

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



SEGURANÇA

FCA 200-5

**GUIA PRÁTICO DE EXECUÇÃO DAS MEDIDAS DO
REGULAMENTO PARA SALVAGUARDA DE
ASSUNTOS SIGILOSOS DA AERONÁUTICA**

2010

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



SEGURANÇA

FCA 200-5

**GUIA PRÁTICO DE EXECUÇÃO DAS MEDIDAS DO
REGULAMENTO PARA SALVAGUARDA DE
ASSUNTOS SIGILOSOS DA AERONÁUTICA**

2010



**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**

PORTARIA Nº 2, DE 20 DE MAIO DE 2010.

Aprova a edição do Folheto que dispõe sobre a prática das medidas do Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica.

O CHEFE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA, tendo em vista o disposto no Inciso II, do art. 4º do Regulamento do Centro de Inteligência da Aeronáutica, aprovado pela Portaria nº C-7/GC3, de 27 de setembro de 2005, resolve:

Art. 1º Aprovar a edição do FCA 200-5 “Guia Prático de Execução das Medidas do Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica”, que com esta baixa.

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

Brig Ar PAULO AFONSO PINHEIRO LARI
Chefe do CIAER

(Publicado no BCA nº 107, de 10 de junho de 2010)

SUMÁRIO

PREFÁCIO

1 DISPOSIÇÕES PRELIMINARES	9
1.1 <u>FINALIDADE</u>	9
1.2 <u>CONCEITUAÇÃO E PADRONIZAÇÃO</u>	9
1.3 <u>ÂMBITO</u>	12
2 SIGILO E SEGURANÇA	13
2.1 <u>CLASSIFICAÇÃO SEGUNDO O GRAU DE SIGILO</u>	13
2.2 <u>RECLASSIFICAÇÃO E DESCLASSIFICAÇÃO</u>	14
2.3 <u>DOCUMENTOS E MATERIAIS SIGILOSOS CONTROLADOS</u>	14
2.4 <u>MARCAÇÃO</u>	16
2.5 <u>EXPEDIÇÃO E COMUNICAÇÃO DE DOCUMENTOS SIGILOSOS</u>	17
2.6 <u>REGISTRO, TRAMITAÇÃO E GUARDA</u>	19
2.7 <u>SEGURANÇA NA PRODUÇÃO</u>	20
2.8 <u>REPRODUÇÃO</u>	20
2.9 <u>AValiação e PRESERVAÇÃO</u>	21
2.10 <u>SEGURANÇA NO ARQUIVAMENTO</u>	21
2.11 <u>SEGURANÇA NA PRESERVAÇÃO</u>	21
2.12 <u>ACESSO</u>	22
2.13 <u>ÁREAS E INSTALAÇÕES SIGILOSAS</u>	23
2.14 <u>SEGURANÇA FÍSICA</u>	24
3 SEGURANÇA DA INFORMAÇÃO	30
3.1 <u>SEGURANÇA DO <i>HARDWARE</i></u>	30
3.2 <u>SEGURANÇA DO <i>SOFTWARE</i> E DE INTERNET</u>	30
4 MEDIDAS GERAIS DE SEGURANÇA	31
5 DISPOSIÇÕES FINAIS	32

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 folheto visa dar praticidade às medidas preconizadas no Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica baseadas nos Decretos nº 4.553, de 27 de dezembro de 2002 e nº 5.301, de 09 de dezembro de 2004.

Com a edição deste documento pretende-se padronizar, no âmbito do COMAER, a execução das medidas adequadas no trato de matéria sigilosa.

Sabe-se da ampla variedade de instalações e atividades que há no COMAER, além da grande gama de situações e ambientes nas quais tais instalações e atividades estão inseridas. Pretende-se, dentro da viabilidade, que tais medidas sejam igualmente implementadas respeitando-se, porém, as particularidades e limitações de cada organização.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

O presente Folheto tem por finalidade elucidar e padronizar, no âmbito do Comando da Aeronáutica (COMAER), os procedimentos regulamentados por meio do RCA 205-1 – Regulamento para a Salvaguarda de Assuntos Sigilosos (RSAS).

1.2 CONCEITUAÇÃO E PADRONIZAÇÃO

1.2.1 ÁREA SIGILOSOSA

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 CLASSIFICAÇÃO E DEMARCAÇÃO

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

A demarcação de áreas deverá ser condizente com os conteúdos e atividades nelas executadas e deve estar aparente e disposta de forma padronizada. Não deverão ser utilizadas outras denominações, tais como: **área restrita ou área sensível**. As denominações devem ser as constantes na legislação, quais sejam: RESERVADA, CONFIDENCIAL, SECRETA ou ULTRASSECRETA.

1.2.3 MEIO DE COMUNICAÇÃO SIGILOSOSA

Aquele no qual se transmitem dados, informações e/ou conhecimentos sigilosos e, portanto requer dispositivos de criptografia para sua utilização. Não fazem parte desses meios os Telefones Vermelhos (RTCAER), a INTRAER, telefones celulares, funcionais ou não, telefones comerciais, aparelhos de fax, entre outros.

No COMAER, são meios de comunicação sigilosos apenas: as redes MERCÚRIO e INTRAGAR, o sistema VOIP provido pelo CIAER para os adidos no exterior e o Telefone Seguro (TSG), com o módulo de segurança ativado, conectado a outro TSG com o seu modo seguro também ativado.

1.2.4 RECLASSIFICAÇÃO

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

O conhecimento classificado pode, assim, ter seu grau de sigilo aumentado ou diminuído, por meio de reclassificação, conforme preconizado pela ICA 200-9 Avaliação de Documentos Sigilosos na Aeronáutica, de 2010.

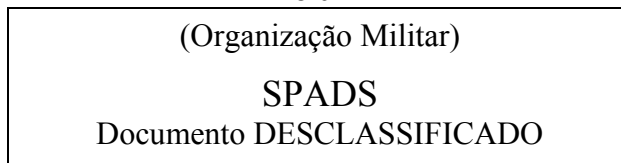
A indicação da reclassificação ou da desclassificação de documentos sigilosos deverá constar da capa, se houver, e da primeira página do documento, mediante aposição de carimbo, de forma que não prejudique os dados, informações ou conhecimentos registrados.

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

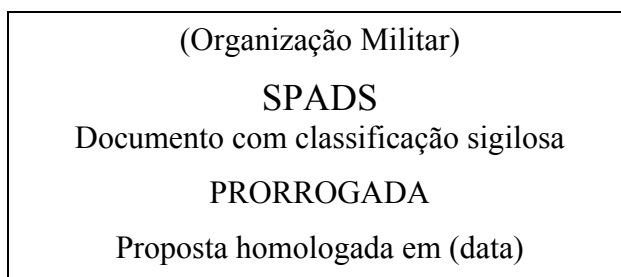
Quando for necessário reclassificar documentos sigilosos do mesmo tipo, reunidos em maço ou pasta, basta colocar, na primeira página, a anotação autenticada. Caso seja necessário destacar algum documento para uso isolado, este receberá idêntica anotação.

Modelos de carimbos para reclassificação e desclassificação de documentos sigilosos.

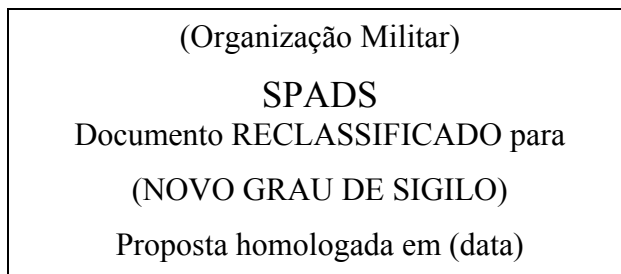
8 cm



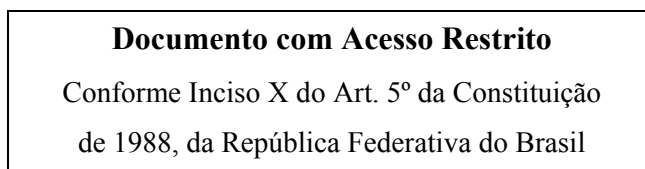
Carimbo 1



Carimbo 2



Carimbo 3



Carimbo 4

1.2.5 COMPARTIMENTAÇÃO

É o resultado desejado das medidas que restringem o acesso de pessoas a conhecimentos e/ou dados sigilosos àquelas que efetivamente tenham necessidade de conhecê-los e que, além disso, possuam, obrigatoriamente, credencial de segurança no grau adequado.

A credencial de segurança não habilita, automaticamente, seu detentor a ter acesso a todos os assuntos sigilosos até o respectivo grau de sigilo. É imprescindível que haja a necessidade de conhecer determinado assunto (por estar envolvido em algum tipo de trabalho, análise, ação ou acompanhamento do mesmo). Este é o fundamento da compartimentação e deve ser rigorosamente observado sob pena de haver comprometimentos ou vazamentos que inviabilizem ou prejudiquem determinadas linhas de ação que estejam sendo planejadas.

1.3 ÂMBITO

O presente folheto aplica-se a todas as OM do COMAER. Pode, 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 As áreas, os dados ou informações e os materiais sigilosos serão classificados em ULTRASSECRETOS, SECRETOS, CONFIDENCIAIS e RESERVADOS, em razão do seu teor ou dos seus elementos intrínsecos.

2.1.2 Quando da classificação deve-se adotar o menor grau de sigilo possível, em função do nível de segurança que se deseja atingir, com vistas a evitar entraves desnecessários quanto ao acesso àqueles dados ou informações, por parte daqueles que têm necessidade de conhecê-los. Frequentemente incorre-se no erro de atribuir grau de sigilo mais elevado que o necessário, banalizando, assim, as medidas de segurança decorrentes da classificação.

2.1.3 Inicialmente atribui-se um grau de sigilo julgado suficiente e que, se for necessário, poderá posteriormente ser aumentado por quem classificou ou por autoridade hierarquicamente superior e competente para dispor sobre o assunto.

2.1.4 São usualmente passíveis de classificação como ULTRASSECRETOS, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares reais de cunho estratégico, às relações internacionais do Estado brasileiro, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse estratégico (ex: projeto do submarino nuclear, de uma nova aeronave de combate, de um satélite militar, de desenvolvimento de armamento de uso estratégico, de bomba nuclear, de mísseis de longo alcance, projetos científicos de tecnologia dual de vanguarda, etc) e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

2.1.5 São passíveis de classificação como SECRETOS, dentre outros, dados ou informações referentes a sistemas (ex: criptografia no COMAER, TSG no MD, satélite de comunicações militares, aquisições de meios estratégicos, operações militares reais de caráter tático, etc), instalações (ex: laboratórios de alta tecnologia no CTA, centros de lançamentos de veículos espaciais, salas de servidores centrais de redes INTRAER, MERCÚRIO, etc), 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.

2.1.6 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 (ex: relatórios de inspeções de segurança, codificações de uso operacional militar, frequências de radares, disponibilidade de meios aéreos e terrestres de combate ou apoio ao combate, estoques de combustível ou de suprimento aeronáutico, políticas nacionais de cunho estratégico, etc).

2.1.7 São passíveis de classificação como RESERVADOS dados ou informações, de qualquer espécie, que não devam ser de conhecimento público (ex: manuais doutrinários de voo, ordens de instrução, tabelas de emprego armado de aeronaves, frequências de comunicação de uso militar, escalas de voo e de serviço de alerta de defesa aérea, distribuição de efetivos, etc) pelo potencial de risco que possa oferecer aos meios materiais e humanos do COMAER em função do uso que possa fazer delas um agente adverso cujos interesses sejam contrários aos interesses da Organização e do País.

2.1.8 As informações que, de alguma forma, possam atingir o resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas poderão ser classificadas como RESERVADAS ou CONFIDENCIAIS, dependendo das circunstâncias nas quais estiverem envolvidas, devendo, porém, possuir alguma classificação.

2.1.9 Os documentos de inteligência, dependendo do assunto, podem ser classificados em qualquer grau desde que não contrariem o previsto pela legislação em vigor.

2.2 RECLASSIFICAÇÃO E DESCLASSIFICAÇÃO

2.2.1 Os procedimentos para reclassificação e desclassificação de documentos sigilosos, além de outras providências, devem seguir o preceituado na ICA 200-9 Avaliação de Documentos Sigilosos na Aeronáutica, de 2010.

2.3 DOCUMENTO E MATERIAL SIGILOSOS CONTROLADOS

2.3.1 Documentos e Materiais Sigilosos Controlados (DSC/MSC) são aqueles que, por sua importância, requerem medidas adicionais de controle.

2.3.1.1 Deve ser feita identificação dos destinatários, em protocolo e recibo próprios, quando da difusão. Deverá seguir junto com o DSC/MSC um recibo discriminando o conteúdo que está sendo enviado e o destinatário que deve recebê-lo, de forma que esse último dê a quitação e retorne o recibo para o remetente. Tudo deve ser devidamente protocolado.

2.3.1.2 Deve ser feita a lavratura de Termo de Custódia e registro em protocolo específico. Será o usado o Termo de Custódia quando o Detentor recebe um DSC/MSC e necessita deixá-lo em outro setor da OM. Tal termo é útil para que o Detentor seja eximido de responsabilidade no caso de furto, roubo ou extravio do DSC/MSC, pois, para os efeitos legais, a responsabilidade pelo DSC/MSC é do Detentor. Vale frisar que a lavratura desse termo é um ato interno para controle da OM que detém o DSC/MSC, não sendo necessário o envio deste para a OM expedidora do DSC/MSC, pois, para a OM difusora, o responsável sempre será o Detentor e não o Custodiante.

2.3.1.3 O prazo para a lavratura anual de termo de inventário é 30 de julho, pelo órgão ou entidades receptoras. Anualmente, as OM devem enviar um Termo de Inventário, de todos os DSC/MSC que possuírem, para as OM que expediram os DSC/MSC. Vale frisar que os termos de cada DSC/MSC serão enviados, respectivamente, para as OM que os expediram. Por exemplo: se o OI tem sob a sua responsabilidade dois DSC - o **A**, expedido pela OM “X”, e o **B**, expedido pela OM “Y” - deverão ser enviados dois Termos de Inventário. Nesse caso, do DSC **A** para a OM “X” e do DSC **B** para a OM “Y”. Não são remetidos ao CIAER termos de inventários de DSC/MSC que não haja sido expedido pelo CIAER, e assim respectivamente.

2.3.1.4 O Termo de Inventário será assinado pelo Detentor do DSC/MSC e por duas testemunhas. O Detentor natural é o Comandante/Chefe/Diretor da OM que delega a competência ao Chefe da SI que, por sua vez, será o responsável imediato pela assinatura do Termo do Inventário. O termo não poderá ser assinado, no impedimento, por uma outra pessoa, uma vez que a delegação de competência não permite tal situação, ou seja, o Termo de Inventário deverá ser assinado pelo detentor (Chefe da SI) ou pelo próprio Comandante/Chefe/Diretor da OM. As testemunhas deverão ser pessoas do próprio setor, credenciadas no nível do DSC/MSC em questão.

2.3.1.5 Deverá ser enviado o Termo de Inventário toda vez em que houver transferência da guarda de DSC/MSC. Tal situação é comum quando há TROCA do Detentor do DSC/MSC.

2.3.1.6 A expedição do Termo de Inventário para a OM difusora, deve ser feita por meio de ofício, via Rede Mercúrio. Mesmo que o DSC/MSC esteja em outro local da OM, que não seja a SI, a responsabilidade pelo envio do termo será sempre do Detentor.

2.3.1.7 Deverá ser feita a lavratura de Termo de Transferência, sempre que se proceder à transferência de custódia ou guarda de DSC/MSC, sendo assinado pelo Detentor substituto e pelo substituído.

2.3.1.8 O Termo de Transferência será expedido em quatro vias, sendo que, conforme dispõe o item 2.6.8 do RSAS, a primeira será enviada, juntamente com um Termo de Inventário atualizado, ao órgão expedidor do DSC/MSC, a segunda ficará arquivada no setor que tem a custódia do documento e as demais com os Detentores substituto e substituído. Vale frisar que o Termo de Inventário será assinado pelo novo detentor, para que este tenha a plena consciência do DSC/MSC que está recebendo.

2.3.2 Os sistemas e os materiais criptográficos ou criptofônicos deverão ser guardados em locais distintos de seus manuais de utilização ou senhas. Os locais (salas e dispositivos de armazenamento) devem obedecer aos requisitos previstos para cada grau de sigilo considerado.

2.3.3 As áreas sigilosas devem respeitar no mínimo, as seguintes especificações:

- a) possuir paredes e tetos de alvenaria, em boas condições de resistência, ou de material que ofereça resistência igual ou superior à alvenaria.
- b) as janelas, se houver, devem possuir vidros de segurança com malha metálica interna e/ou grades de segurança que impeçam o acesso ao ambiente.
- c) não deve haver passagens liberáveis, tais como: aberturas para condicionadores de ar (exceto tipo *split*), forro do teto e sala adjacente que não possua as mesmas características.
- d) a porta de acesso deve possuir resistência a arrombamentos manuais e fechaduras de segurança, preferencialmente de segredo de quatro ou cinco combinações, mecânica ou eletromecânica, de qualidade reconhecida.



Figura 1: Exemplos de fechaduras e porta de segurança.

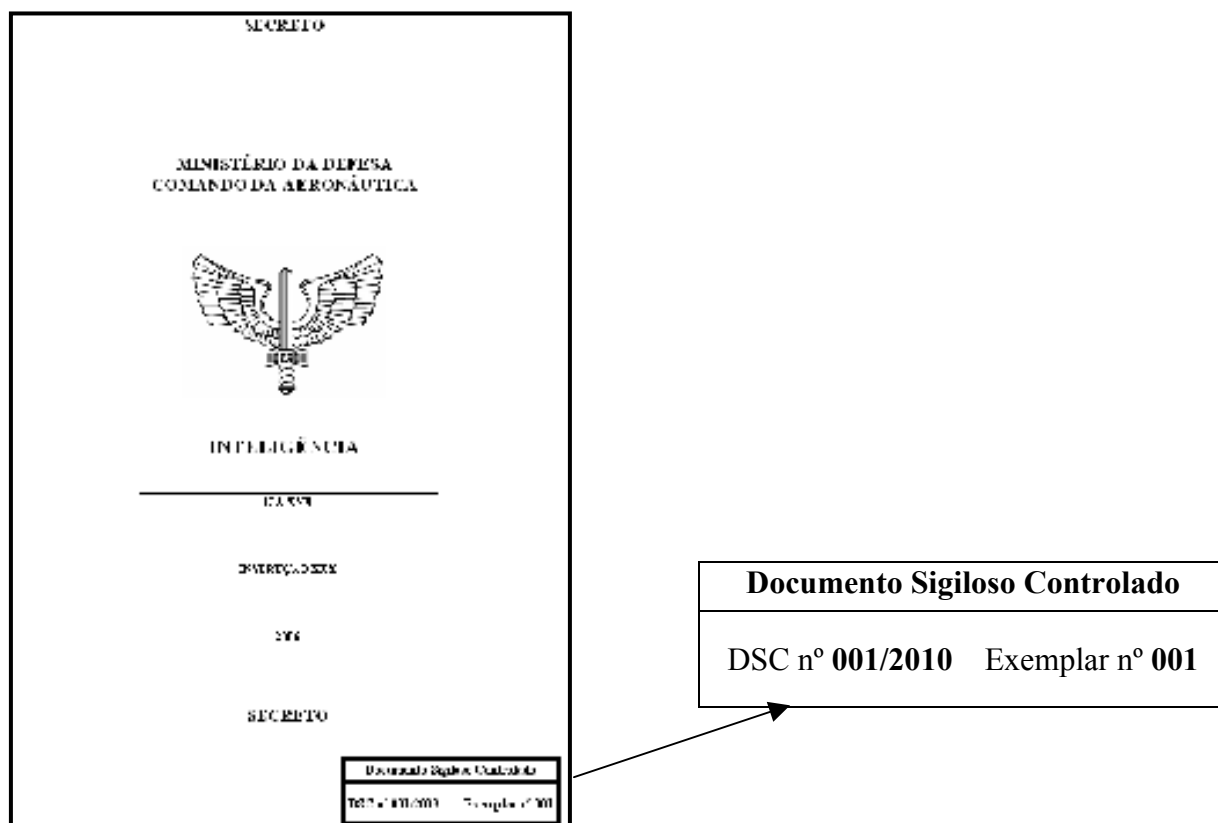
- e) deve haver sensores de movimento, dispositivos eletrônicos de vigilância com alarmes de intrusão e senhas de acesso.

2.3.4 Sempre que ocorrer furto, roubo, extravio ou suspeita de comprometimento de DSC/MSC deve-se proceder à devida investigação (Sindicância ou IPM), 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, cíveis e administrativas decorrentes.

2.3.5 O assunto DSC/MSC ainda está muito focado na documentação, portanto faz-se necessário esclarecer que, além dos documentos já mencionados, há muitos equipamentos e materiais sigilosos que são caracterizados como MSC e, portanto, merecem igual tratamento

2.4 MARCAÇÃO

2.4.1 Um DSC terá em todas as páginas, inclusive na capa, além da marcação de grau de sigilo, a expressão “Documento Sigiloso Controlado”, o número do DSC e o do Exemplar, conforme exemplo abaixo:



2.4.1.1 O CIAER recomenda que tal marcação seja feita, no canto inferior direito, por meio de carimbo com a numeração do DSC e do Exemplar feitas manualmente, pois é mais eficaz para se detectar e analisar adulterações ou vazamentos.

2.4.1.2 O número do DSC é sequencial durante o ano, por exemplo: se a OM faz o primeiro DSC em 2010, será o DSC nº 001/2010. Já o número de Exemplar é aquele que vai controlar a difusão do DSC. Veja como ficaria uma lista de difusão hipotética de certo DSC para cinco OM diferentes:

Difusão do DSC nº 001/2010

Exemplar nº 001.....AFA
Exemplar nº 002.....BAAN
Exemplar nº 003.....BABR
Exemplar nº 004.....BABV
Exemplar nº 005.....BACO

2.4.2 A marcação do grau de sigilo deverá ser feita em todas as páginas e capas do documento sendo que se pode utilizar carimbo, em documentos não digitalizados, ou inserção digital em documento digitalizado.

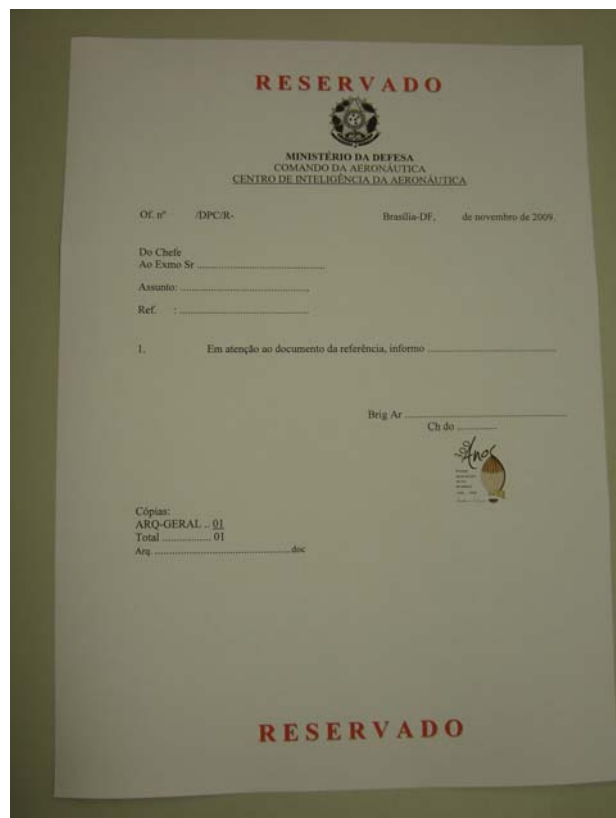
A image shows a document template for marking the level of secrecy. At the top, the word "RESERVADO" is printed in red. Below it is the coat of arms of Brazil, followed by the text "MINISTÉRIO DA DEFESA", "COMANDO DA AERONÁUTICA", and "CENTRO DE INTELIÊNCIA DA AERONÁUTICA". The document includes fields for "Of. nº", "DPCR", "Brasília-DF", and "de novembro de 2009". There are also fields for "Do Chefe", "Ao Exmo Sr.", "Assunto", and "Ref.". A section labeled "1." contains the text "Em atenção ao documento da referência, informo". To the right of this section, there are fields for "Brig Ar" and "Ch do". Below these fields, there is a small circular stamp with a signature. At the bottom left, there is a section for "Cópias:" with sub-entries "ARQ-GERAL... 01", "Total... 01", and "Arq... doc". The word "RESERVADO" is printed in red at the bottom of the document.

Figura 2: Modelo de marcação de sigilo

2.5 EXPEDIÇÃO DE DOCUMENTOS SIGILOSOS

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

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

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

- a) serão acondicionados em envelopes duplos. Envelopes opacos (usualmente de papel pardo, mais resistente), um dentro do outro, de tamanhos adequados ao documento e à inserção do envelope interno no externo;



Figura 3: Envelopamento duplo de documento sigiloso.

- b) no envelope externo, não constará qualquer indicação do grau de sigilo ou do teor do documento, apenas os dados do remetente e do destinatário;



Figura 4: Envelope externo de documento sigiloso.

- c) no envelope interno, serão escritos (por etiqueta autocolante ou digitação no próprio envelope) os dados do destinatário, do remetente, o grau de sigilo e as referências do documento sem constar o assunto. O grau de sigilo do documento será registrado em cor contrastante, usualmente vermelha, nas duas extremidades das aberturas e em ambos os lados de modo a ser identificado logo que removido o envelope externo;



Figura 5: Envelope interno de documento sigiloso.

- d) o envelope externo 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 escrita a palavra pessoal no envelope interno.

2.5.4 Os Documentos ou Materiais Sigilosos Controlados (DSC/MSD), 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 meio de portador credenciado.

2.6 REGISTRO, TRAMITAÇÃO E GUARDA

2.6.1 Cabe aos responsáveis pelo recebimento de documentos sigilosos:

- a) verificar a integridade e registrar (no próprio recibo e em protocolo específico), 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.



Figura 6: Exemplos de violações de envelopes.

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

2.6.2.1 Envelopes contendo a marca “PESSOAL” só poderão ser abertos pelo próprio destinatário. Por exemplo, dados ou informações referentes a resultados de inspeção de saúde, vencimentos, processos judiciais, etc.

2.6.3 O destinatário de documento sigiloso comunicará imediatamente ao remetente qualquer indício de violação ou adulteração do documento. Essa comunicação de violação ou irregularidade visa à apuração, com a maior celeridade possível, dos envolvidos no trâmite do documento. A seguir o responsável pela violação ou adulteração deverá ser identificado para que se possa investigar se houve comprometimento e/ou vazamento.

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

2.6.5 Os agentes responsáveis pela guarda ou custódia de documentos ou materiais sigilosos os transmitirão a seus substitutos, devidamente conferidos, quando da passagem de função ou transferência de responsabilidade. A transmissão de guarda ou custódia de documentos e/ou materiais sigilosos é documentada por meio de termos próprios, cujos modelos encontram-se anexos ao RSAS.

2.7 SEGURANÇA NA PRODUÇÃO

2.7.1 A todo documento, em fase de produção, deverá ser atribuído um grau de sigilo preliminar. Esse grau de sigilo deve estar em conformidade com a necessidade e todo material que estiver envolvido na confecção desse documento (rascunhos, arquivos, cópias, etc) deverá receber o mesmo grau de sigilo preliminar. Depois de concluído, o documento deverá ter seu grau de sigilo retificado ou ratificado.

2.7.2 Os materiais utilizados na confecção devem ser destruídos, pois estes componentes, após a produção do documento sigiloso em sua versão final, acabam se convertendo em fragmentos que podem ser utilizados por elementos adversos para a reprodução de parte ou de todo o documento finalizado e conseqüentemente ao seu conteúdo.

2.8 REPRODUÇÃO

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

2.8.2 Da mesma forma, cópias em máquinas xerox devem ser acompanhadas e feitas por pessoal credenciado ou pelos próprios detentores do documento a ser copiado. Os rejeitos das cópias devem ser retirados imediatamente e destruídos pelo detentor do documento.

2.8.3 Não deve existir chip de memória em copiadoras de documentação sigilosa. As máquinas devem estar sinalizadas como adequadas, ou não, a efetuarem cópias sigilas.

2.8.4 A reprodução total ou parcial de documentos sigilosos controlados condiciona-se à autorização expressa da autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto. Isto quer dizer que a responsabilidade pela

reprodução não autorizada de todo ou parte de Documento Sigiloso Controlado recai sobre seu custodiante. Este é o fundamento da elaboração do Termo de Custódia de DSC, o qual será assinado pelo custodiante e remetido à autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto.

2.9 AVALIAÇÃO E PRESERVAÇÃO

2.9.1 A CPADS e as SPADS previstas no Decreto nº 4.553, de 2002, têm suas atribuições e sistemática de trabalho reguladas pela ICA 200-9 Avaliação de Documentos Sigilosos na Aeronáutica, de 2010.

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

2.10 SEGURANÇA NO ARQUIVAMENTO

2.10.1 Os documentos sigilosos serão guardados em locais adequados, conforme legislação em vigor, que permitam sua integridade, disponibilidade e confidencialidade.

2.10.2 Para a guarda de documentos ultrassecretos e secretos, é obrigatório, no mínimo, o uso de cofre com segredo de três combinações ou material que ofereça segurança equivalente ou superior. Os cofres deverão ser aprovados pelo INMETRO, ou outra entidade certificadora federal, e devem garantir a preservação dos seus conteúdos quanto aos fatores de umidade, temperatura e radiações eletromagnéticas.

2.10.3 Para a guarda de documentos confidenciais e reservados é compulsório, no mínimo, o uso de arquivo de aço e com fechadura de segredo ou chave que ofereça resistência a arrombamentos com ferramentas portáteis.

2.11 SEGURANÇA NA PRESERVAÇÃO

2.11.1 Deverão ser estabelecidos procedimentos relativos à preservação da documentação sigilosa em situações normais e de emergência, como sinistro, calamidades ou evacuação de emergência por riscos à segurança (invasão, bombardeio, atentados, etc). Essas medidas requerem o estabelecimento antecipado de prioridades e responsabilidades.

2.11.2 É imperativo que haja procedimentos claros, padronizados, relativos à evacuação da documentação sigilosa em situações de emergência. Estas ações requerem o estabelecimento de prioridades e responsabilidades para situações de sinistros. Devem estar determinados locais específicos para acolher a documentação recuperada. Deve haver dispositivos recuperáveis de memória – HD externo – que possam carregar de forma rápida prática os arquivos essenciais. Deve haver containeres especiais, resistentes à umidade, esforços mecânicos e resistentes a fogo para evacuação do material sigiloso, tais como: bolsas de couro impermeabilizado ou nylon resistente (tipo *safety-bag*, malote de segurança, etc), tratados com retardantes de fogo e com dispositivos de trancamento a cadeado e/ou lacres de segurança.



Figura 7: Exemplo de dispositivos para evacuação de material sigiloso.

2.11.3 As medidas referidas acima devem estar escritas no Plano de Segurança Orgânica (PSO) de cada OM e devem ser treinadas e **testadas** anualmente. Os setores envolvidos devem possuir o material adequado para a execução de tais medidas e deve haver determinação prévia das responsabilidades de cada componente do setor.

2.12 ACESSO

2.12.1 O acesso ao assunto sigiloso é estritamente funcional e independe de grau hierárquico. Não obstante, é obrigatório o credenciamento de segurança compatível, de acordo com as normas estabelecidas para concessão de Credencial de Segurança, ICA 200-2 Processo de Concessão de Credencial de Segurança de Pessoa Física, de 2006.

2.12.2 O processo de credenciamento deve ser iniciado com antecedência mínima de três meses devido aos trâmites necessários para tal. Não é adequado que haja acesso a áreas ou documentação sigilosa por pessoal que ainda não tenha sido credenciado, mesmo que essa pessoa esteja designada para isso.

2.12.3 Compete ao solicitante da credencial fazer uma “investigação preliminar de segurança”, utilizando-se dos dados disponíveis, a fim de indicar o pessoal adequado para ocupação de cargos e funções com acesso a assuntos sigilosos.

2.12.4 Antes de proceder à solicitação de Credencial de Segurança, os Comandantes, Chefes e Diretores devem ser assessorados no sentido de certificarem-se da inexistência de características pessoais negativas que contraindiquem o candidato para o trato de assuntos sigilosos. Devem ser analisados os atributos pessoais, tais como: lealdade, confiança, discrição, integridade moral e relacionamentos pessoais. Também, devem-se considerar os aspectos disciplinares, familiares e a situação jurídica, civil e militar do candidato.

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

- a) **ultrassecreto**: os Oficiais-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.

2.13 ÁREAS E INSTALAÇÕES SIGILOSAS

2.13.1 As áreas sigilosas deverão ser classificadas em razão do grau de sigilo dos assuntos e materiais nelas tratados, desenvolvidos, guardados, manuseados ou operados, podendo variar de ULTRASSECRETA até RESERVADA. 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, conforme legislação pertinente. Para tanto, deverão ser elaboradas Normas de Controle de Acesso às Áreas Sigilosas, com a finalidade de sistematizar os procedimentos adequados a cada situação.

2.13.2 O acesso de visitas a áreas e instalações sigilosas deverá ser disciplinado por legislação específica de cada OM, atendendo ao que prevê ICA 205-22 Visita às Organizações Militares do COMAER, de 2002, além de outras legislações que tratem do assunto.

2.13.3 As áreas onde são desenvolvidas atividades de Inteligência, TI, Comunicações, Ciência e Tecnologia (C&T), Guerra Eletrônica, Operações Aéreas, Controle de Tráfego Aéreo, entre outras a critério da autoridade classificadora, deverão ser consideradas sigilosas de acordo com a necessidade particular de cada atividade.

2.13.4 O acesso às áreas sigilosas somente deverá ser permitido às pessoas devidamente credenciadas, desde que tenham necessidade de conhecer.

2.13.5 Não deverá ser permitida a entrada de pessoas conduzindo máquinas fotográficas, filmadoras, gravadores ou quaisquer dispositivos de produção ou armazenamento de sons, imagens (telefones celulares multifunção, por exemplo) ou dados em áreas e instalações que tratem de assunto sigiloso.

2.13.6 Deve haver um dispositivo adequado (armário ou escaninho com chave ou cadeado, por exemplo), para guarda do material não adequado, na entrada da instalação ou área sigilosa, de forma que esse material fique estocado, em segurança, para retirada posterior quando da saída da referida área ou instalação.



Figura 7: Modelos de dispositivos para guarda de pertences.

2.13.7 As áreas sigilosas deverão ser indicadas, por intermédio de placas afixadas (nas paredes, cercas, muros, divisórias, acessos, portas, etc) de forma destacada, preferencialmente na cor vermelha (ou outra a critério do setor), com o respectivo grau de sigilo, não só no seu interior, mas principalmente junto às entradas. A marcação tem por finalidade precípua apresentar-se como um primeiro elemento dissuasor ao acesso não autorizado. Da mesma

forma indica a compartimentação do setor e a restrição à entrada de elementos não credenciados e autorizados para tal.

RESERVADO

CONFIDENCIAL

SECRETO

**ACESSO RESTRITO
ÁREA
CONFIDENCIAL**

**ÁREA
ULTRASSECRETA**

2.13.8 Deve haver um controle do fluxo de visitantes para que se possa acompanhar e identificar se há algum tipo de reincidência de atitudes de determinado visitante que possa estar utilizando-se das visitas à organização para efetuar algum tipo de ação adversa, levantamento de dados, introdução ou retirada de material não autorizado, entre outros. O pessoal do setor de inteligência da organização deve acompanhar os registros para que seja feita uma análise que possa detectar indícios de irregularidades. A equipe de serviço ou recepção deve ter sempre uma atitude de questionamento a respeito dos visitantes e não apenas realizar um ato mecânico de registro de entrada e saída. Deve-se observar comportamentos, vestuários, objetos sendo portados, atitudes suspeitas, nervosismos, interesses duvidosos a respeito da organização, alterações de nomes, identidades, entre outros. Mais detalhes a respeito devem ser buscados no FCA 200-3/2009 – Prevenção a Engenharia Social.

2.14 SEGURANÇA FÍSICA

2.14.1 Um Plano de Segurança Orgânica equilibrado deve ter fundamento na segurança física, a qual atuará em conjunto com medidas adequadas de segurança eletrônica, visando a proteger tanto as instalações quanto as informações sigilosas. Não faz sentido despender recursos em vigilância eletrônica, se serviços de inteligência hostis e demais elementos adversos tiverem acesso físico às informações e documentos classificados.

2.14.2 Um Plano de Segurança Orgânica deve ser formulado, implementado e deve abordar a organização e suas instalações por completo. Esta abordagem é estruturada em profundidade e deverá conter elementos mútuos de suporte, tanto para a segurança física quanto para a vigilância eletrônica. Especial atenção deverá ser dedicada à coordenação entre Oficial de Segurança e Defesa, o Chefe do Setor de Inteligência e demais responsáveis pelas instalações, visando a prevenir a ocorrência de lacunas que possam gerar vulnerabilidades na segurança física ou redundância tanto de responsabilidades quanto de desempenho do sistema de segurança como um todo.

2.14.3 Uma abordagem completa da segurança física é baseada em:

- a) exaustiva e contínua análise das medidas de proteção requeridas;

- b) avaliação cuidadosa das medidas de proteção consideradas, quanto a sua praticidade, para que os procedimentos de segurança sejam viáveis;
- c) necessidades e características locais de cada instalação quanto à segurança física; e
- d) consciência de que a medida que os procedimentos de segurança física se tornarem mais restritivos, a capacidade operacional da organização diminuirá.

2.14.4 Elementos mútuos de suporte para a segurança física são aqueles que aumentam a eficiência dos procedimentos de segurança física. Neles incluem-se:

- a) barreiras físicas perimetrais;
- b) áreas livres (onde não deverão, em função da facilidade de controle de acesso, haver pessoas ou materiais que não sejam intencionais);
- c) postos para reação protegida;
- d) instalações para controle de acesso;
- e) sistemas de detecção de intrusão;
- f) postos para proteção do perímetro, se necessário;
- g) guarda armada; e
- h) meios de comunicação.

A combinação de alguns ou todos esses elementos pode proporcionar segurança física satisfatória para cada instalação considerada.

2.14.5 Os recursos disponíveis devem ser utilizados da maneira mais eficiente possível visando a atingir a proteção adequada das instalações que processam informações sigilosas. Todas as medidas de segurança devem ser usadas de maneira a complementar e suplementar umas às outras. A falta de integração das medidas de segurança pode resultar em desperdício de dinheiro, equipamento e força de trabalho. E o mais importante é que tal falta de integração poderá colocar a segurança de determinada instalação em risco. Deverá ser dada ênfase aos requisitos operacionais da instalação considerada para que sejam determinados o tipo e a extensão das medidas de segurança necessárias. Os fatores a seguir devem ser considerados, na ordem em que estão listados, pelo planejador de segurança:

- a) a importância da finalidade de determinada instalação para a organização como um todo;
- b) a área a ser protegida, incluindo: os trabalhos que são executados e sua natureza; o grau de sigilo da instalação; o número de pessoas envolvidas; valor monetário e estratégico do material contido na instalação; ameaças identificadas;
- c) integração dos requisitos de operação e manutenção;
- d) diretrizes do escalão superior, questões de legalidade e financeiras;
- e) exequibilidade, eficiência e vantagens dos vários métodos para o fornecimento da adequada proteção física; e
- f) custo do material e equipamento a ser instalado, bem como da disponibilidade de recursos financeiros para assegurar e manter a proteção adequada a todas as áreas e atividades críticas.

2.14.6 Elementos adversos são ameaças que se caracterizam por atos ou condições que podem resultar em perda ou comprometimento de informação sigilosa, perda ou destruição de equipamento ou propriedade, ou descontinuidade das atividades e da missão da organização. Antes que um eficiente Plano de Segurança Orgânica possa ser desenvolvido, as ameaças que interferem nas operações da instalação e seu potencial de comprometimento devem ser identificados e avaliados. O conhecimento de todos os riscos envolvidos é essencial para que as adequadas medidas de proteção minimizem ou eliminem as vulnerabilidades das instalações. O grau de risco das ameaças depende de variáveis como: o tipo de instalação (centro de comunicações, criptoanálise, análise de inteligência, etc.), *layout* da instalação, missão e estrutura física. Adicionalmente, a localização geográfica, a capacidade dos serviços de inteligência hostis bem como seus interesses e o grau de disciplina dos funcionários civis e militares da organização também são fatores importantes a considerar.

2.14.7 As ameaças à segurança podem ser classificadas em dois tipos: naturais e humanas.

2.14.7.1 Ameaças naturais à segurança são aquelas que:

- a) não podem ser executadas por pessoas;
- b) não podem ser evitadas por meios de segurança física;
- c) são capazes de afetar as funcionalidades dos meios de segurança física adversamente, através da alteração e negação de suas condições normais de operação (fenômenos que destroem cercas e muros, causam paralisação do fornecimento de energia, baixa visibilidade, etc.).

Ameaças naturais requerem medidas de proteção especiais como, por exemplo: guarda armada adicional. Exemplos de ameaças naturais são: inundações, tempestades, nevoeiro, ventanias, terremotos, neve e gelo, deslizamentos de terra ou pedras e incêndios em áreas verdes. Qualquer instalação que esteja exposta a estas ameaças naturais requer medidas previamente planejadas que irão se contrapor aos seus impactos adversos.

2.14.7.2 Ameaças humanas à segurança física são resultado do estado mental, atitude, fraqueza, ou falha de caráter da parte de uma pessoa ou grupo de pessoas. Ameaças humanas consistem de ações disfarçadas ou abertas, executadas ativamente ou passivamente, estas por meio de omissões. Tais ações visam a interromper, destruir ou comprometer a missão e as atividades da instalação alvo. Medidas de segurança física são projetadas para neutralizar estas ameaças, prioritariamente. Exemplos de ameaças humanas à segurança física: sabotagem, espionagem, terrorismo, inteligência sobre fontes humanas (HUMINT), desafeição, deslealdade e antipatia por parte de pessoas.

2.14.8 O planejamento das medidas de segurança física de uma instalação deve ser constante, praticável, flexível em relação à missão e sensível às necessidades do comandante, chefe ou diretor da organização.

2.14.9 Um eficiente planejamento de Segurança Orgânica deve considerar que o evento mais danoso possível está diretamente relacionado à sensibilidade da informação processada e guardada na organização e às ameaças identificadas. Deve considerar também o pessoal, material e equipamento disponível. Medidas adicionais de segurança física devem ser implementadas visando à continuidade de todos os procedimentos de segurança. Enfim, deverão ser sempre considerados os objetivos da organização, prioritariamente.

2.14.10 Barreiras perimetrais, dispositivos detectores de invasão e iluminação de proteção constituem medidas de proteção. Contudo, estas medidas, por si só, não são suficientes. Mecanismos de controle de acesso de pessoas devem ser implementados para conveniência e permissão, apenas, de acessos previamente autorizados. Devem prevenir contra tentativas de acessos indevidos e contra a neutralização adversa dos mecanismos de controle. Pontos de controle de acesso de pessoas às diversas áreas restritas devem ser sempre considerados pelo especialista em segurança de áreas e instalações, na concepção do projeto de segurança física. Credenciais de segurança para as pessoas e procedimentos de identificação serão sempre uma preocupação, em relação à segurança física de instalações.

2.14.11 O acesso a áreas restritas estará condicionado a medidas de controle especiais, por motivos de segurança. Áreas restritas aumentam a segurança por meio de medidas de segurança em profundidade. Estes controles especiais aumentam a eficiência através de níveis de segurança compatíveis com as necessidades operacionais de cada instalação dentro da organização. As áreas restritas são utilizadas para facilitar o equilíbrio entre as necessidades de segurança física e as necessidades de operação de cada instalação. Em vez de estabelecer medidas de controle para a organização como um todo, a divisão em diferentes níveis de segurança reduz a interferência global nas operações realizadas na organização e a eficiência operacional da organização é preservada o tanto quanto possível.

2.14.12 O nível de segurança e controle requerido para uma instalação específica dependerá da natureza, sensibilidade e importância do que se quer proteger. Áreas restritas são estabelecidas para fornecer:

- a) uma eficiente aplicação das medidas de segurança necessárias, como, por exemplo, impedir o ingresso não autorizado de pessoas;
- b) controles de acesso mais rigorosos nas áreas que requerem proteção especial; e
- c) condições para compartimentar informações, materiais e equipamentos sigilosos, com impacto minimizado nas operações da organização como um todo.

No interior das áreas restritas, haverá tantas compartimentações quantas forem necessárias, em função da necessidade de conhecer de cada pessoa. Tais compartimentações podem possuir o mesmo ou diferentes graus de sigilo, dependendo da sensibilidade de cada compartimento.

2.14.13 Os dispositivos de segurança aplicáveis a uma instalação são ditados pela sensibilidade da mesma às ameaças identificadas. Dispositivos de segurança incluem postos de guarda, cerca perimetral de segurança, portões, áreas livres, grades em janelas, portas de segurança, alarmes de detecção de invasão, dispositivos eletrônicos de segurança e outras medidas similares.

2.14.14 Barreiras de proteção são normalmente utilizadas para estabelecer os limites físicos de uma determinada área e para controlar o acesso à mesma. São divididas em duas categorias principais: naturais e estruturais. Barreiras de proteção naturais são montanhas, desertos, rios ou outros terrenos similares que impõem dificuldades para sua travessia. Barreiras de proteção estruturais são construções como cercas, muros, paredes, pisos, barras, tetos ou outros tipos de construções que inibem acessos a determinadas áreas. As barreiras oferecem dois benefícios importantes à segurança física. Primeiramente, estabelecem dissuasão psicológica naqueles que considerarem entrar sem autorização em áreas controladas e restritas. O segundo benefício é que causam impacto direto no número de postos de segurança necessários a determinada instalação.

2.14.15 Barreiras estruturais, como cercas e muros, são necessárias para todo o perímetro das áreas controladas. Há barreiras específicas para cada instalação considerada, mas todas as instalações deverão ter, no mínimo, barreiras estruturais perimetrais e pontos de verificação de autorização de acesso.

2.14.16 A quantidade de pontos de acesso para cada instalação deve ser limitada ao número mínimo necessário à sua segurança e operação. Os pontos de entrada devem ser projetados de maneira que as forças de segurança possam manter total controle sem impedir a passagem de pessoas e veículos pelas entradas existentes. Isso envolve entradas suficientes para acomodar o fluxo de pessoas e o tráfego de veículos e iluminação adequada para a verificação eficiente das credenciais de acesso. Quando houver entradas não utilizadas fora do horário de expediente, devem ser utilizados mecanismos de fechamento robustos para as mesmas. Essas entradas devem ser iluminadas durante períodos de escuridão e monitoradas por meio de circuitos fechados de TV ou inspecionadas por meio de patrulhamento aleatório. Este procedimento também se aplica a portas e janelas que fazem parte do perímetro de proteção.

2.14.17 Quando a barreira perimetral de determinada instalação englobar uma área extensa, uma via interna para a circulação de veículos, adequada para quaisquer condições de tempo, deve ser providenciada para o patrulhamento motorizado se tal área não for monitorada por circuito fechado de TV. Áreas livres devem ser mantidas tanto no interior quanto no exterior da barreira perimetral para que seja possível visualizar os espaços adjacentes sem obstruções. As vias devem estar nas áreas livres e tão próximas da barreira perimetral quanto possível, permitir a adequada passagem de veículos de patrulha e não causar erosão no solo.

2.14.18 Deve haver uma área livre de pelo menos 6 metros entre a barreira perimetral e as construções, estacionamentos e obstáculos naturais. Nas áreas restritas, deve haver uma área livre de pelo menos 15 metros entre a barreira perimetral e as construções, estacionamentos e obstáculos naturais. Quando não for possível haver áreas livres devido a delimitações de propriedade, obstáculos naturais ou construções, será necessário elevar a altura da barreira perimetral (exceto quando se tratar da parede de um prédio), aumentar a frequência dos patrulhamentos, disponibilizar mais iluminação de proteção ou instalar um sistema de detecção de invasão ao longo daquela parte da barreira perimetral.

2.14.19 A iluminação de segurança possibilita um meio de manter, durante os períodos de redução de visibilidade, um nível de proteção próximo ao obtido durante o período diurno. A iluminação de segurança possui valor considerável como meio de dissuasão para prováveis ladrões e vândalos e dificulta as ações de um potencial sabotador. É um elemento essencial de um sistema integrado de segurança física. Sua aplicação em várias instalações depende das condições locais e da natureza das áreas a proteger. Cada situação requer um estudo minucioso com vistas a providenciar a adequada visibilidade para as atividades de segurança, como verificações de credenciais de acesso, prevenção de entradas não autorizadas em áreas restritas e inspeção de situações suspeitas. Quando a disponibilidade de iluminação de segurança for impraticável, serão necessárias medidas de segurança adicionais como aumento da frequência dos patrulhamentos, mais sentinelas ou um sistema de alarme. Para que seja eficiente, a iluminação de segurança deve desencorajar tentativas de invasão e assegurar a detecção quando tais tentativas ocorrerem. Uma iluminação adequada deve levar um potencial intruso a acreditar que a detecção pelas forças de segurança é inevitável. Os engenheiros responsáveis pelas instalações devem consultar os especialistas de segurança física para ajudar a determinar o tipo apropriado e o nível do sistema de iluminação de proteção que melhor atende às necessidades de segurança de cada instalação.

2.14.20 Um Sistema de Detecção de Invasão (SDI) é um elemento integrante de um Plano de Segurança Orgânica em profundidade e desempenha um papel vital na proteção de instalações sigilosas. Para que uma determinada área seja efetivamente protegida, um SDI deve objetivar detectar acessos não autorizados nas entradas (portões, portas, cercas, etc.), áreas (prédios, campo aberto, salas) ou num objeto específico (cofres, arquivos, fechaduras). Deve-se lembrar, ao selecionar um SDI para determinada instalação, que o mesmo será inútil se não estiver integrado a uma força de pronta-resposta, quando seus alarmes forem acionados.

2.14.21 Um SDI é utilizado devido a uma ou mais das seguintes razões:

- a) economia – um SDI permite um uso mais eficiente e econômico dos meios humanos. Ele agrega mais intensivamente os meios humanos às demais forças de segurança;
- b) substituição – pode ser utilizado para substituir medidas de segurança impraticáveis devido a regulamentações de segurança do trabalho, requisitos operacionais, exposição, *layout*, custos e outras razões semelhantes; e
- c) fortalecimento – fornece controles adicionais de segurança física em áreas e pontos críticos.

2.14.22 Os seguintes fatores devem ser considerados para determinar a necessidade e exeqüibilidade da instalação de um SDI:

- a) missão e sensibilidade da instalação ou das informações nela contidas em relação à missão da organização como um todo;
- b) vulnerabilidades da instalação às ameaças humanas;
- c) localização geográfica da instalação e das áreas a proteger em seu interior;
- d) características de construção da instalação;
- e) existência e disponibilidade de outras formas de proteção;
- f) custos de implementação e manutenção do SDI proposto em comparação com o custo (financeiro ou de segurança), em caso de perda de informações e materiais sigilosos;
- g) tempo-resposta das forças de segurança;
- h) economia em meios humanos e recursos financeiros ao longo do tempo; e
- i) requisitos para o tempo de detecção de invasão.

2.14.23 Há vários tipos de SDI e cada um é projetado para atender a um problema de segurança específico. Detectores tipo ponto de acesso, foto-elétrico, sonoro, de vibração, de movimento e pressão são alguns dos componentes que podem ser utilizados para proteger uma instalação. O Oficial de Segurança e Defesa juntamente com técnicos devem determinar qual sistema ou combinação de sistemas melhor atende às necessidades verificadas.

3 SEGURANÇA DA INFORMAÇÃO

3.1 SEGURANÇA DE *HARDWARE*

3.1.1 Qualquer serviço de manutenção a ser executado em equipamento que contenha assunto sigiloso, e não apenas material exclusivo de TI, deverá ser acompanhado pelo responsável por sua utilização, além de que o pessoal envolvido nessa manutenção deve possuir o credenciamento adequado para tal. Isso deve ser observado para todo e qualquer material que possua componentes ou *software* sigiloso (equipamentos de DATA-LINK, sistemas de criptográficos, RWR e similares, radares, rádios, telefones seguros, etc).

3.1.2 O computador ou equipamento que contenha assunto sigiloso e que necessite de manutenção fora da OM deverá ter o seu disco rígido (e outros dispositivos de memória) retirado(s) e guardado(s) em cofre ou de acordo com o grau de sigilo do seu conteúdo.

3.1.3 É terminantemente proibida a utilização de equipamento de rede criptográfica para qualquer fim que não o exclusivo trâmite de documentação sigilosa do COMAER.

3.2 SEGURANÇA DE *SOFTWARE* E DE INTERNET

3.2.1 Os equipamentos e sistemas utilizados para a produção, trâmite e tratamento de documentos com grau de sigilo ultrassecreto somente poderão estar ligados a redes de computadores seguras e que sejam física e logicamente isoladas de qualquer outra.

3.2.2 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.

3.2.3 Todos os arquivos que contenham assuntos sigilosos e os programas em uso deverão possuir cópias de segurança. Essas cópias deverão estar protegidas em dispositivos adequados, resistentes a radiações eletromagnéticas, umidade, calor e em local diverso daquele no qual o original esteja sendo manuseado ou utilizado.

3.2.4 Nenhuma informação sigilosa deverá constar das *Home Page* das OM;

3.2.5 Para fins do que dispõe o item 3.2.4 serão considerados, também, como informações sigilosas (em virtude do potencial para análise de inteligência que possuem): vistas aéreas da OM, fotografias internas de pontos sensíveis da OM (paiol, reserva de armamento, linha de vôo, hangares, sistemas de água, combustível, transportes de superfície, hospitais, refeitórios, alojamentos, torres de controle, casas-de-força, sistemas geradores de energia, etc.), estrutura de comando, organogramas com nomes e dados dos militares ou civis que ocupam os referidos cargos de comando, chefia e direção, peculiaridades do emprego ou características técnicas de meios aéreos ou terrestres de uso militar, informações pessoais dos integrantes da OM, informações contidas nos Quadros de Organização, Lotação ou de Material, dentre outras, que possam servir de subsídios para análises, composição de capacidades operacionais, preparação de ataques, atentados e demais ações adversas.

4 MEDIDAS GERAIS DE SEGURANÇA

4.1 Na classificação dos documentos, será utilizado, sempre que possível, o critério menos restritivo possível, de outra maneira criam-se empecilhos desnecessários aos trâmites dos documentos e gera-se descrédito ao sistema de classificação sigilosa.

4.2 Compete aos Comandantes, Chefes e Diretores exigir Termo de Compromisso de Manutenção de Sigilo dos militares ou civis pertencentes ao seu efetivo e dos empregados de empresas contratadas que, direta ou indiretamente, tenham acesso a dados ou informações sigilosas. Isso deve ser rigorosamente efetuado, também, quando do término dos contratos de prestação de serviços ou fornecimento de materiais, além do desligamento de pessoal militar ou civil que haja tido acesso à documentação e materiais sigilosos.

4.3 Qualquer pessoa vinculada ao COMAER que tenha conhecimento de uma situação na qual um conhecimento sigiloso possa estar, ou venha a ser, comprometido deve participar tal fato ao seu Chefe imediato e/ou à autoridade responsável. Devem estar disponíveis nas OM, em diversos pontos acessíveis ao pessoal em geral, os Relatórios de Vulnerabilidades previstos na ICA 200-5 Gerenciamento de Plano de Segurança Orgânica do Comando da Aeronáutica, de 2009. A utilização desses relatórios deve ser orientada e incentivada no âmbito do pessoal das OM do COMAER.

DISPOSIÇÕES FINAIS

Os casos não previstos deverão ser encaminhados, mediante proposta, ao Centro de Inteligência da Aeronáutica.

ÍNDICE

Disposições finais, 31**Disposições preliminares, 9**

- âmbito, 11
- área sigilosa, 9
- classificação e demarcação, 9
- compartimentação, 10
- conceituação e padronização, 9
- finalidade, 9
- meio de comunicação sigilosa, 9
- reclassificação, 9

Medidas gerais de segurança, 30**Segurança da informação, 29**

- segurança de *hardware*, 29
- segurança de *software* e de Internet, 29

Sigilo e segurança, 12

- acesso, 21
- áreas e instalações sigilosas, 22
- avaliação e preservação, 20
- classificação segundo o grau de sigilo, 12
- documento e material sigilosos controlados, 13
- expedição de documentos sigilosos, 16
- marcação, 15
- prazos, 14
- reclassificação e desclassificação, 13
- registro, tramitação e guarda, 18
- reprodução, 19
- segurança física, 23
- segurança na preservação, 20
- segurança na produção, 19
- segurança no arquivamento, 20