EMA-414 **OSTENSIVO**

NORMAS PARA A SALVAGUARDA DE MATERIAIS CONTROLADOS, DADOS, INFORMAÇÕES, DOCUMENTOS E MATERIAIS SIGILOSOS NA MARINHA

MARINHA DO BRASIL

ESTADO-MAIOR DA ARMADA

2005

NORMAS PARA A SALVAGUARDA DE MATERIAIS CONTROLADOS, DADOS, INFORMAÇÕES, DOCUMENTOS E MATERIAIS SIGILOSOS NA MARINHA

MARINHA DO BRASIL

ESTADO-MAIOR DA ARMADA

2005

FINALIDADE: NORMATIVA

1ª EDIÇÃO

ATO DE APROVAÇÃO

Aprovo, para emprego na MB, a publicação **EMA-414 - NORMAS PARA A SALVAGUARDA DE MATERIAIS CONTROLADOS, DADOS, INFORMAÇÕES, DOCUMENTOS E MATERIAIS SIGILOSOS NA MARINHA.**

BRASÍLIA, DF.
Em 28 de fevereiro de 2005.

RAYDER ALENCAR DA SILVEIRA
Almirante-de-Esquadra
Chefe do Estado-Maior da Armada
ASSINADO DIGITALMENTE

AUTENTICADO PELO ORC	**RUBRICA**
Em _____/_____/_____	**CARIMBO**

ÍNDICE

PÁGINAS

INTRODUÇÃO

1. PROPÓSITO

Esta publicação tem o propósito de estabelecer as normas para a salvaguarda de materiais controlados, dados, informações, documentos e materiais sigilosos na Marinha do Brasil, bem como das áreas e instalações onde tramitam, incluindo os procedimentos das Comissões de Avaliação para a sua renovação, reclassificação, desclassificação e autorização de acesso.

2. DESCRIÇÃO

Esta publicação foi elaborada de acordo com o contido na Lei nº 8.159, de 08 de janeiro de 1991, na Lei nº 9.507, de 12 de novembro de 1997, no Decreto nº 4.553, de 27 de dezembro de 2002, no Decreto nº 4.915, de 12 de dezembro de 2003, no Decreto nº 5301, de 9 de dezembro de 2004, e está dividida em 7 capítulos e quatro anexos, conforme a descrito a seguir:

a) Capítulo 1 - apresenta os conceitos e as definições utilizados;
b) Capítulo 2 - trata de sigilo e segurança;
c) Capítulo 3 - trata da gestão de materiais sigilosos;
d) Capítulo 4 - trata de custódia e controle;
e) Capítulo 5 - trata de avaliação, preservação, acesso e comprometimento;
f) Capítulo 6 - trata de recolhimento e destruição de material controlado ou sigiloso;
g) Capítulo 7 - trata de contratos e cessão de material controlado ou sigiloso;
h) Anexo A - apresenta um modelo para que sejam relacionados os documentos sigilosos desclassificados;
i) Anexo B - apresenta um modelo de notificação diante de pedido de acesso;
j) Anexo C - apresenta um modelo de notificação diante de pedido de retificação; e
k) Anexo D - apresenta um modelo de Termo de Responsabilidade.

3. CLASSIFICAÇÃO

Esta publicação é classificada, de acordo com o EMA-411 (Manual de Publicações da Marinha), como: PMB, não controlada, ostensiva, normativa e norma.

4. SUBSTITUIÇÃO

Esta publicação substitui o EMA-413 - Manual para a Segurança do Material Controlado, 1ª revisão, aprovada em 30 de março de 1999, e o EMA-134 - Normas e Procedimentos para a Comissão e as Subcomissões Permanentes de Acesso a Documentos Públicos Sigilosos na Marinha, 1ª edição, aprovada em agosto de 2001.

CAPÍTULO 1

CONCEITOS E DEFINIÇÕES

1.1 - DEFINIÇÕES

Para efeito desta publicação considera-se:

- ACESSO

Ato de se tomar conhecimento ou examinar dado, informação, documento, material, área ou instalação.

- ASSUNTO SIGILOSO

Aquele cujo conhecimento é restrito e requer, portanto, classificação e adoção de medidas especiais de segurança.

- AUTENTICIDADE

Característica que ocorre quando a origem de um dado, informação ou documento é realmente aquela apresentada.

- CLASSIFICAÇÃO

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

- COMPROMETIMENTO

Perda de segurança física ou de conteúdo de material sigiloso, resultante do acesso não autorizado.

- CONHECIMENTO

É a representação, resultante da aplicação de uma metodologia qualquer, de um fato ou de uma situação, real ou hipotética.

- CREDENCIAL DE SEGURANÇA

Certificado concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados, informações, documentos, materiais, áreas ou instalações em diferentes graus de sigilo, desde que possua necessidade de conhecer.

- CUSTÓDIA

Responsabilidade pela guarda e pela segurança, física ou de conteúdo, de material controlado.

- DADO

É a representação, que não decorra do emprego de uma metodologia qualquer, de um fato ou de uma situação.

- DESCLASSIFICAÇÃO

Cancelamento, pela autoridade competente ou por transcurso de prazo, da classificação, tornando ostensivo algo sigiloso.

- DISPONIBILIDADE

Característica que ocorre quando um dado, informação ou documento está disponível para, quando necessário, ser acessado pelo pessoal autorizado.

- DOCUMENTO

É o registro de uma informação, independente da natureza do suporte que a contém. Os documentos de interesse da MB estão enquadrados nos seguintes grupos:

- Documentos Administrativos;
- Documentos Operativos;
- Publicações; e
- Documentos Especiais (aqueles cujo suporte original não é o papel, como fotografias, negativos, slides, fitas, disquetes etc).

- DOCUMENTO SIGILOSO CONTROLADO

É aquele que, por sua importância, requer medidas adicionais de controle.

- DOCUMENTO PÚBLICO

É aquele produzido e recebido por OM, em decorrência de suas atribuições, ou produzido e recebido por seus titulares ou autoridades por eles delegadas, no exercício de seu cargo ou função.

- DOCUMENTO PÚBLICO SIGILOSO

Para efeito desta publicação, é aquele que contém assunto classificado como sigiloso e que diga respeito à segurança da sociedade e do Estado e à intimidade do indivíduo.

- ENCARREGADO DO MATERIAL CONTROLADO (EMC)

Oficial designado pelo titular de uma OM, por meio de documento oficial, para exercer, perante este, a custódia do material controlado existente na OM.

- ENQUADRAMENTO

Ação a ser executada depois de verificadas todas as circunstâncias que concorreram para o fato que ocasionou a abertura de sindicância, concernentes à adoção, omissão ou violação dos procedimentos preconizados nesta publicação. Deverá, também, ser analisado se o fato correlacionado ao enquadramento pode ser tipificado como infração, segundo o Regulamento Disciplinar para a Marinha (RDM) e o Código Penal

Militar (CPM), caracterizando, assim, a ocorrência de contravenção disciplinar ou crime militar. Sendo considerada a ocorrência de crime, deverá ser emitido um relatório parcial e remetidos os autos à autoridade nomeante, que determinará a instauração do competente Inquérito Policial Militar (IPM), conforme preconizado nas normas em vigor sobre Deserção, Conselho de Disciplina/Justificação, Sindicância/Inquérito Policial Militar e Prisão em Flagrante na MB, promulgadas pela Diretoria Geral do Pessoal da Marinha (DGPM).

- EQUIPAMENTO CRIPTOLÓGICO

É a denominação dada a qualquer equipamento que, empregando processos mecânicos, eletrônicos, eletromecânicos ou computacionais e, operando segundo princípios e métodos criptológicos comandados por um algoritmo especial, possibilita a prática da transformação de uma linguagem clara em criptológica e vice-versa.

- GRAU DE SIGILO

Gradação atribuída a dados, informações, documentos, materiais, áreas ou instalações considerados sigilosos em decorrência de sua natureza ou conteúdo.

- INFORMAÇÃO

É o conhecimento resultante de raciocínio elaborado.

- INFORMAÇÃO DIGITAL

É a representação de dado ou informação em meio eletrônico ou digital.

- INTEGRIDADE

Característica que ocorre quando as modificações de um dado, informação ou documento foram efetuadas somente por alguém autorizado.

- INVENTÁRIO

Relação do material controlado e respectivas informações e identificações.

- INVESTIGAÇÃO PARA CREDENCIAMENTO DE SEGURANÇA

Averiguação sobre a existência dos requisitos indispensáveis para concessão de credencial de segurança. Na MB, está regulamentada pelo Manual de Inteligência da Marinha - Contra-Inteligência, estabelecido pelo Estado-Maior da Armada (EMA).

- MARCAÇÃO

Aposição de marca assinalando o grau de sigilo.

- MATERIAL CONTROLADO

Material, documento ou equipamento, sigiloso ou não, em relação ao qual deva ser exercido um controle de custódia.

- MATERIAL CRIPTOLÓGICO

É o material empregado na criptologia, abrangendo as publicações criptológicas, os equipamentos criptológicos e suas instruções, as cifras, chaves e códigos. O mesmo que recurso criptológico.

- MATERIAL SIGILOSO

Material, documento ou equipamento que deva ser de conhecimento restrito por conter, utilizar ou possibilitar o acesso a assunto sigiloso.

- MEDIDAS ESPECIAIS DE SEGURANÇA

Medidas destinadas a garantir sigilo, autenticidade, integridade e disponibilidade de dados, informações e documentos sigilosos, bem como prevenir, detectar, anular e registrar ameaças reais ou potenciais aos mesmos.

- 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, informações, documentos, materiais, áreas ou instalações sigilosos.

- NIVEL DE COMPROMETIMENTO

Conjunto de fatores que permite concluir sobre como o conhecimento comprometido poderá influenciar o desempenho das tarefas da MB. Os níveis serão classificados como baixo, médio ou alto.

- OFICIAL RESPONSÁVEL PELA CUSTÓDIA (ORC)

Oficial responsável pela custódia do material controlado sigiloso de uma OM.

- OSTENSIVO

Sem classificação, cujo acesso pode ser franqueado.

- POSTAGEM

Expedição pelos serviços de correio (Mala Postal da Marinha, Mala Diplomática, Correio Aéreo Nacional, Empresa Brasileira de Correios e Telégrafos ou similares).

- RECLASSIFICAÇÃO

Alteração, pela autoridade competente, da classificação de material sigiloso.

- RECURSO CRIPTOLÓGICO

É o recurso empregado na criptologia, abrangendo as publicações criptológicas, os equipamentos criptológicos e suas instruções, as cifras, chaves e códigos. O mesmo que material criptológico.

- REPRODUÇÃO

Cópia parcial ou integral de dado, informação ou documento.

- SIGILO

Segredo de conhecimento restrito a pessoas credenciadas e que tenham necessidade de conhecer. Proteção contra revelação não-autorizada.

- VISITA

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

CAPÍTULO 2
ASPECTOS BÁSICOS DE SEGURANÇA E CLASSIFICAÇÃO DO MATERIAL SIGILOSO

2.1 - ASPECTOS BÁSICOS DE SEGURANÇA DO MATERIAL SIGILOSO

As medidas de segurança do material sigiloso englobam a manutenção da segurança e da salvaguarda desse material. São baseadas em dois fundamentos: Segurança Orgânica e Mentalidade de Segurança. Sem um destes fundamentos, a segurança não existe. A Mentalidade de Segurança é construída pela Educação de Segurança e fortalecida pelo contínuo adestramento do pessoal. Além disso, em complemento às medidas de segurança, são necessárias algumas medidas cautelares de salvaguarda, como a assinatura dos Termos de Responsabilidade Individual, referentes à manutenção de sigilo e ao uso dos sistemas de informações digitais.

2.1.1 - Segurança Orgânica

A Segurança Orgânica, conforme definida no Manual de Inteligência da Marinha - Contra-Inteligência, estabelecido pelo EMA, compreende um conjunto de medidas voltadas para a prevenção e a obstrução das ações ou ocorrências adversas de qualquer natureza que comprometam a salvaguarda de itens sigilosos.

2.1.2 - Mentalidade de Segurança

De nada adiantam rigorosos procedimentos de segurança caso os executores não tenham uma perfeita compreensão da necessidade e da importância dos mesmos. Para isso, é necessário que exista uma forte Mentalidade de Segurança.

Para alcançá-la, é preciso um longo e contínuo trabalho de conscientização, constando do ensino de formação, especialização e aperfeiçoamento, bem como do adestramento das OM. Deve haver uma constante doutrinação por parte dos responsáveis pela segurança em seus diversos níveis.

2.1.3 - Educação de Segurança

As OM estabelecerão e cumprirão a Educação de Segurança, conforme previsto no Manual de Inteligência da Marinha - Contra-Inteligência, estabelecido pelo EMA, por meio de um programa de instrução que tem por finalidade criar, desenvolver e manter uma efetiva mentalidade de segurança, bem como transmitir os procedimentos cautelares necessários ao trato de itens sigilosos, previstos nesta e nas demais publicações e normas em vigor na MB.

2.1.4 - Adestramento

As OM promoverão o treinamento, a capacitação, a reciclagem e o aperfeiçoamento de pessoal que desempenhe atividades inerentes à salvaguarda de assuntos, dados, informações, documentos, materiais, áreas, instalações e sistemas de informação digital de natureza sigilosa.

2.1.5 - Termo de Responsabilidade Individual

Conforme as normas estabelecidas pela Diretoria-Geral do Material da Marinha (DGMM), as OM exigirão dos seus militares, servidores civis, empregados terceirizados e prestadores de serviço que, direta ou indiretamente, tenham acesso a assuntos, dados, informações, documentos, materiais, áreas, instalações ou sistemas de informação digital de natureza sigilosa, a assinatura de Termo de Responsabilidade Individual, referente à manutenção de sigilo e ao uso dos sistemas de informações digitais. A manutenção do sigilo deve permanecer mesmo após o afastamento, desligamento, término das atividades ou da prestação de serviços.

2.1.6 - Aspectos básicos no trato de material sigiloso

No trato de material sigiloso, devem ser observados os seguintes aspectos básicos:

a) o acesso a dados, informações, documentos e materiais sigilosos, assim como às áreas e instalações onde tramitam é restrito e condicionado à necessidade de conhecer;

b) as atividades de produção, manuseio, consulta, transmissão, manutenção e guarda de dados, informações, documentos e materiais sigilosos observarão medidas especiais de segurança;

c) toda autoridade responsável pelo trato de dados, informações, documentos, materiais, áreas, instalações ou sistemas de informação digital sigilosos providenciará para que o pessoal sob suas ordens conheça integralmente as medidas de segurança estabelecidas, zelando pelo seu fiel cumprimento; e

d) toda e qualquer pessoa que tome conhecimento de assuntos, dados, informações, documentos, materiais, áreas, instalações ou sistemas de informação digital de natureza sigilosa fica, automaticamente, responsável pela preservação do seu sigilo.

2.2 - CLASSIFICAÇÃO SEGUNDO O GRAU DE SIGILO

Os dados, informações, documentos e materiais sigilosos, assim como as áreas e instalações onde tramitam serão classificados em ultra-secretos, secretos, confidenciais ou reservados, em razão do seu teor ou dos seus elementos intrínsecos.

2.2.1 - Princípio Fundamental da Classificação do Sigilo

São considerados originariamente sigilosos, e serão como tal classificados, dados, informações, documentos e materiais cujo conhecimento irrestrito ou divulgado possa acarretar qualquer risco à segurança da sociedade, do Estado, da MB ou das demais Forças Armadas, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra ou da imagem das pessoas.

2.2.2 - Classificação como Ultra-Secreto

São passíveis de classificação como ultra-secretos, dentre outros, dados, informações ou documentos 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 ou do Estado.

2.2.3 - Classificação como Secreto

São passíveis de classificação como secretos, dentre outros, dados, informações ou documentos 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 MB, da sociedade ou do Estado.

2.2.4 - Classificação como Confidencial

São passíveis de classificação como confidenciais, dentre outros, dados, informações ou documentos que, no interesse da MB, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da MB, da sociedade ou do Estado.

2.2.5 - Classificação como Reservado

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

2.3 - COMPETÊNCIA DA CLASSIFICAÇÃO DO GRAU DE SIGILO

2.3.1 - Ultra-Secreto

A classificação no grau de sigilo 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.

2.3.2 - Secreto

A classificação no grau de sigilo secreto é de competência, além das autoridades mencionadas acima para o grau de sigilo ultra-secreto, dos Almirantes e das autoridades que exerçam funções de direção, comando ou chefia.

2.3.3 - Confidencial e Reservado

A classificação no grau de sigilo confidencial e reservado é de competência, além das autoridades mencionadas acima para os graus de sigilo ultra-secreto e secreto, dos Oficiais e servidores civis equiparados.

2.4 - PRAZO DE DURAÇÃO DA CLASSIFICAÇÃO

Os prazos de duração da classificação do grau de sigilo vigoram a partir da data de produção do dado, documento ou informação e são os seguintes:

a) ultra-secreto: máximo de 30 (trinta) anos;

b) secreto: máximo de 20 (vinte) anos;

c) confidencial: máximo de 10 (dez) anos; e

d) reservado: máximo de 5 (cinco) anos.

2.4.1 - No caso de documentos sigilosos referentes à segurança da sociedade ou do Estado, o prazo de duração da classificação será restrito a um período máximo de 30 (trinta) anos, a contar da data de sua produção, podendo esse prazo ser prorrogado, por uma única vez, por igual período.

2.4.2 - No caso de documentos sigilosos referentes à honra e à imagem das pessoas, o prazo de duração da classificação será restrito a um período máximo de 100 (cem) anos, a contar da data de sua produção.

2.5 - RENOVAÇÃO DO PRAZO DE DURAÇÃO DA CLASSIFICAÇÃO

Os prazos de classificação poderão ser prorrogados uma vez, por igual período, pela autoridade responsável pela classificação ou autoridade hierarquicamente superior competente para dispor sobre a matéria.

2.6 - RECLASSIFICAÇÃO E DESCLASSIFICAÇÃO

2.6.1 - Ultra-secreto

Dados, informações, documentos ou materiais classificados como ultra-secretos somente poderão ser reclassificados ou desclassificados mediante decisão da autoridade responsável pela sua classificação .

2.6.2 - Secreto, Confidencial e Reservado

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

2.7 - PRAZO DE DURAÇÃO DA RECLASSIFICAÇÃO

Na reclassificação, o novo prazo de duração é o mesmo previsto para a classificação e conta-se a partir da data de produção do dado ou informação.

2.8 - DESCLASSIFICAÇÃO AUTOMÁTICA

A desclassificação dos graus ultra-secreto, secreto, confidencial e reservado será automática, após transcorridos os prazos previstos para cada um, salvo no caso de renovação, quando então a desclassificação ocorrerá ao final de seu termo.

2.9 - ENCAMINHAMENTO APÓS DESCLASSIFICAÇÃO

Dados, informações, documentos ou materiais sigilosos de guarda permanente que forem objeto de desclassificação serão encaminhados ao Serviço de Documentação da Marinha (SDM), para fins de organização, preservação e acesso.

2.9.1 - Guarda Permanente

São considerados de guarda permanente os dados, informações, documentos ou materiais de valor histórico, probatório ou informativo que devam ser definitivamente preservados.

2.10 - INDICAÇÃO DA RECLASSIFICAÇÃO OU DA DESCLASSIFICAÇÃO

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

CAPÍTULO 3

GESTÃO DE MATERIAIS SIGILOSOS

3.1 - PROCEDIMENTOS PARA CLASSIFICAÇÃO DE DOCUMENTOS SIGILOSOS

3.1.1 - Partes Componentes do Documento Sigiloso

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.

3.1.2 - Grupo de Documentos

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.

3.1.3 - Atos Sigilosos

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.

3.1.4 - Documentos Especiais Sigilosos

Os mapas, planos-relevo, cartas e fotocartas baseados em fotografias ou em seus negativos, e outros documentos especiais, quando sigilosos, serão classificados em razão dos detalhes que revelem ou informações contidas e não da classificação atribuída às fotografias, negativos ou outros itens que lhes deram origem ou das diretrizes baixadas para obtê-los.

3.1.5 - Extratos de Documentos Sigilosos

Aos extratos serão atribuídos graus de sigilo iguais ou inferiores àqueles atribuídos aos documentos sigilosos que lhes deram origem. 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 da 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.

3.2 - DOCUMENTO SIGILOSO CONTROLADO

Documento Sigiloso Controlado (DSC) é aquele que, por sua importância, requer medidas adicionais de controle.

3.2.1 - Medidas Adicionais de Controle

As medidas adicionais de controle devem, no mínimo, incluir:

a) identificação dos destinatários em protocolo e recibo próprios, quando da difusão;

b) lavratura de termo de custódia e registro em protocolo específico;

c) lavratura anual de Termo de Inventário, pelo setor da MB responsável por determinar a distribuição do documento controlado e pela OM receptora; e

d) lavratura de Termo de Transferência, sempre que se proceder à transferência de sua custódia, como na passagem de cargo do titular da OM ou da função de ORC.

3.2.2 - Termo de Inventário e Termo de Transferência

O Termo de Inventário e o Termo de Transferência ficarão sob a guarda das OM que os lavraram e deverão conter: local e data, inventário dos DSC e, conforme o caso, nome e assinatura do ORC ou nomes e assinaturas dos ORC substituído e substituto.

3.2.3 - Documentos Ultra-secreto ou Secreto

Os documentos Ultra-secretos ou Secretos são, por sua natureza, considerados DSC, desde sua classificação ou reclassificação.

3.2.4 - Documento Confidencial ou Reservado

Os documentos confidenciais ou reservados poderão ser considerados DSC, a critério da autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto.

3.3 - MARCAÇÃO DE DOCUMENTOS SIGILOSOS CONTROLADOS

A marcação ou indicação do grau de sigilo deverá ser feita em todas as páginas do documento e nas capas, se houver.

3.3.1 - Numeração das páginas

As páginas serão numeradas seguidamente, devendo cada uma conter, também, a indicação do total de páginas que compõem o documento.

3.3.2 - Documento Sigiloso Controlado

O DSC também expressará, nas capas, se houver, e em todas suas páginas, a expressão "**DOCUMENTO SIGILOSO CONTROLADO (DSC)"** e o respectivo número de controle.

3.3.3 - Extratos, Rascunhos, Esboços e Desenhos Sigilosos

A marcação em extratos de documentos, rascunhos, esboços e desenhos sigilosos obedecerá ao anteriormente prescrito.

3.3.4 - Documentos Especiais

A indicação do grau de sigilo em mapas, fotocartas, cartas, fotografias, ou quaisquer outras imagens sigilosas deve ser feita nos respectivos envelopes ou invólucros, de modo a ser visualizada antes que se tenha acesso à imagem sigilosa propriamente dita. A marcação ou indicação do grau de sigilo de fitas magnéticas, disquetes, discos ópticos ou quaisquer outros meios de armazenamento de dados ou informações digitais sigilosos deve ser feita em local apropriado, de imediata visualização, antes que se tenha acesso aos dados ou informações sigilosos propriamente ditos.

3.4 - EXPEDIÇÃO E TRAMITAÇÃO DE MATERIAL CONTROLADO

A expedição de material controlado ao seu destinatário, utilizando meios de transporte e salvaguarda adequados, abrange o período desde o acondicionamento ou preparação do material até a chegada ao remetente do recibo assinado pelo destinatário ou da notificação de recebimento.

Na expedição de material controlado devem ser utilizados sistemas de recibos, contra-recibos, protocolos ou notificação de recebimento, que assegurem ao remetente, ao destinatário e, quando for o caso, ao portador, as respectivas responsabilidades pelo material.

Quando o transporte de material controlado for confiado a um portador, o remetente deverá assegurar-se de que as medidas de segurança apropriadas estão sendo adotadas e de que o portador autorizado esteja ciente dos seus deveres e responsabilidades, bem como sobre a maneira de proceder ao pressentir qualquer anormalidade que possa vir a afetar a segurança do material transportado, até a entrega do material ao destinatário.

3.4.1 - Preparação

O material controlado deverá ser cuidadosa e adequadamente preparado para a expedição, tendo-se em mente que o manuseio a que será submetido poderá comprometer sua segurança física ou de conteúdo.

Quando se tratar de documento sigiloso e este tiver que ser acondicionado, cuidados específicos deverão ser observados, de acordo com o grau de sigilo e o tipo do material, conforme abaixo discriminado:

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 conterá, junto ao documento, um recibo, que indicará, necessariamente, remetente, destinatário e número ou outro indicativo que identifique o documento. Como lacre, também poderá ser utilizada fita plástica gomada, passada sobre as aberturas da embalagem. Estas aberturas devem estar coladas e conter o carimbo da OM, sobreposto da rubrica do EMC/ORC;

e) quando se tratar de DSC, terá sobrescrito, no envelope interno, os dizeres "**ESTA EMBALAGEM SÓ PODE SER ABERTA PESSOALMENTE PELO DESTINATÁRIO OU ENCARREGADO DO MATERIAL CONTROLADO**"; e

f) sempre que o assunto for considerado de interesse exclusivo do destinatário, será inscrita a palavra "**PESSOAL**" no envelope interno.

3.4.2 - Documento Ultra-secreto

A expedição, condução, entrega e tramitação de documento ultra-secreto, em princípio, será efetuada pessoalmente, por portador designado de forma oficial, observando-se as prescrições de preparação e sendo terminantemente vedada a sua postagem. A comunicação de assunto ultra-secreto de outra forma que não a prescrita só será permitida excepcionalmente e em casos extremos, que requeiram tramitação e solução imediatas, em atendimento ao princípio da oportunidade e considerados os interesses da MB, da sociedade e do Estado. No caso de uso de meios eletrônicos ou digitais, os documentos ultra-secretos deverão ser assinados digitalmente e duplamente cifrados, utilizando-se os recursos criptológicos em vigor na MB.

3.4.3 - Documento Secreto, Confidencial ou Reservado

A expedição de documento secreto, confidencial ou reservado será efetuada, preferencialmente, por meio eletrônico ou digital. Na impossibilidade do uso desses meios, permite-se, observando-se as prescrições de preparação, o emprego de serviço postal com opção de registro, mensageiro oficialmente designado, sistema de encomendas ou, se for o caso, mala diplomática. No caso de uso de meio eletrônico ou digital, os documentos deverão ser cifrados, utilizando-se os recursos

criptológicos em vigor na MB, sendo que os documentos secretos deverão ser assinados digitalmente e duplamente cifrados.

3.5 - RECEBIMENTO E REGISTRO DE DOCUMENTOS SIGILOSOS

3.5.1 - Recebimento e registro na OM

Cabe aos responsáveis pelo recebimento de documentos sigilosos na OM:

a) verificar a integridade e registrar, se for o caso, indícios de violação ou qualquer irregularidade na correspondência recebida, dando ciência do fato ao seu superior hierárquico e ao destinatário, o qual informará imediatamente ao remetente; e

b) proceder ao registro do documento na OM e ao controle de sua tramitação interna.

3.5.2 - Abertura do envelope interno

O envelope interno só será aberto pelo destinatário, seu representante autorizado ou autoridade competente hierarquicamente superior. Envelope contendo a marca "**PESSOAL**" só poderá ser aberto pelo próprio destinatário.

3.5.3 - Indício de violação no recebimento

O destinatário de documento sigiloso comunicará imediatamente ao remetente, e a quem mais julgar necessário, qualquer indício de violação ou adulteração do documento.

3.6 - GUARDA E ARMAZENAMENTO DE DOCUMENTOS SIGILOSOS EM MEIO ELETRÔNICO OU DIGITAL

3.6.1 - Uso obrigatório de recursos criptológicos

Todos os documentos sigilosos, para serem armazenados em meio eletrônico ou digital, devem ser, obrigatoriamente, criptografados, utilizando-se os recursos criptológicos em vigor da MB e observando-se as normas e procedimentos previstos pela DGMM.

3.6.2 - Meio eletrônico ou digital para documentos ultra-secretos

O meio de armazenamento eletrônico ou digital de documentos ultra-secretos deve ser, preferencialmente, removível e não magnético, como os discos ópticos, observando-se o uso de criptografia. No caso do armazenamento desses documentos diretamente em microcomputadores, estes deverão estar:

a) isolados de qualquer rede;

b) localizados em compartimento fechado e de acesso restrito; e

c) protegidos pelas medidas de segurança física e lógica previstas nas normas da DGMM.

O meio de armazenamento (mídia removível ou microcomputador) contendo documento ultra-secreto será tratado como material confidencial e será controlado.

3.6.3 - Meio eletrônico ou digital para documentos secretos, confidenciais e reservados

O meio de armazenamento eletrônico ou digital de documentos secretos, confidenciais ou reservados deve ser, preferencialmente, removível, como os discos ópticos ou os disquetes, observando-se o uso de criptografia. No caso do armazenamento desses documentos diretamente em microcomputadores, estes deverão estar:

a) localizados em compartimento fechado e de acesso restrito; e

b) protegidos pelas medidas de segurança física e lógica previstas nas normas da DGMM.

3.6.4 - Recomendações Especiais

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

3.7 - GUARDA E ARMAZENAMENTO DE DOCUMENTOS SIGILOSOS EM MEIO DIFERENTE DO ELETRÔNICO OU DIGITAL

3.7.1 - Documentos ultra-secretos e secretos

Para a guarda de documentos ultra-secretos e secretos, em meio diferente do eletrônico ou digital, é obrigatório o uso de cofre de aço ou estrutura que ofereça segurança equivalente ou superior, localizado em compartimento fechado e de acesso restrito. Neste caso, o documento ultra-secreto estará acondicionado em envelope lacrado. Na impossibilidade do uso de cofre de aço ou estrutura de segurança equivalente, os documentos ultra-secretos e secretos deverão ser mantidos em envelope lacrado e sob guarda armada.

3.7.2 - Documentos confidenciais e reservados

A guarda de documentos confidenciais e reservados, em meio diferente do eletrônico ou digital, deve ser feita em armário ou arquivo de metal com fechadura, localizado em compartimento de acesso restrito.

3.7.3 - Recomendações no uso de cofre

A restrição a um mínimo de conhecedores do segredo do cofre é fundamental para a segurança do material sigiloso nele contido. Assim sendo, o responsável pelo cofre deve adotar os seguintes procedimentos:

a) mudar o segredo do cofre sempre que este for recebido na incumbência (oriundo de

outro setor, de outra OM, do comércio ou do fabricante), houver transferência de responsabilidade da incumbência ou ocorrer suspeita de violação física do cofre, ou de comprometimento da combinação de segredo;

b) escolher a combinação de segredo de modo aleatório, tendo o cuidado para não corresponder a data significativa, número de identificação, números consecutivos ou qualquer ordem definida; e

c) manter uma cópia do segredo em envelope lacrado pelo responsável e guardado em local pré-determinado na OM, que proporcione adequada segurança a essa cópia e possibilite o acesso autorizado em caso de emergência.

É recomendável a memorização do segredo do cofre pelo responsável, o qual não deverá anotá-lo como lembrete pessoal em objetos, blocos de notas, agendas, etc.

3.8 - PASSAGEM OU TRANSFERÊNCIA DE RESPONSABILIDADE DE DOCUMENTOS SIGILOSOS

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

3.9 - REPRODUÇÃO DE DOCUMENTOS SIGILOSOS

3.9.1 - Grau de sigilo

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

3.9.2 - Documentos Sigilosos Controlados (DSC)

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

3.9.3 - Autenticação

Eventuais cópias decorrentes de documentos sigilosos, quando necessário (por exemplo, em juízo), serão autenticadas pelo chefe de uma das subcomissões previstas no artigo 5.1 destas normas.

3.9.4 - Certidões

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

3.9.5 - Eliminação de indícios

O responsável pela produção ou reprodução de documento sigiloso deverá providenciar a eliminação de notas manuscritas, tipos, clichês, carbonos, provas ou quaisquer outros recursos que possam dar origem a cópias não autorizadas de parte ou de todo o documento.

3.9.6 - Acompanhamento

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, observando o disposto no inciso anterior quanto à eliminação de indícios.

3.10 - RECURSOS CRIPTOLÓGICOS

3.10.1 - Segurança e salvaguarda

Aplicam-se aos códigos, cifras, chaves, programas, aplicativos, sistemas e equipamentos de criptografia todas as medidas de segurança e salvaguarda previstas nestas normas para os documentos sigilosos, de acordo com os respectivos graus de sigilo.

3.10.2 - Recursos em vigor

Somente devem ser utilizados os programas, aplicativos, sistemas e equipamentos criptológicos homologados e em vigor na MB, de acordo com as normas estabelecidas pela DGMM.

3.10.3 - Uso em razão do serviço

É vedada a utilização de código, cifra ou sistema de criptografia que não seja em função do serviço.

3.10.4 - Comunicação de irregularidades

Devem ser imediatamente comunicados quaisquer indícios de violação, interceptação ou irregularidades na transmissão ou no recebimento de dados, informações digitais ou documentos criptografados.

3.11 - SISTEMAS DE INFORMAÇÃO DIGITAL (SID)

3.11.1 - Segurança e salvaguarda

Aplicam-se à gestão da segurança de sistemas de informação digital todas as medidas de segurança e salvaguarda previstas no Manual de Inteligência da

Marinha – Contra-Inteligência, estabelecido pelo EMA e nas normas específicas de Segurança da Informação Digital (SID) estabelecidas pela DGMM.

3.11.2 - Assinatura digital e criptografia

Os dados e informações digitais sigilosos, constantes de documentos produzidos em meio eletrônico ou digital, serão assinados digitalmente e criptografados, utilizando-se os recursos criptológicos em vigor na MB.

3.11.3 - Produção de documentos ultra-secretos

Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo ultra-secreto só poderão estar ligados a redes de computadores seguras e que estejam física e logicamente separadas da Rede de Comunicações Integradas da Marinha (RECIM) e de qualquer outra rede.

3.11.4 - Produção de documentos secretos, confidenciais e reservados

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 recursos criptológicos e de segurança adequados à proteção dos documentos.

3.12 - MATERIAL SIGILOSO NÃO ENQUADRADO COMO DOCUMENTO

3.12.1 - Segurança e salvaguarda

Sempre que couber, aplicam-se aos materiais sigilosos não enquadrados como documentos todas as medidas de segurança e salvaguarda previstas nestas normas para os documentos sigilosos, de acordo com os respectivos graus de sigilo.

3.12.2 - Grau de sigilo adequado

O titular de OM responsável por projeto ou programa de pesquisa, por fiscalizar ou por controlar atividades de outra OM ou entidade pública ou privada, que julgar conveniente, de acordo com os interesses da MB e da Defesa Nacional, manter sigilo sobre determinado material ou suas partes, em decorrência de aperfeiçoamento, prova, produção, aquisição ou exportação, deverá providenciar para que lhe seja atribuído o grau de sigilo adequado.

3.12.3 - Instruções adicionais de segurança

O titular de OM com atribuições de preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de novo projeto, prova, produção aquisição, armazenagem ou emprego de material sigiloso deverá expedir instruções adicionais de segurança necessárias à salvaguarda desses itens e dos assuntos relacionados.

3.12.4 - Marcação

Todos os modelos, protótipos, moldes, máquinas, equipamentos e outros materiais considerados sigilosos e não enquadrados como documentos, inclusive os que sejam objeto de contrato de qualquer natureza, como empréstimo, cessão, arrendamento ou locação, deverão ser adequadamente marcados para indicar o seu grau de sigilo.

3.12.5 - Dados ou informações de materiais sigilosos

Dados ou informações sigilosos concernentes a programas técnicos ou aperfeiçoamento de material sigiloso somente serão fornecidos aos que, por suas funções oficiais ou contratuais, a eles devam ter acesso.

3.12.6 - Desenvolvimento extra-MB

As OM responsáveis por desenvolvimento de programas ou projetos sigilosos coordenarão e controlarão o fornecimento de dados e informações sigilosos, restrito ao mínimo indispensável, a pessoas físicas e jurídicas extra-MB que participem do desenvolvimento desses programas ou projetos.

3.12.7 - Expedição de material sigiloso

Sempre que possível, os materiais sigilosos não enquadrados como documentos serão expedidos segundo os critérios indicados para a expedição de documentos sigilosos.

3.12.8 - Transporte de material sigiloso

A definição do meio de transporte a ser utilizado para deslocamento de material sigiloso é de responsabilidade do detentor da custódia e deverá considerar o respectivo grau de sigilo.

3.12.9 - Guarda armada no transporte de material sigiloso

A critério da autoridade competente, poderão ser empregados guardas armados para o transporte de material sigiloso.

3.12.10 - Transporte de material sigiloso por empresa contratada

O material sigiloso poderá ser transportado por empresa contratada para tal fim. As medidas necessárias para a segurança do material sigiloso transportado serão estabelecidas em entendimentos prévios, por meio de cláusulas contratuais específicas, e serão de responsabilidade da empresa, sob fiscalização da OM contratante.

3.13 - ÁREAS E INSTALAÇÕES SIGILOSAS

3.13.1 - Segurança e salvaguarda

Aplicam-se à gestão da segurança de áreas e instalações sigilosas todas as medidas de segurança e salvaguarda previstas no Manual de Inteligência da Marinha – Contra-Inteligência, estabelecido pelo EMA e nas normas específicas de SID estabelecidas pela DGMM.

3.13.2 - Instruções adicionais de segurança

O titular da OM é responsável por adotar e fazer cumprir as medidas que visem à definição, demarcação, sinalização, segurança, autorização e controle de acesso às áreas sigilosas sob sua responsabilidade.

3.14 - NOTIFICAÇÃO OBRIGATÓRIA EM CASO DE IRREGULARIDADES

É obrigatória a comunicação imediata, ao superior hierárquico e à autoridade competente, de qualquer anormalidade que represente ameaça ou comprometa, direta ou indiretamente, o sigilo, a autenticidade, a integridade ou a disponibilidade de dados, informações, documentos, materiais, áreas, instalações e sistemas de informação digital sigilosos.

CAPÍTULO 4
CUSTÓDIA E CONTROLE

4.1 - CUSTÓDIA

A custódia constitui ferramenta importante a ser empregada na salvaguarda e no controle do material controlado.

4.1.1 - Custódia sob enfoque da contabilidade patrimonial

A sistemática de custódia do material da MB controlado sob o enfoque da contabilidade patrimonial é normatizada pela Secretaria-Geral de Marinha (SGM).

4.1.2 - Custódia de material controlado sigiloso

Todo material controlado sigiloso existente em uma OM ficará, para fins externos a essa OM, sob a responsabilidade do Oficial Responsável pela Custódia (ORC).

4.1.3 - Oficial Responsável pela Custódia (ORC)

O ORC será o titular da OM ou, nas OM onde o titular for Oficial General, um Oficial Superior ou Intermediário, subordinado, devendo:

a) ser designado de forma oficial;

b) ter sua designação participada externamente tanto à OM que controla o material quanto, caso exista, àquela que realizou a sua distribuição; e

c) responder, para fins externos à OM, pelas funções de ORC.

4.1.4 - Responsabilidades do ORC

Ao ORC caberá cumprir e fazer cumprir, na OM, todas as disposições de controle previstas nestas normas, inclusive no tocante à assinatura dos inventários periódicos, dos recibos e dos respectivos Termos de Destruição.

4.1.5 - Encarregado do Material Controlado (EMC)

O titular da OM poderá designar, formalmente, um oficial subordinado para ser o EMC, a quem caberá:

a) receber do titular da OM o material controlado sigiloso que lhe foi confiado, mediante recibo interno; e

b) custodiar internamente o material controlado sigiloso da OM.

4.2 - DISTRIBUIÇÃO INTERNA DE MATERIAL CONTROLADO SIGILOSO

Quando julgar necessário e mediante recibo, o titular da OM poderá mandar distribuir internamente o material controlado sigiloso.

4.2.1 - Conteúdo do recibo interno

O recibo interno deverá conter os dados necessários à correta identificação, localização e custódia do material.

4.2.2 - Restrições para a distribuição interna de material controlado sigiloso

A distribuição interna de material controlado sigiloso será efetuada somente para aqueles, a quem for transferida a custódia, que dispuserem de local e meios adequados para a sua guarda.

4.2.3 - Delegação de competência

Nas OM onde o titular for Oficial General, este poderá delegar competência ao ORC para executar e fiscalizar a distribuição interna do material controlado sigiloso.

4.2.4 - Custódia transferida de forma sistemática

Quando a distribuição interna for realizada de modo que a custódia sobre esse material seja transferida de forma sistemática, deverão ser adotadas medidas especiais para que o exercício da "custódia temporária" não sofra solução de continuidade.

4.2.5 - Recursos criptológicos

Quando o material controlado sigiloso for criptológico, este somente será distribuído internamente em situações especiais, a fim de atender às necessidades de manuseio durante sua operação, cujos procedimentos constam das normas estabelecidas pela DGMM.

4.3 - CONTROLE

Os setores da MB responsáveis por determinar a distribuição de material controlado efetuarão o controle sobre a custódia desse material. Para isso, produzirão os inventários.

4.3.1 - Inventários

Os inventários deverão conter todos os dados necessários à perfeita identificação do material a ser controlado e devem ser produzidos, obrigatoriamente, nas seguintes situações:

a) transferência de responsabilidade – por ocasião da passagem de cargo do titular da OM ou passagem de função do ORC. Nestes casos, os inventários serão assinados fisicamente pelo Oficial que passa e pelo que assume;

b) anualmente – quando decorrido um ano após o envio do último inventário;

c) criação ou extinção de OM – quando do recebimento da distribuição inicial da dotação de uma OM ou por ocasião de sua desativação ou extinção, respectivamente; e

d) eventualmente – quando determinado pela autoridade responsável pelo controle do material.

4.3.2 - Instruções complementares para o controle

As OM responsáveis por determinar a distribuição de material controlado expedirão instruções complementares específicas para o controle desse material.

4.3.3 - Controle sob enfoque da contabilidade patrimonial

O controle do material da MB sob o enfoque da contabilidade patrimonial é normatizado pela SGM.

4.3.4 - Controle das publicações controladas nas Adidâncias e Missões Navais Brasileiras no Exterior

No caso específico das Adidâncias e das Missões Navais Brasileiras no Exterior, visando manter um acurado controle sobre as publicações controladas, o EMA solicitará às Organizações Militares Aprovadoras (OMA) e encaminhará, automaticamente, até 20 dias antes das datas previstas para a produção de inventários, os pertencentes àquelas Organizações Militares Utilizadoras (OMU) que, por sua vez, após preenchê-los e assiná-los, deverão restituí-los às OMA assinaladas no inventário.

Caberá às OMA, após recebidos os respectivos inventários das Adidâncias/Missões Navais, participar ao EMA a situação regular (ou não) das publicações controladas, de acordo com a seguinte mensagem padrão:

ROTINA/OSTENSIVA

DATA-HORA

DO: OMA

PARA: ARMADA

INFO: ADIDÂNCIA OU MN

GRNC

BT

ACD INCISO 4.3.4 EMA-414 VG INVENTÁRIO DESTA OMA RECEBIDO VG SITUAÇÃO (REGULAR/IRREGULAR) BT

CAPÍTULO 5

AVALIAÇÃO, PRESERVAÇÃO, ACESSO E COMPROMETIMENTO

5.1 - AVALIAÇÃO

A avaliação de material sigiloso tem o propósito de determinar a necessidade de renovação, reclassificação ou desclassificação desse material sigiloso, bem como autorizar ou não o acesso de cidadãos a documentos sigilosos, mediante requerimento e observados os requisitos e procedimentos previstos na legislação vigente. Na MB, é realizada pela Comissão Permanente de Avaliação de Documentos Sigilosos da Marinha (CPADSM), auxiliada pelas Subcomissões Permanentes de Avaliação de Documentos Sigilosos da Marinha (SPADSM) e pelas Comissões de Triagem das OM.

5.1.1 - Comissão Permanente de Avaliação de Documentos Sigilosos da Marinha (CPADSM)

É a comissão, constituída por Oficial General, denominado Presidente da CPADSM, e por dois Oficiais Superiores, todos do EMA, responsável, no âmbito da Alta Administração Naval, pela avaliação periódica e concessão de acesso a documentos sigilosos.

5.1.2 - Subcomissões Permanentes de Avaliação de Documentos Sigilosos da Marinha (SPADSM)

São as comissões criadas:

a) pelos titulares dos Órgãos de Direção Setorial, nas suas áreas de atuação;

b) pelo Vice-Chefe do Estado-Maior da Armada, no âmbito do Órgão de Direção Geral e OM subordinadas; e

c) pelo Chefe de Gabinete do Comandante da Marinha, no âmbito dos órgãos de assessoramento e vinculados, dos Conselhos e Comissões do Comandante da Marinha e do Almirantado.

Essas comissões são responsáveis, nos respectivos setores, pelo acesso e pela análise periódica de documentos públicos sigilosos.

5.1.3 - Atribuições da CPADSM

A CPADSM tem as seguintes atribuições:

a) encaminhar, semestralmente, até o dia 30 dos meses de junho e novembro, ao Serviço de Documentação da Marinha (SDM), com informação à SPADSM competente, a relação dos documentos sigilosos que foram desclassificados, utilizando o modelo do Anexo A;

b) retransmitir à SPADSM competente o pedido de consulta a documento encaminhado diretamente à CPADSM;

c) deliberar, em até 48 horas, para resposta a requerimentos de consulta a documentos sigilosos, comunicando sua decisão ao requerente em até 24 horas após a deliberação, de acordo com o modelo do anexo B;

d) solicitar à SPADSM competente, se necessário, eventuais subsídios para resposta a requerimentos de consulta a documentos sigilosos;

e) supervisionar as atividades das SPADSM;

f) acompanhar as possíveis modificações ocorridas na legislação em vigor, de modo a subsidiar o EMA com as informações necessárias à atualização destas normas; e

g) julgar os casos submetidos à sua apreciação pelas SPADSM.

5.1.4 - Atribuições das SPADSM

As SPADSM têm as seguintes atribuições:

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, alteração ou cancelamento da classificação sigilosa;

c) determinar o destino final da documentação tornada ostensiva, selecionando os documentos para guarda permanente e preservação pelo SDM;

d) encaminhar à CPADSM, semestralmente, até o dia 30 dos meses de maio e outubro, a relação dos documentos sigilosos que foram desclassificados do seu setor, utilizando o modelo do Anexo A;

e) deliberar, em até 48 horas, para resposta a requerimentos de consulta a documentos sigilosos, comunicando sua decisão ao requerente em até 24 horas após a deliberação, de acordo com o modelo do anexo B;

f) expedir certidão de documentos sigilosos que não puderem ser reproduzidos devido ao seu estado de conservação, desde que necessário como prova em juízo;

g) autenticar os documentos sigilosos reproduzidos para instruir processos judiciais;

h) fornecer subsídios à CPADSM sobre possíveis modificações ocorridas na legislação em vigor, que impliquem a atualização destas normas;

i) encaminhar à CPADSM os casos que, a seu critério, necessitem da apreciação daquela Comissão;

j) marcar, na comunicação de deferimento do pedido, o dia e a hora para que o requerente tome conhecimento ou obtenha a reprodução do documento, conforme o caso;

k) justificar, por escrito, a negativa de autorização de acesso;

l) providenciar junto à OM que tenha a custódia do documento acessado para que esta promova a retificação, no prazo de dez dias após a entrada do requerimento, de qualquer dado, conforme solicitado pelo interessado, em petição acompanhada de documentos comprobatórios;

m)providenciar junto à OM que tenha a custódia do documento acessado para que esta dê ciência ao interessado da retificação efetuada; e

n) retransmitir à SPADSM competente o pedido de consulta que não pertença à sua esfera de atuação.

5.1.5 - Atribuições das OM

As OM, por meio de suas respectivas Comissões de Triagem, designadas nos termos das normas sobre documentação administrativa e arquivamento na Marinha, estabelecida pela Secretaria Geral da Marinha (SGM), têm as seguintes atribuições:

a) providenciar para que a Comissão de Triagem se reuna até o dia 30 dos meses de abril e setembro, para análise dos documentos públicos sigilosos sob custódia da OM, submetendo-os à autoridade responsável pela classificação, a qual efetuará a sua desclassificação, reclassificação ou renovação da classificação, conforme o caso;

b) enviar a relação dos documentos públicos sigilosos que foram desclassificados, até o dia 10 dos meses de maio e outubro, para a SPADSM de seu setor, utilizando o modelo do Anexo A;

c) relacionar e encaminhar ao SDM os documentos públicos sigilosos desclassificados que tenham reconhecido valor histórico para, a critério daquele Serviço, compor o arquivo permanente da Marinha, dando conhecimento à SPADSM de seu setor;

d) promover, no prazo estipulado pela SPADSM, a retificação de dados de documento de que tenha a custódia, dando posterior ciência ao interessado, conforme o modelo do anexo C; e

e) encaminhar à SPADSM de seu setor as solicitações de acesso a documentos públicos sigilosos recebidas.

5.1.6 - Generalidades

a) as disposições constantes desta publicação não se aplicam aos documentos ostensivos;

b) a Administração Naval franqueará a consulta aos documentos públicos, devendo o requerente indenizar, exclusivamente, as despesas efetuadas com quaisquer reproduções de documentos solicitados;

c) os documentos que contenham informação que comprometa a vida privada, a honra e a imagem de terceiro são restritos pelo prazo de cem anos, somente podendo ser totalmente reproduzidos, antes de findo este período, se assim autorizado por aquela pessoa ou seus herdeiros;

d) o Poder Judiciário, em qualquer instância, poderá determinar a exibição reservada de qualquer documento público sigiloso, sempre que julgado imprescindível à defesa de direito próprio ou necessário ao esclarecimento de situação pessoal da parte em processo judicial;

e) o Ministério Público poderá requisitar o envio de qualquer documento público sigiloso, em prazo por ele fixado;

f) nenhuma norma de organização, aprovada em âmbito naval, deverá ser interpretada de modo a restringir o disposto nas alíneas d e e; e

g) as disposições constantes desta publicação aplicam-se, também, aos documentos eletrônicos.

5.2 - PRESERVAÇÃO

Os dados, informações, documentos e materiais tornados ostensivos e avaliados como sendo de valor histórico, probatório ou informativo serão considerados de guarda permanente e encaminhados ao SDM, que os organizará, preservará e possibilitará o acesso.

5.2.1 - Obrigatoriedade da preservação

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

5.3 - ACESSO

5.3.1 - Generalidades

O controle de acesso, à semelhança da custódia para o material controlado, é uma ferramenta importante para a salvaguarda do material sigiloso. Desta forma, o acesso

a material sigiloso deverá ser limitado ao menor número possível de pessoas, a fim de tornar mais efetiva esta segurança. Adicionalmente, cuidados especiais com as áreas e instalações sigilosas contribuirão para restringir o acesso e, conseqüentemente, aumentar sua segurança.

Os Encarregados de sindicância poderão orientar-se por esta Publicação para dirigir seus depoimentos, com base nos capítulos que instruem sobre a expedição, custódia, acesso e comprometimento do material controlado.

O extravio de publicação controlada ou vazamento de conhecimento sigiloso deve passar a ser acompanhado por intermédio de um controle das ocorrências, realizado pela OME, para, a qualquer momento, permitir resgatar as circunstâncias em que ocorreu o comprometimento, pois as repercussões desses fatos poderão ocorrer após longos períodos de tempo decorridos desde o evento inicial.

A princípio, uma avaliação qualitativa do comprometimento ou vazamento de conhecimento ou dado sigiloso, contido em uma PMB, transcende a condução de uma Sindicância ou IPM. Cabe ressaltar que, além das limitações expostas no item anterior, nem sempre o encarregado de uma Sindicância ou IPM terá os conhecimentos técnico-profissionais necessários para este tipo de avaliação.

O simples manuseio de material sigiloso, mesmo que momentâneo, deve ser considerado como acesso e, portanto, restrito ao menor número possível de pessoas, a fim de tornar efetiva a salvaguarda da matéria ou dos assuntos contidos nesse material.

5.3.2 - Concessão de acesso

O acesso a material sigiloso será fornecido:

a) ao militar, funcionário civil, prestador de serviço ou agente público que possuir necessidade de conhecer e credencial de segurança dentro do período de validade e de categoria correspondente ao grau de sigilo; ou

b) ao cidadão, naquilo que diga respeito à sua pessoa, ao seu interesse particular ou ao interesse coletivo ou geral, mediante requerimento à CPADSM ou SPADSM e observados os requisitos e procedimentos previstos na legislação vigente.

5.3.3 - Consulta e retirada de publicações por militares e civis brasileiros credenciados pela MB

a) material Ultra-Secreto - poderá ser consultado por pessoa credenciada e com necessidade de conhecer, sem ser retirado do compartimento onde o mesmo esteja

guardado;

b) material Secreto - poderá ser consultado por pessoa credenciada e com necessidade de conhecer, sem sair da OM. Deverá ser restituído antes que a mesma se ausente da OM; e

c) material Confidencial ou Reservado - poderá ser consultado e retirado por pessoa devidamente credenciada, com necessidade de conhecer.

5.3.4 - Consulta e retirada de publicações por militares ou civis estrangeiros

a) material Ultra-Secreto - esse material não poderá, em qualquer circunstância, ser consultado; e

b) material Secreto ou Confidencial - poderá ser consultado e retirado, quando devidamente credenciado e mediante autorização da autoridade brasileira a qual estiver subordinado enquanto em missão na MB.

5.3.5 - Prescrições relativas à concessão de acesso a material sigiloso

Devem ser observadas as seguintes prescrições na concessão de acesso a material sigiloso:

a) todo aquele que tiver conhecimento de assuntos sigilosos fica sujeito às sanções administrativas, civis e penais decorrentes da sua eventual divulgação;

b) os procedimentos ou processos que forem instruídos por dados, informações ou documentos sigilosos passam também a ter grau de sigilo idêntico; e

c) os documentos que contenham informações pessoais somente serão liberados à consulta pública mediante autorização prévia do titular ou de seus herdeiros.

5.3.6 - Credencial de Segurança

A Credencial de Segurança, que pode ser limitada no tempo, é classificada nas categorias de ultra-secreto, secreto, confidencial e reservado e permite que seu possuidor, caso tenha necessidade de conhecer, possa ter acesso a material sigiloso de grau de sigilo igual ou inferior à categoria dessa credencial.

5.3.7 - Concessão e Controle das Credenciais de Segurança

Os procedimentos para emissão e controle das Credenciais de Segurança para acesso a material sigiloso constam no Manual de Inteligência da Marinha – Contra-Inteligência, estabelecido pelo EMA.

5.3.8 - Concessão de Credenciais de Segurança em casos especiais

O titular de OM que necessitar, em casos especiais, emitir Credencial de Segurança, solicitará autorização prévia ao EMA.

5.3.9 - Acesso a documento sigiloso resultante de acordos ou contratos com outros países

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

5.3.10 - Negativa de autorização de acesso

A negativa de autorização de acesso deverá ser justificada.

5.4 - COMPROMETIMENTO

O comprometimento poderá ocorrer em diversas situações como, por exemplo, as relacionadas à deserção de indivíduos, destruição incorreta, extravio, furto, roubo, acesso ou reprodução indevidos, naufrágio, adulteração, captura, fotografia etc., o que pode colocar em risco a segurança de pessoas, instituições ou mesmo de uma nação, dependendo da natureza do material comprometido e da extensão do comprometimento.

Durante a Sindicância instaurada para apurar o comprometimento (ou não) de conteúdo de material controlado, deverão ser verificados fatores que:

a) permitam concluir sobre a real probabilidade de acesso de pessoal não autorizado ao conhecimento constante da publicação em tela, sugerindo-se enquadrá-la como baixa, média ou alta probabilidade;

b) permitam concluir sobre a extensão provável do vazamento, isto é, quantas pessoas não autorizadas poderão ter acesso ao material controlado; e

c) permitam concluir sobre a possibilidade de que pessoas não autorizadas que venham a tomar ciência sejam adversas e que possam utilizar ou permitir que outras utilizem os referidos conhecimentos contra nossa Força, sugerindo-se classificá-la como remota, considerável ou absoluta.

5.4.1 - Comunicação sobre comprometimento

Qualquer pessoa que tenha conhecimento de extravio de material sigiloso ou controlado deverá participar imediatamente ao seu superior.

5.4.2 - Ações imediatas do titular da OM

O titular da OM, ao tomar conhecimento do comprometimento do material sigiloso, deve, imediatamente, iniciar os procedimentos de:

a) comunicação da ocorrência ao EMA, ao COMIMSUP, à OMA/OME e, se o comprometimento for de recurso criptológico ou envolver sistemas de informação digital, à Diretoria de Telecomunicações da Marinha (DTM);

b) verificação do nível de comprometimento;

c) correção de eventuais vulnerabilidades de segurança descobertas;

d) apuração de responsabilidades; e

e) encaminhamento de Informe ao Centro de Inteligência da Marinha (CIM).

5.4.3 - Comunicação da ocorrência ao EMA, ao COMIMSUP e à OM classificadora

Esta comunicação, no grau de sigilo adequado, deverá ser feita de forma oficial e expedita, contendo os seguintes dados, se conhecidos:

a) natureza do comprometimento (como extravio, roubo, acesso ou reprodução indevidos, naufrágio etc);

b) avaliação inicial do nível de comprometimento;

c) localização ou posição geográfica, profundidade local e a situação de acondicionamento do material, quando aplicável;

d) a data e as circunstâncias em que o material foi visto pela última vez, quando aplicável;

e) se foram esgotadas todas as medidas destinadas a recuperar o material, citando essas medidas; e

f) outros dados pertinentes para a avaliação do ocorrido.

5.4.4 - Verificação do nível de comprometimento

O nível de comprometimento pode ser baixo, médio ou alto. Sua verificação é a questão mais importante a ser levantada pois o comprometimento de informações sensíveis obriga à tomada de medidas extraordinárias, que podem envolver diversos setores da MB. Deve-se ter em foco que a apuração de responsabilidades é secundária diante das conseqüências do vazamento de conhecimento sensível, eventualmente contido no material comprometido.

5.4.5 - Avaliação inicial do nível de comprometimento

A avaliação inicial do nível de comprometimento caberá à OM onde ocorreu o comprometimento. Após ser exarada a solução da Sindicância, essa avaliação inicial será objeto de análise da OM sindicante, podendo o nível ser reduzido, mantido ou aumentado.

5.4.6 - Correção de eventuais vulnerabilidades de segurança descobertas

Durante as fases de verificação do nível de comprometimento e de apuração de responsabilidades, devem ser esgotadas as providências cabíveis para:

a) corrigir as vulnerabilidades de segurança descobertas; e

b) minimizar a possibilidade de repetição das ocorrências.

5.4.7 - Apuração de responsabilidades

Serão envidados esforços, também, na apuração de responsabilidades e no enquadramento da ocorrência como contravenção ou crime, observando a legislação em vigor. Uma cópia da Sindicância (ou do Inquérito, caso configurado crime) e de sua Solução serão encaminhadas ao EMA e, adicionalmente, à OMA, no caso de comprometimento de publicação sigilosa, ou à DTM, no caso de comprometimento de recurso criptológico ou de sistemas de informação digital.

Além do que possa ser determinado pelos seus superiores, após conhecerem a instauração da Sindicância ou do IPM, os seguintes pontos deverão ser esclarecidos:

a) quem foi o autor (ou autores) e, se houver, co-autor (ou co-autores) da irregularidade;

b) qual o propósito do (s) autor (es), caso fique comprovada sua intenção;

c) quais foram as pessoas não autorizadas que tomaram conhecimento do assunto sigiloso comprometido; e

d) se o fato compromete o conteúdo, de acordo com o contido neste artigo.

Uma cópia do Relatório e da Solução da Sindicância, contendo necessariamente o nível de comprometimento estabelecido pela OMU, o enquadramento legal da contravenção ou crime e as providências adotadas será enviada ao COMIMSUP, OME e OMA da publicação. Esta analisará os procedimentos e providências iniciais adotados pela OM onde ocorreu o comprometimento, reavaliando ou não o nível estabelecido, podendo alterá-lo, e determinando as ações decorrentes necessárias.

5.4.8 - Ações do EMA no caso de comprometimento de material sigiloso

O EMA, a seu critério, poderá reduzir, manter ou aumentar o nível de comprometimento, a partir do recebimento da notificação inicial da ocorrência ou após a análise da cópia da Sindicância, e tomará todas as ações previstas ou consideradas necessárias, podendo, inclusive, alterar alguma medida já praticada pela OM ou determinar a abertura de IPM. No caso de comprometimento de publicação sigilosa, estas ações serão tomadas pelas OMA, sob coordenação do EMA.

5.4.9 - Ações da Organização Militar Aprovadora (OMA) no caso de comprometimento de publicação sigilosa

A OMA, a seu critério e sob coordenação do EMA, poderá reduzir, manter ou aumentar o nível de comprometimento, tomando, a partir do recebimento da notificação inicial da ocorrência ou após a análise da cópia da Sindicância, todas as

ações previstas ou consideradas necessárias, podendo, inclusive, alterar alguma medida já praticada pela OM, inclusive determinar a abertura de IPM.

5.4.10 - Ações da DTM no caso de comprometimento de recurso criptológico ou que envolva sistemas de informação digital

A DTM tomará, imediatamente, todas as medidas necessárias para a manutenção da segurança e da salvaguarda do Sistema de Comunicações da Marinha (SISCOM) e da RECIM como, por exemplo, suspender o uso do recurso criptológico comprometido ou isolar da RECIM uma determinada rede que esteja comprometida, visando anular ou minimizar os eventuais danos causados pelo comprometimento. Além disso, a DTM assessorará o EMA na divulgação de falhas ocorridas e nas medidas corretivas adotadas, no caso de comprometimento de recurso criptológico ou que envolva sistemas de informação digital.

5.4.11 - Divulgação de falhas ocorridas e das medidas corretivas adotadas

O EMA concentrará os resultados das sindicâncias para, regularmente e observando o sigilo devido, divulgar as falhas ocorridas e as medidas corretivas adotadas (sem especificar autores ou OM envolvidas), para que as demais OM possam sanar eventuais vulnerabilidades existentes e para firmar doutrina e procedimentos.

5.4.12 - Condução das investigações

A investigação para se avaliar a extensão do comprometimento ou vazamento deverá ser objeto de outras averiguações, a serem conduzidas pela autoridade depositária dos conhecimentos comprometidos ou vazados.

Portanto, ao se constatar o comprometimento ou vazamento de uma PMB controlada, poderá ser estabelecida uma comissão “ad hoc”, na estrutura organizacional do Sistema de Publicações da Marinha (SPM), para conduzir averiguações no sentido de pormenorizar os efeitos do comprometimento ou vazamento ocorrido, isto é, realizar uma “avaliação de danos”. Esta comissão será formada no âmbito OMA da PMB comprometida ou vazada, considerando as seguintes observações:

- a comissão deve ser formada por oficiais familiarizados com os conhecimentos e dados contidos na PMB, incluindo, não só oficiais lotados na OMA como também na OME;
- a comissão deve ser formada na ocasião da constatação da ocorrência, para possibilitar a tomada de medidas tempestivas que visem neutralizar imediatamente

os efeitos do comprometimento ou vazamento;

- os membros da comissão podem servir como assessores do encarregado da Sindicância ou IPM, a fim de possibilitar uma melhor orientação nos depoimentos e diligências que se fizerem necessárias;
- o "Relatório" e a "Solução" da Sindicância ou IPM podem ser considerados como fontes para o desenvolvimento das avaliações da comissão;
- a formalização dos trabalhos desenvolvidos pela comissão poderá ser feita por meio de um Parecer, onde, em sua conclusão, serão apresentadas propostas de medidas visando neutralizar os efeitos do comprometimento ou vazamento; e
- de posse do Parecer a OMA tomará as medidas pertinentes a serem implementadas, visando neutralizar o comprometimento ou vazamento ocorrido.

Os Encarregados de Sindicância ou de IPM que estiverem apurando o comprometimento de publicações controladas, deverão estar instruídos que uma sindicância é uma investigação e, como tal, deve ser conduzida de forma a elucidar detalhadamente a ocorrência, não permitindo erros processuais que venham a inviabilizar a sua possível utilização judicial.

Considera-se oportuno indicar a necessidade de realizar investigação de todos aqueles indivíduos envolvidos durante a sindicância, que já não as possuam, nos mesmos moldes da investigação para credenciamento, para o mesmo sigilo do objeto da sindicância, a fim de contribuir como ferramenta auxiliar na investigação final do comprometimento resultante do extravio investigado.

A apresentação dos subsídios aos Encarregados da Sindicância será dividida em quatro fases, a saber:

- **Fase 1** - Verificação das circunstâncias em que ocorreu o comprometimento da publicação;
- **Fase 2** - Verificação da abrangência do comprometimento da publicação;
- **Fase 3** - Verificação da relação entre assunto contido na publicação e a segurança externa do País; e
- **Fase 4** - Conclusão da Sindicância. Tipificação de crime, previsto no Código Penal Militar (CPM) ou de contravenção disciplinar, prevista no RDM.

a) Fase 1 - Verificação das circunstâncias em que ocorreu o comprometimento da publicação

Nesta fase, deve-se realizar uma descrição sumária sobre as circunstâncias que possam ter acarretado o comprometimento do material. Sugere-se que o ORC realize a avaliação inicial do comprometimento do conteúdo de material controlado não criptológico, para cada tipo específico, bem como os procedimentos, instruções e regras a serem adotados, posteriormente. Devem ser verificados, entre outros, os seguintes aspectos:

I) se o comprometimento foi comprovado;

II) quais os fatos que o comprovam;

III) caso não tenha sido comprovado, se é possível que venha a ocorrer o comprometimento da publicação;

IV) se podem ser identificadas pessoas não autorizadas que tomaram conhecimento de seu conteúdo;

V) se este conhecimento foi do todo ou de parte do conteúdo (considerar sempre a pior hipótese);

VI) se houve intenção de praticar o comprometimento;

VII) se o comprometimento se deu por caso fortuito (oportunidade), ou força maior (circunstância inesperada);

VIII) se houve conluio, ou seja, se ocorreu liame subjetivo (trama) com co-autoria ou participação de outras pessoas para buscar o conhecimento;

IX) se houve negligência, imperícia ou imprudência por parte do responsável pela custódia;

X) o data-hora, se conhecido, de quando ocorreram as circunstâncias que possam ter acarretado o comprometimento;

XI) o data-hora, se conhecido, de quando foram percebidas as circunstâncias que possam ter acarretado o comprometimento; e

XII) quais foram as medidas tomadas ao se constatar o comprometimento ou vazamento da PMB.

b) Fase 2 - Verificação da abrangência do comprometimento da publicação

Nesta fase, o ponto a ser verificado pelo Encarregado da Sindicância deve ser a determinação da abrangência do comprometimento da

publicação, ou seja, quais as pessoas não autorizadas que puderam ter acesso a publicação.

Os Encarregados deverão sempre considerar, no decorrer das diligências, o conceito de comprometimento de publicação e, por conseqüência, buscar a identificação da natureza da ocorrência - extravio do material ou extravio temporário (material extraviado reaparece sem o esclarecimento do ocorrido), acesso não autorizado a material controlado ou compartimento restrito, destruição inadequada, roubo, naufrágio, acidente, produção de cópia ou distribuição não autorizada.

Dessa maneira, os seguintes aspectos, entre outros, podem ser considerados na elaboração de perguntas:

I) identificação do responsável pela custódia;

II) existência de eventual usuário cujo material estava acautelado;

III) se o local de guarda da publicação atende às normas em vigor;

IV) qual é o material suspeito de comprometimento;

V) condições (quando/como) em que a publicação foi comprometida;

VI) indícios de violação física do local de guarda da publicação;

VII) possíveis envolvidos no comprometimento da publicação;

VIII) possibilidade da publicação ter saído das dependências da OM;

IX) definição de quem teve acesso ao conteúdo da publicação, se o comprometimento está restrito ao âmbito da MB e quais os lugares para onde a publicação pode ter sido levada;

X) identificação das pessoas que tiveram acesso e suas possíveis motivações, caso a publicação tenha sido retirada de bordo ou o seu conteúdo tenha sido acessado por pessoal estranho à MB;

XI) envolvimento de estrangeiros;

XII) credenciamento das pessoas que tiveram acesso à publicação;

XIII) objetivo com que o envolvido quebrou o comprometimento do documento, buscando identificar se a ação foi dolosa ou se houve negligência quanto aos procedimentos de guarda e manuseio da publicação por parte do Encarregado de Publicações ou do militar que detinha sua guarda, de acordo com as normas em vigor;

XIV) se a comunicação sobre o comprometimento ou vazamento foi feita imediatamente após a constatação do fato;

XV) por quanto tempo a PMB está comprometida ou vazada;

XVI) como a publicação foi comprometida (cópia, foto, acesso momentâneo por pessoa não autorizada, etc.) e se o comprometimento foi de todo o conteúdo ou parte dele, especificando as partes afetadas;

XVII) se foi cumprido o Plano de Segurança Orgânica (PSO) da OM no que diz respeito à segurança das áreas sigilosas; e

XVIII) se o comprometimento irá causar algum dano à MB, tais como: furto, quebra de segurança, acesso a sistemas, etc.

c) Fase 3 - Verificação da relação entre o assunto contido na publicação e a segurança externa do país

A expressão "Segurança Externa" foi empregada porque é a expressão constante no CPM, ainda em vigor. De acordo com Otto Costa, entende-se por segurança externa do País "o estado latente ou ostensivo de defesa nacional, cuja competência exclusiva cabe à União, de acordo com o art. 21 da Constituição Federal, em que deve manter-se permanentemente o País, para evitar que Nações Estrangeiras, Organizações Internacionais, Grupos Terroristas e outras Entidades de finalidade diversa atentem contra o princípio constitucional fundamental previsto no art. 1º - I - a soberania da República Federativa do Brasil, beneficiando outros, Estados/Organizações/Entidades Internacionais com objetivos antagônicos ou conflitantes com os interesses nacionais".

Nesta fase, deve-se verificar os seguintes aspectos:

I) o conteúdo da publicação;

II) até que ponto a publicação trata de assunto que envolva a segurança externa;

III) o sigilo da publicação (Confidencial, Secreta ou Ultra-Secreta);

IV) a finalidade da publicação (Básica, Normativa, Criptológica, Informativa ouTécnica); e

V) o tipo de publicação (Política, Doutrinária, Manual, Cifra, Norma, Procedimento, Instrução, Lista ou Glossário).

d) Fase 4 - Conclusão da Sindicância - Tipificação de crime, previsto no CPM ou contravenção disciplinar, prevista no RDM.

Nesta fase, o Encarregado da Sindicância deverá verificar se foram esgotadas todas as medidas destinadas a localizar o material comprometido, citando essas medidas, e tentar responder às seguintes questões:

I) Houve intenção criminosa na ocorrência?

II) Houve contravenção disciplinar ou crime?

Deverá verificar a aplicabilidade do fato nas seguintes definições/normas jurídicas que abordam o assunto, a saber:

- Crime militar - Considera-se crime a infração penal contida no CPM.

- Contravenção Disciplinar - Considera-se contravenção disciplinar a transgressão do Art. 7º do RDM (Decreto nº 88.545/83).

Para reforçar essa qualificação, podem ser verificados ainda os seguintes aspectos:

1) se ocorreu envolvimento de outro(s) país(es) no comprometimento; e
2) se o nacional ou estrangeiro efetuaram ações que tenham atentado contra a segurança externa do País.

5.4.13 - Enquadramento Legal

a) Aspectos a serem verificados na sindicância:

- responsável regulamentar que detinha a publicação quando do seu comprometimento;
- possíveis co-responsáveis pelo mencionado comprometimento;
- fatores da situação que contribuam como agravantes ou atenuantes; e
- medidas de controle e precaução que foram ou deixaram de ser tomadas.

b) Orientações para a conclusão da sindicância

Mencionar as conclusões alcançadas, o enquadramento no RDM ou o indício de crime.

c) Outros aspectos a serem observados

I) Após verificadas todas as circunstâncias que concorreram para o fato, especificamente as concernentes à adoção, omissão e violação dos procedimentos preconizados nesta publicação, deverá ser analisado se o fato

pode ser tipificado como infração aos itens 48, 75 e 76 do Art. 7º do RDM ou aos Art. 143 a 148 e Art. 326 do CPM, caracterizando assim a ocorrência de contravenção disciplinar ou crime militar, lembrando-se que em sendo considerada a ocorrência de crime, deverá ser emitido um relatório parcial e remetidos os autos à autoridade nomeante, que determinará a instauração do competente IPM.

II) Quanto à realização de investigações, deve ser preocupação primordial identificar junto ao pessoal envolvido no comprometimento da PMB os seguintes aspectos:

- no caso de militares da MB, se possuem entraves na carreira que os inclinem a retaliações; se passam por dificuldades financeiras que expliquem negociação de informações; se residem em áreas de risco onde possam estar sendo ameaçados ou aliciados; se possuem registros ou postura que indiquem vícios em drogas lícitas ou ilícitas; e a existência de relações sentimentais e/ou extra conjugais que expliquem troca de favores ou chantagens por parte de indivíduos adversos;
- no caso de indivíduos extra-Marinha, quais conhecimentos de interesse da MB eles possuem; quais suas áreas de atuação intra e extra-MB; e quais as pessoas e/ou instituições extra-MB com que se relacionam; e
- no caso de publicação extra-MB ou estrangeira, deverá ser comunicado ao país de origem e/ou à empresa projetista ou contentora do material para uma melhor apuração dos prejuízos causados.

5.4.14 - Outros possíveis subsídios aos sindicantes para auxílio na definição de critérios

A fim de subsidiar os Encarregados de Sindicâncias, a perda da integridade física de uma publicação controlada ou parte dela, deve ser analisada, primeiramente, a partir do conhecimento ou não do destino que lhe foi dado. Essa primeira etapa já permitirá uma avaliação da possibilidade do acesso de pessoas não autorizadas ao documento.

Caso os critérios apresentados não sejam suficientes ou não possam ser levantados pelo Sindicante, esse poderá fazer uso de outros ou combinação deles, tais como:

a) violação física do local de guarda ou roubo - a ocorrência de tais fatos poderá determinar se a ação teve como propósito deliberado a busca de informação de interesse;

b) acesso de conteúdo por pessoa estranha à MB - neste caso, deverá ser definido se a informação pode comprometer a segurança do país (p. ex. doutrinas, manutenção de munição, etc.); ou se pode afetar a instituição MB com o vazamento de informações não desejáveis (p. ex. Manual de Inteligência da MB); e

c) comprometimento de conteúdo - definir se o conteúdo de uma publicação foi total ou parcialmente comprometido.

5.4.15 - Níveis de comprometimento

a) Aspectos a serem verificados na sindicância:

- fatores que permitem concluir sobre como o conhecimento comprometido poderá influenciar o desempenho das tarefas de nossa Força por assegurar uma vantagem marcante ao possível oponente, propondo-se em classificá-la em acessória, caso o comprometimento tenha pouca influência para o desempenho das tarefas da Força, em restrita quando o fato acarretar restrição significativa sem impedir a realização das citadas tarefas e em total, quando houver praticamente o impedimento do desempenho das tarefas da Força;
- o sindicante deverá realizar uma acurada avaliação no que tange ao nível de comprometimento;
- quanto à condução da sindicância, o processo deve ser orientado, visando responder às questões fundamentais, a fim de permitir um trabalho mais objetivo do encarregado da mesma, contribuindo para a verificação do nível de comprometimento; e
- o enquadramento deverá ser secundário, diante das conseqüências do vazamento de conhecimento sensível, eventualmente contido no material, tendo o cuidado com o comprometimento de conteúdo, não invertendo o cerne para instauração e, consequentemente, descuidando da defesa da doutrina.

b) Orientações para a conclusão da sindicância

- mencionar as conclusões segundo a classificação do nível de comprometimento sugerido anteriormente;
- para a solução, é fundamental o sindicante ter uma orientação consolidada, de fácil consulta, que norteie seus trabalhos;
- a solução deverá formalizar o “comprometimento” e, nesse caso, definir ações decorrentes necessárias;

- duas questões que devem ser obrigatoriamente respondidas nas sindicâncias são: se pessoas não autorizadas tomaram conhecimento do conteúdo das publicações sigilosas e, em caso afirmativo, quais as reais motivações desse acesso indevido e ilícito;
- é importante analisar se foram esgotadas todas as medidas destinadas a localizar o material comprometido e, caso comprovada a intenção, qual o propósito do autor;
- se ao final da sindicância não se apurar a ocorrência de crime militar, uma vez que a perfeita qualificação do tipo penal não foi alcançada, o Encarregado da Sindicância pode concluir que houve negligência por parte do autor para com o trato com a publicação controlada. Neste caso o autor está incurso no Art. 7º – 47 ou 48 do RDM, dependendo dos fatos apurados. Pode o Encarregado também constatar que não houve contravenção disciplinar, geralmente em caso de ocorrência de força maior (como por exemplo: ocorrência de incêndio na sala onde estava a publicação).

c) Critérios estabelecendo possíveis níveis de comprometimento

I) Definição dos critérios para avaliação dos níveis de comprometimento:

- **temporal**: relaciona-se ao período de tempo entre o momento em que houve o comprometimento do conhecimento e o momento em que aquele conhecimento poderá comprometer as ações futuras de forças navais;
- **relacional**: a relação do conhecimento comprometido com assuntos que possam interferir na preparação e execução das forças navais, independente da moldura temporal em que possam ser empregadas;
- **amplitude**: relaciona-se às atividades dos Escalões de Comando da MB que poderão ser afetados com o comprometimento do conhecimento; e
- **ambiente**: está intrínseco ao grau de antagonismo às forças navais (ou ao governo brasileiro) existente no âmbito local em que ocorreu o comprometimento.

II) Níveis de comprometimento:

- **baixo**: comprometimento de uma publicação, extraviada, cujas informações não afetam a MB ou a segurança do país;
- **médio**: comprometimento de informações contidas em uma publicação que possam afetar a MB ou a segurança do país; e

- alto: violação física do local de guarda ou roubo de publicação que contenha informações que possam afetar a MB ou a segurança do país.

A combinação dos critérios e níveis supramencionados permitirá à OMA/OME estabelecer se o nível de comprometimento foi alto, médio ou baixo e se a publicação deverá ser cancelada, substituída ou parcialmente alterada. A tabela abaixo apresenta exemplos para determinar os critérios e os níveis de comprometimento:

Critérios	**Níveis de comprometimento**		
	BAIXO	**MÉDIO**	**ALTO**
Temporal	Execução da operação a curto prazo.	Execução da operação a médio prazo.	Execução da operação a longo prazo.
Relacional	Não há relacionamento do conhecimento com o planejamento e a condução de forças navais.	Existe parcela de relacionamento do conhecimento com o planejamento e a condução de forças navais.	Todo o conteúdo do conhecimento está relacionado com o planejamento e a condução de forças navais.
Amplitude	O conhecimento comprometido poderá afetar algumas atividades dos escalões de comando subordinados ao Comando de Operações Navais de nível Unidade.	O conhecimento comprometido poderá afetar algumas atividades dos escalões de comando subordinados ao Comando de Operações Navais de nível força.	O conhecimento comprometido poderá afetar algumas atividades dos escalões de comando acima do Comando de Operações Navais.
Ambiente	Existem fortes evidências de que o grau de antagonismo às forças navais (ou ao governo brasileiro) existente no âmbito local, em que ocorreu o comprometimento, é muito baixo.	Existem fortes evidências de que o grau de antagonismo às forças navais (ou ao governo brasileiro) existente no âmbito local, em que ocorreu o comprometimento, é provável.	Existem fortes evidências de que o grau de antagonismo às forças navais (ou ao governo brasileiro) existente no âmbito local, em que ocorreu o comprometimento, é muito alto.
	AÇÃO DA OME/OMA		
	Revisar a publicação, caso necessário.	**Substituição ou cancelamento de partes da publicação.**	**Cancelamento da publicação.**

CAPÍTULO 6
RECOLHIMENTO E DESTRUIÇÃO DE MATERIAL CONTROLADO OU SIGILOSO

6.1 - RECOLHIMENTO

O recolhimento é caracterizado pela restituição do material controlado, determinado ou autorizado pela autoridade responsável pelo seu controle, e será considerado concluído quando for acusado o recebimento do material.

6.1.1 - Recolhimento sob o enfoque da contabilidade patrimonial

O recolhimento do material da MB, sob o enfoque da contabilidade patrimonial, é normatizado pela SGM.

6.1.2 - Recolhimento de material controlado sigiloso

O material controlado sigiloso poderá ser recolhido por cancelamento, substituição, extinção da OM, falta de segurança para sua guarda na OM ou por motivos diversos.

6.1.3 - Recolhimento por cancelamento ou substituição

A autoridade responsável pelo controle do material dará instruções específicas para o seu recolhimento no caso de cancelamento ou substituição desse material.

6.1.4 - Recolhimento por extinção da OM

O titular da OM, ao deixar o cargo ou função por extinção da OM, deverá recolher o material controlado às respectivas autoridades responsáveis pelo seu controle.

6.1.5 - Recolhimento por falta de segurança na OM

Quando o titular da OM julgar que não há condições de segurança para a custódia do material controlado ou sigiloso, participará o fato à autoridade responsável pelo seu controle, solicitando instruções.

Este procedimento poderá também ser adotado no caso de uma OM onde exista apenas um Oficial e este, necessitando se ausentar, não dispõe de outro militar a quem possa ser confiada a custódia do material sigiloso. Neste caso, a autoridade responsável pelo controle do material poderá determinar que este seja recolhido a uma outra OM.

6.1.6 - Recolhimento por motivos diversos

O recolhimento do material controlado poderá ser determinado pela autoridade responsável pelo seu controle ou poderá ser solicitado por titular de OM que julgar pertinente tal solicitação, fazendo-a diretamente à autoridade responsável pelo controle, com informação ao COMIMSUP e acompanhada das justificativas devidas.

É conveniente, também, a apresentação de sugestões para solução dos problemas apontados. São exemplos de justificativas para a solicitação de recolhimento de material controlado:

a) ausência comprovada de utilização;

b) indisponibilidade de espaço físico para armazenamento; ou

c) risco de deterioração do material por inexistência de condições adequadas para armazenamento, como excesso de umidade, de temperatura, etc.

6.2 - DESTRUIÇÃO

A destruição é a inutilização total ou parcial do material controlado ou sigiloso, realizada de forma a garantir a impossibilidade do restabelecimento da sua capacidade original de emprego.

6.2.1 - Alienação e destruição sob o enfoque da contabilidade patrimonial

A alienação e a destruição do material da MB, sob o enfoque da contabilidade patrimonial, são normatizadas pela SGM.

6.2.2 - Destruição de material sigiloso

A destruição de material sigiloso poderá ser determinada por necessidade administrativa ou em situações de emergência.

6.2.3 - Formas de destruição de material não armazenado em meio eletrônico ou digital

A destruição de material não armazenado em meio eletrônico ou digital deve ser feita, preferencialmente, por trituramento seguido de incineração. Na impossibilidade da destruição por esses métodos, devem ser empregadas ferramentas que garantam a impossibilidade de restauração parcial ou revelação de indícios, tais como marretas, machados de CAV, malhos, picaretas, aparelhos de solda, etc.

6.2.4 - Destruição de dados, informações ou documentos sigilosos armazenados em meio eletrônico ou digital

Dados, informações ou documentos sigilosos armazenados em meio eletrônico ou digital podem ser destruídos por método que os sobrescrevam pelo menos dez vezes, garantindo-se, assim, a impossibilidade de recuperação. No impedimento do uso deste método, os meios de armazenamento desses dados, informações ou documentos (fitas, disquetes, discos rígidos, discos ópticos, etc.) devem ser destruídos fisicamente, conforme previsto no inciso anterior.

6.2.5 - Registro e controle da destruição

A destruição do material controlado ou sigiloso deverá ser formalizada por meio de um Termo de Destruição, sigiloso, lavrado em duas vias no ato da destruição, assinado pelo ORC e por, no mínimo, duas testemunhas. A autoridade responsável por determinar a destruição do material deve indicar a forma pela qual deverá ser informada do cumprimento da destruição: por meio de mensagem sigilosa ou por meio de uma das vias do Termo de Destruição, enviada sem ofício.

6.2.6 - Livro de Registro de Termos de Destruição

O arquivamento de uma das vias dos Termos de Destruição comporá um livro confidencial, denominado Livro de Registro de Termos de Destruição, que permanecerá em vigor até a extinção da OM.

6.2.7 - Destruição por necessidade administrativa

A destruição por necessidade administrativa é aquela decorrente de motivos administrativos, como cancelamento, substituição ou fim da vida útil de material controlado ou sigiloso, e só será executada mediante instruções específicas das autoridades competentes. Poderá também ser determinada quando o recolhimento do material controlado não puder ser realizado dentro das condições de segurança adequadas.

6.2.8 - Destruição em situações de emergência

A destruição em situações de emergência é aquela realizada em situações especiais, nas quais há risco para a segurança do material sigiloso e visa a minimizar a possibilidade do seu comprometimento, no caso de captura.

6.2.9 - Formas de destruição em emergência

A destruição em emergência de material sigiloso pode ser feita a bordo de navios ou de aeronaves em sobrevôo ou pouso forçado no mar, pelo lançamento ao mar desse material, acondicionado em sacos confeccionados em material resistente, lastrados e perfurados ou, na falta destes, de forma a garantir o afundamento e o alagamento do material. Havendo tempo disponível, em caso de naufrágio ou captura iminente do navio ou afundamento de aeronave, o material sigiloso poderá ser preparado para afundar junto com o meio. Nesta situação, deverá ser considerada a possibilidade do material ser adequadamente destruído ou, se houver segurança durante o trânsito, transferido para um local que ofereça melhor condição de destruição ou preparação para o afundamento.

6.2.10 - Instruções para Destruição em Emergência (IDE)

O titular da OM deverá providenciar para que sejam elaboradas as Instruções para Destruição em Emergência (IDE) do material sigiloso. As IDE serão tão simples e práticas quanto possível e, na sua elaboração, deverão ser considerados o pessoal disponível para o seu cumprimento, a quantidade e espécie do material a ser destruído e os casos mais comuns de emergência.

As IDE devem, no mínimo, estabelecer:

a) que sejam cumpridas, quando possível, as medidas de registro e controle de destruição, como a lavratura dos Termos de Destruição. Quando não for exeqüível enviar os Termos de Destruição às respectivas autoridades responsáveis, deverá ser informado, se possível, qual o material sigiloso destruído, especialmente o material criptológico. Isto é muito importante para o planejamento de operações futuras. Se não houver meio para transmitir a mensagem de forma sigilosa, ela será expedida em linguagem clara, devendo ser especificados apenas os títulos abreviados do material destruído;

b) quem está autorizado a determinar o cumprimento das IDE no impedimento do titular da OM ou na impossibilidade de comunicação com o mesmo;

c) os responsáveis e seus substitutos eventuais pelo cumprimento das IDE nos diversos compartimentos e estações;

d) onde e como poderão ser obtidas as chaves dos compartimentos e os segredos dos cofres que contêm material a ser destruído, bem como os meios necessários à sua realização;

e) uma ordem de prioridade para a destruição do material, especificada em estágios, podendo ser cumprida, a critério da autoridade competente, sem interrupção ou com intervalos entre os estágios, dependendo da evolução da situação. Para o estabelecimento dessa ordem de prioridade, serão considerados o tipo, o sigilo e a possibilidade de comprometimento do material; e

f) diante da possibilidade de surgimento da situação de emergência, que o EMC da OM separe, em lotes, o material sigiloso que não for ser utilizado, visando facilitar a destruição, caso venha a ser necessária.

6.2.11 - Experiência obtida

A experiência obtida permitiu à MB chegar às seguintes conclusões, em caso de naufrágio:

a) devido à existência de modernos recursos de mergulho, o material poderá ser resgatado a grandes profundidades;

b) o lançamento do material ao mar, em saco perfurado e lastrado, contribuirá para aumentar a rapidez da destruição causada pela água do mar, além de dificultar a recuperação em águas profundas;

c) a simples colocação em sacos lastrados, permanecendo o material a bordo, permitirá a recuperação por mergulhadores e, dependendo do tempo em que permanecer imerso, o material poderá ou não ser recuperado;

d) deixar o material no interior de cofres ou armários permitirá a sua recuperação por mergulhadores, pois estes poderão ser trazidos à superfície para posterior abertura; e

e) o material criptológico sigiloso deve ser destruído, pois, se recuperado intacto, poderá permitir o acesso aos códigos em vigor, com o conseqüente comprometimento de todo material criptológico em uso, bem como do teor do tráfego anteriormente tratado.

CAPÍTULO 7

CONTRATOS E CESSÃO DE MATERIAL CONTROLADO OU SIGILOSO

7.1 - CONTRATOS

Para efeito desta publicação, entende-se por contrato qualquer tipo de acordo firmado entre as partes.

Cabe ao EMA analisar e aprovar os pedidos de celebração de contratos entre as OM e entidades extra-MB, públicas ou privadas, nacionais ou estrangeiras, cujo objeto seja controlado ou sigiloso.

7.1.1 - Restrição para conhecimento das condições e da minuta de contrato

O conhecimento das condições e da minuta de contrato estará condicionado à assinatura de termo de compromisso de manutenção de sigilo pelos interessados na contratação.

7.1.2 - Requisitos para a celebração de contratos cujo objeto seja controlado ou sigiloso

Os contratos cujo objeto seja controlado ou sigiloso, ou que sua natureza implique a divulgação de desenhos, plantas, materiais, dados, informações, documentos, áreas ou instalações sigilosos, devem conter, dentre suas cláusulas, as que determinem que:

a) seja permitida a alteração do contrato para inclusão de cláusula de segurança não estipulada por ocasião de sua assinatura;

b) seja obrigação do contratado manter o sigilo relativo ao objeto contratado, bem como à sua execução e a qualquer outra informação correlacionada ou decorrente;

c) seja 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;

d) sejam prévia e formalmente identificadas, para concessão de credencial de segurança, as pessoas que, em nome do contratado, terão acesso a desenhos, plantas, materiais, dados, informações, documentos, áreas ou instalações sigilosas; e

e) seja responsabilidade do contratado a segurança do objeto, no todo ou em parte.

7.1.3 - Fiscalização

As OM providenciarão 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.

7.1.4 - Contratos sob o enfoque da contabilidade patrimonial

A celebração de contratos sob o enfoque da contabilidade patrimonial é normatizada

pela SGM.

7.2 - CESSÃO DE MATERIAL CONTROLADO OU SIGILOSO

Cabe ao EMA analisar e aprovar os pedidos de cessão de material controlado ou sigiloso entre as OM e entidades extra-MB, públicas ou privadas, nacionais ou estrangeiras.

7.2.1 - Requisitos para a cessão de material controlado ou sigiloso

Para que determinado material controlado ou sigiloso seja cedido, é necessário que:

a) seja exarado e encaminhado, ao EMA, um parecer favorável à cessão pela autoridade responsável por determinar a sua distribuição; e

b) a autoridade competente da organização extra-MB assine um Termo de Responsabilidade, em conformidade como o modelo do Anexo D, no qual declare que cumprirá as exigências da MB em relação à salvaguarda e à segurança do material cedido, manterá o devido sigilo, não transferirá informações contidas no material ou obtidas por meio dele e respeitará os direitos, patenteados ou não.

7.2.2 - Número de vias do Termo de Responsabilidade

O Termo de Responsabilidade será emitido em 3 vias: uma do EMA, uma da OM cedente e uma da entidade extra-MB à qual estiver sendo cedido o material sigiloso ou controlado.

7.2.3 - Arquivamento de pedido que obtiver parecer não favorável

O pedido que obtiver parecer não favorável à cessão do material pretendido será arquivado no EMA, a fim de servir de subsídio para nova análise, caso a entidade extra-MB venha a formular novo pedido.

7.2.4 - Cessão de material da MB sob o enfoque da contabilidade patrimonial

A cessão de material da MB sob o enfoque da contabilidade patrimonial é normatizada pela SGM.

7.2.5 - Limite do grau de sigilo de material cedido

A cessão de material sigiloso está limitada ao grau de sigilo secreto.

7.2.6 - Procedimento em caso de cessão de somente parte de material

Quando somente uma parte do material for cedida, o EMA manterá um registro exato do que foi efetivamente cedido, para controle.

7.2.7 - Controle

O EMA manterá um inventário atualizado de todo o material controlado ou sigiloso que for cedido a entidades extra-MB.

ANEXO A

MODELO PARA QUE SEJAM RELACIONADOS OS DOCUMENTOS SIGILOSOS DESCLASSIFICADOS

DOCUMENTOS DESCLASSIFICADOS

NOME DA OM OU SIGLA	TIPO DO DOCUMENTO	NÚMERO	DATA DO DOCUMENTO	GRAU DE SIGILO ORIGINAL	DESTINATÁRIO(S)	ASSUNTO

ANEXO B

MODELO DE NOTIFICAÇÃO DIANTE DE PEDIDO DE ACESSO

N O T I F I C A Ç Ã O

Notificante: (CPADSM OU SPADSM)

Notificado: (requerente)

Endereço: (completo)

Notifico (V.Exª ou V.Sª) que vosso pedido de acesso, protocolado sob o nº....., foi (deferido ou indeferido) em (data),..... (marcar dia, hora e local para comparecimento ou transcrever a justificativa para o indeferimento).

Local e data.

Nome, posto e cargo da autoridade notificante.

ANEXO C

MODELO DE NOTIFICAÇÃO DIANTE DE PEDIDO DE RETIFICAÇÃO

N O T I F I C A Ç Ã O

Notificante: (OM)

Notificado: (requerente)

Endereço: (completo)

Notifico (V.Exª ou V.Sª) que foi procedida a retificação dos dados, conforme solicitado por meio do .....(documento que solicitou a retificação de dados).

Local e data.

Nome, posto e cargo da autoridade notificante.

ANEXO D

MODELO DE TERMO DE RESPONSABILIDADE

REPÚBLICA FEDERATIVA DO BRASIL

MINISTÉRIO DA DEFESA

MARINHA DO BRASIL

_____

(OM)

TERMO DE RESPONSABILIDADE

Declaro, como autoridade credenciada pela (o) .....(nome da organização)..... para receber o (a) .....(nome do material)..... que serão cumpridas as exigências, feitas pela Marinha do Brasil antes da cessão deste material, de não transferir as informações nele contidas a outras Nações ou Organizações, de manter o grau de sigilo ....(SEC., CONF. OU RES.)..... e de respeitar os direitos, patenteados ou não.

_____

CARGO E ASSINATURA DA AUTORIDADE ESTRANGEIRA

Obs.: Serão extraídas em 3 vias:

1ª - arquivo do EMA;

2ª - p/anexar ao material; e

3ª - autoridade que assinar.