MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

SEGURANÇA

RCA 205-1

REGULAMENTO PARA SALVAGUARDA DE ASSUNTOS SIGILOSOS DA AERONÁUTICA

2006

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNCIA DA AERONÁUTICA

SEGURANÇA

RCA 205-1

REGULAMENTO PARA SALVAGUARDA DE ASSUNTOS SIGILOSOS DA AERONÁUTICA

2006

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

PORTARIA Nº 250/GC3, DE 7 DE MARÇO DE 2006.

Aprova a reedição do Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica.

O COMANDANTE DA AERONÁUTICA, tendo em vista o disposto no Decreto nº 4553, de 27 de dezembro de 2002 e no Decreto nº 5301, de 9 de dezembro de 2004, e considerando o que consta do Processo nº 01-04/201/2005,

RESOLVE:

Art. 1º Aprovar a reedição do RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", que com esta baixa.

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

Art. 3º Fica revogada a Portaria nº 217/GC3, de 18 de fevereiro de 2004, publicada no Diário Oficial da União nº 36, de 20 de fevereiro de 2004, Seção 1, página 19.

Ten Brig Ar LUIZ CARLOS DA SILVA BUENO
(DOU nº 47, de 09 MAR 2006)

(Publicado no BCA nº 048, de 13 de março de 2006)

SUMÁRIO

PREFÁCIO

A salvaguarda de assuntos sigilosos requer, além de conhecimentos e mentalidade de segurança, procedimentos cautelares específicos, os quais devem ser conhecidos por todos aqueles que tratam dos referidos assuntos.

A elaboração deste regulamento atende às orientações contidas no Decreto nº 4.553, de 27 de dezembro de 2002 e no Decreto nº 5.301, de 09 de dezembro de 2004.

Com a reedição deste documento, pretende-se sintetizar, em uma única publicação, a ação dos Comandantes, Chefes e Diretores, norteando, assim, o trato de matéria sigilosa no âmbito da Aeronáutica.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

O presente Regulamento tem por finalidade regular e padronizar, no âmbito do Comando da Aeronáutica (COMAER), procedimentos necessários à salvaguarda de dados, informações, documentos e materiais sigilosos, bem como das áreas e instalações onde tramitam.

1.2 CONCEITUAÇÃO

1.2.1 ÁREA SIGILOSA

É aquela onde documentos, materiais, comunicações e sistemas de informações sigilosos são tratados, manuseados, transmitidos ou guardados e que, portanto, requer medidas especiais de segurança e controle de acesso.

1.2.2 ASSUNTO SIGILOSO

É aquele que, por sua natureza, deva ser de conhecimento restrito e, portanto, requeira a adoção de medidas especiais para sua segurança.

1.2.3 AUTENTICIDADE

Asseveração de que o dado ou informação são verdadeiros e fidedignos tanto na origem quanto no destino.

1.2.4 CLASSIFICAÇÃO

Atribuição, pela autoridade competente, de grau de sigilo a dado, informação, documento, material, área ou instalação.

1.2.5 COMPARTIMENTAÇÃO

É o resultado eficaz de todas as medidas que visam a restringir o acesso de pessoas a conhecimentos e/ou dados sigilosos, envolvendo uma série de medidas preventivas de segurança, de modo que só sejam liberadas ao acesso pessoas que:

a) tenham necessidade de conhecê-los; e

b) possuam credencial de segurança no grau adequado.

1.2.6 COMPROMETIMENTO

Perda de segurança resultante do acesso não autorizado.

1.2.7 CREDENCIAL DE SEGURANÇA

Certificado, concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados ou informações em diferentes graus de sigilo.

1.2.8 CREDENCIAMENTO

É o ato de concessão de Credencial de Segurança.

1.2.9 CUSTÓDIA

É a responsabilidade pela guarda de materiais ou documentos sigilosos.

1.2.10 DESCLASSIFICAÇÃO

Cancelamento, pela autoridade competente ou pelo transcurso de prazo, da classificação, tornando ostensivos dados ou informações.

1.2.11 DISPONIBILIDADE

Facilidade de recuperação ou acessibilidade de dados e informações.

1.2.12 GRAU DE SIGILO

Gradação atribuída a dados, informações, áreas ou instalações considerados sigilosos em decorrência de sua natureza ou conteúdo, que são: ultra-secreto, secreto, confidencial e reservado

1.2.13 INTEGRIDADE

Incolumidade de dados ou informações na origem, no trânsito ou no destino.

1.2.14 LEGITIMIDADE

Asseveração de que o emissor e o receptor de dados ou informações são legítimos e fidedignos tanto na origem quanto no destino.

1.2.15 MARCAÇÃO

Aposição de marca assinalando o grau de sigilo.

1.2.16 MATERIAL SIGILOSO

É toda matéria, substância ou artefato que, por sua natureza, deva ser de conhecimento restrito.

1.2.17 MEDIDAS ESPECIAIS DE SEGURANÇA

Medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade, legitimidade e disponibilidade de dados e informações sigilosos. Também objetivam prevenir, detectar, anular e registrar ameaças reais ou potenciais a esses dados e informações.

1.2.18 MEIO DE COMUNICAÇÃO SIGILOSA

Aquele no qual se transmitem dados, informações e/ou conhecimentos sigilosos e requer dispositivos de criptografia para sua veiculação.

1.2.19 NECESSIDADE DE CONHECER

Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa, possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosos.

1.2.20 OSTENSIVO

Sem classificação, cujo acesso pode ser franqueado.

1.2.21 PRODUTO CRIPTOGRÁFICO

Denominação genérica atribuída a **hardware**, **software**, **firmware**, ou a qualquer combinação deles, que contenha um módulo criptográfico, como também a atribuída a serviço que empregue recursos criptográficos.

1.2.22 RECLASSIFICAÇÃO

Alteração, pela autoridade competente, da classificação de dado, informação, área ou instalação sigilosos.

1.2.23 SIGILO

Segredo; de conhecimento restrito a pessoas credenciadas; proteção contra revelação não autorizada.

1.2.24 SISTEMA DE INFORMAÇÃO

Conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive programas, especificações e procedimentos para sua operação, uso e manutenção.

1.2.25 VAZAMENTO

É a divulgação não autorizada de conhecimento e/ou dado sigiloso.

1.2.26 VISITA

Pessoa cuja entrada foi admitida, em caráter excepcional, em área sigilosa.

1.3 ÂMBITO

O presente Regulamento aplica-se a todas as 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 ou convênio com cláusula de manutenção de sigilo.

2 SIGILO E SEGURANÇA

2.1 CLASSIFICAÇÃO SEGUNDO O GRAU DE SIGILO

2.1.1 Os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos.

2.1.1.1 São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da Defesa Nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

2.1.1.2 São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da Defesa Nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

2.1.1.3 São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito, cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.

2.1.1.4 São passíveis de classificação como reservados dados ou informações cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

2.2 COMPETÊNCIA PARA CLASSIFICAÇÃO, RECLASSIFICAÇÃO E DESCLASSIFICAÇÃO DE DOCUMENTOS SIGILOSOS

2.2.1 A classificação no grau ultra-secreto é de competência das seguintes autoridades:

a) Presidente da República;
b) Vice-Presidente da República;
c) Ministros de Estado e autoridades com as mesmas prerrogativas;
d) Comandantes da Marinha, do Exército e da Aeronáutica; e
e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior.

2.2.1.1 A classificação de documentos no grau secreto somente poderá ser feita pelas autoridades indicadas no item 2.2.1 e as autoridades que exerçam funções de Comando, Chefia ou Direção.

2.2.2 A classificação de documentos no grau confidencial poderá ser feita pelas autoridades indicadas nos itens 2.2.1 e 2.2.1.1 e os demais oficiais superiores, intermediários e subalternos da ativa da Aeronáutica, bem como os servidores civis a eles assemelhados, lotados no COMAER.

2.2.3 A classificação de documentos no grau reservado poderá ser feita pelas autoridades indicadas nos itens 2.2.1, 2.2.1.1 e 2.2.2 e os aspirantes-a-oficial e os graduados da ativa da Aeronáutica, bem como os servidores civis a eles assemelhados, lotados no COMAER.

2.3 PRAZOS

2.3.1 Os prazos de duração da classificação a que se refere este Regulamento vigoram a partir da data de produção do dado ou informação e são os seguintes:

a) ultra-secreto: máximo de trinta anos;
b) secreto: máximo de vinte anos;
c) confidencial: máximo de dez anos; e
d) reservado: máximo de cinco anos.

2.3.1.1 Considerando o interesse da segurança da sociedade e do Estado, poderá a autoridade responsável pela classificação nos graus ultra-secreto, secreto, confidencial e reservado, ou a autoridade hierarquicamente superior competente para dispor sobre o assunto, renovar o prazo de duração, uma única vez, por igual período, previstos nas alíneas do item 2.3.1.

2.4 RECLASSIFICAÇÃO E DESCLASSIFICAÇÃO

2.4.1 Dados ou informações classificados no grau de sigilo ultra-secreto somente poderão ser reclassificados ou desclassificados mediante decisão da autoridade responsável pela sua classificação.

2.4.2 Para os graus secreto, confidencial e reservado, poderá a autoridade responsável pela classificação, ou a autoridade hierarquicamente superior competente para dispor sobre o assunto, respeitados os interesses da segurança da sociedade e do Estado, alterá-la ou cancelá-la, por meio de expediente hábil de reclassificação ou desclassificação dirigido ao detentor da custódia do dado ou informação sigilosos.

2.4.2.1 Na reclassificação, o novo prazo de duração conta-se a partir da data de produção do dado ou informação.

2.4.3 A desclassificação de dados ou informações nos graus ultra-secreto, secreto, confidencial e reservado será automática após transcorridos os prazos previstos nas alíneas "a", "b", "c" e "d" do item 2.3.1, salvo no caso de sua prorrogação, quando, então, a desclassificação ocorrerá ao final de seu termo.

2.4.3.1 A autoridade competente para classificar dados ou informações no grau ultra-secreto poderá, caso haja interesse, após vencido o prazo ou sua prorrogação, previstos no item 2.3, provocar, de modo justificado, a manifestação da Comissão de Averiguação e Análise de Informações Sigilosas para que avalie, previamente a qualquer divulgação, se o acesso ao documento acarretará dano à segurança da sociedade e do Estado.

2.4.3.2 Poderá a autoridade responsável pela classificação dos documentos, ou a autoridade hierarquicamente superior, findando o motivo de sua classificação ou alteração de sua natureza, e considerando o interesse para a pesquisa e para a administração, alterá-la ou cancelá-la, tornando-os ostensivos.

2.4.4 Dados ou informações sigilosos de guarda permanente que forem objeto de desclassificação serão encaminhados ao Centro de Documentação e Histórico da Aeronáutica (CENDOC), para fins de organização, preservação e acesso.

2.4.4.1 Consideram-se de guarda permanente os dados ou informações de valor histórico, probatório e informativo que devam ser definitivamente preservados.

2.4.5 A indicação da reclassificação ou da desclassificação de dados ou informações sigilosos deverá constar das capas, se houver, e da primeira página.

2.5 PROCEDIMENTOS PARA CLASSIFICAÇÃO DE DOCUMENTOS

2.5.1 As páginas, os parágrafos, as seções, as partes componentes ou os anexos de um documento sigiloso podem merecer diferentes classificações, mas ao documento, no seu todo, será atribuído o grau de sigilo mais elevado, conferido a quaisquer de suas partes.

2.5.2 A classificação de um grupo de documentos que formem um conjunto deve ser a mesma atribuída ao documento classificado com o mais alto grau de sigilo.

2.5.3 A publicação dos atos sigilosos, se for o caso, limitar-se-á aos seus respectivos números, datas de expedição e ementas, redigidas de modo a não comprometer o sigilo.

2.5.4 Os mapas, planos-relevos, cartas e fotocartas baseados em fotografias aéreas ou em seus negativos serão classificados em razão dos detalhes que revelem, e não da classificação atribuída às fotografias ou negativos que lhes deram origem, tampouco das diretrizes baixadas para obtê-las.

2.5.5 Poderão ser elaborados extratos de documentos sigilosos, para sua divulgação ou execução, mediante consentimento expresso:

a) da autoridade classificadora: para documentos ultra-secretos;
b) da autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto: para documentos secretos; e
c) da autoridade classificadora, destinatária ou autoridade hierarquicamente superior competente para dispor sobre o assunto: para documentos confidenciais e reservados, exceto quando expressamente vedado no próprio documento.

2.5.5.1 Aos extratos de que trata o item 2.5.5 serão atribuídos graus de sigilo iguais ou inferiores àqueles atribuídos aos documentos que lhes deram origem, salvo quando elaborados para fins de divulgação.

2.6 DOCUMENTO E MATERIAL SIGILOSOS CONTROLADOS

2.6.1 Documento e Material Sigilosos Controlados (DSC/MSC) são aqueles que, por sua importância, requerem medidas adicionais de controle, incluindo:

a) identificação dos destinatários em protocolo e recibo próprios, quando da difusão;
b) lavratura de termo de custódia (Anexo A) e registro em protocolo específico;
c) lavratura anual de termo de inventário (Anexo B), até 30 de julho, pelo órgão ou entidade expedidores e pelo órgão ou entidade receptores; e
d) lavratura de termo de transferência (Anexo C), sempre que se proceder à transferência de sua custódia ou guarda, conforme dispõe o item 2.6.8 deste Regulamento.

2.6.2 O documento ultra-secreto é, por sua natureza, considerado DSC, desde sua classificação ou reclassificação.

2.6.2.1 Os documentos Secretos, Confidenciais e Reservados poderão, a critério da autoridade classificadora ou hierarquicamente superior, ser considerados DSC.

2.6.3 Os equipamentos/materiais criptográficos e/ou criptofônicos, bem como os sistemas de cifra e códigos e os seus respectivos manuais serão, por sua natureza, considerados DSC/MSC.

2.6.4 Os DSC/MSC, quaisquer que sejam suas classificações, deverão ser entregues, via malote ou pessoalmente, ao destinatário, por pessoa credenciada, mediante recibo, com exceção dos materiais criptográficos e/ou criptofônicos, bem como os sistemas de cifra e códigos e os seus respectivos manuais, que só podem ser remetidos por portador credenciado.

2.6.5 Ao receber qualquer DSC/MSC, o responsável pelo recebimento na organização verificará a sua normalidade física e, se for o caso, participará ao órgão controlador as alterações encontradas, tais como rasuras, irregularidades de impressão, violações, paginação etc.

2.6.6 A responsabilidade pela custódia de DSC/MSC será atribuída:

a) ao Comandante, Chefe e Diretor da organização custodiante ou a oficial por ele designado; e
b) nas Aditâncias, aos Adidos Militares.

2.6.7 Os sistemas e os materiais criptográficos e/ou criptofônicos deverão ser guardados em locais distintos de seus manuais de utilização ou senhas.

2.6.8 Quando houver transferência de guarda de documento/material controlado, lavrar-se-á um Termo de Transferência, em quatro vias, datado e assinado pelo antigo e novo detentor; a primeira via será remetida diretamente ao órgão de controle, juntamente com o inventário atualizado; a segunda via ficará arquivada no setor que tem a custódia dos DSC/MSC atualizados; e as demais ficarão, respectivamente, com o antigo e o novo detentor dos documentos.

2.6.9 Sempre que ocorrer furto, roubo ou extravio de DSC/MSC, deve-se proceder à devida investigação, a fim de apurar as causas e os responsáveis, bem como levantar as medidas de segurança orgânica que deverão ser implementadas e as ações penais, civil e administrativa decorrentes.

2.7 MARCAÇÃO

2.7.1 A marcação, ou indicação do grau de sigilo (Anexo D), deverá ser feita em todas as páginas do documento e nas capas, se houver, sendo observada a seguinte formalística:

a) a indicação será centralizada, preferencialmente no alto e no pé de cada página, em cor contrastante com a do documento;
b) as páginas serão numeradas seguidamente, devendo cada uma conter, também, indicação do total de páginas que compõem o documento; e
c) os livros, manuais ou folhetos cujas páginas estejam seguras ou permanentemente reunidas serão marcados, claramente, na capa, na contracapa, na página do título e na primeira e última páginas, quando anexados a documentos sigilosos.

2.7.1.1 O DSC também expressará, nas capas, se houver, e em todas as suas páginas, a expressão "Documento Sigiloso Controlado (DSC)" e o respectivo número de controle.

2.7.2 Os esboços, extratos, rascunhos e desenhos sigilosos terão marcação dos seus respectivos graus de sigilo em local que possibilite sua reprodução em todas as cópias.

2.7.3 No caso específico da indicação do grau de sigilo de negativos, fotografias e imagens digitais sigilosas, observar-se-ão as seguintes disposições:

a) os negativos, cuja falta de espaço impossibilite a indicação de sigilo, serão utilizados em condições que garantam a sua segurança e guardados em recipientes que exibam a classificação correspondente ao conteúdo e, se possível, registrados os seus respectivos graus de sigilo no seu verso, bem como nas respectivas embalagens;
b) os negativos em rolos contínuos, relativos a reconhecimentos e a levantamentos aerofotogramétricos, terão indicados, no princípio e no fim de cada rolo, o grau de sigilo correspondente;
c) os microfilmes e os filmes cinematográficos sigilosos serão acondicionados de modo tecnicamente seguro, devendo as embalagens exibirem o grau de sigilo correspondente a todo seu conteúdo; e
d) a indicação do grau de sigilo em filmes cinematográficos será registrada, também, no início e no fim das imagens.

2.7.4 A indicação do grau de sigilo em mapas, cartas e fotocartas será aposta logo acima do título e na parte inferior, sem prejuízo das imagens registradas.

2.7.4.1 As cartas e fotocartas montadas a partir de fotografias aéreas ou imagens digitais serão classificadas em razão dos detalhes que revelem, e não apenas devido à classificação atribuída às fotografias aéreas ou imagens digitais que lhes deram origem.

2.7.5 A indicação da reclassificação ou da desclassificação de documentos sigilosos deverá constar da capa, se houver, e da primeira página do documento, mediante aposição de carimbo, de forma que não prejudique os dados, informações ou conhecimentos registrados.

2.7.6 O responsável pela posse de documento sigiloso, de classificação alterada ou cancelada, providenciará a anotação autenticada da alteração do documento.

2.7.7 Quando for necessário reclassificar documentos sigilosos do mesmo tipo, reunidos em maço ou pasta, basta colocar, na primeira página, a anotação autenticada. Caso seja necessário destacar algum documento para uso isolado, este receberá idêntica anotação.

2.7.8 Os meios de armazenamento de dados, informações e/ou conhecimentos sigilosos serão marcados, com o grau de sigilo devido, em local adequado.

2.7.8.1 Consideram-se meios de armazenamento a que se refere o item 2.7.8 os discos sonoros e ópticos (CD-ROM), fitas e discos magnéticos (disquetes) e demais meios possíveis de armazenamento de dados e informações.

2.7.9 Todos os modelos, protótipos, moldes, equipamentos e outros materiais considerados sigilosos, que sejam objeto de contrato ou convênio, deverão ser adequadamente marcados para indicar o seu grau de sigilo.

2.7.9.1 Se impossível tal marcação, em função das características do material, a embalagem, se houver, deverá exibir o grau de sigilo correspondente.

2.8 EXPEDIÇÃO E COMUNICAÇÃO DE DOCUMENTOS SIGILOSOS

2.8.1 A segurança relacionada com a expedição de documentos sigilosos é da responsabilidade de todos aqueles que os manusearem.

2.8.2 Todos aqueles que têm contato com documentos sigilosos devem ser instruídos sobre como proceder quando pressentirem qualquer tipo de ameaça ou incidente que possa resultar em comprometimento do documento.

2.8.3 Os documentos sigilosos, em sua expedição e tramitação, obedecerão às seguintes prescrições:

a) serão acondicionados em envelopes duplos;
b) no envelope externo, não constará qualquer indicação do grau de sigilo ou do teor do documento;
c) no envelope interno, serão apostos o destinatário e o grau de sigilo do documento, de modo a serem identificados logo que removido o envelope externo;
d) o envelope interno será fechado, lacrado e expedido mediante recibo, que indicará, necessariamente, remetente, destinatário e número ou outro indicativo que identifique o documento; e
e) sempre que o assunto for considerado de interesse exclusivo do destinatário, será inscrita a palavra pessoal no envelope que contém o documento sigiloso.

2.8.4 A expedição, a condução e a entrega de documento ultra-secreto, em princípio, serão efetuadas pessoalmente, por agente público autorizado, sendo vedada a sua postagem.

2.8.4.1 A comunicação de assunto ultra-secreto de outra forma que não a prescrita no item 2.8.4 só será permitida excepcionalmente e em casos que requeiram tramitação e solução imediatas, em atendimento ao princípio da oportunidade e considerados os interesses da segurança da sociedade e do Estado.

2.8.5 A expedição de documento secreto, confidencial ou reservado poderá ser feita mediante serviço postal, com opção de registro, mensageiro oficialmente designado, sistema de encomendas ou, se for o caso, mala diplomática.

2.8.5.1 A comunicação dos assuntos sigilosos poderá ser feita por outros meios, desde que sejam usados recursos de criptografia compatíveis com o grau de sigilo do documento, e estes sejam aprovados pelo Centro de Inteligência da Aeronáutica (CIAER).

2.8.6 Em todos os casos, serão adotadas providências que permitam o máximo de segurança na expedição de documentos sigilosos.

2.9 REGISTRO, TRAMITAÇÃO E GUARDA

2.9.1 Cabe aos responsáveis pelo recebimento de documentos sigilosos:

a) verificar a integridade e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na correspondência recebida, dando ciência do fato ao seu superior hierárquico e ao destinatário; e
b) proceder ao registro do documento e ao controle de sua tramitação.

2.9.2 O envelope interno só será aberto pelo destinatário, pelo seu representante autorizado ou por autoridade competente hierarquicamente superior.

2.9.2.1 Envelopes contendo a marca pessoal só poderão ser abertos pelo próprio destinatário.

2.9.3 O destinatário de documento sigiloso comunicará imediatamente ao remetente qualquer indício de violação ou adulteração do documento.

2.9.4 Os documentos sigilosos serão mantidos ou guardados em condições especiais de segurança, conforme o seu grau de sigilo.

2.9.5 Os agentes responsáveis pela guarda ou custódia de documentos ou materiais sigilosos os transmitirão a seus substitutos, devidamente conferidos, quando da passagem ou transferência de responsabilidade.

2.10 SEGURANÇA NA PRODUÇÃO

2.10.1 A todo documento, em fase de produção, deverá ser atribuído um grau de sigilo preliminar. Após concluído, o documento deverá ter seu grau de sigilo retificado ou ratificado.

2.10.2 Poderá a autoridade superior à que classificou o documento alterar o grau de sigilo dos documentos em trâmite.

2.10.3 As páginas, os parágrafos, as seções, as partes componentes ou os anexos de um documento podem merecer diferentes classificações, mas ao documento, no seu todo, será atribuído o grau de sigilo mais elevado.

2.10.4 O responsável pela produção de documentos sigilosos deverá eliminar notas manuscritas, tipos, clichês, carbonos, provas, cópias inservíveis ou quaisquer outros elementos que possam dar origem a cópia não autorizada do todo ou parte.

2.10.5 As cópias dos documentos sigilosos deverão ser limitadas estritamente ao necessário para sua difusão e somente deverão ser realizadas mediante o consentimento expresso da autoridade classificadora ou autoridade hierarquicamente superior.

2.10.6 As cópias ou extratos de documentos sigilosos deverão receber um código numérico ou alfa-numérico específico (Anexo E) para cada destinatário, a fim de que se possa identificar a origem de um possível vazamento e facilitar o controle de uma futura eliminação.

2.10.7 O código mencionado no item 2.10.6 deverá ser colocado no corpo do texto, em cada página, de todo o documento, a fim de aparecer em qualquer reprodução gráfica realizada.

2.10.8 No documento original, deverão constar todos os destinatários com os seus respectivos códigos.

2.11 REPRODUÇÃO

2.11.1 A reprodução do todo ou de parte de documento sigiloso terá o mesmo grau de sigilo do documento original.

2.11.1.1 A reprodução total ou parcial de DSC condiciona-se à autorização expressa da autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto.

2.11.1.2 Eventuais cópias decorrentes de documentos sigilosos serão autenticadas pelo Chefe da Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS).

2.11.1.3 Serão fornecidas certidões de documentos sigilosos que não puderem ser reproduzidos devido a seu estado de conservação, desde que necessário como prova em juízo.

2.11.2 O responsável pela reprodução de documentos sigilosos deverá providenciar a eliminação de notas manuscritas, tipos, clichês, carbonos, provas ou qualquer outro recurso, que possam dar origem a cópia não-autorizada do todo ou parte.

2.11.3 Sempre que a preparação, impressão ou, se for o caso, reprodução de documento sigiloso for efetuada em tipografias, impressoras, oficinas gráficas ou similar, essa operação deverá ser acompanhada por pessoa oficialmente designada, que será responsável pela garantia do sigilo durante a confecção do documento.

2.12 AVALIAÇÃO E PRESERVAÇÃO

2.12.1 A CPADS, prevista no Decreto nº 4.553, de 2002, regulada em norma própria, dentre outras atribuições, deverá:

a) analisar e avaliar periodicamente a documentação sigilosa produzida e acumulada no âmbito de sua atuação;
b) propor à autoridade responsável pela classificação, ou autoridade hierarquicamente superior competente para dispor sobre o assunto, renovação dos prazos a que se refere o item 2.3.1 deste Regulamento;
c) propor à autoridade responsável pela classificação, ou autoridade hierarquicamente superior competente para dispor sobre o assunto, alteração ou cancelamento da classificação sigilosa, de conformidade com o disposto no item 2.4.2;
d) determinar o destino final da documentação tornada ostensiva, selecionando os documentos para guarda permanente; e
e) autorizar o acesso a documentos sigilosos.

2.12.1.1 Para o perfeito cumprimento de suas atribuições e responsabilidades, a CPADS poderá ser subdividida em subcomissões.

2.12.2 Os documentos permanentes de valor histórico, probatório e informativo não podem ser desfigurados ou destruídos, sob pena de responsabilidade penal, civil e administrativa, nos termos da legislação em vigor.

2.13 SEGURANÇA NO ARQUIVAMENTO

2.13.1 Os documentos sigilosos serão guardados em locais próprios que permitam sua segurança.

2.13.2 Para a guarda de documentos ultra-secretos e secretos, é obrigatório, no mínimo, o uso de cofre com segredo de três combinações ou material que ofereça segurança equivalente ou superior.

2.13.2.1 Na impossibilidade de se adotar o disposto no item 2.13.2, os documentos ultra-secretos deverão ser mantidos sob guarda armada e para os documentos secretos, em caráter excepcional e temporário, devem ser adotadas as medidas dispostas no item 2.13.3.

2.13.3 Para a guarda de documentos confidenciais e reservados, é compulsório, no mínimo, o uso de arquivo com chave.

2.13.4 Não deverão ser guardados no mesmo cofre ou arquivo o texto em claro e o seu correspondente criptografado.

2.13.5 É importante, também, que sejam estabelecidos procedimentos relativos à evacuação da documentação sigilosa em situações de emergência. Estas ações requerem o estabelecimento de prioridades e responsabilidades para estas situações de sinistro, bem como determinar locais específicos para acolher a documentação recuperada.

2.14 SEGURANÇA NA PRESERVAÇÃO

2.14.1 Os originais dos documentos sigilosos, controlados ou não, deverão ser mantidos em arquivo e submetidos, dentro do período previsto, à apreciação da CPADS.

2.14.2 Os documentos sigilosos desclassificados serão submetidos à análise da CPADS, que os selecionará para a guarda permanente ou determinará a eliminação dos destituídos de valor.

2.14.2.1 No caso de dados ou informações no grau ultra-secreto, a autoridade competente para classificar poderá, caso haja interesse e após vencido o prazo ou sua prorrogação (previstos no item 2.3), provocar, de modo justificado, a manifestação da Comissão de Averiguação e Análise de Informações Sigilosas, criada pelo Decreto nº 5.301, de 9 de dezembro de 2004, para que avalie, previamente a qualquer divulgação, se o acesso ao documento acarretará dano à segurança da sociedade e do Estado.

2.14.3 Para a eliminação de cópias de DSC, bem como para a eliminação de MSC, deverão ser observados os seguintes procedimentos:

a) a autoridade que classificou o original deverá recolher a(s) cópia(s) de DSC ou o MSC que deverá(ão) ser eliminado(s);
b) após certificar-se de que o original foi mantido em arquivo, deverá ser lavrado o respectivo Termo de Eliminação de Cópia(s) de Documento Sigiloso Controlado (Anexo F), assinado pela autoridade que classificou o original e por duas testemunhas;
c) quando se tratar de MSC, será lavrado o Termo de Eliminação de Material Sigiloso Controlado (Anexo G), também assinado pela autoridade classificadora e por duas testemunhas;

d) os termos citados nas alíneas “b” e “c” deste item deverão ser publicados em Boletim Interno Reservado; e
e) deverão ser lançados, no verso da primeira folha do DSC original, o número e data do Boletim Interno que publicou o Termo de Eliminação de sua(s) respectiva(s) cópia(s).

2.14.4 Deverão ser estabelecidos procedimentos relativos à preservação da documentação sigilosa em situações normais e de emergência, como sinistro ou calamidades. Essas medidas requerem o estabelecimento antecipado de prioridades e responsabilidades.

2.15 ACESSO

2.15.1 O acesso a dados ou informações sigilosos em órgãos e entidades públicos e instituições de caráter público é admitido:
a) ao agente público, no exercício de cargo, função, emprego ou atividade pública, que tenha necessidade de conhecê-los; e
b) ao cidadão, naquilo que diga respeito à sua pessoa, ao seu interesse particular ou do interesse coletivo ou geral, mediante requerimento ao órgão ou entidade competente.

2.15.1.1 Todo aquele que tiver conhecimento, nos termos deste Regulamento, de assuntos sigilosos fica sujeito às sanções administrativas, civis e penais decorrentes da eventual divulgação dos conteúdos.

2.15.1.2 Serão liberados à consulta pública os documentos que contiverem informações pessoais, desde que previamente autorizada pelo titular ou por seus herdeiros.

2.15.2 O acesso a dados ou informações sigilosos, ressalvado o previsto no item 2.15.1.2, é condicionado à emissão de credencial de segurança no correspondente grau de sigilo, que pode ser limitada no tempo.

2.15.3 O acesso a qualquer documento sigiloso resultante de acordos ou contratos com outros países atenderá às normas e recomendações de sigilo constantes desses instrumentos.

2.15.4 A negativa de autorização de acesso deverá ser justificada.

2.15.5 O acesso ao assunto sigiloso é estritamente funcional e independe de grau hierárquico, sendo, contudo, obrigatório o credenciamento de segurança compatível, de acordo com as normas estabelecidas para concessão de Credencial de Segurança.

2.15.6 Cabe ao Comandante, Chefe ou Diretor, no âmbito de sua OM, regular o acesso, levando em consideração a necessidade de conhecer e o credenciamento de segurança adequado.

2.15.7 As Credenciais de Segurança serão classificadas nos seguintes graus:
a) ultra-secreto;
b) secreto;
c) confidencial; e
d) reservado

2.15.8 Tendo em vista que o processo de seleção para ocupar posto, graduação, categoria ou cargo pressupõe investigação compatível com o manuseio de assuntos sigilosos, são considerados credenciados, dispensando a devida investigação, até o grau de:

a) ultra-secreto, os oficias-generais da ativa da Aeronáutica;
b) secreto, os oficiais superiores da ativa da Aeronáutica, quando em função de Comando, Direção ou Chefia de OM;
c) confidencial, os demais oficiais superiores, intermediários e subalternos da ativa da Aeronáutica, bem como os civis a eles assemelhados, lotados no COMAER; e
d) reservado, os aspirantes-a-oficial e os graduados da ativa da Aeronáutica, bem como os servidores civis a eles assemelhados, lotados no COMAER.

2.15.9 A Credencial de Segurança que permite o acesso a assunto sigiloso, concedida a determinada pessoa, deverá ser cancelada quando existir vulnerabilidade que coloque em risco o conhecimento ou dado sigiloso.

2.15.10 A Credencial de Segurança que permite o acesso a assunto sigiloso, concedida a determinada pessoa, deverá ser suspensa em caso de transferência, passagem para a reserva remunerada, mudança de função e licenciamento do serviço ativo.

2.15.11 As normas gerais para a concessão de Credencial de Segurança de pessoa física e jurídica estão especificadas em legislação pertinente.

2.16 ÁREAS E INSTALAÇÕES SIGILOSAS

2.16.1 A classificação de áreas e instalações será feita em razão dos dados ou informações sigilosos que contenham ou que no seu interior sejam produzidos ou tratados, em conformidade com o disposto no item 2.1 deste Regulamento.

2.16.2 As áreas sigilosas deverão ser classificadas em razão do grau de sigilo dos assuntos nelas tratados, desenvolvidos, guardados ou manuseados, podendo variar de ultra-secretas até reservadas. Cabe ao Comandante, Chefe ou Diretor, no âmbito de sua OM, a adoção de medidas que visem à definição, demarcação, sinalização, segurança e autorização de acesso às áreas sigilosas sob sua responsabilidade. Para tanto, deverão ser elaboradas Normas de Controle de Acesso às Áreas Sigilosas ou Restritas, com a finalidade de sistematizar procedimentos.

2.16.3 O acesso de visitas a áreas e instalações sigilosas deverá ser disciplinado em legislação específica de cada OM, atendendo ao que prevê ICA 205-22 "Visita às Organizações Militares do COMAER", de 12 de dezembro de 2002.

2.16.3.1 Para efeito do que dispõe o item 2.16.3, não são considerados visitas o militar, o agente público ou o particular que oficialmente execute atividade pública diretamente vinculada à elaboração de estudo ou trabalho de natureza sigilosa e voltado para a segurança da sociedade e do Estado.

2.16.4 As áreas onde são desenvolvidas atividades de Inteligência, Informática, Comunicações, Ciência e Tecnologia, Guerra Eletrônica, Operações Aéreas, Controle de Tráfego Aéreo e Tecnologia da Informação deverão ser consideradas sigilosas.

2.16.5 Deverão ser consideradas como áreas restritas aquelas vitais para o pleno funcionamento da OM, tais como reservas de armamento, paiol, caixa d'água, casas de força, centrais de climatização, dentre outras.

2.16.6 O acesso às áreas sigilosas ou restritas somente deverá ser permitido às pessoas devidamente credenciadas.

2.16.7 Não deverá ser permitida a entrada de pessoas conduzindo máquinas fotográficas, filmadoras e/ou gravadores, em áreas e instalações que tratem de assunto sigiloso.

2.16.8 As áreas sigilosas deverão ser indicadas, por intermédio de placas afixadas na(s) parede(s), de forma destacada, preferencialmente na cor vermelha, com o respectivo grau de sigilo, não só no seu interior, mas principalmente junto à(s) entrada(s). Tal marcação tem por finalidade precípua apresentar-se como um primeiro elemento dissuasor ao comprometimento.

2.17 SEGURANÇA DO MATERIAL

2.17.1 Se for responsável por programa de pesquisa ou por projeto, o Comandante, Chefe ou Diretor de OM que julgar conveniente manter sigilo sobre determinado material, ou suas partes, em decorrência de aperfeiçoamento, prova, produção ou aquisição, deverá providenciar para que ao programa ou projeto seja atribuído o grau de sigilo adequado.

2.17.2 Aplica-se também o disposto no item 2.17.1 ao Comandante, Chefe ou Diretor de OM encarregada da fiscalização e do controle de atividades de entidade privada, para fins de produção e/ou exportação de material de interesse da Defesa Nacional.

2.17.3 Os Comandantes, Chefes e Diretores de OM da Aeronáutica, assim como os titulares de empresas privadas contratadas pelo COMAER, encarregadas da preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de novo projeto, prova, produção, aquisição, armazenagem ou emprego de material sigiloso, conforme o credenciamento recebido, são responsáveis pela expedição das instruções adicionais que se tornarem necessárias à salvaguarda dos assuntos sigilosos a eles relacionados.

2.17.4 As empresas privadas que desenvolvam pesquisas ou projetos de interesse nacional que contenham materiais sigilosos deverão providenciar a sua classificação de forma adequada, mediante entendimentos com a OM a que estiverem ligadas, para efeito daquelas pesquisas ou projetos.

2.17.5 Todos os modelos, protótipos, moldes, equipamentos e outros materiais similares considerados sigilosos e que sejam objeto de contrato, de qualquer natureza, com entidade pública, militar ou privada, envolvendo empréstimo, cessão, arrendamento ou locação, serão, adequadamente, marcados para indicar o seu grau de sigilo.

2.17.6 Se for impossível a marcação citada no item 2.17.5, a entidade será notificada do grau de sigilo de tais artigos.

2.17.7 Em qualquer caso, as entidades públicas ou privadas contratadas pelas OM do Comando da Aeronáutica deverão ser notificadas das medidas de segurança a serem adotadas, obedecendo às normas específicas quando do credenciamento.

2.17.8 Dados e informações sigilosos concernentes a programas técnicos ou aperfeiçoamentos de material só serão fornecidos aos que, por suas funções oficiais ou contratuais, a eles devam ter acesso.

2.17.9 O COMAER, por intermédio de seus Comandantes, Chefes e Diretores, controlará e coordenará o fornecimento de informações e dados sigilosos necessários ao desenvolvimento dos programas às pessoas físicas e jurídicas interessadas.

2.17.10 A definição do meio de transporte a ser utilizado para o deslocamento de material sigiloso é de responsabilidade do detentor, que deverá considerar o grau de sigilo atribuído ao respectivo material.

2.17.11 O material sigiloso poderá ser transportado por empresas para tal fim contratadas, as quais providenciarão as medidas necessárias para a segurança do material, estabelecidas em entendimentos prévios e contidas em cláusulas específicas de contrato.

2.17.12 Se o tamanho e quantidade permitirem, os materiais sigilosos poderão ser tratados segundo os critérios estipulados para a expedição de documentos sigilosos.

2.17.13 A critério da autoridade competente, poderão ser empregados guardas armados no transporte de material sigiloso.

3 SEGURANÇA DA INFORMAÇÃO

3.1 SEGURANÇA DAS COMUNICAÇÕES E DOS SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO

3.1.1 CRIPTOGRAFIA

3.1.1.1 Todo documento criptografado é considerado sigiloso.

3.1.1.2 As tecnologias empregadas na segurança dos Sistemas de Informação são consideradas sigilosas.

3.1.1.3 É vedado o uso de qualquer código, sistema de cifra ou dispositivo cifrador que não seja em razão do serviço.

3.1.2 SEGURANÇA E CONTROLE CRIPTOGRÁFICO

3.1.2.1 Os Comandantes, Chefes e Diretores designarão um responsável pela segurança criptográfica nas suas OM, com atribuições específicas, o qual deverá firmar termo de responsabilidade.

3.1.2.2 Aplicam-se aos equipamentos e materiais criptográficos e aos sistemas de cifras e códigos todas as medidas de segurança previstas para os documentos e materiais sigilosos controlados 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 à atribuição de grau de sigilo para documento criptografado, indício de violação, irregularidade na transmissão ou recebimento da informação criptografada.

3.2 DA SEGURANÇA NA TRANSMISSÃO

3.2.1 A segurança relacionada com transmissão de assunto sigiloso é da responsabilidade de todo aquele que o manusear para tal fim. As medidas de segurança variarão de acordo com os respectivos graus de sigilo e o meio de remessa ou transmissão utilizado.

3.2.2 A remessa de documentos ultra-secretos deverá, sempre que possível, ser efetuada por intermédio de mensageiros credenciados. Atendendo ao princípio da oportunidade, tais documentos poderão ser transmitidos por meio elétrico ou eletrônico, em situações excepcionais, desde que obrigatoriamente criptografados, utilizando-se da Rede de Comunicações de Dados Sigilosos, mantida e normatizada pelo CIAER.

3.2.3 Documentos sigilosos, classificados com o grau secreto, confidencial ou reservado, poderão ser transmitidos por meio elétrico ou eletrônico, desde que obrigatoriamente criptografados, utilizando-se da Rede de Comunicações de Dados Sigilosos, mantida e normatizada pelo CIAER.

3.2.4 Deve-se considerar a extrema vulnerabilidade de telefones, fax ou INTERNET, sem a devida proteção criptográfica, para o trato de assuntos sigilosos.

3.3 DA SEGURANÇA DO CONTEÚDO

3.3.1 Todo documento criptografado recebido deverá ser tratado como sigiloso.

3.3.2 É proibida a utilização de qualquer sistema de cifra e código ou material criptográfico, para a confecção de mensagens que não tratem exclusivamente de assunto de serviço.

3.3.3 Os processos empregados na segurança dos Sistemas de Tecnologia da Informação, em uso no COMAER, deverão ser considerados como sigilosos.

3.3.4 Os dados e informações sigilosos, constantes de documento produzido em meio eletrônico, serão assinados e criptografados mediante o uso de certificados digitais emitidos por autoridade certificadora no âmbito do COMAER, respeitando as resoluções da Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil).

3.4 DA SEGURANÇA DA INFORMÁTICA

3.4.1 SEGURANÇA DE **HARDWARE**

3.4.1.1 Qualquer serviço de manutenção a ser executado em computador que contenha assunto sigiloso deverá ser acompanhado pelo responsável por sua utilização.

3.4.1.2 O computador que contenha assunto sigiloso e que necessite de manutenção fora da OM deverá ter o seu disco rígido retirado e guardado em um cofre.

3.4.2 SEGURANÇA DE **SOFTWARE**

3.4.2.1 Deverão ser utilizados apenas os **softwares** adquiridos de fornecedores credenciados ou desenvolvidos pelo COMAER, devidamente licenciados de acordo com a legislação em vigor, ou aqueles de interesse da Instituição, de domínio público, disponíveis na INTERNET para cópia **download**.

3.4.2.2 A instalação dos **softwares** adquiridos de fornecedores credenciados ou desenvolvidos pelo COMAER somente deverá ser realizada pelos setores de Informática existentes nas diversas OM.

3.4.2.3 Todos os arquivos que contenham assuntos sigilosos e os programas em uso deverão possuir cópias de segurança.

3.4.2.4 Deverá ser instalado e atualizado, periodicamente, um sistema antivírus, de modo a evitar a disseminação de vírus e/ou conteúdo impróprio da INTERNET.

3.4.3 SEGURANÇA FÍSICA

3.4.3.1 Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo ultra-secreto somente poderão estar ligados a redes de computadores seguras e que sejam física e logicamente isoladas de qualquer outra.

3.4.3.2 As cópias de segurança dos arquivos contendo assuntos sigilosos, bem como os originais dos programas em uso, deverão estar armazenados em cofres localizados fora dos setores de Informática, a fim de evitar a interrupção do processamento de dados em caso de sinistro ou de sabotagem.

3.4.3.3 Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo secreto, confidencial e reservado só poderão integrar redes de computadores que possuam sistemas de criptografia e segurança adequados à proteção dos documentos.

3.4.3.4 A eliminação de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do órgão a eliminação lógica, deverá ser providenciada a eliminação física por incineração dos dispositivos de armazenamento.

3.4.3.5 O armazenamento de documentos sigilosos, sempre que possível, deve ser feito em mídias removíveis, que podem ser guardadas com maior facilidade.

3.4.3.6 Objetivando melhorar a segurança e a presteza nos trabalhos, o Setor de Informática deverá utilizar, sempre que possível, equipamentos de **no-break** e geradores, para garantir a continuidade da alimentação elétrica.

3.4.4 SEGURANÇA NA INTERNET

3.4.4.1 As páginas eletrônicas deverão estar de acordo com as "Normas para Elaboração de Páginas Eletrônicas pelas OM do Comando da Aeronáutica", na Rede Mundial de Computadores, ou outro instrumento legal que venha a substituí-las.

3.4.4.2 As páginas eletrônicas das OM deverão estar hospedadas nos domínios disponibilizados pelo COMAER.

3.4.4.3 Nenhuma informação sigilosa dos militares da ativa, da reserva/reformado ou dos servidores civis deverá constar das páginas eletrônicas das OM.

3.4.4.3.1 Para fins do que dispõe o item 3.4.4.3, serão consideradas como informações sigilosas: vista aérea da OM, fotografias internas de pontos importantes da OM (paiol, reserva de armamento, etc.), estrutura de comando, peculiaridades do emprego, características técnicas do material de emprego militar, informações pessoais dos integrantes da OM, informações contidas nos Quadros de Organização/Lotação ou de Material, dentre outras.

3.4.4.4 Os computadores que estiverem conectados à INTERNET ou a outras redes com acesso remoto não deverão conter assunto sigiloso, se não forem providos dos recursos de proteção e criptografia adequados e homologados pelo CIAER.

3.4.5 SEGURANÇA NO CORREIO ELETRÔNICO

3.4.5.1 O correio eletrônico (e-mail) somente deverá ser utilizado para o envio de mensagens contendo assunto sigiloso quando for utilizado um sistema criptográfico homologado pelo CIAER.

3.4.5.2 Os certificados digitais deverão ser utilizados com o objetivo de permitir a autenticação e o não-repúdio das mensagens remetidas via correio eletrônico ou **World Wide Web** (www).

3.4.6 SEGURANÇA EM SISTEMAS CORPORATIVOS, INTRAER E REDES LOCAIS

3.4.6.1 Deverão ser estabelecidas senhas individuais e intransferíveis para cada usuário, bem como de acesso para os sistemas e ambientes de rede, as quais deverão ser trocadas, freqüentemente, para dificultar o acesso por pessoa não autorizada a dados sigilosos.

3.4.6.2 O controle de acesso lógico deverá permitir o acesso, em diferentes níveis, de acordo com a "necessidade de conhecer".

3.4.6.3 As operações de inclusão, pesquisa, alteração e exclusão de dados nos Sistemas Corporativos, que contenham dados sigilosos, deverão ser realizadas por pessoas devidamente credenciadas, em diferentes níveis de acesso.

3.4.6.4 Toda a rede local, conectada à INTRAER, que trafegue dados sigilosos, deverá possuir ferramentas capazes de identificar quem acessou e/ou impedir o acesso de pessoas não credenciadas.

3.4.6.5 Toda a rede local, conectada à INTRAER, que trafegue dados sigilosos, deverá possuir ferramentas específicas, mantendo-as sempre atualizadas, capazes de rastrear e emitir relatórios sobre os pontos vulneráveis que poderão ser utilizados como porta de entrada para invasão nos sistemas.

3.4.6.6 A realização de cópias em disquetes ou a inserção de arquivos em redes que contenham assuntos sigilosos somente deverá ocorrer a partir de uma única unidade de disco flexível (drive de 3½) habilitada.

3.4.6.6.1 Procedimento semelhante deverá ser adotado para os copiadores de **CD-ROM** e outros meios que permitam gravação de dados.

3.4.6.7 A pasta PÚBLICO ou similar, normalmente disponível nas redes locais, não deverá ser utilizada com arquivos que contenham assuntos sigilosos.

3.4.7 SEGURANÇA CONTRA FURTO, ROUBO OU EXTRAVIO DE DADOS

3.4.7.1 Não deverá ser utilizado computador portátil, tipo **laptop**, para o trato de assunto sigiloso considerando que:

a) os arquivos apagados do seu disco rígido poderão ser recuperados por pessoa não autorizada, com a utilização de programas específicos; e
b) a segurança do equipamento é relativa, em se tratando dos imprevistos por ocasião do seu transporte.

3.4.7.2 Antes de ausentar-se do local de trabalho, o usuário deverá fechar todos os programas em uso, evitando, dessa maneira, o acesso por pessoas não autorizadas.

3.4.7.3 Os arquivos pessoais, existentes no computador de uso particular, não deverão conter assunto sigiloso.

3.4.7.4 Cuidados especiais deverão ser observados por ocasião das instruções ou palestras fora do ambiente normal de trabalho e que tratem de assunto sigiloso. Após o procedimento descrito, o arquivo original e outros a ele relacionados deverão ser apagados do disco rígido.

3.4.7.4.1 Sempre que possível, deverá ser evitada a utilização do disco rígido para armazenar as palestras, pois, mesmo apagadas, poderão ser recuperadas por pessoas não autorizadas, com a utilização de programas específicos.

3.4.7.4.2 A autorização para a realização de cópias em discos flexíveis, **CD-ROM** ou outros meios de armazenamento é da exclusiva responsabilidade de quem ministrou ou proferiu as palestras.

4 CONTRATOS QUE ENVOLVAM CLÁUSULAS DE SIGILO

4.1 A celebração de contrato cujo objeto seja sigiloso, ou que sua execução implique a divulgação de desenhos, plantas, materiais, dados ou informações de natureza sigilosa, obedecerá aos seguintes requisitos:

a) o conhecimento da minuta de contrato estará condicionado à assinatura de termo de compromisso de manutenção de sigilo (Anexos H, I, J e L) pelos interessados na contratação;
b) a alteração do contrato para inclusão de cláusula de segurança não estipulada por ocasião da sua assinatura;
c) a obrigação do contratado manter o sigilo relativo ao objeto contratado, bem como à sua execução;
d) a obrigação do contratado adotar as medidas de segurança adequadas, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto contratado;
e) a identificação, para fins de concessão de credencial de segurança, das pessoas que, em nome do contratado, terão acesso a material, dados e informações sigilosos; e
f) a responsabilidade do contratado pela segurança (manutenção de sigilo) do objeto subcontratado, no todo ou em parte.

4.2 Cabe aos Comandantes, Chefes e Diretores, a quem os contratantes estejam vinculados, providenciar para que seus fiscais ou representantes adotem as medidas necessárias para a segurança dos documentos ou materiais sigilosos em poder dos contratados ou subcontratados, ou em curso de fabricação em suas instalações.

4.3 Além das medidas estabelecidas neste Regulamento e na NSMA 205-2 "CREDENCIAL DE SEGURANÇA DE PESSOA JURÍDICA", poderão ser expedidas instruções complementares pelo COMAER necessárias à salvaguarda de materiais e/ou documentos sigilosos em poder dos seus contratados ou subcontratados.

4.4 A pessoa física ou jurídica que assina contrato com o COMAER para a execução de trabalho sigiloso torna-se responsável, no âmbito das atividades que estiverem sob o seu controle, pela segurança de todos os assuntos sigilosos ligados ao desenvolvimento do trabalho contratado.

5 MEDIDAS GERAIS DE SEGURANÇA

5.1 Na classificação dos documentos, será utilizado, sempre que possível, o critério menos restritivo possível.

5.2 Compete aos Comandantes, Chefes e Diretores exigir Termo de Compromisso de Manutenção de Sigilo dos militares e civis pertencentes ao seu efetivo e empregados de empresas contratadas que, direta ou indiretamente, tenham acesso a dados ou informações sigilosos.

5.3 Os militares e civis pertencentes ao efetivo do COMAER, cientes do item 5.2, comprometer-se-ão a não revelar ou divulgar dados ou informações sigilosos dos quais tiveram conhecimento no exercício de cargo, função ou emprego público, mesmo após terem sido desligados.

5.4 Os responsáveis pela custódia de documentos e de materiais e pela segurança de áreas, de instalações ou de Sistemas de Tecnologia da Informação de natureza sigilosa sujeitam-se às normas referentes ao sigilo profissional, em razão do ofício, e ao seu código de ética específico, sem prejuízo de sanções penais.

5.5 Compete aos Comandantes, Chefes e Diretores promover o treinamento, a capacitação, a reciclagem e o aperfeiçoamento de pessoal que desempenhe atividades inerentes à salvaguarda de documentos, materiais, áreas, instalações e Sistemas de Tecnologia da Informação de natureza sigilosa.

5.6 O conhecimento de assunto sigiloso depende da função desempenhada pela pessoa e não de seu grau hierárquico, posição ou precedência.

5.7 Toda e qualquer pessoa vinculada ao COMAER que tome conhecimento de assunto sigiloso fica, automaticamente, responsável pela manutenção do seu sigilo.

5.8 Verificando-se qualquer ocorrência que possa implicar o comprometimento de assunto sigiloso, a autoridade competente deverá tomar as providências necessárias para sanar a deficiência, verificar a extensão do comprometimento e apurar as responsabilidades.

5.9 Qualquer pessoa vinculada ao COMAER que tenha conhecimento de uma situação na qual um assunto sigiloso possa estar ou venha a ser comprometido participará tal fato ao seu Chefe imediato e/ou à autoridade responsável.

6 DISPOSIÇÕES FINAIS

Os casos não previstos deverão ser submetidos ao Comandante da Aeronáutica, mediante proposta a ser encaminhada ao Centro de Inteligência da Aeronáutica.

Anexo A - Modelo de Termo de Custódia de Documento Sigiloso Controlado/Material Sigiloso Controlado (DSC/MSC)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE CUSTÓDIA DE
(DOCUMENTOS E/OU MATERIAIS) SIGILOSOS CONTROLADOS
Nº ____/____

Em cumprimento ao disposto no item _____ do RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", declaro que, ao(s) _____ dia(s) do mês de _____ do ano de dois mil e _____, passei a ser custodiante do(s) Documento(s) e/ou Material(is) Sigiloso(s) Controlado(s) abaixo relacionados:

Documento / Material Sigiloso Controlado	Número	Órgão Controlador

_____, ____ de _____ de _____.

_____
(Nome completo, Posto e Função do detentor)

GRAU DE SIGILO COMPATÍVEL

Anexo B - Modelo de Termo de Inventário de Documento Sigiloso Controlado/Material Sigiloso Controlado (DSC/MSC)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE INVENTÁRIO DE (DOCUMENTOS E/OU MATERIAIS) SIGILOSOS CONTROLADOS Nº ____/____

Inventário do(s) **(DOCUMENTOS E/OU MATERIAS)** Sigilosos Controlados pelo(a) _____(ÓRGÃO CONTROLADOR), nos termos do item _____ do RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)".

Documento / Material Sigiloso Controlado	Número

_____, ____ de _____ de _____.

_____
(Nome completo, Posto e Função do detentor)

Testemunhas:

_____
(Nome completo, Posto e Função)

_____
(Nome completo, Posto e Função)

GRAU DE SIGILO COMPATÍVEL

Anexo C - Modelo de Termo de Transferência de Guarda de Documento Sigiloso Controlado/Material Sigiloso Controlado (DSC/MSC)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE TRANSFERÊNCIA DE GUARDA DE
(DOCUMENTOS E/OU MATERIAIS) SIGILOSOS CONTROLADOS
Nº ____/____

Ao(s) _____ dia(s) do mês de _____ do ano de dois mil e _____, em cumprimento ao disposto no item _____ do RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", reuniram-se na(o) **(OM DETENTORA)** o Sr _____, substituído, e o Sr _____, substituto, para conferir os (Documentos e/ou Materiais) Sigilosos Controlados, produzidos e recebidos pela(o) _____, então sob a custódia do primeiro, constantes do Termo de Inventário nº _____/___, anexo ao presente Termo, os quais, nesta data, passam para a custódia do segundo.

Cumpridas as formalidades exigidas e conferidas todas as peças constantes do Termo de Inventário, foram julgadas (conforme ou com as seguintes alterações), sendo, para constar, lavrado o presente Termo de Transferência, em 4 (quatro) vias, datadas e assinadas pelo substituído e pelo substituto.

_____, ____ de _____ de _____.

_____
(Nome completo, Posto e Função do substituído)

_____
(Nome completo, Posto e Função do substituído)

GRAU DE SIGILO COMPATÍVEL

Anexo D - Modelos de carimbos para classificação sigilosa de documentos

Anexo E - Modelo de carimbo para a cópia de documento sigiloso

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

Ofício nº _____/SEÇÃO/_____ _____, ___ de _____ de ____.

Do
Ao

Assunto: ..... .

Ref : 1 - .....; e
2 - ..... .

Anexos: A - .....; e
B - ..... .

1. _____
_____
_____
_____

2. _____
_____
_____
_____

3 _____
_____
_____

A14087B

GRAU DE SIGILO COMPATÍVEL

Anexo F - Modelo de Termo de Eliminação de Cópia(s) de Documento Sigiloso Controlado (DSC)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE ELIMINAÇÃO DE CÓPIA(S) DE DOCUMENTO SIGILOSO CONTROLADO
Nº ____/___

Ao(s) ____ dia(s) do mês de _____ do ano de dois mil e ____, em cumprimento ao disposto no RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", reuniram-se no(a) _____ o Sr _____, o Sr _____, e o Sr _____, os dois últimos como testemunhas, para proceder à eliminação da(s) cópia(s) do(s) Documento(s) Controlado(s) (DSC), pelo(a) _____.

Cumprido o procedimento previsto no RCA 205-1, foi(ram) eliminada(s) a(s) cópia(s) do DSC abaixo discriminada(s):

Documento Sigiloso Controlado	Exemplar Número

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.

_____, ____ de _____ de _____.

AUTORIDADE QUE CLASSIFICOU O ORIGINAL:

_____
(Nome completo, Posto, Identidade e Função)

TESTEMUNHAS:

_____
(Nome completo, Posto, Identidade e Função)

_____
(Nome completo, Posto, Identidade e Função)

GRAU DE SIGILO COMPATÍVEL

Anexo G - Modelo de Termo de Eliminação de Material Sigiloso Controlado (MSC)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE ELIMINAÇÃO DE MATERIAL SIGILOSO CONTROLADO
Nº ____/___

Ao(s) ____ dia(s) do mês de _____ do ano de dois mil e ____, em cumprimento ao disposto no RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", reuniram-se no(a) _____
o Sr _____,
o Sr _____,
e o Sr _____,
os dois últimos como testemunhas, para proceder à eliminação do(s) Material(is) Sigiloso(s) Controlado(s) (MSC), pelo(a) _____, conforme autorização contida no(a) _____.

Cumpridos os procedimentos previstos no RCA 205-1, foi(ram) eliminado(s) o(s) MSC abaixo discriminado(s):

Material Sigiloso Controlado	Número de Série

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

_____, ____ de _____ de _____.

DETENTOR:

_____
(Nome completo, Posto, Identidade e Função)

TESTEMUNHAS:

_____
(Nome completo, Posto, Identidade e Função)

_____
(Nome completo, Posto, Identidade e Função)

GRAU DE SIGILO COMPATÍVEL

Anexo H - Modelo de Termo de Compromisso de Manutenção do Sigilo (Militar)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO (MILITAR)

Eu, _____, identidade _____, do(a) _____, nos termos do item _____ do RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", declaro que tenho pleno conhecimento de minha responsabilidade no que concerne ao sigilo que deve ser mantido sobre as atividades desenvolvidas ou as ações realizadas no(a) _____, bem como sobre todas as informações que, por força de minha função ou eventualmente, venham a ser do meu conhecimento, comprometendo-me a guardar o sigilo necessário a que sou obrigado nos termos da legislação vigente.

_____, ____ de _____ de _____.

_____
(Nome completo, Posto e Identidade)

GRAU DE SIGILO COMPATÍVEL

Anexo I - Modelo de Termo de Compromisso de Manutenção do Sigilo (Servidor Civil)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO

Eu, _____, identidade _____, do(a) _____, nos termos do item _____ do RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", declaro que tenho pleno conhecimento de minha responsabilidade no que concerne ao sigilo que deve ser mantido sobre as atividades desenvolvidas ou as ações realizadas no(a) _____, bem como sobre todas as informações que, por força de minha função ou eventualmente, venham a ser do meu conhecimento, comprometendo-me a guardar o sigilo necessário a que sou obrigado nos termos da legislação vigente.

_____, ____ de _____ de _____.

_____
(Nome completo e Matrícula)

Anexo J - Modelo de Termo de Compromisso de Manutenção do Sigilo (Representante da Empresa/Órgão Contratado/Conveniado)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO

Eu, _____, identidade _____, do(a) _____, nos termos do RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", declaro que tenho pleno conhecimento de minha responsabilidade, junto ao _____, para adotar as medidas de segurança adequadas, no âmbito das atividades sob meu controle, no que concerne à manutenção do sigilo relativo ao _____, bem como sobre todas as informações que, por força de minha função ou eventualmente, venham a ser do meu conhecimento, comprometendo-me a guardar o sigilo necessário a que sou obrigado nos termos da legislação vigente.

_____, ____ de _____ de _____.

_____.
(Nome completo, Identidade, CPF e Função)

Anexo L - Modelo de Termo de Compromisso de Manutenção do Sigilo (Funcionário da Empresa/Órgão Contratado/Conveniado)

GRAU DE SIGILO COMPATÍVEL

(CABEÇALHO PADRÃO DE OFÍCIO DEFINIDO PELO CENDOC)

TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO

Eu,_____, identidade _____, do(a) _____, nos termos do RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica (RSAS)", declaro que tenho pleno conhecimento de minha responsabilidade, junto ao _____, para adotar as medidas de segurança adequadas, no âmbito das atividades sob meu controle, no que concerne à manutenção do sigilo relativo ao _____, bem como sobre todas as informações que, por força de minha função ou eventualmente, venham a ser do meu conhecimento, comprometendo-me a guardar o sigilo necessário a que sou obrigado nos termos da legislação vigente.

_____, ____ de _____ de _____.

_____
(Nome completo, Identidade, CPF e Função)

GRAU DE SIGILO COMPATÍVEL

ÍNDICE