com informação classificada.

### **1.2.9 COMPROMETIMENTO**

É a perda de segurança resultante do acesso de pessoa não autorizada a documento ou a material classificado ou sob restrição de acesso.

### **1.2.10 CONTRATO SIGILOSO**

É o ajuste, convênio ou termo de cooperação, cujo objeto ou execução, implique tratamento de informação classificada ou sob restrição de acesso.

### **1.2.11 CREDENCIAL DE SEGURANÇA**

É o certificado que habilita pessoa a ter acesso e a realizar o tratamento de informação classificada ou sob restrição de acesso e de acordo com o nível de necessidade de conhecer a ela atribuído.

### **1.2.12 CREDENCIAMENTO DE SEGURANÇA**

É o processo utilizado para credenciar pessoa para o tratamento de informação classificada ou sob restrição de acesso.

### **1.2.13 CUSTÓDIA**

É a responsabilidade pela guarda de documento ou de material classificado ou sob restrição de acesso.

### **1.2.14 DECIFRAÇÃO**

É o ato de decifrar, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, revertendo processo de cifração original.

### **1.2.15 DESCLASSIFICAÇÃO**

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

### **1.2.16 DETENTOR**

É a pessoa que tem a responsabilidade pela custódia de documento ou material.

### **1.2.17 DETENTOR DIRETO**

É a pessoa encarregada da custódia física de um documento ou material.

**1.2.18 DETENTOR INDIRETO**

É a pessoa que, recebendo um documento ou material, transfere, por imperiosa necessidade do serviço, sua custódia para um detentor direto.

**1.2.19 DISPOSITIVO MÓVEL**

É o equipamento portátil dotado de capacidade computacional ou dispositivo de memória para armazenamento passível de remoção.

**1.2.20 DOCUMENTO**

É a unidade de registro de informação, qualquer que seja o suporte material ou formato.

**1.2.21 DOCUMENTO CONTROLADO (DC)**

É todo e qualquer documento classificado ou sob restrição de acesso, que, por sua importância, necessita de medidas adicionais de controle.

**1.2.22 DOCUMENTO PREPARATÓRIO**

É o documento formal utilizado como fundamento para a tomada de decisão ou de ato administrativo.

**1.2.23 ELIMINAÇÃO**

É o ato de se destruir documento que foi considerado sem valor para fins de arquivo e/ou consulta ou material que não mais atende à finalidade a que se destina.

**1.2.24 GESTÃO DOCUMENTAL**

É o conjunto de medidas e rotinas, visando à racionalização e eficiência na criação, tramitação, classificação, avaliação, arquivamento, acesso e uso de informação registrada em documento.

**1.2.25 GRAU DE SIGILO**

É a gradação atribuída à classificação de uma informação.

**1.2.26 INFORMAÇÃO**

É o dado processado, segundo uma metodologia própria que pode ser utilizado para produção e transmissão de conhecimento registrado em um documento.

**1.2.27 INFORMAÇÃO CLASSIFICADA**

É a informação sigilosa em poder do órgão ou entidade pública, que recebeu de autoridade competente, classificação no grau de sigilo ULTRASSECRETO, SECRETO ou RESERVADO devido ao seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado.



**1.2.28 INFORMAÇÃO DE ACESSO RESTRITO**

É aquela que, não sendo passível de receber classificação sigilosa, por sua utilização ou finalidade, demanda medidas especiais de proteção.

**1.2.29 INFORMAÇÃO PESSOAL**

É a informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.

**1.2.30 INFORMAÇÃO PÚBLICA**

É a informação produzida, guardada, organizada e gerenciada pelo Estado em nome da sociedade.

**1.2.31 INFORMAÇÃO SIGILOSA**

É a informação submetida, temporariamente, à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, ou por ser abrangida pelas demais hipóteses legais de sigilo.

**1.2.32 INVESTIGAÇÃO PARA CREDENCIAMENTO DE SEGURANÇA**

É o procedimento de averiguação da existência de requisitos indispensáveis para a concessão da credencial de segurança à pessoa natural, para o acesso e o tratamento de informação classificada ou sob restrição de acesso.

**1.2.33 MATERIAL CONTROLADO (MC)**

É todo material classificado ou sob restrição de acesso que, por sua importância, necessita de medidas adicionais de controle.

**1.2.34 MATERIAL DE ACESSO RESTRITO**

É aquele que, não sendo passível de receber classificação sigilosa, por sua utilização ou finalidade, demanda medidas especiais de proteção.

**1.2.35 MARCAÇÃO**

É a aposição de marca que indica o grau de sigilo da informação classificada ou o amparo legal que permite a imposição de restrição de acesso ao seu conteúdo.

**1.2.36 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.

**1.2.37 NECESSIDADE DE CONHECER**

É a condição pessoal, inerente ao efetivo exercício de cargo, da função, do emprego ou da atividade, indispensável para que uma pessoa tenha acesso à informação classificada ou sob restrição de acesso.

**1.2.38 NÍVEL DE RESTRIÇÃO DE ACESSO**

É o parâmetro relacionado ao rigor das medidas de segurança a serem adotadas a fim de garantir a restrição de acesso a determinado material, conforme o dano causado pela sua divulgação ou acesso desautorizado.

**1.2.39 ÓRGÃO CONTROLADOR**

É a Organização Militar (OM) que elabora e expede um DC ou a responsável pelo controle de um MC.

**1.2.40 QUEBRA DE SEGURANÇA**

É a ação ou omissão que implica no comprometimento ou no risco de comprometimento de informação classificada ou sob restrição de acesso.

**1.2.41 RECLASSIFICAÇÃO**

É o ato pelo qual a autoridade competente altera a classificação original de uma informação.

**1.2.42 RECURSO CRIPTOGRÁFICO**

É o sistema, programa, processo, equipamento isolado ou em rede, que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

**1.2.43 RESTRIÇÃO DE ACESSO**

É o ato de se limitar ou impedir o contato de uma pessoa não credenciada ou não autorizada com documento, área, instalação ou material, segundo as normas legais vigentes.

**1.2.44 TRATAMENTO DA INFORMAÇÃO CLASSIFICADA**

É o conjunto de ações referentes à produção, à recepção, à classificação, à desclassificação, à utilização, ao acesso, a reprodução, ao transporte, à transmissão, à distribuição, ao arquivamento, ao armazenamento, à eliminação, à avaliação, à destinação ou ao controle de informação classificada.

**1.2.45 SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES**

É o conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a inviolabilidade, a integridade, a confiabilidade e a autenticidade das informações.

**1.2.46 VISITANTE**

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

**1.3 COMPETÊNCIA**

É de competência do Centro de Inteligência da Aeronáutica (CIAER), Órgão Central do Sistema de Inteligência da Aeronáutica, editar os procedimentos relativos ao

tratamento de informação classificada em qualquer grau de sigilo ou sob restrição de acesso, no âmbito do COMAER.

#### **1.4 ÂMBITO**

A presente Instrução aplica-se a todas as Organizações Militares (OM) do COMAER. Podendo, também, ser cedida, à guisa de orientação, às empresas vinculadas e a outras empresas e órgãos com os quais o COMAER mantém contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada em qualquer grau de sigilo, ou cuja execução envolva informação classificada.

## **2 DAS RESTRIÇÕES DE ACESSO**

**2.1** O COMAER manterá sob restrição de acesso, independentemente de classificação, o documento, a área ou a instalação sob sua custódia, que contenha:

- a) informação classificada;
- b) informação de acesso restrito;
- c) informação pessoal;
- d) informação protegida por legislação específica como de natureza sigilosa, tal como sigilo bancário, fiscal ou patrimonial, etc;
- e) processo judicial sob segredo de justiça;
- f) identificação do denunciante que origine procedimento investigativo;
- g) papel de trabalho e procedimento relativo a ações de controle e de inspeção correcional ou de qualquer espécie de ação investigativa, nos termos do § 3º do art. 26 da Lei nº 10.180, de 6 de fevereiro de 2001;
- h) relatório e nota técnica decorrente de investigação, auditoria, fiscalização, e outros documentos relativos à atividade de correição;
- i) informação referente a projeto de pesquisa e desenvolvimento científico ou tecnológico de interesse da Defesa Nacional;
- j) documento preparatório;
- k) documento ou informação de natureza técnica, produzido por órgão ou entidade não vinculado, ainda que não se caracterize a custódia;
- l) área e instalação que contenha informação classificada ou sob restrição de acesso;
- m) informação constante de manual de instrução ou de documento que trate do emprego de material de acesso restrito;
- n) materiais de acesso restrito;
- o) correspondência pessoal e outras abrangidas pelas demais hipóteses legais de sigilo; e
- p) outros julgados pertinentes pelo COMAER.

**2.2** Cabe às autoridades mencionadas nos itens 3.2.1 e 3.2.2 desta Instrução definir a adoção de medidas de restrição de acesso, dentro dos preceitos estabelecidos nos dispositivos legais vigentes.

### **3 DAS INFORMAÇÕES CLASSIFICADAS**

#### **3.1 DAS CONDICIONANTES PARA A CLASSIFICAÇÃO DA INFORMAÇÃO**

**3.1.1** Os graus de sigilo para a classificação de informação são:

- a) RESERVADO;
- b) SECRETO; e
- c) ULTRASSECRETO.

**3.1.2** Somente será passível de classificação a informação considerada imprescindível à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possa:

- a) pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
- b) prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
- c) pôr em risco a vida, a segurança ou a saúde da população;
- d) oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
- e) prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
- f) prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
- g) pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
- h) comprometer atividade de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

**3.1.3** Para a classificação da informação deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

- a) a gravidade do risco ou dano à segurança da sociedade e do Estado; e
- b) o prazo máximo de restrição de acesso ou o evento que defina seu termo final.

**3.1.4** Quanto à gravidade do risco ou dano à segurança da sociedade e do Estado:

**3.1.4.1** A informação de grau de sigilo ULTRASSECRETO é aquela cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave, tal como referente a (à):

- a) soberania e à integridade territorial nacionais;
- b) relações internacionais do País;
- c) plano e operação militar que afetem as letras “a” e “b” do presente item;

- d) projeto de pesquisa e desenvolvimento científico e tecnológico de interesse da Defesa Nacional; e
- e) programa econômico.

**3.1.4.2** A informação de grau de sigilo SECRETO é aquela cujo conhecimento não autorizado possa acarretar dano grave, tal como referente a (à):

- a) sistema;
- b) instalação;
- c) programa;
- d) projeto;
- e) plano ou operação de interesse da Defesa Nacional;
- f) assunto diplomático e de Inteligência; e
- g) plano ou seus detalhes.

**3.1.4.3** A informação de grau de sigilo RESERVADO é aquela cujo conhecimento não autorizado possa acarretar dano, tal qual a que frustre ou comprometa:

- a) objetivo de interesse do Poder Executivo;
- b) objetivo ou atividade de interesse do Comando da Aeronáutica; e
- c) plano, operação ou objetivo nele previsto ou referido.

**3.1.5** Os prazos máximos de restrição de acesso à informação classificada vigoram na data de sua produção e são os seguintes:

**3.1.5.1** Para o grau de sigilo ULTRASSECRETO: vinte e cinco anos;

**3.1.5.2** Para o grau de sigilo SECRETO: quinze anos; e

**3.1.5.3** Para o grau de sigilo RESERVADO: cinco anos.

**3.1.6** Somente a informação classificada no grau de sigilo ULTRASSECRETO é passível de prorrogação, uma única vez, de prazo de restrição de acesso.

**3.1.7** A informação que puder colocar em risco a segurança do Presidente e do Vice-Presidente da República e respectivos cônjuges e filhos (as) será classificada no grau de sigilo RESERVADO e ficará sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.

**3.1.8** Poderá ser estabelecida como termo final de restrição de acesso a ocorrência de determinado evento, observados os prazos máximos de classificação.

**3.1.9** Transcorrido o prazo máximo de classificação, a informação tornar-se-á, automaticamente, de acesso público dentro das prescrições da legislação vigente, observadas as restrições de acesso previstas no item 2.1 desta Instrução.

### **3.2 DA COMPETÊNCIA PARA A CLASSIFICAÇÃO DA INFORMAÇÃO**

**3.2.1** O Comandante da Aeronáutica tem competência para classificar a informação sigilosa nos graus de sigilo ULTRASSECRETO, SECRETO e RESERVADO, sendo vedada a delegação de competência para a classificação nos graus de sigilo ULTRASSECRETO e SECRETO.

**3.2.2** O Comandante (Cmt), Chefe (Ch) ou Diretor (Dir) de OM, Adido Aeronáutico ou Oficial-General que produza documento, tem competência para classificar informação sigilosa no grau RESERVADO, sendo vedada a delegação ou a assinatura no impedimento do documento classificado e do Termo de Classificação de Informação (TCI).

**3.2.2.1** A autoridade que responde pelo comando, chefia ou direção, eventual ou interinamente, situação esta devidamente publicada em Boletim Interno da OM, poderá classificá-lo.

**3.2.2.2** A autoridade citada em 3.2.2 deverá dar ciência do seu ato de classificação de documento no grau RESERVADO ao Comandante da Aeronáutica, no prazo de 90 (noventa) dias, por intermédio da cadeia hierárquica de sua respectiva estrutura organizacional, encaminhando, para tanto, a tabela de classificação ou desclassificação de documentos elaborada pela respectiva CPADS/SPADS.

**3.2.3** A classificação de informação no grau de sigilo ULTRASSECRETO, pelo Comandante da Aeronáutica, deverá ser ratificada pelo Ministro de Estado da Defesa, no prazo de trinta dias.

**3.2.4** Enquanto não ratificada, a classificação de que trata o item 3.2.3 acima considera-se válida, para todos os efeitos legais.

### **3.3 DOS PROCEDIMENTOS PARA CLASSIFICAÇÃO, DESCLASSIFICAÇÃO E PRORROGAÇÃO DO PRAZO DE SIGILO DA INFORMAÇÃO**

#### **3.3.1 DA CLASSIFICAÇÃO DA INFORMAÇÃO**

**3.3.1.1** A decisão de classificar a informação deverá ser formalizada pela emissão de TCI, que conterá os seguintes itens:

- a) código de indexação de documento;
- b) grau de sigilo;
- c) categoria na qual se enquadra a informação;
- d) tipo de documento;
- e) data da produção do documento;
- f) indicação de dispositivo legal que fundamenta a classificação;
- g) razão da classificação, observados os critérios estabelecidos no item 3.1.3;
- h) indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no 3.1.5;
- i) data da classificação; e
- j) identificação da autoridade que classificou a informação.

**3.3.1.2** A informação prevista na letra “g” acima deverá ser mantida no mesmo grau de sigilo da informação classificada.

**3.3.1.3** A informação somente será considerada classificada após a assinatura do respectivo TCI.

**3.3.1.4** O TCI é único para cada documento classificado.

**3.3.1.5** Para confecção do TCI, a informação a ser classificada deverá receber número único de protocolo/número único de documento (NUP/NUD), mesmo que não seja um documento padrão, como esboço, desenho, mapa, carta, fotografia, imagem, negativo ou slide.

**3.3.1.6** A competência para a assinatura do TCI é das autoridades previstas nos itens 3.2.1 e 3.2.2.

**3.3.1.7** O TCI deverá ser confeccionado em duas vias, conforme modelo contido no anexo “D” desta Instrução.

**3.3.1.8** O documento RESERVADO terá a 1ª via do TCI arquivada na OM que o produziu, a fim de possibilitar sua atualização e controle (desclassificação ou redução do prazo). A 2ª via do TCI seguirá anexada à informação.

**3.3.1.9** O TCI referente à informação classificada como ULTRASSECRETA ou SECRETA deverá ser submetido ao Comandante da Aeronáutica, e sua cópia deverá ser encaminhada ao CIAER, que providenciará a devida remessa à Comissão Mista de Reavaliação de Informações (CMRI).

**3.3.1.10** A Informação classificada receberá o Código de Indexação de Documento que contém Informação Classificada (CIDIC), conforme modelo constante do anexo “D”.

**3.3.1.11** O CIDIC será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada e será estruturado em duas partes:

**3.3.1.11.1** A primeira parte do CIDIC será composta pelo Número Único de Protocolo (NUP), originalmente cadastrado conforme legislação de gestão documental; e

**3.3.1.11.2** A segunda parte do CIDIC será composta dos seguintes elementos:

- a) grau de sigilo: indicação do grau de sigilo, ULTRASSECRETO (U), SECRETO (S) ou RESERVADO (R), com as iniciais na cor vermelha;
- b) categoria: indicação, com dois dígitos, da categoria relativa ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), conforme anexo II do Decreto nº 7.845/2012;
- c) data de produção do documento classificado: registrar a data de produção do documento, no formato dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);
- d) data de desclassificação do documento: registrar a potencial data de desclassificação desse documento, efetuada no ato de desclassificação, no formato dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);



- e) indicação de reclassificação: indicação de ocorrência ou não, S (sim) ou N (não), de reclassificação de documento classificado, respectivamente, conforme as seguintes situações:
  - reclassificação de documento resultante de reavaliação; ou
  - primeiro registro da classificação.
- f) indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente, para informação classificada no grau de sigilo ULTRASSECRETO, no formato dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos), na cor vermelha, quando possível;
- g) o documento classificado, quando de sua desclassificação, manterá apenas o NUP;
- h) não será utilizada tabela de classificação de assunto ou de natureza do documento, em razão de exigência de restrição temporária de acesso a documento classificado, sob pena de pôr em risco sua proteção; e
- i) no que concerne à gestão documental, deverá ser guardado o histórico de alterações do CIDIC.

### **3.3.2 DA DESCLASSIFICAÇÃO E DA REAVALIAÇÃO DA INFORMAÇÃO CLASSIFICADA**

**3.3.2.1** A classificação da informação será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, para desclassificação ou redução do prazo de sigilo.

**3.3.2.1.1** Para o cumprimento do disposto acima, além do previsto no item 3.1.3, deverá ser observado:

- a) o prazo máximo de restrição de acesso à informação, previsto no item 3.1.5;
- b) o prazo máximo de quatro anos para revisão de ofício da informação classificada no grau de sigilo ULTRASSECRETO ou SECRETO, previsto no inciso I do caput do art. 47 do Decreto nº 7.724, de 16 de maio de 2012;
- c) a permanência das razões da classificação;
- d) a possibilidade de danos ou riscos decorrentes da divulgação ou acesso irrestrito da informação; e
- e) a peculiaridade da informação produzida no exterior por autoridade ou agente público.

**3.3.2.2** Os procedimentos para reavaliação e desclassificação de informação classificada serão os previstos na ICA 200-12 – Avaliação de Documentos Classificados no Comando da Aeronáutica.

**3.3.2.3** O pedido de desclassificação ou de reavaliação da classificação de informação poderá ser apresentado ao órgão ou entidade, independente de existir prévio pedido de acesso à informação.

**3.3.2.4** O pedido de que trata o item anterior será endereçado à autoridade classificadora, que tomará uma decisão no prazo de trinta dias.

**3.3.2.5** No caso de informação produzida por autoridade ou agente público no exterior, o requerimento de desclassificação e reavaliação será apreciado pela autoridade hierarquicamente superior que estiver em território brasileiro.

**3.3.2.6** Negado o pedido de desclassificação ou de reavaliação da informação pela autoridade classificadora, o requerente poderá apresentar recurso no prazo de dez dias, contado da ciência da negativa, primeiramente perante o Comandante da Aeronáutica e, em caso de negativa, ao Ministro de Estado da Defesa.

**3.3.2.7** Será apresentada uma decisão no prazo de trinta dias após a apreciação do recurso.

**3.3.2.8** Desprovido o recurso de que trata o caput, poderá o requerente apresentar recurso à Comissão Mista de Reavaliação de Informações, instituída nos termos do § 1º do art. 35 da Lei nº 12.527/2011, no prazo de dez dias, contado da ciência da decisão.

**3.3.2.9** A decisão sobre a desclassificação, a reclassificação ou a redução do prazo de sigilo de informação classificada deverá constar da capa do processo, se houver, e do campo apropriado no TCI.

#### **3.4 DA PUBLICAÇÃO DE INFORMAÇÕES CLASSIFICADAS EM BOLETIM SIGILOSO**

**3.4.1** Toda informação classificada passível de publicação em Boletim será realizada de acordo com o seu grau de sigilo, como segue:

- a) Informação RESERVADA será publicada em BOLETIM RESERVADO;
- b) Informação SECRETA será publicada em BOLETIM SECRETO; e
- c) Informação ULTRASSECRETA será publicada em BOLETIM ULTRASSECRETO.

**3.4.2** O Boletim Classificado receberá o TCI de acordo com o seu grau de sigilo, conforme modelo constante no anexo “D”.

**3.4.3** O Boletim Classificado estará sujeito aos termos de divulgação da Lei nº 12.527/2011, e quando da sua desclassificação todo seu conteúdo será desclassificado, conforme avaliação da CPADS/SPADS.

**3.4.4** A publicação do Boletim Classificado ocorrerá sob demanda.

**3.4.5** O Boletim Classificado deverá receber marcação na parte superior e inferior de todas as suas páginas, existindo ou não classificação de sigilo, conforme modelo constante do anexo “A”.

## **4 DAS DEMAIS SITUAÇÕES COM RESTRIÇÃO DE ACESSO**

### **4.1 DAS INFORMAÇÕES PESSOAIS**

**4.1.1** O tratamento da informação pessoal, quanto ao acesso, deve assegurar a sua proteção, observadas a disponibilidade, a autenticidade, a integridade e as restrições de acesso.

**4.1.2** A informação pessoal de militar e de servidor, relativa à intimidade, vida privada, honra e imagem, terá seu acesso restrito, independente de classificação de sigilo, pelo prazo máximo de cem anos a contar da data de sua produção.

**4.1.3** Terão acesso à informação pessoal, militares ou servidores que, devidamente autorizados, têm a necessidade de conhecer seu conteúdo por força de atribuição funcional e, a pessoa a que essa informação se refere, observando-se os termos do art. 31 da Lei nº 12.527/2011 e dos art. 55 a 62 do Decreto nº 7.724/2012.

**4.1.4** A divulgação ou acesso por terceiros a informação pessoal poderá ter autorização diante de previsão legal ou consentimento expresso da pessoa a que ela se referir.

**4.1.5** Aquele que obtiver acesso à informação de que trata o item 4.1.2 será responsabilizado por seu uso indevido.

**4.1.6** O pedido de acesso à informação pessoal deverá observar os procedimentos previstos nos art. 55 a 61 do Decreto 7.724/2012.

**4.1.7** O documento que contenha informação pessoal deverá receber marcação na parte superior e inferior de todas as páginas, existindo ou não classificação de sigilo, conforme modelo do anexo “A”.

### **4.2 DAS INFORMAÇÕES REFERENTES A PROJETOS DE PESQUISA E DESENVOLVIMENTO CIENTÍFICO OU TECNOLÓGICO**

**4.2.1** A informação referente a projeto de pesquisa e desenvolvimento científico ou tecnológico, cujo sigilo seja imprescindível à segurança da sociedade e do Estado, terá seu acesso restrito, independentemente de classificação de sigilo, a militar ou servidor que, devidamente autorizado, tenha a necessidade de conhecer seu conteúdo por força de atribuição funcional.

**4.2.2** A restrição de acesso perdurará pelo período que for necessário à consecução desse projeto ou até que sua divulgação não possibilite vantagem de qualquer natureza a outra nação ou a empresa não envolvida no respectivo projeto.

**4.2.3** A informação a que se refere o item 4.2.1 deverá receber marcação na parte superior e inferior de todas as suas páginas, existindo ou não classificação de sigilo, conforme modelo constante do anexo “A”.

### **4.3 DAS INFORMAÇÕES CONTIDAS EM DOCUMENTOS PREPARATÓRIOS**

**4.3.1** Para efeito desta Instrução, são exemplos de documentos preparatórios:

**4.3.1.1** Pareceres;

**4.3.1.2** Notas técnicas;**4.3.1.3** Documentos de Inteligência, tais como:

- a) informe;
- b) informação;
- c) apreciação;
- d) estimativa;
- e) relatório, mensagem e síntese de Inteligência;
- f) levantamento estratégico de área;
- g) conjuntura e suas avaliações; e
- h) demais documentos, informações ou conhecimentos produzidos pela atividade de Inteligência.

**4.3.1.4** Documentos operacionais, de pessoal ou de logística, tais como:

- a) sumário e mensagem diária de operações;
- b) mensagens operacionais; e
- c) sumário ou mapa de situação de pessoal ou material.

**4.3.1.5** Sindicância, processo administrativo ou disciplinar e outros.

**4.3.2** O acesso à informação contida em documento preparatório seguirá as prescrições contidas no art. 20 do Decreto nº 7.724, de 16 de maio de 2012.

**4.3.3** O documento preparatório deverá receber marcação na parte superior e inferior de todas as suas páginas, conforme modelo do anexo “A”.

**4.4** DAS ÁREAS E INSTALAÇÕES DE ACESSO RESTRITO

**4.4.1** A área ou instalação que contenha documento, sistema de informações, meios de comunicação, classificados ou sob restrição de acesso, ou material que, por sua utilização ou finalidade, demandar proteção, terá seu acesso restrito a militar ou servidor cadastrado e com a autorização do Cmt, Ch ou Dir da OM que possui sua jurisdição.

**4.4.2** Na área ou instalação de acesso restrito deverá ser fixada, em local visível, uma ou mais placas indicativas, conforme modelos constantes do anexo “A”, de modo a possibilitar sua visualização por qualquer pessoa que tente abordá-la.

**4.5** DOS MATERIAIS DE ACESSO RESTRITO

**4.5.1** Para efeito desta Instrução, 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 e do Estado, tais como:

- a) equipamento, 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.

**4.5.2** As medidas a serem adotadas para evitar a quebra de segurança serão graduadas em níveis crescentes conforme a gravidade do dano a ser causado pela violação, divulgação ou comprometimento do material de acesso restrito, como segue:

**4.5.2.1** O material de acesso restrito graduado com nível 3 é aquele que pode acarretar dano excepcionalmente grave.

**4.5.2.2** O material de acesso restrito graduado com nível 2 é aquele que pode acarretar dano grave.

**4.5.2.3** O material de acesso restrito graduado com nível 1 é aquele que pode acarretar dano.

**4.5.3** Todo conteúdo com restrição de acesso, quando cabível, deverá ser publicado no Boletim de Acesso Restrito, à exceção das informações pessoais que serão publicadas no Boletim Interno de Informações Pessoais, de acordo com a Instrução de Padronização de Processos Administrativos – ICA 35-1/2013.

**4.5.4** A publicação do Boletim de Acesso Restrito ocorrerá sob demanda.

**4.5.5** Todo material de acesso restrito deverá receber marcação (impressa ou fixada) prevista nos modelos constantes do anexo “A”.

## **5 DAS MEDIDAS DE CONTROLE**

**5.1** Compete ao Comandante, Chefe ou Diretor de OM manter o pessoal sob suas ordens atualizado sobre as medidas de controle da informação classificada ou sob restrição de acesso em vigor.

**5.2** Qualquer militar ou servidor, que tenha conhecimento de uma situação na qual uma informação classificada ou sob restrição de acesso possa estar ou venha a ser comprometida, deverá informar tal fato ao seu chefe imediato e/ou à autoridade responsável pela proteção da mesma.

**5.3** Qualquer militar ou servidor, que tenha extraviado documento ou material classificado ou sob restrição de acesso, deverá participar imediatamente ao seu chefe imediato e/ou à autoridade responsável pela custódia.

**5.3.1** Idêntica providência deverá ser tomada quando se encontre ou se tenha conhecimento de que foi achado documento ou material classificado ou sob restrição de acesso.

**5.4** Constatando-se ocorrência, que possa implicar o comprometimento de informação classificada ou sob restrição de acesso, a autoridade competente tomará as providências necessárias para verificar a extensão do comprometimento e apurar responsabilidades.

**5.5** Todo militar ou servidor, ao deixar o exercício de determinado cargo ou função, deverá passar ao seu substituto todo o documento ou material classificado, até então sob sua custódia, devidamente conferido.

### **5.6 DO ACESSO**

**5.6.1** Nos termos do inciso XXXIII do art. 5º da Constituição Federal, todo cidadão tem o direito a receber do órgão público informação de seu interesse particular, ou de interesse coletivo ou geral, que será prestada no prazo da lei, sob pena de responsabilidade, ressalvada aquela cujo sigilo seja imprescindível à segurança da sociedade ou do Estado.

**5.6.2** Cabe ao Cmt, Ch ou Dir, no âmbito de sua OM, observadas as normas e procedimentos específicos aplicáveis, assegurar a:

- a) gestão transparente da informação, propiciando amplo acesso e divulgação da mesma seguindo as prescrições constantes nas normas vigentes que tratam do assunto; e
- b) proteção da informação classificada ou sob restrição de acesso, observada a sua disponibilidade, a sua autenticidade e a sua integridade.

**5.6.3** O acesso à informação classificada é estritamente funcional e independe de grau hierárquico do militar, sendo, contudo, obrigatório o credenciamento de segurança compatível, de acordo com as normas de credenciamento vigentes.

**5.6.3.1** O acesso de militar ou civil, não credenciado ou não autorizado por legislação específica, a documento ou material classificado ou sob restrição de acesso, poderá, excepcionalmente, ser permitido mediante a assinatura de Termo de Compromisso e Manutenção de Sigilo (TCMS), conforme modelo constante no anexo “C” desta Instrução, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

**5.6.3.2** Cabe ao Cmt, Ch ou Dir, no âmbito de sua OM, regular o acesso, considerando os seguintes aspectos:

- a) necessidade do serviço;
- b) necessidade de conhecer; e
- c) nível de credenciamento.

**5.6.4** Os demais acessos previstos na legislação em vigor serão concedidos de acordo com o que prescreve a Lei nº 12.527/2011, seus decretos e legislação específica do COMAER sobre o assunto.

**5.6.4.1** Não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais.

## **5.7 DOS DOCUMENTOS E MATERIAIS CONTROLADOS**

**5.7.1** O documento ou material classificado como ULTRASSECRETO deverá, por sua natureza, ser considerado Documento Controlado (DC) ou Material Controlado (MC).

**5.7.2** Qualquer documento classificado ou sob restrição de acesso ou, ainda, material que o contenha, poderá, a critério da autoridade que o produziu ou o classificou, ser considerado como DC/MC.

**5.7.2.1** O material criptográfico e/ou criptofônico deverá, mesmo não sendo classificado e devido à sua natureza, ser considerado sob restrição de acesso e MC.

**5.7.2.2** Os manuais de equipamento criptográfico ou criptofônico deverão ser considerados MC.

**5.7.3** O sistema de cifra deverá ser guardado em local distinto de seus códigos.

**5.7.4** O DC/MC, sempre que possível, deverá ser entregue pessoalmente ao seu destinatário, por pessoa credenciada, mediante assinatura de recibo.

**5.7.5** Ao receber qualquer DC/MC, o detentor deverá verificar a sua normalidade física e, se for o caso, informar, via canal de comando, ao órgão controlador as alterações encontradas.

**5.7.6** Toda OM que possuir DC/MC sob sua guarda, deve fazer a lavratura de Termo de Custódia atribuindo responsabilidade legal para o detentor do DC/MC. Tal termo é um ato interno da OM, não havendo necessidade de envio deste para o expedidor do DC/MC.

**5.7.7** Para o tratamento do DC/MC, deverá ser observado o previsto no FCA 200-6/2013.

**5.7.8** O detentor de DC/MC deverá remeter uma cópia do Termo de Inventário ao órgão controlador, conforme prazo e modelo previsto no FCA 200-6/2013.

**5.7.9** Sempre que houver a substituição do detentor indireto de DC/MC, este deverá proceder à passagem de custódia dos DC/MC para o seu substituto e remeter o termo de transferência de guarda de documento e/ou material controlado, conforme o FCA 200-6/2013, ao órgão controlador.

**5.7.10** Os termos de inventário e os de transferência de guarda não serão classificados e deverão receber a designação de “MATERIAL DE ACESSO RESTRITO”, sendo aposto o carimbo conforme o modelo constante no anexo “A”.

**5.7.11** Ao receber o termo de inventário e/ou transferência de guarda, o órgão controlador deverá acusar o recebimento, fazendo constar, na oportunidade, qualquer divergência encontrada.

**5.7.12** Sempre que ocorrer furto, roubo ou extravio de DC/MC, o Cmt, Ch ou Dir de OM deverá instaurar uma sindicância, a fim de apurar as causas e os responsáveis, levantar as medidas de segurança orgânica que deverão ser revistas ou outras novas que devam ser implementadas, bem como tomar as medidas penal, civil e administrativa decorrentes.

**5.7.12.1** O órgão controlador poderá remeter um novo exemplar de DC, em substituição ao anteriormente distribuído, desde que a divulgação de seu conteúdo não tenha acarretado grave comprometimento da segurança da informação.

**5.7.12.2** Em se tratando de DC relativo a sistema de cifra e código, o órgão controlador deverá substituir todos os exemplares comprometidos.

## **5.8 DAS MARCAÇÕES DE SIGILO**

**5.8.1** A marcação do grau de sigilo de um documento deverá constar de todas as suas páginas, observadas as seguintes formalidades:

- a) a marcação será centralizada, no alto e no rodapé de cada página, em cor contrastante com a do documento, utilizando-se, preferencialmente, a cor vermelha conforme modelo constante do anexo “A”; e
- b) somente deverá ser usada outra cor para assinalar a classificação sigilosa quando o documento, pela sua natureza, não permitir que se obtenha o contraste desejado.

**5.8.2** O esboço, desenho, fotografia aérea ou não, imagem digital, arquivo digital, multimídia, negativo ou slide classificado ou sob restrição de acesso terá marcado seu grau de sigilo em local que possibilite sua reprodução, em todas as suas cópias.

**5.8.2.1** O negativo ou slide de que trata este artigo, cuja falta de espaço impossibilite a marcação de grau de sigilo ou da condição que permite a restrição ao seu acesso, será utilizado em condição que garanta a sua segurança e guardado em recipiente que exiba a classificação correspondente à do seu conteúdo ou condição que permite o estabelecimento de restrições ao seu acesso.

**5.8.3** Fotografia e reprodução de negativo sem legenda terá marcado o seu respectivo grau de sigilo ou da condição que permite o estabelecimento de restrição ao seu acesso, no seu verso, bem como na respectiva embalagem.

**5.8.4** O negativo em rolo contínuo, relativo a reconhecimento e a levantamento aerofotogramétrico, terá marcado o grau de sigilo correspondente ou da condição que permite o estabelecimento de restrição ao seu acesso no início e no fim de cada rolo.

**5.8.5** O microfilme e o filme cinematográfico classificado ou sob restrição de acesso será acondicionado de modo tecnicamente seguro, devendo a embalagem exibir a marcação do



grau de sigilo correspondente ao seu conteúdo ou da condição que permite o estabelecimento de restrição ao seu acesso.

**5.8.6** A marcação do grau de sigilo em mapa, carta e fotocarta deverá ser feita logo acima do título e na parte inferior, sem prejuízo das imagens registradas, mesmo que este arquivo esteja digitalizado, ou seja, exibido em formato digital.

**5.8.6.1** A carta e fotocarta montada a partir de fotografias aéreas ou imagens digitais será classificada em razão dos detalhes que revelem e não apenas da classificação atribuída às fotografias aéreas ou imagens digitais que lhes deram origem.

## **6 DA SEGURANÇA DA INFORMAÇÃO**

### **6.1 DA SEGURANÇA DO PESSOAL**

#### **6.1.1 DA SEGURANÇA NO PROCESSO SELETIVO**

**6.1.1.1** A avaliação de cargo ou função, com o objetivo de determinar o seu grau de sensibilidade, bem como a investigação de segurança, necessária para o desempenho de uma função ou cargo sensível, deverá estar de acordo com a norma para a concessão de credencial de segurança vigente.

**6.1.1.2** A função ou cargo que trate com informação classificada ou sob restrição de acesso deverá ser compartimentada, a fim de restringir o acesso, considerando a necessidade de conhecer.

**6.1.1.3** O acesso de pessoal às áreas citadas no item 6.4 desta Instrução deverá estar de acordo com a norma de concessão de credenciamento vigente.

#### **6.1.2 DA SEGURANÇA NO DESEMPENHO DA FUNÇÃO**

**6.1.2.1** O credenciamento para o desempenho de cargo ou função deverá ocorrer antes do início do desempenho da mesma e estar de acordo com a norma para concessão de credencial de segurança vigente.

**6.1.2.2** O Cmt, Ch ou Dir de OM deverá verificar:

- a) comportamento e/ou vulnerabilidade incompatível com o cargo ou função;
- b) descontentamento no desempenho da função; e
- c) vulnerabilidades em relação ao recrutamento e/ou aliciamento adversos.

#### **6.1.3 DA SEGURANÇA NO DESLIGAMENTO DA FUNÇÃO**

**6.1.3.1** Após o desligamento de um militar ou servidor de um cargo ou função que exige credenciamento de segurança, sempre que possível, o Comandante, Chefe ou Diretor de OM deverá:

- a) manter, em banco de dados, para contato futuro, o endereço de ex-integrante, possibilitando o acompanhamento do militar ou do servidor que ocupava função sensível;
- b) solicitar ao ex-integrante a exclusão de todas as pastas e arquivos temporários, por ele produzidos no(s) computador(es) existente(s) na OM;
- c) solicitar ao ex-integrante que informe, de imediato, qualquer tentativa de cooptação que venha a ser alvo;
- d) informar ao militar e ao servidor desligado que o sigilo das informações que tomou conhecimento deverá ser mantido; e
- e) assinar a Declaração de Responsabilidade (Anexo “G”) na entrevista de desligamento.

## **6.2 DA SEGURANÇA DA DOCUMENTAÇÃO**

**6.2.1** As medidas de segurança da documentação previstas nesta Instrução devem ser adotadas para as fases de produção, expedição, recepção, manuseio, arquivamento e eliminação.

**6.2.2** As medidas de segurança da documentação devem ser adotadas para toda a documentação classificada ou sob restrição de acesso.

**6.2.3** A publicação de ato normativo relativo à informação classificada ou sob restrição de acesso, esta devido a sigilo legal ou judicial, poderá limitar-se, quando necessário, aos respectivos números, data de expedição ou ementas, redigidos de modo a não comprometer o seu sigilo.

### **6.2.4 DA SEGURANÇA NA PRODUÇÃO**

**6.2.4.1** Todo documento preparatório poderá ser classificado. Devendo, na fase de produção, ser marcado como **DOCUMENTO PREPARATÓRIO - ACESSO RESTRITO**, conforme previsto no item 4.3.3 desta Instrução.

**6.2.4.2** Após concluído, caso a informação contida no documento se enquadre nas condicionantes do art. 23 da Lei nº 12.527/2011, este documento poderá ser classificado, recebendo seu grau de sigilo por meio da confecção do TCI.

**6.2.4.3** Página, parágrafo, seção, parte componente ou anexo de um documento pode merecer diferente classificação, mas ao documento, no seu todo, será atribuído o grau de sigilo mais elevado.

**6.2.4.4** Na hipótese de documento que contenha informações classificadas em diferentes graus de sigilo, fica assegurado o acesso à parte não classificada por meio de certidão, extrato ou cópia, com ocultação da parte sob restrição.

**6.2.4.5** A classificação de um grupo de documentos, que formem um conjunto, deve ser a do documento de mais alta classificação que ele contenha.

**6.2.4.6** O responsável pela produção de documento classificado ou sob restrição de acesso deverá eliminar nota manuscrita, clichê, carbono, prova, cópia inservível ou qualquer outro elemento que possa dar origem a cópia não autorizada, do todo ou de parte do documento original.

**6.2.4.7** Em todo o documento classificado ou sob restrição de acesso, as páginas serão numeradas seguidamente, devendo cada uma conter, também, a indicação sobre o total de páginas que o compõe (Exemplos: 05/09, 02/17 e 01/34).

**6.2.4.8** Sempre que a produção de documento classificado ou sob restrição de acesso for efetuada em tipografia, oficina gráfica, copiadora ou em impressora, instalada em local diferente daquele da produção, deverá, esta operação, ser acompanhada por militar ou servidor devidamente credenciado, que será o responsável, durante esta fase, pela garantia do sigilo.

## **6.2.5 DA SEGURANÇA NA EXPEDIÇÃO E RECEPÇÃO**

**6.2.5.1** O documento classificado ou sob restrição de acesso poderá ser encaminhado fisicamente, obedecidas as seguintes prescrições:

- a) é permitida a remessa por intermédio dos correios, desde que registrado;
- b) é permitida a remessa por intermédio de mala diplomática; e
- c) pode ser empregado mensageiro, desde que credenciado.

**6.2.5.2** A expedição, a condução e a entrega de documento impresso com informação classificada em grau de sigilo ULTRASSECRETO será efetuada pessoalmente, por mensageiro credenciado, sendo vedada sua postagem.

**6.2.5.3** O mensageiro deverá ser instruído sobre como proceder quando pressentir qualquer tipo de ameaça ou incidente que possa resultar em comprometimento do sigilo do documento ou do material transportado.

**6.2.5.4** Na expedição do documento impresso classificado ou de acesso restrito deverão ser observadas as seguintes prescrições:

- a) o documento a ser expedido deverá ser acondicionado em envelope duplo;
- b) o envelope externo deverá conter apenas a função do destinatário e seu endereço, sem qualquer anotação que indique o grau de sigilo ou o motivo da restrição de acesso ao seu conteúdo;
- c) no envelope interno deverá ser inscrito o nome e a função do destinatário, o seu endereço e, claramente indicado, o grau de sigilo ou o motivo da restrição de acesso ao conteúdo do documento, de modo a ser visto logo que removido o envelope externo;
- d) o envelope interno deverá ser lacrado e o documento classificado ou sob restrição de acesso far-se-á acompanhado de um recibo; e
- e) o recibo destinado ao controle da expedição/recepção e da custódia do documento classificado ou sob restrição de acesso deverá conter, necessariamente, indicação sobre o remetente, o destinatário e o número ou outro indicativo que identifique o documento.

**6.2.5.5** O expediente que encaminha documento classificado ou sua cópia não será classificado, desde que não contenha frações significativas deste, sendo assim não será necessária a confecção de TCI para o mesmo.

**6.2.5.5.1** Como medida complementar de segurança para o trâmite e manuseio desse tipo de expediente, deverá constar, em vermelho, ou na impossibilidade, em negrito, no campo “assunto” um dos seguintes textos, “encaminhamento de DOCUMENTO CLASSIFICADO” ou “encaminhamento de DOCUMENTO SOB RESTRIÇÃO DE ACESSO”.

**6.2.5.5.2** Até o recebimento pelo destinatário, o expediente de encaminhamento deverá receber o tratamento e as medidas cautelares correspondentes ao grau de sigilo do anexo, sendo, inclusive, acondicionado no envelope interno junto com o anexo classificado e o TCI do anexo, ou o anexo sob restrição de acesso.

**6.2.5.6** O trâmite eletrônico destes documentos será conforme previsto no item 6.5.6 desta Instrução.

**6.2.5.7** Quando, inicialmente, for necessário que somente o destinatário tome conhecimento do assunto tratado, o envelope interno deverá conter, além do nome do destinatário, a inscrição "PESSOAL", precedendo a indicação da restrição ou classificação, quando houver.

**6.2.5.8** Para documento oficial, com número único de protocolo/ número único de documento (NUP/NUD), a situação de documento "PESSOAL" será temporária e somente define quem terá o primeiro acesso ao conteúdo desse documento.

**6.2.5.9** Providências adicionais poderão ser adotadas pelo Comandante, Chefe ou Diretor de OM, visando a aumentar a segurança na expedição de documento classificado ou sob restrição de acesso.

**6.2.5.10** A expedição de documento classificado ou sob restrição de acesso deverá ser registrada em protocolo sigiloso utilizado pela Organização Militar.

**6.2.5.11** O responsável pelo serviço de correio ou qualquer militar ou servidor, quando constatar que a correspondência recebida é um documento classificado ou sob restrição de acesso, deverá encaminhá-la ao setor que tiver sob seu encargo a atividade de Inteligência, para despacho da autoridade competente.

**6.2.5.12** Após despacho da autoridade competente, deverá ser confeccionado um registro onde ficarão anotados todos os dados identificadores da divisão/seção onde tramitou ou foi distribuído o documento classificado ou sob restrição de acesso e do militar ou do servidor que teve contato com a documentação.

**6.2.5.13** Além do efeito de protocolo, o registro indicará a tramitação e o responsável pela custódia do documento.

**6.2.5.14** Ao responsável pelo recebimento de documento classificado ou sob restrição de acesso incumbe:

- a) verificar e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na correspondência recebida, dando ciência do fato ao destinatário, o qual informará ao remetente; e
- b) proceder ao registro do documento e ao controle de sua tramitação, conforme previsto no item 6.2.5.12 desta Instrução.

**6.2.5.15** Recebido o documento impresso classificado ou sob restrição de acesso, o recibo anexado ao mesmo deverá ser assinado e datado pelo destinatário e devolvido ao remetente.

**6.2.5.16** A remessa do recibo não deve ser feita com características de sigilo.

**6.2.5.17** O destinatário de documento impresso classificado ou sob restrição de acesso deverá comunicar ao remetente qualquer indício de violação do documento, tal como rasuras, irregularidades de impressão ou de paginação.

## **6.2.6 DA SEGURANÇA NO MANUSEIO**

**6.2.6.1** O documento classificado ou sob restrição de acesso somente poderá ser manuseado por pessoa credenciada que tenha a necessidade de conhecer seu conteúdo e devidamente autorizada pelo Cmt, Ch ou Dir da OM.

**6.2.6.1.1** Para tal, deve-se correlacionar o grau de sigilo ou nível de restrição de acesso com a categoria da credencial de segurança de quem manuseará o documento classificado ou sob restrição de acesso.

**6.2.6.2** Todo o documento classificado ou sob restrição de acesso deverá ser manuseado pelo menor número possível de pessoas, a fim de tornar mais efetiva a sua segurança.

**6.2.6.3** Poderá ser elaborada cópia ou extrato de documento classificado ou sob restrição de acesso, mediante consentimento expresso:

- a) da autoridade classificadora, para documento no grau de sigilo ULTRASSECRETO;
- b) da autoridade classificadora ou autoridade hierarquicamente superior, para documento no grau de sigilo SECRETO e RESERVADO; e
- c) da autoridade destinatária, para documento sob restrição de acesso, exceto quando expressamente vedado no próprio documento.

**6.2.6.3.1** A cópia será autenticada pela autoridade que a autorizou.

**6.2.6.4** A confecção de cópia de documento classificado ou sob restrição de acesso deverá ser limitada ao estritamente necessário.

**6.2.6.4.1** À cópia ou ao extrato de documento classificado será atribuído grau de sigilo igual àquele atribuído ao documento que lhe deu origem.

**6.2.6.4.2** A cópia do documento classificado deverá conter cópia do respectivo TCI.

**6.2.6.5** A cópia ou o extrato de documento classificado ou sob restrição de acesso deverá receber um código numérico ou alfanumérico específico para cada destinatário, a fim de identificar a origem de um possível vazamento e facilitar o seu controle.

**6.2.6.5.1** O código citado acima deverá ser colocado no corpo do texto, em cada página de todo o documento, sendo visível e de fácil identificação em qualquer reprodução gráfica realizada, conforme modelo constante do anexo “E”.

**6.2.6.5.2** No documento original deverá constar a relação de todos os destinatários com os seus respectivos códigos.

**6.2.6.6** O responsável pela cópia de documento classificado ou sob restrição de acesso deverá destruir a cópia inservível ou qualquer outro elemento que possa dar origem à cópia não autorizada do todo ou de parte do documento original.

**6.2.6.7** Sempre que a cópia de documento classificado ou sob restrição de acesso for efetuada em copiadora ou em impressora, instalada em local diferente daquele onde foi produzido o documento original, deverá, esta operação, ser acompanhada pelo responsável por documento para, durante esta fase, garantir a manutenção do sigilo.

**6.2.6.8** À cópia ou ao extrato de documento classificado ou sob restrição de acesso será atribuída a classificação ou a situação de restrição de acesso igual àquela atribuída ao documento que lhe deu origem.

**6.2.6.8.1** Para tal, os seguintes procedimentos deverão ser adotados:

- a) a cópia deverá receber marcação adequada, em cor contrastante com o documento, preferencialmente em vermelho, conforme modelo constante do anexo “A”; e
- b) no corpo do documento que deu origem à cópia, deverá constar, de forma correlacionada, o número e o destinatário da mesma.

## **6.2.7 DA SEGURANÇA NO ARQUIVAMENTO**

**6.2.7.1** O documento classificado ou sob restrição de acesso deverá ser guardado em condições especiais de segurança.

**6.2.7.1.1** Para a guarda de documento no grau de sigilo ULTRASSECRETO é obrigatório, no mínimo, o uso de cofre com segredo de três combinações ou material que ofereça segurança equivalente ou superior.

**6.2.7.1.2** Na impossibilidade de se adotar o disposto no item 6.2.7.1.1 acima, o documento no grau de sigilo ULTRASSECRETO deverá ser mantido sob guarda armada.

**6.2.7.1.3** Para a guarda de documento no grau de sigilo SECRETO é obrigatória sua guarda em cofre e, se possível, a adoção de medidas de segurança idênticas àsquelas a que se referem os itens anteriores.

**6.2.7.1.4** Para a guarda de documento no grau de sigilo RESERVADO ou sob outra restrição de acesso, que não as dos itens 6.2.7.1.1 e 6.2.7.1.3, é obrigatório, no mínimo, o uso de arquivo com chave.

**6.2.7.1.5** Não deverá estar guardado no mesmo cofre ou arquivo o texto em claro e o seu correspondente criptografado.

**6.2.7.2** É importante, também, que se estabeleçam procedimentos relativos à evacuação da documentação classificada ou sob restrição de acesso em situações de emergência, em conformidade com o previsto no FCA 200-6/2013.

**6.2.7.2.1** Esta medida requer o estabelecimento de prioridades, de responsabilidades e a determinação antecipada de local alternativo para abrigar os documentos a serem salvos.

## **6.2.8 DA SEGURANÇA NA ELIMINAÇÃO**

**6.2.8.1** O original do documento classificado deverá ser mantido em arquivo e submetido, dentro do período previsto, à apreciação da respectiva Comissão/Subcomissão Permanente de Avaliação de Documentos Sigilosos (CPADS/SPADS), de acordo com a Instrução que dispõe sobre a avaliação de documentos classificados no Comando da Aeronáutica.

**6.2.8.2** O original da informação com grau de sigilo ULTRASSECRETO ou SECRETO, mesmo após desclassificado, é de guarda permanente, devendo ser preservado de acordo com o art. 39 do Decreto nº 7.724/2012.

**6.2.8.2.1** A cópia de documento com grau de sigilo ULTRASSECRETO ou SECRETO, após desclassificado, destituída de valor para fins de arquivo e/ou consulta, poderá ser eliminada tão logo se torne inservível, seguindo-se o que prescreve a Instrução que dispõe sobre a avaliação de documentos classificados no Comando da Aeronáutica.

**6.2.8.3** O original e a cópia de documento com grau de sigilo RESERVADO, após desclassificado ou destituída de valor para fins de arquivo ou consulta, poderá ser eliminada tão logo se torne inservível, seguindo-se o que prescreve a Instrução que dispõe sobre a avaliação de documentos classificados no Comando da Aeronáutica.

**6.2.8.4** Para a eliminação de cópia de DC deverá ser seguido o que prescreve a Instrução que dispõe sobre a avaliação de documentos classificados no Comando da Aeronáutica e observados os seguintes procedimentos:

- a) a autoridade que classificou o original deverá determinar o recolhimento da(s) cópia(s) que será(ão) eliminada(s);
- b) após certificar-se de que o original foi mantido em arquivo, deverá ser lavrado o respectivo termo de eliminação de cópia de documento controlado, conforme modelo constante do anexo “B”, assinado pela autoridade que classificou o original e por duas testemunhas;
- c) o termo citado no inciso anterior deverá ser publicado em Boletim Interno; e
- d) deverão ser lançados, no verso da primeira folha do DC original, o número e data do boletim que publicou o termo de eliminação de sua(s) respectiva(s) cópia(s).

**6.2.8.5** No caso de impossibilidade de recolhimento do DC/MC, nos termos da alínea (a) do item 6.2.8.4, a cópia inservível de DC deve ser eliminada pela autoridade que mantém a custódia.

**6.2.8.5.1** Para tanto, a autoridade custodiante e a autoridade controladora devem adotar os seguintes procedimentos:

- a) Autoridade Controladora:
  - informar à OM que mantém a custódia do DC para que proceda à eliminação e à publicação em Boletim Interno do termo de eliminação, conforme modelo constante do anexo “B”;
  - solicitar a remessa à autoridade controladora de cópia do termo de eliminação e da folha do Boletim que publicou o ato;
  - manter o original do DC arquivado; e
  - manter o controle da eliminação de cópias e de seus respectivos termos, arquivando os termos de eliminação, juntamente com o DC original.
- b) Autoridade que mantém a custódia de DC:
  - eliminar o DC de acordo com as orientações da autoridade controladora;
  - confeccionar o termo de eliminação e publicá-lo em Boletim Interno; e
  - remeter cópia do termo de eliminação e da cópia da folha de Boletim que publicou a eliminação à autoridade controladora.



### **6.3 DA SEGURANÇA DO MATERIAL**

**6.3.1** Deverão ser adotadas, com relação à segurança do material classificado ou sob restrição de acesso, as mesmas prescrições previstas para segurança da documentação, no que for aplicável.

**6.3.2** O Comandante, Chefe ou Diretor, particularmente de órgão técnico ou estabelecimento de ensino, responsável por programa de pesquisa ou por projeto para o qual julgar conveniente manter sigilo sobre determinado material ou suas partes, deverá providenciar para que a ele seja atribuída a restrição de acesso correspondente.

**6.3.2.1** Aplica-se o disposto neste artigo ao Chefe ou Diretor de órgão encarregado da fiscalização e do controle de atividades de empresa vinculada ou privada, para fins de produção e/ou exportação de material de interesse da Defesa Nacional.

**6.3.3** A empresa vinculada ou privada, que desenvolva pesquisa ou projeto de interesse nacional, o qual contenha material sob restrição de acesso, que se enquadre em um dos incisos do art. 23 da Lei nº 12.527/2011, deverá providenciar a sua classificação, mediante entendimento com o órgão a que estiver ligado, para efeito daquela pesquisa ou projeto.

**6.3.4** O Comandante, Chefe, Diretor ou titular de órgão técnico, estabelecimento de ensino ou de empresa vinculada, encarregada da preparação de plano, pesquisa, trabalho de aperfeiçoamento, projeto de P&D, prova, produção, aquisição, armazenagem ou emprego de material classificado ou sob restrição de acesso, é responsável pela expedição das instruções adicionais que se tornarem necessárias à salvaguarda das informações com ele relacionado.

**6.3.5** A informação classificada ou sob restrição de acesso concernente a programa técnico ou aperfeiçoamento de material só deverá ser fornecida ao militar, servidor, pesquisador ou empresa que, por sua função oficial ou contratual, a ela deva ter acesso.

**6.3.5.1** Em nenhuma hipótese, a informação classificada ou sob restrição de acesso será controlada ou coordenada por pessoa jurídica de direito privado.

**6.3.5.2** O órgão responsável pelo desenvolvimento de pesquisa ou projeto de interesse nacional deverá controlar e coordenar o fornecimento de informação classificada ou sob restrição de acesso à pessoa física ou jurídica envolvida nesse evento.

**6.3.6** Em demonstração, exposição ou exibição pública, cabe ao Comandante, Chefe ou Diretor de OM, por ela responsável, tomar as medidas necessárias de segurança relativa ao contato de pessoas não integrantes da instituição com o material exposto que esteja sob restrição de acesso, bem como com relação a divulgação das características técnicas.

**6.3.7** Pedido para fotografar material classificado ou sob restrição de acesso ou gravar imagem de trabalho ou processo de fabricação, conduzido por empresa civil e considerado sigiloso, deverá ser encaminhado ao órgão responsável pelo desenvolvimento da pesquisa ou projeto, por intermédio do chefe do segmento técnico responsável.

**6.3.7.1** A autorização deverá ser concedida mediante a garantia de que a fotografia ou a imagem só poderá ser utilizada para os fins especificados na solicitação, depois de analisada por aquele órgão.

**6.3.8** No âmbito do COMAER, o pedido para fotografar ou gravar imagem de material classificado ou sob restrição de acesso poderá ser autorizado pelo Comandante, Chefe ou Diretor da OM responsável pela custódia.

**6.3.8.1** Tal fotografia somente poderá ser utilizada depois de analisada por aquele Comando, Chefia ou Direção.

### **6.3.9 DA SEGURANÇA NO TRANSPORTE**

**6.3.9.1** A definição do meio de transporte e do nível de segurança a ser utilizado para deslocamento de material classificado ou sob restrição de acesso é de responsabilidade do detentor da sua custódia, que deverá considerar o grau de sigilo atribuído ao respectivo material, se este for classificado, a extensão do percurso e o grau de risco do itinerário a ser percorrido.

**6.3.9.1.1** O material classificado ou sob restrição de acesso poderá ser transportado por empresa para tal fim contratada, que deverá providenciar as medidas necessárias para a segurança do material, estabelecidas em entendimento prévio, as quais deverão estar contidas em cláusulas específicas do contrato.

**6.3.9.2** Se a distância de transporte, o seu tamanho e a sua quantidade permitirem, o material classificado ou sob restrição de acesso deverá ser entregue pessoalmente ao destinatário, por pessoa credenciada, mediante assinatura de recibo.

**6.3.9.3** A critério da autoridade competente, poderão ser empregados guardas armados, civis ou militares, no transporte de material classificado ou sob restrição de acesso.

### **6.3.10 DA SEGURANÇA NA ELIMINAÇÃO DE MATERIAL CONTROLADO**

**6.3.10.1** Para a eliminação de Material Controlado (MC) deverão ser obedecidas as seguintes prescrições:

- a) somente o órgão controlador poderá autorizar a eliminação;
- b) deverá ser lavrado o respectivo Termo de Eliminação de Material Controlado, conforme modelo constante do anexo “F”, assinado pelo detentor e por duas testemunhas;
- c) o termo de eliminação citado na alínea anterior, deverá ser publicado no boletim interno da OM custodiante;
- d) após a eliminação, a autoridade que mantém a custódia deverá encaminhar cópia do termo de eliminação e cópia da(s) folha(s) do Boletim Interno, que publicou tal eliminação ao órgão controlador que deverá transcrever essa publicação em seu Boletim; e
- e) o método utilizado para a destruição deverá assegurar a desintegração do MC.

**6.3.10.1.1** Para os demais materiais e produtos deverão ser obedecidas as normas de controle dos respectivos órgãos gestores.

## **6.4 DA SEGURANÇA DAS ÁREAS E INSTALAÇÕES**

**6.4.1** Caberá ao Comandante, Chefe ou Diretor a definição, a demarcação, a sinalização, a segurança e a concessão de acesso à área restrita, no âmbito de sua OM (seção, divisão, etc).

**6.4.1.1** Para tanto, deverá ser elaborada norma de controle de acesso às áreas restritas, com a finalidade de normatizar procedimentos.

**6.4.1.2** As áreas de Inteligência, Tecnologia da Informação, Jurídica, Cibernética, Comunicações, Ciência e Tecnologia, Guerra Eletrônica, Operações Aéreas, Controle de Tráfego Aéreo e as consideradas vitais para o pleno funcionamento da OM, tais como reserva de armamento, paiol, caixa d'água, central elétrica, dentre outras, deverão ser consideradas de acesso restrito.

**6.4.1.3** A norma de controle de acesso, citada no 6.4.1.1, deverá contemplar a proibição da entrada de pessoas conduzindo máquina fotográfica, filmadora, celular, gravador ou qualquer meio de captura ou transmissão de imagens e sons, em área e instalação que seja armazenado documento ou material classificado ou sob restrição de acesso, sem a autorização expressa do Comandante, Chefe ou Diretor.

**6.4.1.4** A norma de controle de acesso, citada no 6.4.1.1, deverá atender ao que prevê a ICA 205-22/2015 e o FCA 200-6/2013.

**6.4.1.5** Não é considerado visitante o ingresso de agente público ou o particular que, oficialmente, execute atividade pública diretamente vinculada à elaboração de estudo ou trabalho considerado sigiloso.

**6.4.2** A área ou instalação de acesso restrito deverá ser indicada, por intermédio de placa(s) afixada(s) na(s) parede(s) externa(s), de forma destacada, preferencialmente na cor vermelha, principalmente junto à(s) entrada(s), conforme modelo constante do anexo "A".

**6.4.2.1** Tal marcação tem por finalidade precípua apresentar-se como um primeiro elemento dissuasor ao comprometimento ou à quebra de segurança.

**6.4.3** As instalações das OM, particularmente as de Informática, de Cibernética, de Guerra Eletrônica, de Comunicações, de Operações Aéreas e de Controle de Tráfego Aéreo, deverão utilizar rede elétrica dimensionada ao número de equipamentos a ela ligados, visando à sua proteção contra sobrecargas.

**6.4.3.1** Igual procedimento deverá ser adotado quanto a pára-raios e aterramento adequado, visando à proteção contra descargas atmosféricas.

## **6.5 DA SEGURANÇA NOS MEIOS DE TECNOLOGIA DA INFORMAÇÃO**

**6.5.1** Somente deverá ser adotado o serviço de correio eletrônico oferecido por órgão ou entidade da administração pública federal.

**6.5.2** O programa ou equipamento destinado à atividade de que trata o item 6.5.1 deverá ter características que permitam a auditoria para fins de garantia da disponibilidade, da integridade, da confidencialidade e da autenticidade das informações.

**6.5.3** O armazenamento e a recuperação de dados a que se refere o caput deverá ser realizada em centro de processamento de dados fornecido por órgão ou entidade da administração pública federal.

**6.5.4** A segurança relacionada com a remessa ou transmissão de informação classificada ou sob restrição de acesso é de responsabilidade de todo aquele que a manusear para tal fim.

**6.5.5** As medidas de segurança deverão ser tomadas de acordo com as restrições de acesso necessárias e o meio de remessa ou transmissão utilizado.

**6.5.6** A transmissão de informação classificada poderá ser realizada por meio eletrônico, desde que obrigatoriamente criptografado, em sistema de cifra de alta confiabilidade, com algoritmo de Estado, homologado pelo CIAER, dentro da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra de segurança.

**6.5.7** A informação sob restrição de acesso que trate de assunto de inteligência, de emprego ou de suporte logístico de operações de garantia da lei e da ordem, de transporte de munição e de armamento deverá seguir o mesmo tratamento dispensado à transmissão de informação classificada descrito neste documento.

**6.5.8** Na escolha do meio de transmissão eletrônica a ser utilizado, deverão ser priorizados os meios integrantes das diversas redes do COMAER.

**6.5.9** É proibido o uso de ligação telefônica e de fax para o trato de informação classificada ou sob restrição de acesso, sem a devida proteção criptográfica, devido à extrema vulnerabilidade desse meio de comunicação.

**6.5.10** No tratamento da informação classificada deverão ser utilizados sistemas de informação e canais seguros que atendam aos padrões mínimos de qualidade e segurança definidos pela legislação federal e homologados pelo CIAER.

**6.5.11** Quaisquer procedimentos relativos à segurança da transmissão deverão estar de acordo com os preceitos da legislação específica que trata da segurança da informação classificada ou sob restrição de acesso.

**6.5.12** Todo documento criptografado recebido deverá ser tratado como estando sob restrição de acesso.

**6.5.13** É proibida a utilização de qualquer sistema de cifra e código ou material criptográfico, em uso no COMAER, para o preparo de mensagem que não trate de assunto de serviço.

**6.5.14** As tecnologias empregadas na segurança dos sistemas de informação, em uso no COMAER, deverão ser consideradas sob restrição de acesso.

**6.5.15** A necessária manutenção em equipamento informatizado deverá ser, preferencialmente, executada pelo pessoal da própria OM especializado em informática.

**6.5.16** Qualquer serviço a ser executado por empresa contratada em equipamento informatizado, que contenha assunto classificadado ou sob restrição de acesso, deverá ser acompanhado pelo responsável por sua utilização.

**6.5.17** O computador que contenha informação classificada ou sob restrição de acesso e que necessite de manutenção fora da OM deverá ter o seu disco rígido retirado e guardado em um cofre.

**6.5.18** Deverá ser utilizado apenas o “software” licenciado de acordo com a legislação em vigor ou de domínio público, após parecer favorável e assessoramento técnico de pessoal especializado da divisão ou seção de tecnologia da informação da OM.

**6.5.19** A instalação de “software” somente deverá ser realizada por pessoal habilitado do setor de tecnologia da informação existente na OM.

**6.5.20** Deverá ser instalado e atualizado, periodicamente, um sistema antivírus, com o objetivo de se evitar a disseminação de vírus nas redes de informática.

**6.5.21** Todo arquivo digital que contenha informação classificada deverá possuir cópia de segurança.

**6.5.22** A cópia de segurança de arquivo digital, contendo informação classificada, bem como o original de programa em uso, deverá estar armazenada em cofre localizado fora do setor de informática.

**6.5.23** O setor de tecnologia da informação deverá utilizar, sempre que possível, gerador ou outro equipamento que garanta a continuidade no fornecimento de energia elétrica aos equipamentos de informática.

**6.5.24** Os portais das OM, dos militares da ativa, da reserva ou dos servidores civis, bem como os computadores que estiverem conectados à Rede Mundial de Computadores ou a outras redes com acesso remoto, não deverão conter informação classificada ou sob restrição de acesso.

**6.5.25** Para fins desta Instrução, serão considerados como informações da OM sob restrição de acesso, as abaixo especificadas:

- a) vista aérea;
- b) fotografias internas de pontos importantes (paiol, reserva de armamento, etc);
- c) peculiaridades do seu emprego;
- d) características técnicas do material de emprego militar;
- e) informações pessoais dos seus integrantes; e
- f) informações contidas nos quadros de organização ou de material, dentre outras.

**6.5.26** A mensagem eletrônica de procedência desconhecida não deverá ser aberta, utilizando-se computador ligado à rede de informática da OM, principalmente a que contenha arquivo anexado.

**6.5.27** A certificação digital deverá ser utilizada com o objetivo de permitir a autenticação e o não repúdio da mensagem remetida via correio eletrônico.

**6.5.28** Deverá ser estabelecida senha para acesso, individual e intransferível, para cada usuário, aos sistemas e ambientes de rede, a qual deverá ser trocada, frequentemente, para dificultar o acesso por pessoa não autorizada.

**6.5.29** O controle de acesso lógico deverá restringir o acesso, em diferentes níveis, de acordo com a necessidade de conhecer de cada usuário do sistema.

**6.5.30** A operação de inclusão, pesquisa, alteração e exclusão de dados nos sistemas corporativos deverá ser realizada por pessoa devidamente credenciada a acessar os diferentes níveis de administração do sistema.

**6.5.31** Toda a rede da OM, conectada ou não à Rede Mundial de Computadores, deverá possuir ferramenta ou sistema capaz de rastrear e identificar a origem e o responsável pelo acesso à rede e de dificultar o acesso à pessoa não credenciada.

**6.5.32** Toda a rede da OM, conectada ou não à Rede Mundial de Computadores, deverá possuir ferramenta/sistema específico, sempre atualizado, capaz de rastrear e emitir relatório sobre pontos vulneráveis que poderão ser utilizados como porta de entrada para invasão nos sistemas dessa rede.

**6.5.33** 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, homologados pelo CIAER.

**6.5.34** Para um controle mais eficaz, tal computador não deverá ter a placa de fax-modem e deverá ter desabilitado ou bloqueado o recurso de conexão remota (sem fio).

**6.5.35** A pasta “PÚBLICO” ou similar, normalmente disponível em redes das Organizações Militares, não deverá ser utilizada para armazenamento de arquivo que contenha informação classificada ou sob restrição de acesso.

**6.5.36** Caso seja necessário o uso de “dispositivo de armazenamento portátil (pendrive, cartão de memória, etc)” em máquina utilizada por sistema corporativo, intranet e rede local, esse dispositivo de memória deverá ser do tipo institucional, padronizado em cor e tamanho, identificado e etiquetado com orientações sobre seu uso, o que diminui significativamente o risco de comprometimento ou de propagação de vírus.

**6.5.37** É vedado o uso de dispositivo de armazenamento móvel particular para o trato de informação classificada ou de serviço.

**6.5.38** Não deverá ser utilizado computador pessoal para o trato de informação classificada ou sob restrição de acesso de cunho funcional, considerando:

- a) que o arquivo apagado do seu disco rígido poderá ser recuperado por pessoa não autorizada, com a utilização de programa específico; e
- b) que a segurança do equipamento é relativa, levando-se em conta a possibilidade de ocorrência de imprevisto por ocasião do seu transporte.

**6.5.39** Antes de ausentar-se do seu local de trabalho, mesmo que de forma breve, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso à informação classificada ou sob restrição de acesso por pessoa não autorizada.

**6.5.40** Cuidados especiais deverão ser adotados por ocasião da realização de instrução ou palestra, fora do ambiente normal de trabalho, que trate de informação classificada ou sob restrição de acesso.

**6.5.41** Sempre que possível, deverá ser evitada a utilização do disco rígido para armazenar o conteúdo da palestra ou instrução, pois mesmo após deletado o arquivo que a contém, esta poderá ser recuperada por pessoa não autorizada, por meio da utilização de programa específico.

**6.5.42** A autorização para a confecção de cópia da palestra ou instrução, em pendrive, CD/DVD ou outro meio de armazenamento é da exclusiva responsabilidade de quem a ministrou ou a proferiu.

**6.5.43** Após a remessa ou transmissão de documento eletrônico que contenha informação classificada ou sob restrição de acesso deverá ser confeccionada uma cópia em dispositivo de armazenamento portátil, devendo esta cópia ser guardada em local seguro.

**6.5.44** Quando for inevitável o transporte de informação classificada ou sob restrição de acesso, este procedimento deverá ser realizado em equipamento portátil (notebook, tablet, disco rígido externo, etc) fornecido pela OM, sendo que para tal transporte deverá ser utilizado programa que crie um contêiner seguro criptografado.

**6.5.45** A segurança da informação é responsabilidade de todos, mas por envolver alguns aspectos técnicos, é encargo do setor de contrainteligência, que, com o auxílio dos demais setores, deverá:

- a) elaborar o Plano de Segurança da OM, mantendo-o atualizado;
- b) realizar, frequentemente, auditorias a fim de levantar vulnerabilidades nas redes instaladas, acessos indevidos, tentativas de acesso, dentre outros aspectos julgados pertinentes; e
- c) aplicar, periodicamente, a lista de verificação de segurança orgânica, divulgando seus resultados por intermédio de um relatório, o qual deverá ser apresentado ao Cmt, Ch ou Dir e publicado em boletim interno, para a melhoria do nível de segurança da OM.

**6.5.46** Aplicam-se aos equipamentos e materiais criptográficos e aos sistemas de cifras e códigos todas as medidas de segurança previstas para o tratamento de informação classificada e, ainda, os seguintes procedimentos:

- a) a realização de vistorias periódicas em todos os materiais criptográficos, com a finalidade de assegurar uma perfeita execução das operações criptográficas;
- b) a manutenção de inventários completos e atualizados dos equipamentos e material criptográfico existente; e
- c) a comunicação aos Comandantes, Chefes ou Diretores de qualquer anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à

autenticidade, à legitimidade e à disponibilidade da informação criptografada.



## **7 DA CELEBRAÇÃO DE CONTRATOS**

**7.1** A entidade privada com expectativa de assinatura de contrato sigiloso deverá ser habilitada para tratar informação classificada ou sob restrição de acesso, conforme a norma de concessão de credenciamento vigente.

**7.2** A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo conteúdo seja classificado ou esteja sob restrição de acesso, é condicionada à assinatura de Termo de Compromisso de Manutenção do Sigilo (TCMS) e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:

- a) o conhecimento do aviso do edital se houver, e/ou do edital propriamente dito, só deverá ser permitido após a assinatura do Termo citado neste artigo;
- b) obrigação de manter o sigilo relativo ao objeto e sua execução;
- c) possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;
- d) obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;
- e) identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso à informação classificada e ao material de acesso restrito;
- f) obrigação de receber inspeções para habilitação de segurança e sua manutenção; e
- g) responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.

**7.3** Ao órgão contratante ou que celebre convênio caberá providenciar para que o seu representante ou fiscal adote as medidas necessárias, de acordo com as prescrições contidas nesta Instrução, para a segurança do documento e/ou material ou sob restrição de acesso, em poder do seu contratado, subcontratado, conveniado, subconveniado ou em curso de fabricação em suas instalações.

**7.4** Os ajustes, acordos, protocolos de intenções e outros instrumentos congêneres, deverão seguir as prescrições previstas para a celebração de contratos e convênios, no que for aplicável.

## **8 DAS DISPOSIÇÕES FINAIS**

**8.1** A segurança da informação classificada ou sob restrição de acesso é responsabilidade do militar que tenha acesso a estas informações, estando sujeito às regras referentes ao sigilo profissional, em razão do ofício, da legislação vigente e do Estatuto dos Militares.

**8.2** A segurança da informação classificada ou sob restrição de acesso é responsabilidade do servidor civil que tenha acesso a estas informações, no âmbito do COMAER, estando sujeito às regras referentes ao sigilo profissional, em razão do ofício, da legislação vigente e do Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

**8.3** Fica resguardado o direito de indenização pelo dano material ou moral decorrente da violação do sigilo, sem prejuízo das ações penal, civil e administrativa.

**8.4** Constituem condutas ilícitas que ensejam responsabilidade civil, administrativa e/ou penal do militar ou civil, as previstas no art. 32 da Lei nº 12.527/2011.

## REFERÊNCIAS

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, DF, 2013.

\_\_\_\_\_. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Avaliação de Documentos Classificados no Comando da Aeronáutica: ICA 200-12. Brasília, DF, 2013.

\_\_\_\_\_. Comando da Aeronáutica. Diretoria de Administração do Pessoal. Padronização de Processos Administrativos: ICA 35-1. Rio de Janeiro, RJ, 2013.

\_\_\_\_\_. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Visitas às Organizações Militares do Comando da Aeronáutica: ICA 205-22. Brasília, DF, 2015.

\_\_\_\_\_. Comando da Aeronáutica. Portaria Normativa nº 45/GC3, de 15 JAN 14. Delega competência aos ocupantes de cargos que menciona para fins de classificação de documentos sigilosos. Diário Oficial da República Federativa do Brasil. Brasília, DF, 16 JAN 2014.

\_\_\_\_\_. Controladoria-Geral da União. Acesso à Informação Pública: uma introdução à Lei nº 12.527, de 18 de novembro de 2011. Brasília, 2011.

\_\_\_\_\_. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR nº 2, de 5 FEV 13. Dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

\_\_\_\_\_. Ministério da Defesa. Portaria Normativa nº 524-MD, de 2 MAR 12. Estabelece diretrizes gerais para a implantação do Serviço de Informações ao Cidadão (SIC) e constitui Grupo de Trabalho (GT), no âmbito do Ministério da Defesa - MD, com a finalidade de elaborar e articular estratégias, planos e metas para a implementação da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, 5 MAR 12.

\_\_\_\_\_. Ministério da Defesa. Portaria Normativa nº 1.234-MD, de 11 MAIO 12. Estabelece procedimentos para a concessão de audiências a particulares no âmbito do Ministério da Defesa e disponibilização de agenda de autoridades que menciona. Diário Oficial da República Federativa do Brasil. Brasília, 14 MAIO 2012.

\_\_\_\_\_. Ministério da Defesa. Portaria Normativa nº 1.235/MD, de 11 MAIO 12. Estabelece normas para o funcionamento e a tramitação de demandas do Sistema de Informações ao Cidadão no âmbito da administração central do Ministério da Defesa (SIC-MD), nos termos da lei nº 12.527, de 18 de novembro de 2011. Diário Oficial da República Federativa do Brasil. Brasília, 14 MAIO 2012.

\_\_\_\_\_. Ministério da Defesa. Portaria Normativa nº 2.229/MD, de 23 AGO 12. Altera a Portaria Normativa nº 1.235/MD, de 11 de maio de 2012. Diário Oficial da República Federativa do Brasil. Brasília, 24 AGO 2012.

\_\_\_\_\_. Ministério da Defesa. Portaria Normativa nº 1.813-MD, de 13 JUN 13. Altera a Portaria Normativa nº 1.235/MD, de 11 de maio de 2012. Diário Oficial da República Federativa do Brasil. Brasília, 14 JUN 2013.

\_\_\_\_\_. Ministério da Defesa. Portaria Normativa nº 2.975-MD, de 24 OUT 13. Disciplina no âmbito do Ministério da Defesa, os procedimentos de lavratura do Termo de Classificação de Informação (TCI), de classificação, desclassificação, reclassificação ou reavaliação da informação, de remessa de TCI à Comissão Mista de Reavaliação de Informações (CMRI), de elaboração e atualização das listas das informações classificadas e desclassificadas, e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, 2013.

\_\_\_\_\_. Ministério da Justiça. Conselho Nacional de Arquivos. Resolução nº 7 do CONARQ, de 20 MAIO 1997. Dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Poder Público. Diário Oficial da República Federativa do Brasil. Brasília, 23 MAIO 2007.

\_\_\_\_\_. Ministério da Justiça. Resolução nº 14 do CONARQ, de 20 OUT 01. Aprova a versão revisada e ampliada da Resolução nº 4, de 28 MAR 1996, que dispõe sobre o Código de Classificação de Documentos de Arquivos para a Administração Pública: Atividades-Meio, a ser adotado como modelo para os arquivos correntes dos órgãos e entidades do Sistema Nacional de Arquivos (SINAR), e os prazos de guarda e a destinação de documentos estabelecidos na Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo Relativo às Atividades-Meio da Administração Pública. Diário Oficial da República Federativa do Brasil. Brasília, 8 FEV 02.

\_\_\_\_\_. Ministério da Justiça. Resolução nº 21 do CONARQ, de 4 AGO 04. Dispõe sobre o uso da subclasse 080 - Pessoal Militar do Código de Classificação de Documentos de Arquivo para a Administração Pública: Atividades-Meio e da Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo Relativos às Atividades-Meio da Administração Pública aprovados pela Resolução nº 14, de 24 OUT 2001, do conselho Nacional de Arquivos - CONARQ. Diário Oficial da República Federativa do Brasil. Brasília, 9 AGO 04.

\_\_\_\_\_. Ministério do Planejamento Orçamento e Gestão. Portaria Interministerial nº 140, de 16 MAR 06. Disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores - internet, e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, 2006.

\_\_\_\_\_. Presidência da República. Lei nº 7.115, de 29 de agosto de 1983. Dispõe sobre prova documental nos casos que indica e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, 30 AGO 1983.

\_\_\_\_\_. Presidência da República. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, 9 JAN 1991.

\_\_\_\_\_. Presidência da República. Lei nº 10.048, de 8 de novembro de 2000. Dá prioridade de atendimento às pessoas que especifica, e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, 9 NOV 1991.

\_\_\_\_\_. Presidência da República. Lei nº 10.180, de 6 de fevereiro de 2001. Organiza e disciplina os Sistemas de Planejamento e de Orçamento Federal, de Administração Financeira

Federal, de Contabilidade Federal e de Controle Interno do Poder Executivo Federal e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, 7 FEV 2001.

\_\_\_\_\_. Presidência da República. 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 República Federativa do Brasil. Brasília, 18 NOV 2011. Edição extra.

\_\_\_\_\_. Presidência da República. Decreto nº 4.073, de 3 de janeiro de 2002. Regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados. Diário Oficial da República Federativa do Brasil. Brasília, 4 JAN 2002.

\_\_\_\_\_. Presidência da República. Decreto nº 5.482, de 30 de junho de 2005. Dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores - Internet. Diário Oficial da República Federativa do Brasil. Brasília, 1º JUL 2005.

\_\_\_\_\_. Presidência da República. Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre 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. Diário Oficial da República Federativa do Brasil. Brasília, 16 MAIO 2012.

\_\_\_\_\_. Presidência da República. Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e o tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Diário Oficial da República Federativa do Brasil. Brasília, 16 NOV 2012.

**Anexo A - Modelos de Marcação para Informações, Materiais e Áreas Sigilosas**

a. Documentos Classificados:

**ULTRASSECRETO****SECRETO****RESERVADO**

b. Documento Preparatório - Acesso Restrito:

**DOCUMENTO PREPARATÓRIO - ACESSO RESTRITO**  
**Art. 3º, Inciso XII e Art. 20 do Decreto nº 7.724, de 16 de maio de 2012**

c. Informação Pessoal - Acesso Restrito:

**INFORMAÇÃO PESSOAL - ACESSO RESTRITO**  
**Art. 5º, Inciso X, da Constituição Federal do Brasil/1988**  
**Art. 31 da Lei nº 12.527, de 18 de novembro de 2011**  
**Art. 55 ao Art. 62 do Decreto nº 7.724, de 16 de maio de 2012**

d. Informação de Pesquisa e Desenvolvimento – Acesso Restrito:

**INFORMAÇÃO DE PESQUISA E DESENVOLVIMENTO - ACESSO RESTRITO**  
**§1º do Art. 7º da Lei nº 12.527, de 18 de novembro de 2011**  
**Inciso II do Art. 6º do Decreto nº 7.724, de 16 de maio de 2012**

e. Material de Acesso Restrito – Nível 1, 2 ou 3:

**MATERIAL DE ACESSO RESTRITO**  
**Art. 44, 45 e 46 do Decreto nº 7.845, de 14 de novembro de 2012**  
**NÍVEL 1**

f. Área de Acesso Restrito:

(Nome da OM)

**ÁREA DE ACESSO RESTRITO**  
**Entrada proibida a pessoas não autorizadas**  
**Art. 42 do Decreto nº 7.845, de 14 de novembro de 2012**

g. Cópia Extra:

**Cópia Extra Nº**  
\_\_\_\_\_

## Anexo B - Modelo de Termo de Eliminação de Cópia(s) de Documento Controlado

**MATERIAL DE ACESSO RESTRITO**  
**Art. 44, 45 e 46 do Decreto nº 7.845, de 14 de novembro de 2012**  
**NÍVEL 1**



**MINISTÉRIO DA DEFESA**  
**COMANDO DA AERONÁUTICA**  
**(CONTINUAÇÃO DO CABEÇALHO DA OM)**

**TERMO DE ELIMINAÇÃO DE CÓPIA(S) DE DOCUMENTO CONTROLADO**

Nº \_\_\_\_/\_\_\_\_

Ao(s) \_\_\_\_ dia(s) do mês de \_\_\_\_\_ do ano de dois mil e \_\_\_\_, em cumprimento ao disposto no item 6.2.8.4 das Instruções para Salvaguarda de Assuntos Sigilosos (ICA 205-47), reuniram-se na(o) \_\_\_\_\_ **(OM DETENDORA)** o Sr.

**(NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA AUTORIDADE QUE CLASSIFICOU O ORIGINAL)**, o Sr.

**(NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DE UMA DAS TESTEMUNHAS)**, e o Sr.

**(NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA OUTRA TESTEMUNHA)**, os os dois

últimos como testemunhas, para proceder à eliminação da(s) cópia(s) do(s) Documento(s) Controlado(s) (DC), pelo(a) \_\_\_\_\_ **(ÓRGÃO CONTROLADOR)**.

Cumpridas as formalidades exigidas e conferidas todas as peças constantes do termo de eliminação, foi(ram) eliminada(s) a(s) cópia(s) do DC abaixo discriminado(s):

Título Convencional	Nº do Exemplar

E, para constar, foi lavrado o presente Termo de Eliminação, que se acha digitado, assinado pela autoridade que classificou o original, datado e assinado pelas testemunhas, todas acima qualificadas.

AUTORIDADE QUE CLASSIFICOU O ORIGINAL:

**(ou AUTORIDADE QUE MANTÉM A CUSTÓDIA):**

\_\_\_\_\_, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_  
**(LOCAL E DATA)**

Testemunhas:

\_\_\_\_\_  
**(Nome completo, Posto, Identidade e Função do Detentor)**

\_\_\_\_\_  
**(Nome completo, Posto, Identidade e Função)**

\_\_\_\_\_  
**(Nome completo, Posto, Identidade e Função)**

**MATERIAL DE ACESSO RESTRITO**  
**Art. 44, 45 e 46 do Decreto nº 7.845, de 14 de novembro de 2012**  
**NÍVEL 1**

## Anexo C - Modelo de Termo de Compromisso de Manutenção do Sigiloso



MINISTÉRIO DA DEFESA

COMANDO DA AERONÁUTICA  
(CONTINUAÇÃO DO CABEÇALHO DA OM)**TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILOSO**

Eu, \_\_\_\_\_, **(NOME COMPLETO)**, BRASILEIRO CPF nº **(Nº, DATA E LOCAL DE EXPEDIÇÃO DO CPF)** FILIAÇÃO e ENDEREÇO, **(PRESTADOR DE SERVIÇO NA - CITAR EMPRESA) (MILITAR SERVINDO NO - CITAR OM)** perante ao **(CITAR O ÓRGÃO)**, declaro ter ciência inequívoca da legislação sobre o tratamento de informação classificada ou sob restrição de acesso cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, e me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011 e a:

- a) tratar as informações ou materiais classificados ou sob restrição de acesso que me forem fornecidos pelo \_\_\_\_\_ e preservar o seu sigilo, de acordo com a legislação vigente;
- b) preservar o conteúdo das informações ou materiais classificados ou sob restrição de acesso, sem divulgá-los a terceiros;
- c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações ou materiais classificados ou sob restrição de acesso, ou dos materiais; e
- d) não copiar ou reproduzir, por qualquer meio ou modo:
  - (1) informações classificadas ou sob restrição de acesso;
  - (2) informações relativas aos materiais de acesso restrito do \_\_\_\_\_, salvo autorização da autoridade competente.

Declaro que **(recebi) (tive acesso)** ao (à) **(documento ou material entregue ou exibido ao signatário)**, e por estar de acordo com o presente Termo, assino na presença das testemunhas abaixo identificadas.

\_\_\_\_\_, \_\_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_  
**(Local e Data)**

\_\_\_\_\_  
**(Nome completo, Posto, Identidade e Função)**

Testemunhas:

\_\_\_\_\_  
**(Nome completo, Posto, Identidade e Função)**



**Anexo D - Modelos de Termo de Classificação de Informação (TCI)**

**ULTRASSECRETO**

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO	
ÓRGÃO/ENTIDADE: <i>(OM que produziu)</i>	
CÓDIGO DE INDEXAÇÃO: <i>(1)</i>	
GRAU DE SIGILO: <b>ULTRASSECRETO</b>	
CATEGORIA: <b>05</b> <i>(2)</i>	
TIPO DE DOCUMENTO: <i>(Ofício, Mensagem Fac-símile, etc)</i>	
DATA DE PRODUÇÃO: <i>(data da assinatura do documento)</i>	
FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO: Inciso <i>(I a VIII)</i> do Art. 23, da Lei nº 12.527, de 18 NOV 11.	
RAZÕES PARA A CLASSIFICAÇÃO: - <b>ULTRASSECRETO</b> - <i>(3)</i>	
PRAZO DA RESTRIÇÃO DE ACESSO: <i>(4)</i>	
DATA DE CLASSIFICAÇÃO: <i>(DD/MM/AAAA da assinatura deste TCI)</i>	
AUTORIDADE CLASSIFICADORA	Nome: Cargo:
AUTORIDADE RATIFICADORA	Nome: Cargo:
DESCCLASSIFICAÇÃO em <i>DD/MM/AAAA</i>	Nome: Cargo:
RECLASSIFICAÇÃO em <i>DD/MM/AAAA</i>	Nome: Cargo:
REDUÇÃO DE PRAZO em <i>DD/MM/AAAA</i>	Nome: Cargo:
PRORROGAÇÃO DE PRAZO em <i>DD/MM/AAAA</i>	Nome: Cargo:
<p align="center">_____ ASSINATURA DA AUTORIDADE CLASSIFICADORA</p>	
<p align="center">_____ ASSINATURA DA AUTORIDADE RATIFICADORA</p>	
<p align="center">_____ ASSINATURA DA AUTORIDADE responsável por DESCCLASSIFICAÇÃO</p>	
<p align="center">_____ ASSINATURA DA AUTORIDADE responsável por RECLASSIFICAÇÃO</p>	
<p align="center">_____ ASSINATURA DA AUTORIDADE responsável por REDUÇÃO DE PRAZO</p>	
<p align="center">_____ ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO</p>	

## Continuação do Anexo D

**SECRETO**

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO	
ÓRGÃO/ENTIDADE: <i>(OM que produziu)</i>	
CÓDIGO DE INDEXAÇÃO: <i>(1)</i>	
GRAU DE SIGILO: <b>SECRETO</b>	
CATEGORIA: <b>05</b> <i>(2)</i>	
TIPO DE DOCUMENTO: <i>(Ofício, Mensagem Fac-símile, etc)</i>	
DATA DE PRODUÇÃO: <i>(data da assinatura do documento)</i>	
FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO: Inciso <i>(I a VIII)</i> do Art. 23, da Lei nº 12.527, de 18 NOV 11.	
RAZÕES PARA A CLASSIFICAÇÃO: - <b>SECRETO</b> - <i>(3)</i>	
PRAZO DA RESTRIÇÃO DE ACESSO: <i>(4)</i>	
DATA DE CLASSIFICAÇÃO: <i>(DD/MM/AAAA da assinatura deste TCI)</i>	
AUTORIDADE CLASSIFICADORA	Nome: Cargo:
DESCCLASSIFICAÇÃO em <i>DD/MM/AAAA</i>	Nome: Cargo:
RECLASSIFICAÇÃO em <i>DD/MM/AAAA</i>	Nome: Cargo:
REDUÇÃO DE PRAZO em <i>DD/MM/AAAA</i>	Nome: Cargo:
PRORROGAÇÃO DE PRAZO em <i>DD/MM/AAAA</i>	Nome: Cargo:
<hr/> ASSINATURA DA AUTORIDADE CLASSIFICADORA	
<hr/> ASSINATURA DA AUTORIDADE responsável por DESCCLASSIFICAÇÃO	
<hr/> ASSINATURA DA AUTORIDADE responsável por RECLASSIFICAÇÃO	
<hr/> ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO	

## Continuação do Anexo D

**RESERVADO**

<b>TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO</b>	
ÓRGÃO/ENTIDADE: <i>(OM que produziu)</i>	
CÓDIGO DE INDEXAÇÃO: <i>(1)</i>	
GRAU DE SIGILO: <b>RESERVADO</b>	
CATEGORIA: <b>05</b> <i>(2)</i>	
TIPO DE DOCUMENTO: <i>(Ofício, Mensagem Fac-símile, etc)</i>	
DATA DE PRODUÇÃO: <i>(data da assinatura do documento)</i>	
FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO: Inciso <i>(I a VIII)</i> do Art. 23, da Lei nº 12.527, de 18 NOV 11.	
RAZÕES PARA A CLASSIFICAÇÃO: - <b>SECRETO</b> - <i>(3)</i>	
PRAZO DA RESTRIÇÃO DE ACESSO: <i>(4)</i>	
DATA DE CLASSIFICAÇÃO: <i>(DD/MM/AAAA da assinatura deste TCI)</i>	
AUTORIDADE CLASSIFICADORA	Nome: Cargo:
DESCCLASSIFICAÇÃO em <i>DD/MM/AAAA</i>	Nome: Cargo:
REDUÇÃO DE PRAZO em <i>DD/MM/AAAA</i>	Nome: Cargo:
ASSINATURA DA AUTORIDADE CLASSIFICADORA	
ASSINATURA DA AUTORIDADE responsável por DESCCLASSIFICAÇÃO	
ASSINATURA DA AUTORIDADE responsável por REDUÇÃO DE PRAZO	
ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO	

Legenda:

(1) Código de Indexação de Documento que Contém Informação Classificada (CIDIC)

Exemplo: 1111.000001/2013-99.**U**.05.05/12/2012.04/12/2037.N

NUP/NUD	Grau de sigilo	Categoria	Data de Produção	Data de Desclassificação	Indicação da Reclassificação	Data da Prorrogação (U)
1111.000001/2013-99	<b>.U</b>	05	.05/12/2012	.04/12/2037 .	.N	

(2) No campo “CATEGORIA” deve ser registrado o número “05”, que equivale à categoria “Defesa e Segurança”.

(3) O campo “RAZÕES PARA A CLASSIFICAÇÃO” é destinado à análise pela CMRI. A redação não poderá ser cópia do inciso do fundamento legal. Deve-se procurar explicar o motivo pelo qual o documento em questão deve ser classificado.

Ex: Para TCI de documento SECRETO

RAZÕES PARA A CLASSIFICAÇÃO: - SECRETO Sua divulgação pode causar constrangimento diplomático com país vizinho.
--

(4) No campo “PRAZO DA RESTRIÇÃO DE ACESSO” deve ser fixado o tempo em anos, no prazo máximo para cada classificação. (Ex: até 5 anos (ERRADO); 5 anos (CERTO))

**Anexo E - Modelo de Identificação de Cópia de Documento Sigiloso  
(Segurança na Produção)**

**CLASSIFICAÇÃO SIGILOSA**



**MINISTÉRIO DA DEFESA  
COMANDO DA AERONÁUTICA  
(CONTINUAÇÃO DO CABEÇALHO DA OM)**

Ofício nº \_\_\_\_\_

Protocolo COMAER: \_\_\_\_\_

\_\_\_\_\_ - \_\_\_\_, de \_\_\_\_\_ de \_\_\_\_\_

**Do:**

**Ao:**

**Assunto:**

**Referência:**

**Anexo:**

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

**A140872**

**CLASSIFICAÇÃO SIGILOSA**

## Anexo F - Modelo de Termo de Eliminação de Material Controlado

**MATERIAL DE ACESSO RESTRITO**  
**Art. 44, 45 e 46 do Decreto nº 7.845, de 14 de novembro de**  
**2012**  
**NÍVEL 1**



MINISTÉRIO DA DEFESA

**COMANDO DA AERONÁUTICA**  
**(CONTINUAÇÃO DO CABEÇALHO DA OM)**

**TERMO DE ELIMINAÇÃO DE MATERIAL CONTROLADO**

Nº \_\_\_\_/\_\_\_\_

Ao(s) \_\_\_\_ dia(s) do mês de \_\_\_\_ do ano de dois mil e \_\_\_\_, em cumprimento à letra b do item 6.3.10.1 da Instrução para Salvaguarda de Assuntos Sigilosos (ICA 205-47), reuniram-se na(o) \_\_\_\_ (OM) o Sr.

**(NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA AUTORIDADE QUE CLASSIFICOU O ORIGINAL)**, o Sr.

**(NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DE UMA DAS TESTEMUNHAS)**, e o Sr.

**(NOME COMPLETO, POSTO, IDENTIDADE E FUNÇÃO DA OUTRA TESTEMUNHA)**, os dois últimos como testemunhas, para proceder à eliminação do(s) Material(is) Controlado(s) (MC), pelo(a) \_\_\_\_ (ÓRGÃO CONTROLADOR), conforme autorização contida no(a) \_\_\_\_

**(CITAR O DOCUMENTO QUE AUTORIZOU A ELIMINAÇÃO)**.

Cumpridas as formalidades exigidas e conferidas todas as peças constantes do termo de eliminação, foi(ram) eliminado(s) o(s) cópia(s) do MC abaixo discriminado(s):

Título Convencional	Nº de Série

E, para constar, foi lavrado o presente Termo de Eliminação.

**Detentor:**

\_\_\_\_\_  
(Nome completo, Posto, Identidade e Função)

\_\_\_\_\_, \_\_\_\_ de \_\_\_\_ de \_\_\_\_

**Testemunhas:**

\_\_\_\_\_  
(Nome completo, Posto, Identidade e Função)

\_\_\_\_\_  
(Nome completo, Posto, Identidade e Função)

**MATERIAL DE ACESSO RESTRITO**  
**Art. 44, 45 e 46 do Decreto nº 7.845, de 14 de novembro de 2012**  
**NÍVEL 1**

