

DGMM-0540

OSTENSIVO

**NORMAS DE TECNOLOGIA DA
INFORMAÇÃO DA MARINHA**

MARINHA DO BRASIL

DIRETORIA-GERAL DO MATERIAL DA MARINHA

2019

OSTENSIVO

DGMM-0540

NORMAS DE TECNOLOGIA DA INFORMAÇÃO DA MARINHA

MARINHA DO BRASIL

DIRETORIA-GERAL DO MATERIAL DA MARINHA

2019

FINALIDADE: BÁSICA

3^a REVISÃO

ATO DE APROVAÇÃO

Aprovo, para emprego na MB, a publicação **DGMM-0540 - NORMAS DE TECNOLOGIA DA INFORMAÇÃO DA MARINHA - 3^a REVISÃO.**

RIO DE JANEIRO, RJ.

Em 9 de julho de 2019.

LUIZ HENRIQUE CAROLI
Almirante de Esquadra
Diretor-Geral do Material da Marinha
ASSINADO DIGITALMENTE

AUTENTICADO PELO ORC	RUBRICA
Em ____ / ____ / ____	CARIMBO

ÍNDICE

	PÁGINAS
Folha de Rosto.....	I
Ato de Aprovação.....	II
Índice.....	III
Introdução.....	IX

PARTE I**ESTRUTURA DE TI DA MARINHA****CAPÍTULO 1 - ATRIBUIÇÕES DOS ÓRGÃOS DE TI**

1.1 - Disposições iniciais.....	1-1
1.2 - Atribuições.....	1-1

CAPÍTULO 2 - GERENCIAMENTO DE SERVIÇOS DE TI

2.1 - Conceitos.....	2-1
2.2 - Propósito.....	2-2
2.3 - Componentes principais.....	2-3
2.4 - Serviços de TI e respectivo suporte.....	2-8

PARTE II**RECIM E INTERNET****CAPÍTULO 3 - GERENCIAMENTO DA REDE DE COMUNICAÇÕES INTEGRADA DA MARINHA (RECIM)**

3.1 - Propósito.....	3-1
3.2 - Definições e estruturas da RECIM.....	3-1
3.3 - Requisitos básicos da RECIM.....	3-3
3.4 - Atividades de gerenciamento na RECIM.....	3-5
3.5 - Execução do gerenciamento na RECIM.....	3-6
3.6 - Gerenciamento de estruturas físicas da RECIM.....	3-8
3.7 - Criação e manutenção dos serviços na RECIM.....	3-9

CAPÍTULO 4 - INTRANET

4.1 - Propósito.....	4-1
4.2 - Definição.....	4-1
4.3 - Implementação.....	4-1
4.4 - Aquisição de endereçamento “IP”.....	4-1
4.5 - Sistemas de nomes – domínios de OM.....	4-2
4.6 - Padronização de aplicativos para a Intranet.....	4-3
4.7 - Responsabilidades.....	4-3
4.8 - Suporte técnico.....	4-3

CAPÍTULO 5 - INTERNET

5.1 - Propósito.....	5-1
5.2 - Definição.....	5-1
5.3 - Método de acesso.....	5-1
5.4 - Limitações.....	5-2
5.5 - Medidas de segurança.....	5-3
5.6 - Recursos da RECIM para a Internet.....	5-4
5.7 - Protocolo de transferência de hipertexto (http).....	5-4
5.8 - Domínio da Marinha na Internet.....	5-5
5.9 - Cadastramento para acesso à Internet.....	5-5
5.10 - Auditoria.....	5-6
5.11 - Uso da Internet.....	5-7
5.12 - Suporte técnico.....	5-8
5.13 - Padrões para divulgação da MB via Internet.....	5-8

CAPÍTULO 6 - CORREIO ELETRÔNICO NA MB

6.1 - Propósito.....	6-1
6.2 - Definição.....	6-1
6.3 - Concessão de caixas postais.....	6-1
6.4 - Segurança de correio eletrônico- medidas antispam.....	6-1
6.5 - Restrições de uso de correio eletrônico.....	6-2
6.6 - Auditorias.....	6-3

6.7 - Aspectos a serem observados na administração das caixas postais.....	6-3
6.8 - Atribuições.....	6-4

PARTE III
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

INTRODUÇÃO

Apresentação.....	III-2
Propósito.....	III-3
Estrutura de gestão de segurança da informação e comunicações na MB.....	III-3

CAPÍTULO 7 - CONSIDERAÇÕES INICIAIS

7.1 - Propósito.....	7-1
7.2 - Conceitos.....	7-1
7.3 - Aplicabilidade das instruções de SIC.....	7-5

CAPÍTULO 8 - RESPONSABILIDADES E ATRIBUIÇÕES

8.1 - Propósito.....	8-1
8.2 - Da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM).....	8-1
8.3 - Do Centro de Tecnologia da Informação da Marinha (CTIM).....	8-2
8.4 - Dos Centros Locais de Tecnologia da Informação (CLTI).....	8-2
8.5 - Do Titular da OM.....	8-3
8.6 - Do Oficial de Segurança da Informação e Comunicações (OSIC).....	8-4
8.7 - Da Equipe de Auditoria (EA) de SIC.....	8-5
8.8 - Administrador da rede local (ADMIN).....	8-6
8.9 - Do usuário.....	8-8

CAPÍTULO 9 - SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SIC)

9.1 - Definição.....	9-1
9.2 - Conceituação.....	9-1
9.3 - Segurança orgânica.....	9-4
9.4 - Segurança física da informação e comunicações.....	9-4
9.5 - Segurança lógica da informação e comunicações.....	9-8
9.6 - Segurança do tráfego da informação e comunicações	9-16

9.7 - Segurança na utilização de mídias e redes sociais.....	9-17
9.8 - Segurança criptológica da informação e comunicações.....	9-18
9.9 - Mentalidade de segurança	9-19
9.10 - Forense computacional e registros de acesso.....	9-21
9.11 - Gestão de riscos em segurança da informação e comunicações.....	9-21
9.12 - Dispositivos periféricos de armazenamento.....	9-22

CAPÍTULO 10 - DOCUMENTOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

10.1 - Ações de segurança.....	10-1
10.2 - Grau de sigilo dos documentos de SIC.....	10-1
10.3 - Instrução de Segurança da Informação e Comunicações (ISIC).....	10-2
10.4 - Planos de Contingência (PLCONT).....	10-2
10.5 - Histórico da Rede Local (HRL).....	10-3
10.6 - Relatório de auditoria (RAD) de SIC.....	10-4
10.7 - Relatório de Análise de Vulnerabilidades (RAV).....	10-4
10.8 - Registro de acesso.....	10-4
10.9 - Termo de apreensão.....	10-5
10.10 - Cadeia de custódia.....	10-5
10.11 - Planos de adestramento de SIC.....	10-5
10.12 - Controle de entrada na OM de dispositivos armazenadores de informações digitais.....	10-6

CAPÍTULO 11 - AUDITORIAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

11.1 - Finalidade das auditorias de SIC.....	11-1
11.2 - Tipos de auditorias de SIC.....	11-1
11.3 - Planejamento das auditorias de SIC.....	11-1
11.4 - Procedimentos para auditorias de SIC.....	11-2
11.5 - Relatório de auditoria (RAD) de SIC.....	11-6

CAPÍTULO 12 – SEGURANÇA APLICADA AOS DISPOSITIVOS MÓVEIS E TELEFONES CELULARES

12.1 - Propósito.....	12-1
-----------------------	------

12.2 - Disposições gerais.....	12-1
12.3 - Ameaças e vulnerabilidades dos dispositivos móveis.....	12-3
12.4 - Políticas de uso de dispositivos móveis na OM.....	12-5
12.5 - Recomendações de configuração para dispositivos móveis.....	12-9
12.6 - Considerações finais.....	12-10

PARTE IV - SISTEMAS DIGITAIS**INTRODUÇÃO**

Apresentação.....	IV-2
Propósito.....	IV-2
Referências.....	IV-2

CAPÍTULO 13 - CATEGORIZAÇÃO, CLASSIFICAÇÃO E OM REGULAMENTADORAS

13.1 - Propósito.....	13-1
13.2 - Definições.....	13-1
13.3 - Classificações complementares.....	13-2
13.4 - Organização militar regulamentadora (OMREL).....	13-2

CAPÍTULO 14 - CICLO DE VIDA DE UM SISTEMA DIGITAL

14.1 - Definição.....	14-1
14.2 - Planejamento (PLA).....	14-1
14.3 - Obtenção.....	14-2
14.4 - Produção.....	14-2
14.5 - Manutenção.....	14-2
14.6 - Desativação.....	14-2

CAPÍTULO 15 - FASE DE PLANEJAMENTO

15.1 - Definição.....	15-1
15.2 - PLA01 - Apresentação da necessidade de SD.....	15-1
15.3 - PLA02 - Avaliação da necessidade de SD pela OM	15-2
15.4 - PLA03 - Verificação de Conformidade do SD pela DCTIM.....	15-2
15.5 - PLA04 - Avaliação da necessidade de SD pela COTEC-TIC.....	15-3
15.6 - PLA05 - Avaliação da necessidade de SD pelo COTIM.....	15-3

CAPÍTULO 16 - FASE DE OBTENÇÃO

16.1 - Definição.....	16-1
16.2 - OBT01 - Designação de um Gerente de Projeto.....	16-1
16.3 - OBT02 - Elaboração do projeto básico do SD.....	16-2
16.4 - OBT03 - Avaliação da estratégia de Obtenção do SD.....	16-3
16.5 - OBT04 - Seleção de produtos.....	16-4
16.6 - OBT05 - Seleção de fornecedores.....	16-4
16.7 - OBT06 - Construção do SD.....	16-5
16.8 - OBT07 - Contratação de serviços.....	16-5
16.9 - OBT08 - Avaliação de SD pronto.....	16-6
16.10 - OBT09 - Aceitação do produto ou SD.....	16-6
16.11 - OBT10 - Recebimento do produto ou SD.....	16-7
16.12 - OBT11 - Homologação do SD.....	16-7

CAPÍTULO 17 - FASE DE PRODUÇÃO

17.1 - Definição.....	17-1
17.2 - PRO01 - Acordo de Nível de Serviço (ANS) para hospedagem em Centro de Dados.....	17-1
17.3 - PRO02 - Implantação do SD	17-1
17.4 - PRO03 - Acompanhamento do SD em produção.....	17-2

CAPÍTULO 18 - FASE DE MANUTENÇÃO

18.1 - Definição.....	18-1
18.2 - MAN01- Manutenção corretiva do SD.....	18-1
18.3 - MAN02- Manutenção adaptativa do SD.....	18-2
18.4 - MAN03- Manutenção evolutiva do SD.....	18-2
18.5 - MAN04- Manutenção preventiva do SD.....	18-2
18.6 - MAN05- Manutenção preditiva do SD.....	18-2

CAPÍTULO 19 - FASE DE DESATIVAÇÃO

19.1 - Definição.....	19-1
19.2 - RET01 - Elaboração do plano de desativação.....	19-1
19.3 - RET02 - Notificação aos usuários.....	19-1
19.4 - RET03 - Desativação (exclusão do SD).....	19-2

19.5 - RET04 - Preservação dos dados.....	19-2
---	------

CAPÍTULO 20 - ADMINISTRAÇÃO DE DADOS

20.1 - Definição	20-1
20.2 - Administração dos Dados nos SD.....	20-1
20.3 - Administração Global de Dados.....	20-1
20.4 - Projeto do Banco de Dados.....	20-2
20.5 - Padronização do modelo de dados.....	20-4
20.6 - Hospedagem das bases de dados no Centro de Dados da MB (CD-MB)....	20-4
20.7 - Atribuição de responsabilidades.....	20-4

CAPÍTULO 21 - PROCESSOS DE APOIO

21.1 - Definição.....	21-1
21.2 - APO01 - Documentação.....	21-1
21.3 - APO02 - Gerência de configuração.....	21-1
21.4 - APO03 - Gerência de qualidade.....	21-1
21.5 - APO04 - Verificação.....	21-2
21.6 - APO05 - Validação.....	21-2
21.7 - APO06 - Gerência de riscos.....	21-3
21.8 - APO07 - Gerência de comunicações.....	21-3

PARTE V - SÍTIOS ELETRÔNICOS**INTRODUÇÃO**

Apresentação.....	V-2
Propósito.....	V-2
Referências.....	V-2
Definições.....	V-3

CAPÍTULO 22 - FASES DO CICLO DE VIDA DE UM SÍTIO ELETRÔNICO

22.1 - Fase de planejamento	22-1
22.2 - Fase da produção do sítio eletrônico.....	22-3
22.3 - Fase de implantação do sítio eletrônico.....	22-4
22.4 - Fase de administração.....	22-5
22.5 - Fase de manutenção.....	22-5

22.6 - Fase de desativação.....	22-5
22.7 - Estrutura Documental relacionada a sítio eletrônico.....	22-6
22.8 - Responsabilidades.....	22-6

ANEXOS

ANEXO A - Relação de Documentos de Segurança da Informação e Comunicações..	A-1
APÊNDICE I - Modelo do Termo de Responsabilidade Individual.....	A-I-1
APÊNDICE II - Modelo do Termo de Recebimento de Estação de Trabalho.....	A-II-1
APÊNDICE III - Modelo do Histórico da Rede Local.....	A-III-1
APÊNDICE IV - Modelo de programação das atividades de auditoria de SICRL...	A-IV-1
APÊNDICE V - Modelo da capa do relatório de auditoria (RAD).....	A-V-1
APÊNDICE VI - Modelo da parte de introdução do RAD.....	A-VI-1
APÊNDICE VII - Modelo da parte de constatações do RAD.....	A-VII-1
APÊNDICE VIII - Modelo da parte de considerações finais e assinaturas do RAD..	A-VIII-1
APÊNDICE IX - Glossário de Termos de SIC.....	A-IX-1
ANEXO B - Modelos esquemáticos do ciclo de vida dos SD.....	B-1
ANEXO C - Modelos esquemáticos do ciclo de vida de um sítio eletrônico.....	C-1

INTRODUÇÃO

As Normas de Tecnologia da Informação da MB (DGMM-0540) foram aprovadas em 12 de agosto de 2009, detalhando a Rede de Comunicações Integrada da Marinha (RECIM) sob a perspectiva de suas três principais áreas: Infraestrutura de Redes e Serviços, Segurança da Informação e Comunicação (SIC) e Desenvolvimento de Sistemas Digitais. Ressalta-se que a referida Publicação sofreu sua segunda Revisão em 19 de dezembro de 2017.

A terceira revisão da DGMM-0540 é baseada: em restrições quanto ao uso de dispositivos móveis e telefones celulares na MB.

De modo geral, a TIC tornou-se fundamental para as estratégias organizacionais de grandes organizações e, nesse dinâmico contexto, inclui-se a Marinha do Brasil, onde a TIC consolida-se como a espinha dorsal do Sistema de Comunicações da Marinha (SISCOM), atuando de forma marcante no suporte às atividades de Comando e Controle de Forças Navais. Neste cenário reforça-se a preocupação com a necessidade de definição e normatização de práticas capazes de reduzir os riscos operacionais e garantir a continuidade dos serviços.

Por outro lado, a utilização de forma indiscriminada da TIC, por meio da contínua evolução tecnológica das redes sociais, dos dispositivos periféricos de armazenamento (pendrives, Hard Disk externo e cartões de memória) e de dispositivos móveis inteligentes (celulares, tablets, câmeras fotográficas e similares), tornou-se uma porta de entrada para a exploração de vulnerabilidades das redes de computadores e ampliação da possibilidade de vazamento de dados sigilosos das instituições.

Nesta direção, ressalta-se a Convenção Coletiva de Trabalho, firmada por Sindicatos dos Trabalhadores das Indústrias da Construção Civil do Estado de Goiás, que trouxe uma regra polêmica e inovadora acerca da proibição expressa da utilização de celulares, smartphones, tablets e dispositivos similares, durante o horário de trabalho, sob pena de advertência e até dispensa por justa causa. Cabe mencionar, que tal proibição têm sido aceita pelos Tribunais Regionais do Trabalho.

A parte I (Estrutura de TI da MB) apresenta as principais atribuições das estruturas organizacionais de TIC na MB, em complemento à Doutrina de TI da MB (EMA-416), sendo composta pelo Capítulo 1 (Atribuições dos Órgãos de TI) e Capítulo 2 (Gerenciamento de Serviços de TI).

A parte II (RECIM e Internet) descreve os conceitos e normatiza os aspectos relativos à infraestrutura e serviços de TI na RECIM, tanto no contexto da Intranet, Internet e Correio Eletrônico, sendo composta pelo Capítulo 3 (Gerenciamento da RECIM), Capítulo 4 (Intranet), Capítulo 5 (Internet) e Capítulo 6 (Correio Eletrônico na MB).

A parte III (Segurança da Informação e Comunicações - SIC) normatiza as atividades operacionais e de gerenciamentos relativos à segurança da informação e comunicações e visa resguardar os requisitos de confiabilidade, integridade, autenticidade e disponibilidade das informações de interesse da MB, sendo composta pelo Capítulo 7 (Considerações Iniciais), Capítulo 8 (Responsabilidades e atribuições), Capítulo 9 (Segurança da Informação e Comunicações), Capítulo 10 (Documentos de SIC), Capítulo 11 (Auditorias de SIC) e Capítulo 12 (Segurança Aplicada aos Dispositivos Móveis e Telefones Celulares). Dentre as principais atualizações destacam-se a restrição quanto ao uso dos dispositivos móveis e telefones celulares.

A parte IV (Sistemas Digitais) aborda o ciclo de vida de um sistema digital (SD), desde sua concepção até a desativação, sendo composta: pelos Capítulos 13 e 14, que apresentam conceitos introdutórios e a definição do ciclo de vida de um SD; pelos capítulos 15 ao 19, que detalham as diversas fases do ciclo de vida de um SD (Planejamento, Obtenção, Produção, Manutenção e Desativação); pelo Capítulo 20 (Administração de Dados), o qual apresenta, de forma sucinta, algumas definições sobre administração de dados; e pelo Capítulo 21, que conceitua os processos de apoio presentes em todas as fases do ciclo de vida dos SD.

A parte V (Sítios Eletrônicos) trata dos aspectos normativos referentes aos padrões de acessibilidade definidos para a Administração Pública Federal em relação aos sítios de Internet. O Capítulo 22 apresenta as fases do ciclo de vida de um sítio eletrônico.

PARTE I

ESTRUTURA DE TI DA MB

CAPÍTULO 1 - ATRIBUIÇÕES DOS ÓRGÃOS DE TI

CAPÍTULO 2 - GERENCIAMENTO DE SERVIÇOS DE TI

CAPÍTULO 1

ATRIBUIÇÕES DOS ÓRGÃOS DE TI

1.1 - DISPOSIÇÕES INICIAIS

O presente capítulo amplia e/ou detalha as atribuições de órgãos da estrutura organizacional da MB para a condução das atividades de TI, em complemento à Doutrina de TI da MB (EMA-416).

1.2 - ATRIBUIÇÕES

1.2.1 - Direção Especializada – DCTIM

Como Coordenador Diretor da TI (nível estratégico), tem as seguintes funções além daquelas já descritas na Doutrina de TI:

- a) controlar e supervisionar tecnicamente, com apoio do CTIM, toda a infraestrutura de redes da MB (RECIM);
- b) estabelecer normas de utilização e de padronização de sistemas para emprego na RECIM;
- c) estabelecer doutrinas e normas referentes às atividades de Segurança da Informação e Comunicações (SIC) e à Defesa Cibernética (DC);
- d) executar os processos de verificação de conformidade de sistemas de informação, definindo a melhor arquitetura, autorizando (ou não) seu uso na RECIM e recomendando (ou não) a hospedagem em Centro de Dados;
- e) apoiar os processos de homologação de sistemas de TI, definindo a melhor arquitetura, autorizando (ou não) seu uso na RECIM e recomendando (ou não) a hospedagem no Centro de Dados;
- f) avaliar e dimensionar a capacidade da RECIM, em termos de equipamentos (hardware e software), de atendimento aos requisitos de sistema e de cumprimento dos acordos de níveis de serviço para todos os serviços ofertados (dados, voz e vídeo);
- g) coordenar, executar e analisar todos os projetos que impliquem em alterações e ampliações da RECIM, bem como na oferta de serviços e TI que a utilizem;
- h) coordenar, executar e analisar todos os projetos que impliquem atividades de

Segurança da Informação e Comunicações (SIC) e de Defesa Cibernética (DC);

- i) realizar visitas técnicas para levantamento de necessidades e de subsídios para projetos de TI;
- j) coordenar as ações do CTIM quanto à implantação de novas tecnologias;
- k) elaborar projetos relativos ao Centro de Dados da MB (CD-MB), bem como gerenciar a utilização e os acordos de níveis de serviço estabelecidos com as OM responsáveis pelos sistemas hospedados;
- l) gerenciar a capacitação dos profissionais de TI de toda a MB nas tecnologias utilizadas na RECIM;
- m) coordenar as atividades e o cumprimento das melhores práticas de governança de TI na MB;
- n) elaborar estudos e pareceres técnicos sobre assuntos relacionados à TI, sempre que solicitados;
- o) gerenciar os planos e programas da MB referentes à TI; e
- p) estabelecer instruções para o funcionamento da Autoridade Certificadora Reserva do Ministério da Defesa, sob competência da Marinha do Brasil.

1.2.2 - Órgão Operacional - CTIM

Como executor Coordenador da TI (nível operacional), tem as seguintes funções além daquelas já descritas na Doutrina de TI:

- a) apoiar a DCTIM no controle e na supervisão técnica da RECIM;
- b) controlar os recursos de TI (hardware e software) em uso na RECIM;
- c) subsidiar a DCTIM quanto às informações de gerenciamento necessárias às avaliações de capacidade e de segurança das diversas redes e serviços componentes da RECIM;
- d) monitorar, gerenciar, prestar suporte e emitir relatórios de desempenho, utilização e disponibilidade dos principais recursos de TI da RECIM (enlaces; sistemas hospedados no CD-MB) e do SISCOMIS, sob a responsabilidade da MB;
- e) apoiar e supervisionar os CLTI no suporte aos serviços de TI e nas suas

- atividades de gerenciamento;
- f) operacionalizar uma Central de Suporte aos usuários, a fim de controlar o registro de incidentes e prestar o respectivo suporte aos serviços de TI disponibilizados na RECIM;
 - g) gerenciar e executar, sob a supervisão da DCTIM, as atividades de implantação de serviços de TI na MB, incluindo novas tecnologias, implantação de novos sistemas de conectividade e novos sistemas de segurança da informação e comunicações (detecção, proteção e controle de acesso aos recursos da RECIM);
 - h) gerenciar e executar, sob a supervisão da DCTIM, as atividades de Defesa Cibernética e de Segurança da Informação e Comunicações (SIC), tais como: manutenção de registros de acesso aos recursos de TI da MB e de incidentes de segurança; realização de auditoria de SIC; análise de vulnerabilidades de sistemas de TI; avaliação técnica dos recursos de SIC (antivírus, *firewalls*, proteção contra intrusos etc.); gerenciamento e manutenção dos recursos criptográficos;
 - i) posicionar, manter e monitorar os sensores, dispositivos de alertas e concentradores de *logs*, mantendo seus registros e análises, de forma a possibilitar estudos e respostas aos incidentes identificados pela Central de Tratamento de Incidentes em Redes de Computadores da Marinha do Brasil (CTIR.mar);
 - j) executar as atividades de suporte, manutenção e gerenciamento operacional referente à estrutura e aos serviços de TI hospedados no Centro de Dados da MB (CD-MB);
 - k) emitir instruções para a otimização dos contratos de manutenção;
 - l) realizar visitas técnicas, para fins de gerência operacional das diversas redes componentes da RECIM, bem como para atividades específicas de suporte ou para implementação de projetos de TI originados na DCTIM;
 - m) definir, para a finalidade de gerenciamento, os elementos críticos a serem monitorados pelos CLTI e Administradores de redes locais, bem como a periodicidade de tal controle;
 - n) gerenciar e manter atualizado o catálogo de serviços de TI disponibilizado à MB; e

- o) executar as atividades de suporte, manutenção e gerenciamento operacional referente à estrutura e aos serviços de TI prestados pela AC Reserva.

1.2.3 - Elemento Organizacional de Apoio - CLTI (nível operacional regional e ou local)

Como elemento organizacional de apoio (nível operacional regional e ou local), tem as seguintes funções além daquelas já descritas na Doutrina de TI:

- a) apoiar o CTIM na resolução de todo e qualquer tipo de incidente relativo às redes, e/ou aos sistemas de TI, nos locais sob sua área de jurisdição que afetem o bom funcionamento da RECIM e consequentemente o nível de satisfação dos usuários locais em relação aos serviços prestados;
- b) efetuar o controle operacional e administrativo das redes de dados de sua área de jurisdição, apoiando, por solicitação da OM, ou caso considere necessário, na resolução de incidentes, de forma a garantir a operação adequada da RECIM e seus serviços;
- c) fiscalizar o cumprimento dos procedimentos operacionais na utilização da rede no âmbito de sua área de jurisdição;
- d) estabelecer contatos operacionais com as prestadoras de serviço de telecomunicações em sua área de jurisdição, mantendo a DCTIM e o CTIM informados;
- e) acrescentar, caso considere necessário, novos elementos críticos a serem monitorados pelas OM de sua área de responsabilidade, bem como alterar a periodicidade das monitorações;
- f) manter o nível de adestramento dos administradores das redes locais das OM e da RETELMA, em sua área de responsabilidade, mediante a realização de cursos e palestras;
- g) realizar visitas periódicas às OM sob sua responsabilidade, a fim de verificar o funcionamento adequado de suas redes locais, bem como o cumprimento da doutrina e das normas vigentes;
- h) manter um inventário atualizado dos recursos de TI das OM em sua área de jurisdição;

- i) avaliar o dimensionamento da RECIM em sua área, informando respectivamente à DCTIM e ao CTIM as necessidades de futuras expansões/alterações e as necessidades operacionais de suporte/manutenção;
- j) fiscalizar o cumprimento dos requisitos de manutenção e de funcionamento dos equipamentos de conectividade e seus acessórios existentes nas OM de sua área de atuação;
- k) guardar, operar e manter os ativos de TI que não estiverem sob responsabilidade direta das OM subordinadas;
- l) apoiar, dentro de sua área de atuação, a manutenção de 2º escalão e, quando necessário, a manutenção de 1º escalão de Sistemas Digitais (SD) nas OM sob sua responsabilidade direta; e
- m) concentrar os serviços comuns às OM sob a sua responsabilidade, quando possível, tais como, correio, SIGDEM, servidor de domínio e servidor de arquivos provendo estrutura de backup para estes serviços.

1.2.4 - Órgão de Execução.

Todas as OM da MB que utilizam serviços de TI. O Administrador da Rede Local como elemento organizacional de apoio (nível operacional local), tem as seguintes funções:

- a) operar e manter os ativos de TI existentes na sua rede local, em conformidade com as normas vigentes;
- b) resguardar a integridade física dos equipamentos de conectividade da RECIM, porventura instalados no âmbito de sua OM, comunicando ao CLTI, com informação ao CTIM, qualquer avaria detectada ou a impossibilidade de manter os referidos equipamentos em um ambiente adequado ao seu funcionamento; e
- c) manter o CLTI informado sobre a atualização (aquisição/baixa) dos ativos de TI da OM.

CAPÍTULO 2

GERENCIAMENTO DE SERVIÇOS DE TI

2.1 - CONCEITOS

À medida em que as atividades das OM da MB tornam-se mais complexas, ocorre naturalmente uma dependência maior da tecnologia, aumentando a demanda por serviços de TI de alta qualidade (disponíveis e confiáveis) e, preferencialmente, de baixo custo.

Portanto, torna-se vital a adoção de melhores práticas no gerenciamento de serviços de TI visando alcançar e manter um elevado valor do serviço prestado e ao mesmo tempo permanecer alinhado com as mudanças de necessidades de TI da MB. Neste contexto, o gerenciamento de serviços de TI deve ser permanentemente voltado para o emprego eficiente e eficaz das pessoas, dos processos, dos produtos e parceiros, como definido nas melhores práticas para gerenciamento de TI.

2.1.1 - Pessoas

As pessoas são os usuários (ou clientes), equipes e gerentes de TI. Comunicação, treinamento e definição clara das atribuições, funções e responsabilidades é essencial para máximo aproveitamento das pessoas.

2.1.2 - Processos

Um processo é uma sequência de atividades executadas visando um propósito definido. O foco principal dos processos de TI está em duas áreas: entrega de serviços e suporte à serviços. Os processos de entrega são aqueles que fornecem os serviços de TI para apoiar as diversas OM na condução de suas missões. Já os processos de suporte procuram garantir a disponibilidade, a confiabilidade, o desempenho e a segurança destes serviços.

2.1.3 - Produtos

São as ferramentas e tecnologias utilizadas para execução dos serviços de TI. Apesar de ser uma tendência comum, as ferramentas não devem ser vistas como o único componente de uma solução de TI.

2.1.4 - Parceiros

Consistem nos grupos constituídos para viabilizar o fornecimento do serviço de TI. Esses grupos podem estar dispersos pela MB ou mesmo fora dela, tais como: fornecedores, entidades de ensino, órgãos públicos ou privados conveniados e provedores comerciais. Um bom gerenciamento de serviços garante transparência e uniformidade para o usuário, que não deve perceber quando ocorre uma eventual contribuição de parceiros externos à MB.

2.1.5 - Serviços de TI na MB

Consistem em um conjunto de funções integradas fornecidas por sistemas de informação que suportam uma ou mais atividades ou missões das OM da MB. Um serviço pode ser composto por hardware, software e componentes de rede e de comunicação, sendo percebido pelos usuários e clientes como uma entidade coerente e independente. Assim, uma falha, não importa onde ocorra ou quão insignificante seja, é visível ao usuário por sua interrupção, ou seja, indisponibilidade completa do serviço. Exemplos: correio eletrônico, divulgação de informações na Intranet, gerenciamento eletrônico documentos etc.

2.2 - PROPÓSITO

O gerenciamento de serviços de TI tem como efeitos desejados: redução de custo no suporte e na entrega; aumento da disponibilidade e da confiabilidade; ajuste da capacidade e do dimensionamento ideal dos sistemas e serviços; melhora da escalabilidade possibilidade de expansão; e aumento da eficiência e da eficácia em relação às atividades ou missões que suportam. A obtenção desses efeitos desejados é buscada por meio da implantação de uma “cultura de serviços” para a MB, aliada à implementação de metodologias consagradas de mercado e programas de melhoria contínua da qualidade.

A “cultura de serviços” consiste em reconhecer que a TI existe apenas para apoiar as missões e atividades das OM da MB. Todos os membros da equipe de TI têm participação importante na entrega e no suporte dos serviços, devendo estar motivados e comprometidos a fornecer/ e suportar, no mínimo, os níveis de serviços acordados. Além disso, é fundamental que todos adquiram uma perfeita compreensão da perspectiva dos clientes (usuários) e das OM apoiadas, garantindo que suas necessidades sejam refletidas com precisão dentro da

organização de serviços de TI e tendo a exata dimensão do impacto causado por serviços prestados de forma deficiente.

O programa de melhoria (consolidação e controle) contínua da qualidade dos serviços de TI é uma sequência de etapas que visam aperfeiçoar os processos, aumentando o nível de maturidade da TI com o passar do tempo. Ele é composto de quatro estágios principais: planejar, executar, verificar e agir. O plano caracteriza-se como uma abordagem conduzida por processos que continuamente são avaliados (medidos) para verificação de conformidade com resultados esperados.

2.3 - COMPONENTES PRINCIPAIS

O gerenciamento de serviços de TI engloba diversas atividades no âmbito dos processos de entrega e suporte a serviços. Não se espera que esses processos trabalhem isoladamente, mas sim integrados numa estrutura organizacional de TI na MB.

2.3.1 - Entrega de Serviços

Atividade que compete à DCTIM. Voltada para o ciclo de gerenciamento de médio prazo. Composta por atividades de gerenciamento de nível de serviços; gerenciamento da disponibilidade; gerenciamento da capacidade; gerenciamento financeiro; gerenciamento da continuidade e gerenciamento de liberações (verificação de conformidade).

a) Gerenciamento do Nível de Serviços

Esta atividade visa manter e gradualmente aperfeiçoar a qualidade do nível dos serviços de TI, por meio de um ciclo constante de negociação, monitoração, divulgação, e revisão dos níveis de serviço prestados. Com base em um catálogo de serviços de TI, a DCTIM estabelecerá Acordos de Níveis de Serviços (ANS) junto às OM , principalmente no tocante aos serviços prestados pelo CTIM e hospedados no CD-MB. De forma análoga, estabelecerá acordos internos para os serviços oriundos da própria Diretoria e do CTIM em prol de toda a MB. A DCTIM adotará também uma abordagem multi-nível nos seus acordos. Em um nível corporativo tratará dos acordos que abrangem todos os usuários e OM da MB. No nível OM cobrirá as questões relativas aos sistemas de TI utilizados por

uma OM em particular. Finalmente, no nível serviço, cobrirá todas as questões específicas de um dado serviço prestado. O conteúdo de um acordo de nível de serviço envolve: medidas de disponibilidade e confiabilidade, detalhes do suporte, tempos de resposta e reparo, especificações técnicas do serviço, responsabilidades de ambas as partes (DCTIM/CTIM e OM), processos de revisão, melhoria etc. O gerenciamento do nível de serviços está totalmente integrado com todas as outras atividades de gerenciamento.

b) Gerenciamento da Disponibilidade

Esta atividade visa otimizar a organização do suporte (CTIM) de forma a garantir a disponibilidade a um custo justificado e em um nível sustentável. Prevê-se a integração do suporte a serviços pelo CTIM e pelos CLTI, de forma a reduzir a frequência e a duração dos incidentes, bem como acelerar as ações corretivas. Esta atividade também possui interação com o gerenciamento da segurança. Apesar de apoiado operacionalmente pelo CTIM e pelos CLTI, o gerenciamento da disponibilidade compete à DCTIM, pois, com frequência, envolve interação com os provedores externos contratados.

c) Gerenciamento da Capacidade

Esta atividade visa assegurar o melhor emprego da infraestrutura de TI de forma a atender apropriadamente, a um custo justificado, às necessidades das OM para cumprimento de suas missões. Para tal, os recursos de TI devem ser eficientemente planejados e empregados pela DCTIM para entrega dos serviços conforme os níveis acordados, no presente e futuro. Envolve as tarefas de monitoração e análise da evolução de demanda (utilização) e das respectivas variações pelos serviços prestados; do emprego de novas tecnologias que possam resultar em melhorias; e economia nos mesmos serviços prestados. Inclui também a modelagem do comportamento da infraestrutura de TI sob um determinado volume e tipo de trabalho, na previsão de necessidades futuras.

d) Gerenciamento Financeiro

Esta atividade visa proporcionar uma administração efetiva do custo dos ativos de TI e dos recursos financeiros disponibilizados para o fornecimento dos serviços de TI. Compete à DCTIM a habilidade de contabilizar os gastos relacionados ao provimento de serviços de TI, individualizando-os por OM, bem

como a habilidade para auxiliar os órgãos superiores na tomada de decisões relacionadas a investimentos em TI. Em síntese, a gerência financeira procura equilibrar os custos com a capacidade e com os requisitos compatíveis com os níveis desejados de serviço. Esta atividade ainda permite a conscientização por parte das OM quanto ao custo dos serviços de TI prestados (transparência).

e) Gerenciamento da Continuidade

Esta atividade visa gerenciar os riscos de falhas em serviços críticos de TI por meio da prevenção e do planejamento da recuperação desses serviços estratégicos em uma contingência, dando suporte ao seu funcionamento contínuo, dentro de um determinado conjunto de circunstâncias. Envolve a identificação contínua por parte da DCTIM, CTIM e OM usuárias dos serviços considerados críticos para a MB e dos respectivos efeitos da indisponibilidade. Procura minimizar o impacto das severas interrupções, garantindo o fornecimento de um nível mínimo de serviço, assegurando assim que os mínimos recursos técnicos (sistemas computacionais, redes, aplicações, telecomunicações, suporte técnico e central de serviços) possam ser recuperados nos tempos necessários e acordados. A avaliação dos recursos a serem alocados para essa atividade inclui um criterioso trabalho de análise e gerência de risco que deve ser coordenado pela DCTIM junto aos órgãos envolvidos e OM clientes. A DCTIM deverá confeccionar e manter atualizado um plano de continuidade dos serviços críticos de TI que será objeto de uma publicação própria.

f) Gerenciamento de Liberações

Esta atividade visa assegurar que todos os aspectos para liberação de itens de software e hardware no ambiente de produção, tanto técnicos como não técnicos, sejam considerados em conjunto. É uma atividade posicionada entre o desenvolvimento e a entrada em produção de um serviço de TI. Inclui as atividades de verificação de conformidades, com base em critérios previamente definidos, entre a concepção, o desenvolvimento e a subsequente liberação do serviço para produção. Assegura que haja otimização dos recursos de TI, que as políticas de licenciamento sejam cumpridas e que somente as versões autorizadas, testadas e corretamente liberadas dos itens de configuração sejam empregadas na RECIM, além de impedir a multiplicidade de gastos em ativos de

TI. Esta atividade compete à DCTIM, com apoio do CTIM.

2.3.2 - Suporte a Serviços

Voltado para a operação e ciclo de gerenciamento de curto prazo. Composto por gerenciamento de incidentes, gerenciamento de problemas, central de serviços, gerenciamento de configuração e gerenciamento de mudanças. Tais atividades competem ao CTIM, apoiado pelos CLTI, no âmbito de suas áreas de responsabilidade.

a) Central de Suporte aos Serviços e Ativos da RECIM (CSRECIM)

A CSRECIM é responsável por tratar e gerenciar os incidentes e processar as consequentes requisições de serviços e as requisições de mudanças. Atua como ponto único de contacto entre os administradores de rede local, o CLTI e o CTIM, mantendo a monitoração e um adequado fluxo de comunicação entre eles. A CSRECIM é composta de equipe qualificada de profissionais que, prioritariamente, assumem a perspectiva do usuário para vislumbrar o impacto e a urgência no tratamento do incidente.

Portanto, a CSRECIM designa o grau de prioridade no tratamento do incidente, procurando maximizar a satisfação do cliente na OM garantindo a disponibilidade e confiabilidade do serviço, restaurando-o rapidamente ao estado considerado normal. Ela seleciona e indica o grupo de resolução mais provável com base na descrição do incidente e também elabora relatórios gerenciais, com informações obtidas a partir de métricas previamente definidas. As informações são relevantes para medição de desempenho, disponibilidade, comparação com as metas (acordos de nível de serviço), bem como também para tomada de decisões gerenciais. Dependendo da gravidade do incidente, a CSRECIM poderá escalá-lo tanto funcionalmente (com base no conhecimento técnico dos especialistas) quanto hierarquicamente (com base na hierarquia funcional do CTIM). A CSRECIM poderá disponibilizar ferramentas que automatizem o diagnóstico e a solução de incidentes pelos CLTI ou pelos próprios administradores de rede local. Opcionalmente, também poderá permitir que o usuário acompanhe o progresso do incidente reportado. A CSRECIM é também o ponto de contacto para efeito de suporte relacionado aos sistemas hospedados no CD-MB, respeitando os acordos de nível de serviço pré-

estabelecidos. Compete ao CTIM operar a CSRECIM, estabelecendo orientações específicas para seu acionamento.

b) Gerenciamento de Incidentes

Um incidente é qualquer evento que não faz parte da operação padrão de um serviço e que causa, ou poderá causar, uma interrupção ou perda de qualidade do serviço. O gerenciamento de incidentes, desempenhado pelo CTIM e pelos CLTI em diferentes níveis, visa, portanto, restabelecer a operação normal do serviço o mais rapidamente possível, com um mínimo de interrupção, assegurando assim que os melhores níveis de qualidade e disponibilidade do serviço sejam mantidos. O padrão normal de operação é estabelecido pelo respectivo ANS.

c) Gerenciamento de Problemas

Esta atividade visa prevenir a ocorrência dos incidentes e minimizar o impacto adverso de incidentes e problemas nos serviços prestados às OM causados por erros na infraestrutura. Busca-se identificar a causa raiz dos incidentes, encontrando inicialmente soluções de contorno e gerando uma requisição de mudança/alteração para obtenção de uma solução permanente. Os erros conhecidos são registrados em bancos de dados apropriados.

Procura-se atuar de forma pró-ativa, encontrando e atenuando os problemas antes que eles ocorram ou quando ainda estiverem em seus estágios iniciais. Deve, portanto, prevenir a ocorrência, bem como a recorrência de problemas, além de reduzir o número e o impacto de incidentes. Normalmente, demanda mais tempo que o gerenciamento de incidentes e é uma atividade que compete exclusivamente ao CTIM.

d) Gerenciamento da Configuração

Esta atividade visa fornecer um modelo lógico da infraestrutura de TI por meio de identificação, controle, manutenção e verificação das versões de todos os itens de configuração que compõem a infraestrutura de TI da MB e determinar o relacionamento entre tais itens. Um banco de dados é continuamente atualizado para armazenar essas informações relevantes para todas as atividades de gerenciamento, tanto na entrega quanto no suporte a serviços de TI. O banco de dados é administrado pelo CTIM e contém os itens de configuração, os seus

atributos e seus relacionamentos com outros itens dentro da estrutura de TI.

e) Gerenciamento de Mudanças

Esta atividade visa assegurar que métodos e procedimentos padronizados sejam usados para tratamento rápido e eficiente de todas as mudanças, de modo a minimizar o impacto de quaisquer incidentes relacionados a serviços de TI. Essa atividade exige uma abordagem cuidadosa da avaliação do risco, do impacto potencial da mudança, dos requisitos dos recursos necessários e do processo de aprovação das mudanças. Abrange áreas que incluem: hardware, software (em desenvolvimento e em produção e desenvolvimento), ambiente e instalações, documentação, e procedimentos, organização e pessoas. Engloba os processos de requisição, avaliação, autorização e implementação das mudanças. Os CLTI e o CTIM, em diferentes níveis, devem avaliar o impacto das mudanças e a estimativa dos recursos necessários para implementá-las. Compete à DCTIM a autorização e a coordenação da implementação de mudanças que, pelo grau de complexidade e custo, impliquem em grandes alterações de topologia/arquitetura ou tecnologia empregada e/ou que gerem a necessidade de realização de projetos. As mudanças atualizam o banco de dados de configuração, mantido pelo CTIM.

2.4 - SERVIÇOS DE TI E RESPECTIVO SUPORTE

2.4.1 - Propósito

Prover apoio na área de TI, às OM clientes, em consonância com as melhores práticas adequadas de Governança da Tecnologia da Informação.

2.4.2 - Atividades da Central de Suporte de Serviços e Ativos da RECIM (CSRECIM)

A CSRECIM existe com o propósito de atuar como ponto único de contato para os administradores de redes locais, e é operacionalizada pelo CTIM, devendo ser acionada quando necessário conforme as orientações contidas no subitem 5.4.3.

A Central tem como tarefas o registro, o diagnóstico e o tratamento de incidentes relativos aos serviços de TI, propiciando um suporte com mais agilidade e qualidade. Compete à CSRECIM realizar um diagnóstico inicial do incidente e tentar, quando possível, restaurar o serviço, usando uma variedade

de ferramentas e técnicas disponíveis (por exemplo, Bases de Dados de Conhecimento, Bases de Dados de Erros Conhecidos etc.).

Relação dos serviços de suporte prestados pela CSRECIM:

- Meios Físicos (Radioenlaces, Fibra, Satélite, Par Metálico etc.);
- Telefonia IP;
- Conectividade;
- Sistema Operacional de Rede;
- Correio Eletrônico;
- Intranet e Internet;
- Certificação digital, DNS, Portal, Proxy (Internet), Servidor WEB, Intranet (acessos), Correio Eletrônico Internet (SMTP), Servidor de Autenticação, “Chat” e demais serviços de colaboração e compartilhamento de conhecimento na RECIM;
- Segurança: Antivírus, Anti-Spyware, Firewall Pessoal e de Rede, Atualização do Sistema Operacional, Configuração/Bloqueio de Portas Lógicas, Suspeita de Vírus, Aplicativos da Rede Segura e Serviço de Concentrador de Log, Auditorias, recursos criptológicos vigentes na MB, análise de Conteúdo, vulnerabilidades e ameaças aos serviços da RECIM (acessos indevidos, suspeitas de ataque, etc.);
- Aplicações de Redes sem fio;
- Aplicações de Videoconferência;
- Gerenciamento do Desempenho das aplicações da RECIM; e
- Infraestrutura de conectividade e segurança para sistemas hospedados no CD-MB.

2.4.3 - Interação entre Administradores de Rede Local, CLTI e CTIM

Para incidentes sem condições de resolução no âmbito local, os administradores de rede local deverão concentrar as solicitações de usuários, e encaminhá-las ao suporte na CSRECIM, por meio das orientações e recursos disponibilizados pelo

CTIM. Quando necessário, a CSRECIM acionará o CLTI da respectiva área de jurisdição, a fim de prestar suporte na resolução de todo e qualquer tipo de incidente relativo às redes e/ou aos sistemas de TI que afetem o bom funcionamento da RECIM e dos serviços associados, visando ao aprestamento da sua resolução.

PARTE II

RECIM E INTERNET

CAPÍTULO 3 - GERENCIAMENTO DA REDE DE COMUNICAÇÕES

INTEGRADA DA MARINHA (RECIM)

CAPÍTULO 4 - INTRANET

CAPÍTULO 5 - INTERNET

CAPÍTULO 6 - CORREIO ELETRÔNICO NA MB

CAPÍTULO 3
GERENCIAMENTO DA REDE DE COMUNICAÇÕES
INTEGRADA DA MARINHA (RECIM)

3.1 - PROPÓSITO

Descrever a Rede de Comunicações Integradas da Marinha (RECIM), a fim de evidenciar as suas fundamentais características técnicas e administrativas, sua importância na oferta de serviços e recursos de TI para todos usuários da MB, e a necessidade de estruturas e sistemas de coordenação/gerenciamento adequados, em função de sua dimensão, complexidade e constantes processos de evolução.

3.2 - DEFINIÇÕES E ESTRUTURAS DA RECIM

3.2.1 - RECIM

A RECIM é o conjunto de elementos computacionais, organizados em rede, que compõem a infra-estrutura responsável pelo tráfego de informações (digitais e analógicas) no âmbito da MB. A integração das comunicações consiste na possibilidade de tráfego combinado de dados, voz (áudio e telefonia) e vídeo, nas seguintes formas: com ou sem compressão; com ou sem criptografia e encapsulado ou não em pacotes que obedeçam a protocolos padronizados de comunicação (Ex.: TCP/IP). A RECIM abrange a rede de telefonia (RETELMA) e utiliza o conceito de Intranet para prover aos seus usuários o acesso a recursos e serviços de TI no âmbito da MB. Adicionalmente, a RECIM possui dispositivos de conexão e barreiras de segurança que permitem sua interligação segura à Internet e a outras redes de interesse da MB (redes de outras Forças/MD, governo federal, empresas conveniadas etc.), viabilizando o acesso controlado de seus usuários internos aos serviços de TI disponibilizados nas redes externas, bem como a oferta, igualmente controlada, de serviços de TI a usuários externos à RECIM.

3.2.2 - Rede Local

É uma rede que conecta dispositivos eletrônicos através de meios físicos (fios metálicos, cabos, microondas e fibras ópticas), desempenhando serviços independentes e mantendo a comunicação entre esses dispositivos. Seu limite geográfico alcança, aproximadamente, um raio de 10 km (normalmente limitado

por um prédio, uma fábrica, uma OM ou Complexos compostos por OM vizinhas). Normalmente, as redes locais, conhecidas como LAN (local area network) são interligadas por radioenlaces digitais, enlaces de fibra óptica ou enlaces contratados junto aos provedores de serviços de telecomunicações, possuem altas taxas de transmissão e baixo custo. Estão associadas às redes internas das OM e aos Complexos de OM (Ex.: Complexo Naval de Mocanguê, Complexo Naval de Abastecimento da Av. Brasil).

3.2.3 - Rede Metropolitana

É uma rede que pode conectar várias redes locais (LAN), com ou sem a utilização de prestadoras de serviço de telecomunicações locais. A área metropolitana alcança um raio de aproximadamente 100 km e, devido ao seu pequeno raio de ação, ela pode proporcionar altas taxas de velocidade de transmissão. As redes metropolitanas, conhecidas como MAN (metropolitan area network) estão associadas às redes dos Distritos Navais, compostas individualmente por um conjunto de redes locais interligadas e localizadas na mesma área geográfica. (Ex.: Rede do Comando 7ºDN).

3.2.4 - Rede de Grande Área

É uma rede caracterizada pela comunicação a longa distância (superior a 100km). Normalmente, são utilizados enlaces de fibra-óptica e enlaces satélite para cobrir grandes distâncias. Uma rede de grande área, conhecida por WAN (wide area network) pode ser composta por várias MAN ou LAN interligadas, empregando os citados meios físicos de transmissão. Normalmente, devido à cobertura de grandes distâncias, esses enlaces são contratados junto aos provedores de serviços de comunicações.

3.2.5 - Aplicativos de rede

São os aplicativos executados em um ambiente de rede de computadores, constituindo serviços disponibilizados na RECIM, como um todo ou em parte. Como exemplo, podemos citar o SINGRA, o SISPAG, os serviços de correio eletrônico, os acessos a bancos de dados da DPMM, os serviços baseados em aplicações web, etc.

3.2.6 - RETELMA (Rede Telefônica da Marinha)

Abrange todas as centrais telefônicas da MB, seus acessórios e suportes de interligação. As centrais estão distribuídas pela RECIM organizadas de acordo com o nível de tráfego, abrangência de ramais e áreas de responsabilidade, podendo ser digitais, analógicas ou híbridas. A interligação entre as diversas centrais digitais e híbridas é realizada por meio de links de dados e as analógicas por meio de linhas de junção (tie-lines) que podem ser constituídas por: cabos telefônicos, cabos ópticos, radio enlaces digitais; e linhas privadas contratadas junto a provedores de telecomunicações comerciais ou troncos de dados (troncos IP). As ligações no âmbito interno da RETELMA não sofrem tarifação. As centrais componentes da RETELMA possuem interfaces de conexão com a Rede Pública de Telefonia (fixo e celular), permitindo ligações de/para ramais pertencentes a esta rede. As chamadas destinadas à rede pública sofrem tarifação, de acordo com o contrato estabelecido junto à provedora comercial de telecomunicações.

3.2.7 - SISCOMIS

O Sistema de Comunicações Militares por Satélite tem por finalidade atender à Estrutura Militar de Defesa (EMiD). É constituído por Estações Terrenas (ETN) distribuídas estrategicamente em todo território nacional que, por meio de cabos de fibras óticas, radioenlaces digitais e, principalmente, enlaces satélite, formam uma grande rede de comunicações de dados e voz com diversas estações fixas e móveis, terrestres e navais, das Forças e do MD. A RECIM se interliga, em dados, com a rede do SISCOMIS por meio de interconexão com a rede do MD.

3.3 - REQUISITOS BÁSICOS DA RECIM

Ao prover recursos de TI para todos usuários da MB, a RECIM deve obedecer aos seguintes requisitos básicos: confiançabilidade, rapidez nas respostas às solicitações (desempenho), disponibilidade, eficiência e segurança.

3.3.1 - Confiabilidade

Consiste na garantia de que um dado recurso irá desempenhar sua função, plenamente de acordo com as expectativas e conforme previsto em projeto, em um intervalo de tempo pré-determinado. O nível de qualidade de todos os

dispositivos componentes da estrutura e do ambiente de conexão, o gerenciamento para detecção e /correção de erros nos diversos meios de comunicação, bem como as atividades de segurança das informações constituem ações pró-ativas primordiais para a garantia desse requisito.

3.3.2 - Rapidez nas respostas às solicitações

A rapidez nas respostas é diretamente relacionada às taxas de transmissão (banda), à latência dos meios de comunicação dos dados, à arquitetura do sistema que disponibiliza o serviço de TI e à capacidade de processamento e /memória de todos os dispositivos eletrônicos que compõem o sistema e os nós de comunicação. Assegurando-se o pleno atendimento desse requisito, obtém-se rápido acesso às informações, ou ótimo desempenho, de forma a que o tempo despendido para o tráfego de dados entre o requisitante e o provedor das informações e /serviços de rede seja minimizado.

3.3.3 - Disponibilidade

Consiste em garantir para os usuários o acesso contínuo aos recursos, aos serviços e aos aplicativos existentes na RECIM, observando-se, sempre, as permissões de acesso. O uso de enlaces de contingência; a infraestrutura e os dispositivos computacionais de redundância, tais como: sistemas computacionais agregados em cluster e sistemas de fornecimento ininterrupto de energia, são exemplos de recursos relacionados com a disponibilidade.

3.3.4 - Eficiência

Requisito diretamente ligado às tecnologias e aos procedimentos operacionais utilizados pela RECIM, de forma a satisfazer às expectativas dos usuários, com o menor dispêndio de recursos (materiais e humanos) possível. O emprego de técnicas de compartilhamento de recursos, virtualização de servidores, compressão de dados, automatização de procedimentos de gerência, automatização na detecção e correção de erros e incidentes, assim como a consolidação de serviços em ambiente de Centro de Dados, são exemplos que contribuem para a obtenção da eficiência.

3.3.5 - Segurança

Requisito que visa, conforme a necessidade, garantir a confidencialidade, a

integridade, a autenticidade e a disponibilidade das informações que trafegam pela RECIM. O emprego de recursos criptológicos, barreiras de segurança (*firewalls*), zonas desmilitarizadas, registros de autenticação, programas antivírus, redes privadas virtuais e processos de auditoria são exemplos de técnicas relacionadas com a segurança.

3.4 - ATIVIDADES DE GERENCIAMENTO NA RECIM

Os propósitos básicos do gerenciamento aqui tratados visam manter os níveis de serviço da RECIM dentro dos requisitos anteriormente mencionados, realizando as seguintes funções:

3.4.1 - Alarmes de Falhas

Possibilita a detecção e isolamento rápido de falhas ocorridas em equipamentos considerados críticos para o funcionamento da rede, possibilitando o registro histórico e uma ação corretiva imediata.

3.4.2 - Contabilização

Possibilita o controle físico/logístico (identificação, documentação e inventário) dos recursos de rede, incluindo aferição de custos, tarifação e taxas de utilização dos serviços de TI.

3.4.3 - Desempenho

Possibilita a criação de perfis de comportamento dos diversos serviços de rede, de forma a servir de base para as ações que garantam o funcionamento de acordo com as expectativas dos usuários (acordos de nível de serviço).

3.4.4 - Configuração

Possibilita o controle e a constante atualização das configurações dos diversos dispositivos, sistemas e serviços de TI.

3.4.5 - Segurança

Possibilita a identificação e o controle de acesso (autenticação) a determinados recursos de rede, bem como a detecção e a correção de incidentes de segurança relativos aos sistemas de rede (invasões, vírus, etc.). Essa função de gerenciamento exige definição de políticas de segurança (o que se deseja proteger) e a subsequente definição das ações necessárias para implementar

essas políticas (como proteger).

3.5 - EXECUÇÃO DO GERENCIAMENTO NA RECIM

3.5.1 - Áreas de Gerenciamento

A RECIM pode ser vista como a infraestrutura para uma rede de grande área (WAN), de caráter corporativo, composta pela integração das redes metropolitanas Distritais (MAN) que, por sua vez, são compostas de diversas redes locais das OM concentradas em determinada área geográfica. Por ser uma rede predominantemente corporativa, a RECIM deve, sempre que possível, ser constituída por recursos próprios da MB, tornando-se independente das prestadoras de serviço de telecomunicações. Entretanto, os requisitos de eficiência, disponibilidade e rapidez, quando observadas a abrangência e a capilaridade necessárias para atingir OM situadas em locais remotos do nosso país, muitas vezes impõem a contratação de enlaces de dados comerciais. A RECIM utiliza equipamentos de conectividade, que dispõem de módulos com capacidade de manipulação de voz e dados, para efetuar a eficiente integração das redes que fazem parte de um Distrito Naval ou Complexo Naval. Pode ser estruturada em três áreas de atuação:

3.5.1.1 - Área restrita à OM

A primeira área de atuação restringe-se, basicamente, a uma OM. Cada OM pode ter ao menos uma rede de dados local (LAN) que, em conjunto com ramais telefônicos ou centrais telefônicas são integradas à RECIM. Em prol da eficiência operacional da OM, é fundamental que um militar ou servidor civil seja designado formalmente como responsável administrativo e técnico pela respectiva rede, ficando a critério da própria OM a indicação do mesmo, com base no perfil e na qualificação técnica para a função. Igualmente, é necessária a indicação de um Oficial, com a qualificação técnica necessária, para atuar como Oficial de Segurança das Informações e Comunicações (OSIC), de forma a garantir o correto cumprimento dos procedimentos de segurança atinentes às atividades de TI da OM.

3.5.1.2 - Área dos Distritos Navais ou Complexos Navais

A segunda área de atuação refere-se aos Distritos ou Complexos Navais (exemplo: Complexo Naval de Mocanguê). Cada um desses elementos constitui uma rede integrada pelas redes locais das OM situadas em sua área de responsabilidade, compondo, desse modo, uma rede metropolitana. A responsabilidade administrativa e técnica por essas redes fica a cargo dos respectivos CLTI.

3.5.1.3 - Integração das redes metropolitanas

A terceira área de atuação abrange a integração de todas as redes metropolitanas, formando uma rede de grande área (WAN) corporativa. A WAN possibilita a integração de todas as sub-redes da Marinha. Compete ao CTIM, as responsabilidades técnica e administrativa de gerenciamento e suporte para a WAN. Cabe especificamente à DCTIM a supervisão técnica do CTIM, o gerenciamento de nível doutrinário e estratégico, bem como as responsabilidades administrativa e técnica pelos projetos e contratos que impliquem alteração na WAN.

3.5.2 - Estrutura Organizacional

A estrutura organizacional é composta por um coordenador no nível estratégico (DCTIM) e um Coordenador no nível operacional (CTIM). Adicionalmente, cada área de responsabilidade conta com um CLTI dotado de estrutura organizacional adequada para execução da coordenação no nível operacional localizado, de forma dedicada e formal. Os CLTI apoiam os administradores de redes locais de sua área de jurisdição. Os militares e civis componentes dos CLTI deverão, preferencialmente, ter formação acadêmica compatível (nível graduação ou pós-graduação) nas áreas definidas pela OMOT-TI e previstas em TL. Os CLTI, dentre outras atribuições, deverão darão suporte aos recursos e serviços de TI das OM de sua área de responsabilidade, mantendo um relacionamento de subordinação funcional com o CTIM, para fins de comunicação de ocorrência e a respectiva resolução de incidentes de TI.

3.5.3 - Responsabilidades no gerenciamento

As responsabilidades de gerenciamento são distribuídas da seguinte forma:

- a) cada OM, constituindo uma rede local, efetua o seu próprio gerenciamento, sendo designado um militar (ou civil) para execução da função de administrador de redes;
- b) cada CLTI efetua o gerenciamento da rede que engloba as redes locais das OM localizadas em sua área de jurisdição podendo atuar ao nível de OM em caso de necessidade. Os CLTI devem solicitar ao CTIM as ferramentas de gerenciamento disponíveis para auxílio ao exercício de suas funções; e
- c) o CTIM efetua o gerenciamento operacional de toda a RECIM, conduzindo um acompanhamento pró-ativo de todas as atividades do gerenciamento dos CLTI, inclusive descendo ao nível da OM, podendo intervir caso julgue necessário ou mediante solicitação. É importante ressaltar que, devido à complexidade atual da RECIM, os problemas de uma rede local podem afetar um grande conjunto de OM, além de tornar difícil a identificação de seu causador. Ressalta-se, então, a importância da ação de supervisão até o nível de OM. A DCTIM efetua o gerenciamento de toda a RECIM ao nível estratégico, sendo responsável por atividades de planejamento, doutrina, homologação de sistemas de TI, contratos, projetos de reformulação/ampliação da capacidade da RECIM, e as implantações e avaliações de novas tecnologias.

3.6 - GERENCIAMENTO DE ESTRUTURAS FÍSICAS DA RECIM

Em sua estrutura física, a RECIM é dividida em duas grandes redes, estando, atualmente, seu gerenciamento diferenciado em REDE DE DADOS (dados e VoIP) e REDE DE TELEFONIA CONVENCIONAL (RETELMA – voz).

Essas redes possuem nós por onde são exercidas as diversas funções de gerenciamento.

3.6.1 - Nós de Rede de Dados

O gerenciamento integrado de dados e VoIP consiste, principalmente, na monitoração e na ação sobre: os equipamentos de conectividade (roteadores, *switches*, servidores); os dispositivos de segurança (*firewall*, sensores, sistemas antivírus etc.); os dispositivos de telefonia IP; e sobre os ativos do CD-MB que hospedam os diversos serviços de TI ofertados na RECIM. O gerenciamento, em nível nacional e sob o aspecto operacional, é exercido pelo CTIM, podendo ser

delegado ou fornecido direito de gerenciamento aos CLTI sobre os equipamentos de suas respectivas áreas de responsabilidade.

3.6.2 - Nós de Telefonia Tradicional

O gerenciamento de voz consiste, primordialmente, em monitorar e rotear todo o tráfego de voz que passa pelas Centrais Telefônicas tradicionais.

A monitoração do tráfego consiste em verificar e analisar o estado e o comportamento da rede de telefonia de forma geral. Consiste, ainda, nas operações de programação, de cancelamento ou de alteração de dados de ramais, facilidades oferecidas pelas centrais, e no aumento da capacidade operativa (troncos, ramais, linhas de junção) das mesmas.

3.6.3 - Estações e Gerenciamento do SISCOMIS

O SISCOMIS é operado e mantido pelo Ministério da Defesa. Em caso de inoperância de Central ou Ramal Telefônico, a OM deverá abrir chamado diretamente no setor responsável do MD.

3.7 - CRIAÇÃO E MANUTENÇÃO DOS SERVIÇOS NA RECIM

3.7.1 - Homologação e Hospedagem de Sistemas de Informação

Conforme consta no EMA-416 e na Parte IV desta publicação, qualquer novo sistema de TI ou aplicação de rede de dados deve ser submetida à análise da DCTIM, a fim de: avaliar sua conformidade com os padrões de arquitetura de sistemas pré-definidos; avaliar o impacto sobre a infraestrutura de redes existente; analisar os aspectos de segurança da aplicação; e recomendar o melhor ambiente para hospedagem, priorizando as diretrizes de consolidação de serviços de TI em ambiente de Centro de Dados.

O sistema e a aplicação somente serão liberados para uso na RECIM após autorização formal da DCTIM. Incluem-se, nesse caso, quaisquer aplicações de TI envolvendo serviços de rede, mesmo aquelas que não transcendam a utilização no âmbito da rede local da OM. Isto porque a utilização de mecanismos, de protocolos ou de técnicas de comunicação, não apropriadas para o funcionamento em um ambiente de rede de computadores, pode ser extremamente prejudicial ao desempenho de outros serviços de TI da RECIM, causando potenciais falhas de segurança, além do risco de poder inviabilizar o

desempenho da própria aplicação em questão. A necessidade de recursos adicionais (banda, por exemplo) para suportar novos serviços de TI e sua respectiva implementação/liberação precisam ser previstos com a devida antecedência, de forma a serem planejadas as alterações necessárias e possibilitar a manutenção de um alto nível de qualidade para todos os serviços. É importante salientar que os suportes da infraestrutura de comunicação, principalmente entre os DN, são, normalmente, caros, escassos e de implantação lenta.

Especial atenção deve ser dada a aplicações de videoconferência, em função do elevado impacto sobre a estrutura da RECIM em termos de consumo de banda. Assim, igualmente aos demais serviços de TI, a sua implantação na RECIM condiciona-se à autorização formal da DCTIM, tomando-se por base a necessidade do serviço, as limitações das redes e os custos operacionais envolvidos.

3.7.2 - Acréscimo de novos serviços na RETELMA

No tocante à telefonia, a ampliação da RECIM, mediante acréscimo de novas Centrais Telefônicas em relação à capacidade dimensionada, somente será realizada com a aprovação da DCTIM. O quantitativo de ramais privilegiados da RETELMA, dentro da capacidade instalada, deverá ser autorizado pelos CLTI. Nenhum equipamento ou programa aplicativo utilizado na RETELMA poderá ser adquirido ou sofrer qualquer alteração, sem autorização da DCTIM.

3.7.3 - Sugestões de Aperfeiçoamento

As OM apoiadas devem encaminhar aos CLTI sugestões que possam vir a ser utilizadas no aperfeiçoamento da RECIM. Após sua análise inicial, os CLTI devem encaminhá-las, juntamente com seu parecer, ao CTIM, com cópia para a DCTIM.

3.7.4 - Manutenção Preventiva e Corretiva

A prontificação e o funcionamento adequado da RECIM dependerão de eficientes manutenções preventiva e corretiva de seus dispositivos e meios. Em algumas situações será necessária a elaboração de contratos para garantir a manutenção. Esses contratos são de responsabilidade dos CLTI, nas respectivas

áreas de atuação, e deverão prever cláusulas rígidas de manutenções preventivas e corretivas, inclusive com atendimento em horário não comercial. As manutenções preventivas e corretivas das redes de distribuição (telefonia), internas às OM, serão atribuição das OM responsáveis pelas redes metropolitanas, utilizando seu próprio pessoal. São vedados quaisquer manipulações, configurações e acessos aos equipamentos de conectividade de borda (roteadores) instalados para interligar redes de OM, sem prévia autorização da DCTIM e do CTIM. Sob a orientação do CTIM, os CLTI estabelecerão o gerenciamento pró-ativo de suas respectivas áreas de responsabilidade, a fim de permitir a rápida e eficiente correção dos problemas encontrados na infraestrutura da RECIM, permitindo seu funcionamento ininterrupto.

CAPÍTULO 4

INTRANET

4.1 - PROPÓSITO

Este capítulo visa estabelecer os procedimentos a serem cumpridos por todas as OM da MB para utilização, divulgação e acesso aos serviços disponibilizados na Intranet.

4.2 - DEFINIÇÃO

A consolidação da RECIM, no seu segmento de comunicação de dados, juntamente com a experiência adquirida com a Internet, permitiram a introdução do conceito de Intranet na MB. Uma Intranet visa fornecer às diversas unidades componentes de uma organização os mesmos serviços oferecidos ao público em geral pela Internet. A diferença está no alcance das informações: na Internet o alcance é global e na Intranet o alcance é apenas nos limites da própria corporação. O modelo de rede adotado na Intranet baseia-se no protocolo “TCP/IP” (o mesmo empregado na Internet), e nos diversos protocolos e aplicativos de rede que se utilizam da plataforma TCP/IP, tais como: o HTTP (*HiperText Transfer Protocol*), o SFTP (*Secure File Transfer Protocol*), o VoIP (*Voice Over IP*), etc. A Intranet da Marinha está disponível para todas as OM cujas redes locais estejam interligadas à RECIM. Entretanto, existem serviços de TI cujos acessos são concedidos em função da necessidade de conhecer dos usuários e são controlados por processos de autenticação.

4.3 - IMPLEMENTAÇÃO

Normalmente, as OM que possuem uma rede local já reúnem as condições técnicas necessárias para acesso à Intranet. Para implementar o acesso das estações de trabalho componentes da rede local da OM à Intranet, é necessário conectar o sistema de roteamento dessa rede a um ponto físico do *backbone* (tronco principal da rede, com maior capacidade, e tem o objetivo de conectar outras redes) da RECIM. A execução da interconexão é de responsabilidade do CTIM, apoiado pelo CLTI da área. Ela deverá ser solicitada pela OM diretamente à DCTIM para definição da tecnologia e da solução de conexão que ofereça melhor relação custo-benefício.

4.4 - AQUISIÇÃO DE ENDEREÇAMENTO “IP”

Na interligação da OM à RECIM, o CTIM atribuirá uma faixa de endereços “IP” (*Internet Protocol*) fixos para configuração das estações da rede local da OM. Esses endereços deverão ser controlados pelo administrador de cada rede local que, adicionalmente, deverá manter um

registro atualizado dos usuários, máquinas e seus respectivos IP, para fins de auditoria e /ou gerenciamento, mantendo o CLTI informado. Quaisquer necessidades de alterações de faixa de endereços ou de recebimento de nova faixa deverão ser encaminhadas ao CTIM, com informação para a DCTIM e o CLTI. Cabe ressaltar que o endereço “IP” da Intranet é o mesmo que permitirá também o acesso à Internet. Caso a DCTIM ou o CTIM tenham necessidade de alterar a faixa fornecida de endereços “IP”, a OM será participada formalmente. É expressamente proibida a utilização de endereços “IP” fora da faixa fornecida, sem o prévio conhecimento do CTIM e da DCTIM, mesmo que se constituam de endereços reservados para implementação de redes locais. As dúvidas ou problemas referentes ao endereçamento “IP” devem ser enviadas à CSRECIM. As seguintes informações, relativas à rede local da OM, devem ser fornecidas para obtenção de faixa de endereçamento “IP”:

- a) Número de servidores e de estações de trabalho; e
- b) Sistemas operacionais empregados na rede e nas estações de trabalho.

4.5 - SISTEMAS DE NOMES - DOMÍNIOS de OM

O domínio de primeiro nível (DPN) padrão para a Intranet da Marinha é “mb”. É expressamente proibido às OM a utilização de outros domínios na Intranet. Para as OM que desejarem tornar disponíveis informações e serviços na Intranet, o CTIM disponibilizará um sub-domínio para esta finalidade. Este sub-domínio – denominado domínio de segundo nível (DSN) – segue uma padronização específica para sua formação (a sigla da OM) e, somente em casos muito especiais, poderá ser modificado. Por exemplo:

<u>OM</u>	<u>DSN</u>
DCTIM	dctim.mb
DAdM	dadm.mb
Com1DN	1dn.mb
GCM	gcm.mb

Ainda, dependendo das necessidades da OM, poderão ser criados domínios de terceiro nível (D3N). Esta possibilidade é fundamentada na característica hierárquica do serviço de nome adotado na Intranet (DNS - *Domain Name System*). Porém, deve ser evitada a criação de domínios acima do terceiro nível, ou seja, domínios de quarto, quinto ou sexto níveis. Esta restrição decorre do aumento exponencial da complexidade do sistema de resolução de

nomes, tornando-o menos eficiente. Para a solicitação de criação, ou de modificação, de domínios de segundo e terceiro níveis para as OM, deverá ser enviada mensagem ao CTIM, com informação à DCTIM. Domínios de segundo nível especiais, necessários a alguns serviços corporativos (aqueles que atendem a toda ou grande parte da MB) de OM específicas, e que não se enquadrem na lei de formação, poderão ser solicitados ao CTIM, que aprovará ou não seu emprego, após avaliação e análise técnicas. Ficam proibidos cadastramentos de DSN com nomes comerciais de produtos ou que indiquem a utilização dos referidos produtos, como por exemplo, xyz.dctim.mb, linux.dadm.mb, servidor_notes.dabm.mb etc. Orientações adicionais a respeito poderão ser obtidas na página da DCTIM na Intranet.

4.6 - PADRONIZAÇÃO DE APLICATIVOS PARA A INTRANET

Em cumprimento à política de adoção de software livre e de sistemas de código aberto disseminada pelo Governo Federal, as OM deverão utilizar somente os softwares e aplicativos padronizados pela DCTIM. Qualquer necessidade adicional, a DCTIM deverá ser consultada. A DCTIM mantém em sua página na Intranet uma cópia para download das ferramentas mais utilizadas para tal finalidade, bem como define os padrões de conformidade e identidade visual dos sítios eletrônicos da MB.

4.7 - RESPONSABILIDADES

A responsabilidade pelas informações divulgadas nas páginas das OM na Intranet é da própria OM que as disponibiliza. Cabe à DCTIM e ao CTIM apenas a supervisão técnica do serviço. Dúvidas, sugestões e informações sobre discrepâncias deverão ser encaminhadas para a CSRECIM.

4.8 - SUPORTE TÉCNICO

As OM poderão solicitar suporte técnico acionando a CSRECIM pelos meios em vigor, mantendo o CLTI de sua área informado. Não obstante, é pré-requisito para a OM que se propõe a interagir com a Intranet, ter um mínimo de conhecimento técnico para esse fim. Foge à finalidade do CTIM e da DCTIM ministrar esse tipo de instrução.

CAPÍTULO 5

INTERNET

5.1 - PROPÓSITO

Este capítulo visa estabelecer procedimentos a serem cumpridos pelas OM da MB, para divulgar informações e obter acesso à Internet. A DCTIM é responsável pelos projetos e contratos associados à interligação da RECIM à Internet. O CTIM é responsável pela gerência operacional da conexão das OM à Internet. Atualmente, todas as OM da MB possuem o direito de acesso à Internet. Para permitir tal acesso, a DCTIM e os Comandos de Distritos Navais, periodicamente, realizam contratos ou convênios, respectivamente, junto às empresas prestadoras de serviços de telecomunicações ou órgãos públicos, para interligação da RECIM à Internet.

5.2 - DEFINIÇÃO

A Internet é uma grande rede de computadores em escala mundial que permite o acesso às informações e às variadas formas de transferência de dados. Alguns dos serviços disponíveis na Internet são os acessos a páginas web, o acesso remoto a outras máquinas, transferência de arquivos, correio e boletins eletrônicos.

5.3 - MÉTODO DE ACESSO

A MB está conectada à Internet por vários modos distintos, possuindo conexões principais e redundantes com pontos físicos de acesso situados no CTIM (área do Com1°DN). Existem também os acessos secundários, cujos pontos físicos de acesso situam-se nos Comandos de DN (ou grandes complexos). Esses acessos, fora da área do Com1°DN, possuem bandas que variam caso a caso, custeados pela OM contratante, e são chamadas, no âmbito da MB, de enlaces de Internet Distrital. Os referidos acessos de Internet Distrital devem ser encarados apenas como uma opção para aumento de flexibilidade e de desempenho das OM situadas nos DN, uma vez que os acessos baseados no Com1°DN continuarão sendo disponibilizados para toda a MB, independentemente da contratação da Internet Distrital. Todo acesso à Internet, a partir de estações interligadas à RECIM, deve ser realizado por uma das formas de conexão mencionadas, não sendo autorizada nenhuma outra forma de interligação à Internet em qualquer outro ponto da RECIM. Dessa forma, nenhuma OM está autorizada a contratar comercialmente serviço de acesso à Internet para uma de suas estações de trabalho pertencentes à RECIM. Também não é permitido que um usuário, porventura possuidor de

modem particular de acesso celular 3G ou superior, possa conectar esse dispositivo a uma estação de trabalho da RECIM. Além disso, em todos os casos supracitados, para fins de garantia do cumprimento das leis de informática vigentes no país, o acesso à Internet é feito por intermédio de dispositivos intermediários (proxies) e as páginas visitadas estão sujeitas a ferramentas de controle de conteúdo que bloqueiam acessos a páginas de conteúdos considerados impróprios, no ambiente corporativo da MB. Todos os acessos são, portanto, registrados para fins de auditorias interna e externa. Qualquer exceção a essas formas de acesso devem ser solicitadas formalmente à DCTIM, com as devidas justificativas para análise.

5.4 - LIMITAÇÕES

Embora a Internet se caracterize por ser uma rede livre, algumas regras deverão ser observadas no âmbito da MB a fim de impor limitações de natureza administrativa e condicionar o seu uso aos assuntos de interesse do serviço. Isto significa que a Internet disponibilizada pela MB em suas estações de trabalho, só pode ser utilizada para assuntos oficiais da MB.

5.4.1 - Segurança

Uma vez interligada à Internet, a MB tem, virtualmente, acesso a diversas informações contidas em redes de computadores em todo o mundo, mas a recíproca também é verdadeira. Portanto, é necessário implantar medidas de segurança a fim de controlar esse acesso, proveniente tanto de ambientes externos à RECIM quanto daqueles originados a partir da RECIM. Tais medidas implicam, por exemplo, em seleção parcimoniosa e criteriosa do pessoal com direito à utilização da Internet e o uso de dispositivos e de procedimentos operacionais de segurança, para proteção da RECIM e para a detecção de potências ameaças externas.

5.4.2 - Provedores externos

Por razões de segurança é expressamente proibido às OM interligadas à RECIM contratar serviços de acesso à Internet de provedores externos sem autorização da DCTIM, mesmo que para isso utilizem estações de trabalho não interligadas à sua rede local. Desse modo, o acesso à Internet, por essas OM, só poderá ser feito por meio do canal disponível da RECIM. Esta política visa, principalmente, resguardar a responsabilidade do Comandante/Diretor da OM perante à lei, por algum acesso indevido, não registrado/controlado, e originado a partir de uma estação de trabalho de sua OM.

As OM não interligadas à RECIM (por exemplo, navios atracados em portos extra-MB ou adidâncias), que justificarem junto à DCTIM a necessidade de acesso à Internet para fins de eficiência operacional, podem ser liberadas dessa limitação. Lembrando que, de maneira análoga, a usual inexistência de sistemas de registros e controle de conteúdo neste tipo de acesso (geralmente comercial) expõe o Comandante/Diretor da OM no caso de acessos indevidos realizados a partir de uma estação de trabalho da rede da OM. Portanto, mesmo que concedido pela DCTIM, o acesso à Internet nesses casos deve ser oferecido de forma limitada e de algum modo controlado para fins de auditoria.

5.4.3 - Linhas de comunicação de dados

A rede de dados da RECIM é constituída por vários enlaces e linhas de comunicação interligando as redes locais e metropolitanas dos Distritos Navais. O tráfego de acesso à Internet utiliza essa malha de comunicações, compartilhando-a com o tráfego de aplicações consideradas mais relevantes da rede corporativa, tais como: o tráfego de sistemas operativos de comando e controle, os sistemas digitais administrativos (SINGRA, SISPAG etc.), os sistemas de VoIP, o gerenciamento da RECIM e outras aplicações comuns da Intranet. Tal compartilhamento da malha de comunicações da RECIM para aplicações de Intranet e Internet, aliado aos elevados custos para ampliação das bandas dos diversos enlaces, devem condicionar as permissões para acessos à Internet, evitando a distribuição indiscriminada de autorizações.

5.5 - MEDIDAS DE SEGURANÇA

A DCTIM planejou, juntamente com o CTIM, diversas medidas de segurança, sendo algumas visíveis pelos usuários, enquanto outras não. Entretanto, tais medidas não dispensam cuidados por parte das OM e, em especial, dos usuários com direitos de acesso. Dentre essas medidas, o CTIM instalou vários mecanismos (*IPS, firewall* e analisadores de conteúdo) a fim de controlar, nos dois sentidos, os acessos aos diversos nós de conexão com a Internet. Graças a esses mecanismos, é proibido o acesso não autorizado do público externo à Intranet da Marinha, e o acesso à Internet a partir da RECIM está condicionado a um elenco de serviços, protocolos, aplicações e usuários autorizados. Para o acesso à Internet a partir da RECIM, o protocolo HTTP (transferência de hipertexto) está disponível por meio de “proxies”, sendo executado com a utilização de um programa cliente, como, por exemplo, o navegador Firefox (HTTP). O acesso à Internet, utilizando outros protocolos específicos, necessários a aplicações especiais das OM, podem ser solicitados à DCTIM, que avaliará a viabilidade

técnica de sua liberação e determinará a melhor forma de sua implementação pelo CTIM. Em qualquer caso, todos os acessos são registrados em arquivos de transações (*logs*), sendo periodicamente examinados pelo CTIM e pela DCTIM, ficando disponíveis para eventuais auditorias, durante um período de tempo limitado, conforme previsto em lei. Além dessas medidas, devem ser observados os procedimentos de segurança previstos nesta publicação. Vale lembrar que segurança na utilização da Internet se obtém, antes de tudo, por meio de uma mentalidade que deve ser comum a todos e cultivada no âmbito da OM por meio de palestras e programas de adestramento.

5.6 - RECURSOS DA RECIM PARA A INTERNET

5.6.1 - Servidor “World Wide Web”

A fim de permitir a interação de qualquer entidade externa à MB, o CTIM disponibiliza um servidor HTTPS, de páginas do tipo “World Wide Web” (WWW), liberado para acesso do público externo. Cabe ao CTIM manter a infraestrutura tecnológica necessária ao serviço e à DCTIM o estabelecimento dos requisitos mínimos, normas, padrões e procedimentos técnicos a serem seguidos pelas OM que desejarem divulgar informações por meio de seus sítios hospedados no servidor para o público da Internet. Qualquer OM da MB poderá divulgar informações úteis ao público externo, criando suas próprias páginas e as hospedando no servidor “www” instalado no CTIM. As OM deverão atender aos procedimentos administrativos e às especificações técnicas contidas nesta publicação e terão a responsabilidade pela manutenção de suas páginas (segurança e conteúdo).

5.6.2 - Portal de Serviços da MB

O Portal de Serviços da MB, doravante denominado apenas de Portal, é uma aplicação que permite aos militares e civis da MB, realizando missões oficiais em localidades não conectadas à rede de dados da MB, o acesso a alguns recursos da RECIM, mediante o emprego de sistema de autenticação administrado pelo CTIM. As regras de concessão, utilização e solicitação de acesso ao portal estão definidas em DCTIMARINST.

5.7 - PROTOCOLO DE TRANSFERÊNCIA DE HIPERTEXTO (HTTP)

Esse tipo de acesso será realizado sempre através de um servidor de encaminhamento (“Proxy”), bastando configurar adequadamente o navegador da estação de trabalho para operar

com “proxy”. Por meio dessa facilidade, também está disponível o serviço de FTP (para “downloads” de arquivos). Orientações adicionais a respeito das configurações de “proxy” poderão ser obtidas na página do CTIM da Intranet.

5.8 - DOMÍNIO DA MARINHA NA INTERNET

Os endereços IP são os identificadores das estações de trabalho e dos servidores em uma rede do tipo Intranet ou Internet. Como os seres humanos encontram dificuldades em se lembrar de conjuntos de números tais como "200.244.193.132", preferindo nomes associativos como identificadores (por exemplo, "www.marinha.mil.br"), foi disponibilizado um sistema denominado “Domain Name System” (DNS), que age como um tradutor entre os nomes, chamados domínios, e os endereços IP requeridos pelos sistemas. O domínio da Marinha do Brasil na Internet é "marinha.mil.br". Os usuários da MB utilizam um servidor de nomes interno disponibilizado pelo CTIM. Para balancear a carga no serviço DNS, são utilizados mais de um servidor de nomes (um primário e outros secundários), para a resolução de nomes. Orientações adicionais a respeito do DNS bem como os endereços IP dos servidores de nomes poderão ser obtidos na página do CTIM na Intranet.

5.9 - CADASTRAMENTO PARA ACESSO À INTERNET

O acesso à Internet será no modo síncrono, ou seja, por OM interligada à rede de dados da RECIM. Nesse caso, a infraestrutura necessária para acesso à Internet é a mesma empregada para acesso à Intranet. O cadastramento para acesso à Internet é realizado pelo administrador da rede local da própria OM, de acordo com instruções elaboradas pelo CTIM e, opcionalmente, utilizando um sistema automatizado desenvolvido para esta finalidade.

5.9.1 - Quantidade de usuários com direito de acesso por OM

Não há restrição técnica quanto ao quantitativo de oficiais ou servidores civis assemelhados para concessão de acesso. Entretanto, em todas as OM, os titulares devem efetuar uma criteriosa seleção, buscando limitar o quantitativo de acessos a serem concedidos, contemplando somente aqueles usuários com real necessidade funcional para acessar a Internet. Deve-se considerar que, quanto maior o número de usuários, maior a concorrência pelos recursos computacionais e pela infraestrutura de rede e, sobretudo, maior será a possibilidade de quebra da segurança. Em se tratando de praças ou servidores civis

assemelhados, para as OM da MB comandadas ou dirigidas por Almirante, OM da MB que exerçam função de CLTI, e para as OM das áreas de ensino e pesquisa, desde que interligadas à RECIM, não há limites quanto ao número de usuários permitidos para acessar a Internet. As demais OM deverão restringir o acesso ao nível de praça ou servidor civil assemelhado. Uma boa prática é definir, junto ao administrador de rede local e ao Oficial de Segurança das Informações e Comunicações (OSIC), a limitação de número de acessos e um coerente critério interno para concedê-los. Vale lembrar que a RECIM não deve ser confundida com um típico provedor de acesso à Internet, cujo interesse é angariar o maior número de usuários possíveis, com finalidade comercial, sua utilização deve ser feita em prol do bom andamento do serviço e a fim de ajudar no cumprimento da missão da OM. Os administradores das redes locais das OM devem, também, efetuar o cancelamento de determinado cadastramento quando este não for mais necessário como, por exemplo, quando ocorrer o desembarque ou mudança de função do usuário. A DCTIM e o CTIM poderão cancelar automaticamente qualquer cadastramento, informando à OM responsável, quando identificar mau uso do serviço como, por exemplo, tentativas de burlar as medidas de segurança.

5.10 - AUDITORIA

O CTIM dispõe de recursos para auditar todos os acessos à Internet, inclusive os de correio eletrônico. É possível identificar a origem de todo e qualquer acesso a sítios externos, individualmente. O planejamento das auditorias é atribuição da DCTIM, podendo ser solicitadas pelas próprias OM, em caráter especial.

5.11 - USO DA INTERNET

O acesso à Internet pelo pessoal da MB por meio da RECIM tem como regra geral o bom senso. Isto porque não é viável estabelecer normas rígidas quanto aos sítios que se pode ou não ter acesso, considerando a diversidade de informações sob várias nomenclaturas e a evolução do interesse da MB em informações disponibilizadas na Internet. Alguns procedimentos, evidentemente, não são válidos, inclusive do ponto-de-vista técnico, pois

trazem prejuízo ao tráfego das informações de maior utilidade e prioridade. Assim sendo, é expressamente proibido acessar sítios contendo matéria atinente a relacionamentos não profissionais, utilizar-se de quaisquer tipos de “mecanismos que permitam a troca de mensagens em tempo real com usuários externos à RECIM” (CHAT), aplicações P2P (peer-to-peer), bem como acessar páginas de conteúdo considerado impróprio. A DCTIM e o CTIM têm capacidade de monitorar tais acessos e, ao realizar auditoria, se os detectar, dará conhecimento às OM para as medidas disciplinares cabíveis. Em caso de acesso involuntário, o usuário deverá, de imediato, registrar o fato em sua OM, participando-o aos seus superiores. Também estão instalados mecanismos que restringem alguns tipos de acesso indevido: abrangendo restrições a alguns tipos de arquivos com determinadas extensões, a alguns sítios específicos e/ou sítios pertencentes a uma dada categoria (ex: pornográficos), e definindo períodos do dia para determinados acessos. Esses mecanismos, ditos analisadores de conteúdo, procuram restringir a ocupação de recursos, normalmente caros, com tráfego de informações não relacionadas com as atividades da Marinha. Caso alguma OM identifique a necessidade de acesso que esteja restrita por esses mecanismos, deve submeter à Central de Suportes sua necessidade, devidamente justificada. Em casos conflitantes, a DCTIM avaliará a concessão do acesso. Os critérios básicos de bloqueio/liberação do acesso estão definidos em publicação pertinente da DCTIM. No que diz respeito ao correio eletrônico, não será permitida a utilização de assinatura de listas de discussão de assuntos que não sejam atinentes ao interesse da MB. O CTIM poderá implantar mecanismos para evitar que mensagens provenientes de servidores de listas de discussão sejam recebidas pelos servidores de correio da MB.

5.12 - SUPORTE TÉCNICO

As OM poderão solicitar suporte técnico acerca do que trata este capítulo por meio da CSRECIM. Considera-se pré-requisito para a OM que se propõe a interagir com a Internet, ter um mínimo de conhecimento técnico para esse fim. Foge à finalidade do CTIM e da DCTIM ministrar esse tipo de instrução. Portanto, as OM que não se enquadram nesse perfil, devem procurar, antes de tudo, adquirir a cultura necessária por meio dos cursos ministrados pelo Sistema de Ensino Naval (SEN).

5.13 - PADRÕES PARA DIVULGAÇÃO DA MB VIA INTERNET

O padrão para divulgação de informações pelas OM na Internet, formato de construção das páginas, é de responsabilidade da DCTIM, que regulará o assunto em documentos de instrução próprios, em conformidade com o preconizado nesta publicação.

CAPÍTULO 6

CORREIO ELETRÔNICO NA MB

6.1 - PROPÓSITO

Este capítulo visa estabelecer procedimentos a serem cumpridos pelas OM para o emprego do correio eletrônico na MB, incluindo as regras para a criação de caixas postais e as restrições inerentes ao uso desse serviço.

6.2 - DEFINIÇÃO

O correio eletrônico é um serviço de TI que tem como propósito principal oferecer aos usuários da MB um recurso eletrônico para troca oficial de informações na RECIM. Por meio do correio eletrônico, um usuário da RECIM, possuidor de caixa postal, recebe e envia mensagens (e-mails) de/para qualquer outro usuário da RECIM e de/para qualquer usuário da Internet, possuidor de e-mail.

6.3 - CONCESSÃO DE CAIXAS POSTAIS

O quantitativo de caixas postais da MB a ser distribuído pelas diversas OM será definido em publicação própria. Estes valores serão considerados como de referência (limite máximo), sendo adotados pela DCTIM para planejamento e alocação de recursos financeiros, a serem aplicados no contrato vigente com a empresa fornecedora.

Caso haja a necessidade de se elevar o número de caixas postais além do permitido, as OM deverão solicitar autorização, seguindo as instruções complementares definidas por seus ODG/ODS, acrescentando as respectivas justificativas. Os Admin somente poderão criar caixas postais excedentes após autorização das OM definidas pelos ODG/ODS em instrução própria, devendo manter os devidos controles para Inspeção Administrativa-Militar (IAM) ou Auditorias.

6.4 - SEGURANÇA DE CORREIO ELETRÔNICO-MEDIDAS ANTISPAM

O SPAM é uma mensagem enviada a um usuário da Internet sem que o mesmo a tenha solicitado ao remetente. Inicialmente, essa técnica era utilizada apenas para fins comerciais (propaganda). Atualmente, é a técnica mais empregada para disseminação de vírus e outros programas com finalidades maliciosas, no âmbito da Internet. Para tentar diminuir a entrada desse tipo de mensagem na RECIM, foram implementadas algumas verificações de segurança (medidas antispam) no

servidor de correio eletrônico (*gateway*) localizado no CTIM e que atende pelo domínio “marinha.mil.br” na Internet.

Basicamente, essas medidas antispam verificam a autenticidade do servidor origem da mensagem, se esse servidor não se encontra cadastrado em listas negras de servidores sabidamente remetentes de SPAM, a correta formação dos nomes do remetente e do destinatário da mensagem, a validade dos domínios envolvidos na troca de mensagens, o número total de destinatários de uma mesma mensagem e o tamanho total da mensagem (incluindo anexos) enviada para o destinatário da MB.

Todas as tentativas de entrega de mensagens no *gateway* de correio da RECIM são registradas em arquivos de transações (*logs*) por um período de tempo, de no máximo dois anos, para fins de auditoria. Desta forma, é possível a recuperação das tentativas de entregas de mensagens que não obtiveram sucesso por violarem as regras das medidas antispam adotadas.

A qualquer tempo, uma caixa-postal da MB pode ter a verificação das medidas antispam suspensas. Para isto, a OM deve acionar o CTIM via CSRECIM, solicitando a suspensão da verificação antispam para as caixas-postais desejadas, justificando a solicitação. Após análise da necessidade do pedido de suspensão, o CTIM dará ciência à OM quanto à implementação ou não, da suspensão e dos motivos dessa decisão.

Devido à natureza adaptativa das técnicas de envio de SPAM na Internet, o CTIM modificará as medidas implementadas de modo a mantê-las atualizadas e eficazes.

6.5 - RESTRIÇÕES DE USO DE CORREIO ELETRÔNICO

É vedado e considerado uso indevido do ambiente correio eletrônico pelos usuários da RECIM, os seguintes procedimentos:

- envio de *spams* para outros usuários. É considerado spam o envio de e-mail para 50 (cinquenta) ou mais usuários da RECIM/e-mails externos;
- envio de arquivos em anexo que contenham assuntos não afetos ao serviço;
- uso de e-mail funcional (fornecido pela MB) em atividades não relacionadas ao serviço, tais como: compras eletrônicas de caráter particular, grupos de discussão de caráter particular, redes sociais (caráter particular), mala direta,

- atividades ilícitas, dentre outros; e
- uso de e-mail particular em atividades relacionadas ao serviço.

6.6 - AUDITORIAS

A DCTIM poderá, a qualquer tempo, por meio do CTIM ou dos CLTI, realizar auditorias, sem necessidade de autorização formal, a fim de verificar:

- discrepâncias numéricas de caixas postais em relação aos valores de referência; e
- ocorrências de uso indevido da ferramenta de correio.

Em caso de verificação de discrepâncias ou uso indevido, a OM e seu ComImSup serão notificados para as providências cabíveis.

6.7 - ASPECTOS A SEREM OBSERVADOS NA ADMINISTRAÇÃO DAS CAIXAS POSTAIS

O Administrador do correio eletrônico da OM deverá observar os seguintes aspectos no tocante à gerência das caixas postais:

- zelar pela correta manutenção do valor de referência do quantitativo de caixas postais;
- periodicamente eliminar caixas postais sem uso. Este procedimento deve ser observado principalmente no caso de OM com grande movimentação de pessoal;
- não criar caixas postais para cargos funcionais não efetivamente ocupados, mesmo que constem no organograma da OM;
- evitar a criação de duas ou mais caixas postais para um mesmo usuário por motivo de acúmulo de função na OM;
- evitar a criação de caixas postais para usuários que utilizarão o serviço de forma esporádica, visto que existem formas alternativas de trocas de informações, tais como a rede local e o serviço de compartilhamento de arquivos;
- definir junto aos titulares de OM, os usuários que, por necessidade funcional, necessitem possuir uma caixa postal;
- definir quota para as caixas postais observando o limite estabelecido pela

DCTIM em norma própria; e

- adestrar os usuários da respectiva OM sobre propósito da ferramenta de correio, alertando quanto ao uso indevido.

6.8 - ATRIBUIÇÕES

ODG/ODS

- Adotar e divulgar para as OM subordinadas instruções referentes a criação de caixas postais excedentes (acima do valor de referência) e o remanejamento dos tetos de caixas postais das OM subordinadas, mantendo a DCTIM informada;
- Prever nas instruções a transferência para a DCTIM dos recursos financeiros referentes ao licenciamento/manutenção das caixas postais excedentes (acima do valor de referência) das suas OM subordinadas, de acordo com os valores informados pela DCTIM; e
- Manter o controle do quantitativo autorizado de caixas postais excedentes dentro do seu Setor.

DCTIM

- Estabelecer as orientações de emprego de correio eletrônico na MB e zelar pelo seu cumprimento, reservando-se o direito de realizar auditorias nas OM;
- Divulgar o quantitativo autorizado de caixas postais por OM;
- Informar anualmente aos ODS os procedimentos para a transferência dos recursos financeiros referentes ao licenciamento/manutenção das caixas postais excedentes;
- Informar o valor correspondente a uma (01) caixa postal para licenciamento e manutenção;
- Gerenciar o contrato de aquisição, manutenção e suporte da ferramenta de correio eletrônico adotada junto à empresa fornecedora;
- Manter o controle do quantitativo de caixas postais existentes e autorizadas por OM/ODS.

CTIM/CLTI

- Realizar, sob coordenação da DCTIM, atividades de auditoria local ou remota no ambiente de correio eletrônico das OM; e
- Operacionalizar as normas, definidas pela DCTIM, de emprego do serviço de correio eletrônico na MB.

TITULAR DE OM

- Zelar para que a OM permaneça em conformidade com a norma vigente de emprego de correio eletrônico na MB.

ADMINISTRADOR DE CORREIO ELETRÔNICO

- Informar irregularidades operacionais ao CLTI/CTIM, via Central de Suporte.
- Zelar para que a OM permaneça em conformidade com a norma vigente de emprego de correio eletrônico na MB.

PARTE III
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

INTRODUÇÃO

CAPÍTULO 7 - CONSIDERAÇÕES INICIAIS

CAPÍTULO 8 - RESPONSABILIDADES E ATRIBUIÇÕES

CAPÍTULO 9 - SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SIC)

CAPÍTULO 10 - DOCUMENTOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

CAPÍTULO 11 - AUDITORIAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

CAPÍTULO 12 - SEGURANÇA APLICADA AOS DISPOSITIVOS MÓVEIS E TELEFONES CELULARES

INTRODUÇÃO

1 - APRESENTAÇÃO

A informação é um bem de valor intangível e nem sempre mensurado. Por esta razão, ela é classificada como ativo para uma organização. Como qualquer outro ativo, a informação e o seu correto uso são partes essenciais no cumprimento das missões, devendo, assim, ser adequadamente protegidos. Nos dias atuais, os maiores repositórios de informações são os ambientes computacionais, especialmente os interconectados por redes. Para proteger as informações, tais ambientes devem ser considerados seguros. Contudo, ser um ambiente seguro é um estado para dado momento, em face dos riscos inerentes, do valor do ativo, das ameaças e das vulnerabilidades. Logo, a segurança é uma busca constante do aperfeiçoamento da mentalidade de segurança, dos procedimentos e da tecnologia que envolvem o ativo informação. No cenário da MB, as redes estão cada vez mais interconectadas, chegando até aos meios navais e OM no Brasil e exterior. Com isto, a informação fica exposta a um crescente número e variedades de ameaças e vulnerabilidades inerentes aos sistemas, protocolos de rede, configurações e compartilhamento dos canais de transmissão e recepção de dados, voz e vídeo. A informação pode estar impressa em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é fundamental que ela seja sempre protegida adequadamente.

A Segurança da Informação e Comunicações (SIC) é, portanto, um conjunto de medidas que visam garantir os requisitos de sigilo, autenticidade, integridade e disponibilidade em face dos riscos corretamente medidos em função do valor do ativo, das ameaças e das vulnerabilidades dos ambientes que a armazenam, processam e trafegam. Ela é obtida a partir da manutenção constante de um conjunto de normas e procedimentos adequados, incluindo políticas, processos, estruturas organizacionais, configurações de software, hardware, protocolos de redes e proteção dos enlaces de dados, voz e vídeo. Além disso, é fundamental uma permanente construção de mentalidade de segurança da informação em todos os integrantes da MB, desde os altos escalões até as escolas de formação. Outrossim, controles precisam ser estabelecidos, implementados, monitorados, analisados e aperfeiçoados, onde necessário, para garantir que os propósitos da SIC sejam atendidos. É imprescindível que tais tarefas sejam feitas em conjunto com outros processos de gestão da MB.

2 - PROPÓSITO

Estabelecer a Política de Segurança da Informação e Comunicações da MB, definindo procedimentos e instruções a fim de reger as atividades relacionadas à SIC da MB, complementando as instruções contidas em outras publicações correlatas em uso, devendo ser de conhecimento de todo o pessoal credenciado e autorizado a operar e manusear equipamentos conectados à RECIM.

3 - ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA MB

A Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República de 13JUN2008 (IN nº 01 GSI/PR/2008), elaborada pelo Comitê Gestor de Segurança da Informação e aprovada pela Secretaria Executiva do Conselho de Defesa Nacional, é a norma que orienta a atividade de Segurança da Informação e Comunicações no âmbito do Governo Federal, apresentando a estrutura administrativa para a gestão da segurança das informações e comunicações nos órgãos da Administração Pública Federal (APF). A estrutura administrativa da MB referente a SIC é aderente ao proposto pela IN nº 01 GSI/PR/2008, mostrando assim, a atenção que a MB despende ao assunto buscando e mantendo-se atualizada em relação às melhores práticas de SIC. Com o objetivo de manter a MB alinhada à Instrução Normativa, a MB criou a estrutura de gestão de segurança da informação e comunicações, dentro da estrutura de TI da MB, onde a DCTIM atua como Gestor de Segurança da Informação e Comunicação (GSIC).

CAPÍTULO 7

CONSIDERAÇÕES INICIAIS

7.1 - PROPÓSITO

Este capítulo visa apresentar considerações iniciais relativas a Segurança da Informação e Comunicações na MB.

7.2 - CONCEITOS

A organização deve estabelecer, implementar, manter e continuamente melhorar o Sistema de Gestão da Segurança da Informação (SGSI), de acordo com os requisitos desta Norma.

Para tanto, é necessária a observação dos conceitos abaixo.

7.2.1 - Quanto à Cibernética:

- a) Ativos de Informação - meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão), os sistemas utilizados para tal, os sistemas de informação de um modo geral, os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
- b) Cibernética - termo que se refere à comunicação e controle relacionados aos Ativos de Informação, como uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação.
- c) Espaço Cibernético - espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.
- d) Espaço Cibernético de Interesse da Marinha (ECiber-MB) - Espaço Cibernético composto pelos Ativos de Informação da MB.
- e) Ameaça Cibernética - causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse.
- f) Artefato Cibernético - equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração ou ataque cibernéticos.
- g) Segurança Cibernética - garantia da confidencialidade, integridade e da disponibilidade de um Espaço Cibernético. Adicionalmente, outras propriedades, tais

como autenticidade, responsabilidade, não-repúdio e confiabilidade, podem também estar envolvidas.

h) Defesa Cibernética - conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento de nível estratégico, com as finalidades de proteger os interesses da Marinha e comprometer os sistemas de informação do oponente.

7.2.2 - Quanto à Segurança da Informação e Comunicações (SIC) e suas propriedades:

- a) Disponibilidade - Garante a acessibilidade e utilização sob demanda da informação ou dos ativos de informação por uma pessoa física, órgão, entidade ou sistema.
- b) Integridade - Garante que a informação não seja modificada ou destruída de maneira não autorizada ou acidental;
- c) Confidencialidade - Garante que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- d) Autenticidade - Garante que a informação seja produzida, expedida, modificada ou destruída por uma determinada pessoa física, órgão, entidade ou determinado sistema.
- e) Não-repúdio: Garante que o autor de uma informação ou dado não negue falsamente a sua autoria.
- f) Evento de Segurança da Informação - Qualquer ocorrência observável em um Espaço Cibernético que indique uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- g) Incidente de Segurança da Informação - Indicado por um único ou por uma série de eventos, sequenciais ou não, de segurança da informação indesejados ou inesperados, por agentes internos ou externos, voluntários ou não, que tenham probabilidade de comprometer as operações de sistema de comunicações e ameaçar a segurança da informação.
- h) Segurança da Informação e Comunicações (SIC) - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade e a confidencialidade de dados e informações de forma a minimizar os incidentes de segurança da informação.

Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não-repúdio e confiabilidade, podem também estar envolvidas.

i) Política de Segurança da Informação e Comunicações - Doutrina a ser cumprida pela organização para orientação e apoio às medidas de implementação de segurança da informação e comunicações. Esta parte da Norma representa a Política de Segurança da Informação para a MB. Observando as orientações e princípios existentes nela, busca-se o constante apoio e o comprometimento com a SIC.

7.2.3 - Quanto à sensibilidade e sigilo:

a) Acesso - É a possibilidade ou a oportunidade de uma pessoa obter conhecimento ou dado sigiloso, bem como material digital ou valor. Portanto, o termo acesso expressa não apenas o ato de uma pessoa obter conhecimentos, dados ou material digital de interesse, mas, também, a condição para fazê-lo, seja por meio de autorização oficial emanada de autoridade competente, seja pela exploração das vulnerabilidades das medidas de salvaguarda aplicadas aos mesmos.

b) Compartimentação Digital - É o resultado eficaz de todas as medidas que visam a restringir o acesso a dados e conhecimentos digitais sigilosos às pessoas que não possuem a necessidade de conhecer.

c) Área Digital Sensível - Área considerada vital para o pleno funcionamento da OM, em função do material digital existente na mesma ou das atividades digitais ali desenvolvidas.

d) Área Digital Sigilosa - São áreas sensíveis que abrigam material digital sigiloso.

7.2.4 - Quanto à criticidade de uma infraestrutura:

a) Infraestruturas Críticas - instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

b) Infraestrutura Crítica da Informação da MB - subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão da MB e a segurança do seu pessoal.

7.2.5 - Quanto à segregação de redes de computadores:

- a) Rede Segregada Fisicamente - É a rede que possui um perímetro de segurança orgânica física clara e que nenhuma informação sai do perímetro por nenhum meio ou dispositivo digital, impresso ou físico, incluindo dispositivos USB, CD, DVD etc. A rede segregada fisicamente não pode estar conectada a nenhuma outra rede e não pode ter nenhum tipo de acesso remoto. Qualquer pessoa que tenha necessidade de conhecer a informação gerada, armazenada ou processada pelos usuários da rede segregada, deverá estar dentro do perímetro de segurança.
- b) Rede Segregada Logicamente - É a rede que se utiliza de diversos mecanismos computacionais para garantir a segurança e o controle da informação em todos os seus estágios, ou seja, no processamento, armazenamento e trâmite. Vários mecanismos, técnicas e produtos podem ser utilizados, sendo as principais, a virtualização de estação de trabalho, a utilização de gerenciador de segurança centralizado, o uso de criptografia de arquivos e dispositivos, o uso de ferramentas que viabilizem o controle sobre a transferência de dados por meio de unidades USB, impressoras e canais como e-mail e uma arquitetura de rede segura.

7.2.6 - Quanto à gestão de riscos

- a) Risco cibernético - probabilidade de ocorrência de um incidente de segurança da informação associado à magnitude do dano por ele provocado.
- b) Identificação de riscos - processo para localizar, listar e caracterizar elementos do risco. O propósito da identificação de riscos é determinar eventos que possam causar um incidente potencial e indicar onde e por quais motivos podem ocorrer.
- c) Avaliação de riscos - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
- d) Tratamento dos riscos - processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco.
- e) Evitar o risco - uma forma de tratamento de risco na qual a autoridade competente decide não realizar uma ação, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco.
- f) Reduzir o risco - uma forma de tratamento de risco na qual a autoridade competente

decide adotar ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

g) Reter o risco - uma forma de tratamento de risco na qual a autoridade competente decide assumir as responsabilidades caso ocorra o risco identificado;

h) Transferir o risco – uma forma de tratamento de risco na qual um determinado risco é transferido para outra entidade que possa gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos;

i) Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC) - Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

7.3 - APLICABILIDADE DAS INSTRUÇÕES DE SIC

As Instruções para a SIC visam garantir um nível aceitável de segurança em termos do risco calculado, aplicando-se a:

a) todas as atividades que envolvam algum trâmite, processamento ou arquivamento de informação em meio eletrônico nas redes locais da MB;

b) todos os ativos da MB;

c) todo usuário dos serviços disponibilizados pela rede local; e

d) contratos efetuados pela MB com empresas privadas, cujo escopo envolva algum tratamento de informações em meio eletrônico ou integradas por meio de uma rede local.

CAPÍTULO 8

RESPONSABILIDADES E ATRIBUIÇÕES

8.1 - PROPÓSITO

O presente capítulo amplia e detalha as atribuições de órgãos e integrantes da estrutura organizacional da MB para a condução das atividades de SIC.

8.2 - DA DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO DA MARINHA (DCTIM)

Compete à DCTIM a elaboração, a revisão e o gerenciamento das normas gerais para a SIC da MB, exercendo as seguintes atividades:

- a) planejar, coordenar e controlar as atividades técnicas e administrativas de SIC;
- b) assessorar a DGMM nos assuntos de SIC;
- c) supervisionar e analisar todas as atividades que possam afetar os requisitos de SIC da MB;
- d) coordenar e orientar as atividades do CTIM;
- e) autorizar a execução de serviços nas redes locais, inclusive segregadas, das OM por pessoal externo, pois estes serviços (implementações ou correções) podem afetar os requisitos de SIC da MB;
- f) determinar as necessidades e adotar programas, equipamentos e materiais específicos para as atividades de SIC;
- g) normatizar e homologar soluções de equipamentos e programas que promovam a segurança dos dispositivos periféricos de armazenamento e dispositivos móveis na MB;
- h) coordenar as atividades de auditoria de SIC nas OM da MB que possuam informações digitais integradas por meio de rede local;
- i) promover e fomentar o incremento progressivo da mentalidade de SIC, por meio de ferramenta de gestão do conhecimento, palestras, seminários, simpósios e cursos;
- j) manter atualizadas na página de Intranet da DCTIM as listas de verificação para realização das auditorias de SIC;
- k) exercer ou delegar a competência da auditoria de SIC nas OM da MB;
- l) designar por Portaria os integrantes da equipe de auditoria de SIC, realizadas pela DCTIM, nas OM da MB;

- m) definir os requisitos para qualificação e certificação do pessoal da MB em auditorias de SIC;
- n) estabelecer os requisitos mínimos de segurança para recursos computacionais de uso individual, de acordo com as normas em vigor; e
- o) aprovar as diretrizes gerais e as normas referentes ao processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) na MB, observadas as demais normas vigentes.

8.3 - DO CENTRO DE TECNOLOGIA DA INFORMAÇÃO DA MARINHA (CTIM)

Compete ao CTIM, sob a coordenação da DCTIM, a execução das tarefas de:

- a) monitoramento da RECIM;
- b) configuração de dispositivos de conectividade e de segurança de redes;
- c) varreduras de vulnerabilidades em servidores e redes;
- d) forense computacional;
- e) gerência dos recursos criptológicos em uso;
- f) administração e atualização dos programas de segurança homologados;
- g) atualização dos ambientes operacionais na RECIM;
- h) execução técnica das atividades de defesa cibernética;
- i) implantação de novas soluções de SIC homologadas pela DCTIM; e
- j) outras tarefas inerentes a SIC designadas pela DCTIM;

8.4 - DOS CENTROS LOCAIS DE TECNOLOGIA DA INFORMAÇÃO (CLTI)

Compete aos CLTI tomar as providências necessárias para manter pessoal capacitado a efetuar auditorias de SIC nas OM sob sua área de jurisdição, conforme os requisitos definidos pela DCTIM.

- a) acessorar as OM apoiadas nos assuntos de SIC;
- b) elaborar um programa de adestramento (PAD) anual para as OM apoiadas, que dissemine e incorpore a mentalidade de SIC;
- c) zelar pelo fortalecimento da mentalidade de segurança, junto as OM apoiadas;
- d) alterar, propor, analisar e verificar se os requisitos de SIC das OM apoiadas estão sendo

- praticados em conformidade com as normas estabelecidas;
- e) realizar visitas técnicas, auditorias programadas e prover apoio às auditorias internas de SIC nas OM da sua área de jurisdição;
 - f) supervisionar a atualização dos sistemas operacionais das OM apoiadas e ferramentas de segurança homologadas pela DCTIM;
 - g) efetuar o monitoramento dos ativos críticos de conectividade das OM apoiadas
 - h) estabelecer e supervisionar o serviço de monitoramento de incidentes: de infraestrutura, de SID, repassando ao CTIM informações sobre os mesmos de acordo com suas orientações técnicas, visando à manutenção da consciência situacional de TIC na MB;
 - i) apoiar o CTIM na resolução de incidentes de maior complexidade que requeiram ações locais para restabelecimento de sistemas e serviços ou para proteção da RECIM;

8.5 - DO TITULAR DA OM

Compete ao Titular da OM que possui informações digitais integradas por meio de rede local de computadores as seguintes responsabilidades:

- a) manter o fiel cumprimento das normas, procedimentos e instruções pertinentes à SIC na sua OM;
- b) zelar para que a operação e a manutenção dos equipamentos, instalações e sistemas da rede local da OM sigam as instruções em vigor;
- c) criar ordem interna quanto ao uso de dispositivos de armazenamento periférico e dispositivos móveis atendendo às especificidades da própria OM;
- d) zelar pelo fortalecimento da mentalidade de segurança;
- e) manter um programa de adestramento de SIC para todo o pessoal da OM;
- f) manter a OM preparada para eventuais auditorias referentes à SIC;
- g) reportar prontamente os incidentes de SIC ao CTIR.mar, após uma avaliação preliminar, com informação ao seu COMIMSUP, DCTIM e CLTI apoiador;
- h) autorizar a execução de serviços nas redes locais da OM por pessoal externo, pois estes serviços (implementações ou correções) podem afetar os requisitos de SIC da OM;
- i) designar o Oficial de Segurança da informação e Comunicações (OSIC) da OM;

- j) designar o Administrador da rede local (ADMIN) da OM; e
- k) designar a Equipe de Auditoria de SIC para realização das Auditorias Internas.

8.6 - DO OFICIAL DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (OSIC)

Oficial de qualquer corpo ou quadro, ou civil assemelhado, que tenha, preferencialmente, realizado o curso do SEN necessário para auditoria em redes locais. O OSIC da OM deverá ser nomeado formalmente por Ordem de Serviço do Titular da OM, sendo desejável possuir conhecimentos mínimos de redes locais de computadores, serviços disponibilizados pela rede (Intranet, correio eletrônico e assinaturas digitais) e conhecimento em auditoria de redes. Compete ao OSIC estabelecer procedimentos para o gerenciamento da infraestrutura de SIC de acordo com as normas em vigor. Para isso, deve realizar, no mínimo, as seguintes atividades:

- a) estabelecer e divulgar, por meio de Ordem Interna, a Instrução de Segurança da Informação e Comunicações (ISIC) – para a OM, bem como verificar sua implementação;
- b) coordenar, junto aos demais setores da OM, o estabelecimento dos Planos de Adestramento de SIC e zelar pelo seu cumprimento;
- c) assessorar o Titular da OM nos assuntos de SIC;
- d) identificar os recursos de informática que necessitam de proteção, de acordo com o respectivo grau de sigilo da informação por eles processada ou armazenada. Este procedimento de identificação deve estar explícito na ISIC da OM;
- e) reportar prontamente os incidentes de SIC, após uma avaliação preliminar, ao Titular da OM;
- f) supervisionar a elaboração e a manutenção do Histórico da Rede Local (HRL);
- g) supervisionar a elaboração e a manutenção do Plano de Contingência (PLCONT);
- h) garantir que todos estejam cientes das instruções em vigor para a segurança das informações digitais do ambiente computacional da OM, por meio da assinatura do Termo de Responsabilidade Individual (Apêndice I do Anexo A) pelos usuários que acessam a rede local;
- i) garantir que todos os usuários que possuam estações de trabalho tenham assinado o Termo de Recebimento de Estação de Trabalho (Apêndice II do Anexo A);
- j) realizar auditoria interna de SIC na OM, com apoio do CLTI, caso necessário, uma vez por

ano, emitindo Relatório de Auditoria (RAD) a ser arquivado no HRL, utilizando-se das listas de verificações disponibilizadas pela DCTIM;

k) exigir do pessoal da MB externo à OM, autorizado a executar serviços na rede local (segregada ou não), a assinatura do Termo de Responsabilidade Individual (Apêndice I do Anexo A) e o cumprimento das regras estabelecidas no referido Termo para guarda e proteção do sigilo das informações que possa ter acesso. Além disso, deverá ser cumprido os procedimentos sobre segurança orgânica, previstos em publicações específicas da MB;

l) divulgar recomendações referentes as técnicas de Engenharia Social para todo o pessoal da OM, a fim de minimizar a probabilidade de estranhos à OM obterem sucesso na aplicação de tais técnicas pelos meios de comunicações disponíveis;

m) buscar a atualização técnica através de cursos na MB, participação nos ambientes de gestão do conhecimento providos pela DCTIM, palestras, seminários e simpósios sobre SIC na MB; e

n) coordenar a GRSIC e o tratamento de resposta à incidentes de SIC em sua OM.

8.7 - DA EQUIPE DE AUDITORIA (EA) DE SIC

A EA será constituída para cada auditoria de SIC a ser realizada, na qual o mais antigo será designado Chefe da Equipe de Auditoria. Os componentes da EA serão designados formalmente por Portaria de designação. Somente poderão ser designados para compor a EA o pessoal devidamente qualificado. Representantes dos CLTI poderão ser designados para compor a EA. O período de vigência de uma EA tem início na data prevista na Portaria de designação e se encerra com a aprovação do Relatório de Auditoria.

Compete à EA, após sua designação formal, as seguintes atividades:

- a) preparar todo o material necessário para plena realização das atividades de auditoria, obtendo também as listas de verificação apropriadas na página da DCTIM, na Intranet;
- b) planejar as atividades específicas da auditoria a que foi designada;
- c) executar, de forma imparcial, soberana e independente, as atividades de auditoria;
- d) garantir o sigilo de toda informação obtida pela auditoria;
- e) elaborar o Relatório de Auditoria (RAD) conforme as normas vigentes e submetê-lo à aprovação da DCTIM no prazo estabelecido; e
- f) não divulgar os resultados de auditoria. Esta tarefa cabe à DCTIM.

8.8 - ADMINISTRADOR DA REDE LOCAL (ADMIN)

Praça da MB de qualquer especialidade ou civil que tenha realizado os cursos do SEN, necessários para atuar como administrador de rede local da OM em que serve. O perfil técnico do militar ou civil deve ser compatível com a complexidade das atividades a serem realizadas na respectiva OM. O ADMIN será nomeado formalmente por Ordem de Serviço do Titular da OM, devendo ter, preferencialmente, capacitação em Administração de Rede de Computadores e, se possível, para os sistemas operacionais que estejam sendo utilizados dentro da OM, assim como conhecimentos mínimos em auditoria de sistemas computacionais. Compete ao ADMIN gerenciar a rede local de forma a mantê-la operando dentro dos seus requisitos operacionais e com todos seus serviços em funcionamento. São desempenhadas pelo ADMIN, com o apoio do CLTI, as seguintes atividades:

- a) promover adestramentos periódicos aos usuários da OM quanto aos procedimentos e serviços de TI;
- b) resguardar a integridade física dos equipamentos de conectividade, porventura instalados no âmbito de sua OM (como roteadores, servidores web, equipamentos de radioenlace, *switches*, pares metálicos, cabos ópticos etc), comunicando imediatamente ao CLTI e ao CTIM, com informação à DCTIM, qualquer avaria detectada ou a impossibilidade de manter os referidos equipamentos em um ambiente adequado ao seu funcionamento;
- c) não permitir a divulgação de características da rede local a pessoas externas à OM sem a autorização prévia e formal do OSIC. Informações sobre as características da rede local e de seus componentes são consideradas sigilosas. É imperioso dar-lhes o devido tratamento, observando-se o grau de sigilo atribuído pelo OSIC. No caso de prestação de serviço de TI por pessoas externas a OM, deve-se ter o cuidado de expor apenas as informações necessárias atinentes ao serviço específico. Além disso, deve-se exigir a assinatura do Termo de Responsabilidade Individual (Apêndice I do Anexo A) por parte dos prestadores de serviço.
- d) elaborar, controlar e manter o Histórico da Rede Local (HRL), conforme estabelecido no Capítulo 10;
- e) auxiliar o OSIC na divulgação da ISIC da OM e das respectivas normas, conforme estabelecido neste capítulo;
- f) assessorar o OSIC na avaliação dos incidentes de segurança;
- g) criar, apagar ou alterar perfis ou privilégios de usuários ou grupos de usuários, documentando estas atividades;

- h) controlar e gerenciar os acessos aos sistemas;
- i) estabelecer um rígido controle dos acessos aos serviços disponibilizados na rede local e das suas respectivas autorizações;
- j) manter um cadastro atualizado de todos os usuários que utilizam os sistemas da rede local e os que não têm autorização para tal;
- k) realizar manutenções periódicas das contas e direitos dos usuários, observando eventuais inatividades de contas, incidência de algum usuário em grupos diferentes e tentativas de acessos não-autorizados;
- l) efetuar e garantir as atualizações dos sistemas existentes no ambiente computacional e rede local
- m) estabelecer procedimentos para garantir que as cópias de segurança (“backups”) estejam sendo feitas e guardadas de forma correta e segura;
- n) elaborar procedimentos para o acesso ao sistema computacional da OM ;
- o) configurar as estações de trabalho com privilégio mínimo para o usuário e entregá-las, mediante a assinatura do Termo de Recebimento de Estação de Trabalho (Apêndice II do Anexo A). No caso de transferência de estações de trabalho entre usuários, ter o cuidado de “formatar” o disco rígido e restabelecer a configuração padrão da OM;
- p) somente atribuir privilégios de administrador nas estações de usuários àqueles devidamente autorizados pelo Titular da OM, com as respectivas justificativas de exceção registradas no HRL e lançadas no TRI;
- q) analisar o impacto da descontinuidade dos serviços e suas consequências para o ambiente computacional da OM, estabelecendo um Plano de Contingência;
- r) testar o Plano de Contingência com as áreas envolvidas da OM, com periodicidade inferior a dois anos;
- s) garantir que os serviços (instalações, manutenções ou correções) realizados na rede local sejam feitos sem afetar a segurança dos sistemas de informações digitais;
- t) garantir que o acesso ao ambiente computacional da OM por terceiros seja realizado por meio de equipamento específico, sem conexão à rede local ou à RECIM. Além disso, este equipamento deve estar configurado para que o usuário criado não tenha privilégios de administrador de sistemas e que não exista nenhum arquivo ou documento pertencente a MB no equipamento;

- u) coibir acessos à Internet por modem, conexões 3G, 4G, WiMAX, WiFi e outras redes sem fio não autorizadas pela DCTIM;
- v) atualizar os sistemas operacionais da OM e ferramentas de segurança homologadas pela DCTIM;
- w) buscar a atualização técnica através de cursos na MB, participação nos ambientes de gestão do conhecimento providos pela DCTIM, palestras, seminários e simpósios na MB;
- x) auxiliar o OSIC na garantia de que todos estejam cientes das instruções em vigor para a SIC do ambiente computacional da OM, por meio da assinatura do Termo de Responsabilidade Individual (Apêndice I do Anexo A) pelos usuários que acessam a rede local; e
- z) auxiliar o OSIC na garantia de que todos os usuários que possuam estações de trabalho tenham assinado o Termo de Recebimento de Estação de Trabalho (Apêndice II do Anexo A).

8.9 - DO USUÁRIO

O usuário de serviços e equipamentos interligados pela rede local da OM, seja militar, servidor civil ou prestador de serviço, deverá estar ciente das suas responsabilidades sobre SIC. Para garantir o atendimento desse requisito, ele estará apto a receber uma estação de trabalho somente após a assinatura do Termo de Recebimento de Estação de Trabalho (Apêndice II do Anexo A), ficando autorizado a acessar o sistema da OM após tomar ciência das normas de SIC e assinar o Termo de Responsabilidade Individual (Apêndice I do Anexo A). São consideradas basilares as seguintes normas:

- a) tratar a informação digital como patrimônio da MB e como um recurso que deva ter seu sigilo preservado;
- b) utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso da MB exclusivamente para o interesse do serviço;
- c) preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;
- d) não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua Credencial de Segurança (CREDSEG) ou cujo teor não tenha autorização ou necessidade de conhecer;
- e) não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros;
- f) não alterar o endereço de rede ou qualquer outro dado de identificação de sua estação de

trabalho;

- g) utilizar em sua estação de trabalho somente programas homologados para uso na MB;
- h) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;
- i) não compartilhar, transferir, divulgar ou permitir o conhecimento das suas autenticações de acesso (senhas) utilizadas no ambiente computacional da OM, por terceiros;
- j) seguir as regras básicas para o uso de senhas, conforme especificado no Capítulo 8 desta norma;
- k) seguir as orientações da área de informática da OM relativas ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;
- l) comunicar imediatamente ao seu superior hierárquico e ao OSIC da OM a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de SIC estabelecidos;
- m) responder, perante a MB, as auditorias e o OSIC da OM, por acessos, tentativas de acessos ou uso indevidos da informação digital, realizados com a sua identificação ou autenticação;
- n) não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação;
- o) não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;
- p) não realizar nenhum tipo de acesso a redes “P2P” e redes sociais sem a devida autorização e obedecer a instruções próprias para os casos autorizados;
- q) não transferir qualquer tipo de arquivo que pertença à MB para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;
- r) adotar política de mesa e tela limpa a fim de reduzir os riscos de acessos não autorizados, perda e dano da informação durante e fora do horário normal de trabalho.

A política de mesa e tela limpa deve levar em consideração que:

- 1 - informações sensíveis ou críticas, por exemplo, em papel ou mídia de armazenamento eletrônico, sejam guardadas em lugar seguro (idealmente em cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando a sala está desocupada;

2 - computadores e terminais sejam mantidos desligados ou protegidos com mecanismos de travamento de tela, com senha, ou mecanismos de autenticação similar quando sem monitoração ou não usados; e

3 - documentos que contém informação sensível ou classificada sejam removidos de impressoras imediatamente.

s) estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional da OM;

t) estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional da OM pode ser auditada;

u) estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada, recebida ou retransmitida no ambiente computacional da OM deve obedecer a este preceito; e

v) caso seja usuário do Portal de serviços da MB, assinar o Termo de Responsabilidade de acesso ao Portal. As assinaturas e o conhecimento do Termo de Responsabilidade Individual (Apêndice I do Anexo A) e do Termo de Recebimento de Estação de Trabalho (Apêndice II do Anexo A) servem de registro oficial da ciência, pelo usuário, do pleno conhecimento das normas.

CAPÍTULO 9

SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SIC)

9.1 - DEFINIÇÃO

A Segurança da Informação e Comunicações (SIC) prevê ações que objetivam viabilizar e assegurar a disponibilidade, integridade e confidencialidade de dados e informações de forma a minimizar os incidentes de segurança da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não-repúdio e confiabilidade, podem também estar envolvidas.

A SIC é a proteção resultante de todas as medidas postas em execução visando negar, impedir ou minimizar a possibilidade de obtenção do conhecimento de dados que trafeguem ou sejam armazenados digitalmente nos sistemas de redes locais, compreendendo, segundo definição estabelecida pelo Governo Federal, ações voltadas às Seguranças física, lógica, de tráfego e criptológica das Informações Digitais. Portanto, a SIC corresponde não só ao conjunto de procedimentos, como também aos recursos (programas e equipamentos específicos de segurança) e às normas aplicáveis que irão garantir os seus requisitos básicos.

9.1.1 - Requisitos Básicos de SIC

- a) Disponibilidade - capacidade da informação digital estar disponível para alguém autorizado a acessá-la no momento próprio;
- b) Integridade - capacidade da informação digital somente ser modificada por alguém autorizado;
- c) Confidencialidade - capacidade da informação digital somente ser acessada por alguém autorizado;
- d) Autenticidade - capacidade da origem da informação digital ser aquela identificada.

9.2 - CONCEITUAÇÃO

9.2.1 - Ameaças às Informações Digitais

Uma ameaça ao ambiente computacional consiste na possibilidade de não se resistir a um ataque à rede que produza um determinado efeito nas informações digitais integradas. Os tipos de ameaça às informações digitais em redes são os seguintes:

- a) ameaça de interrupção: possibilidade de não se resistir a um ataque que impeça o acesso, pelo usuário, à informação digital desejada, afetando o requisito de disponibilidade;
- c) ameaça de modificação: possibilidade de não se resistir a um ataque que permita a alteração do conteúdo da informação digital por alguém não autorizado, afetando o requisito de integridade;
- b) ameaça de interceptação: possibilidade de não se resistir a um ataque que permita o acesso à informação digital por alguém não autorizado para tal, afetando o requisito de confidencialidade; e
- d) ameaça de fabricação: possibilidade de não se resistir a um ataque que permita a geração, por alguém não autorizado, de informações digitais falsas ou em nome de outrem, afetando o requisito de autenticidade.

9.2.2 - Ataques às Informações Digitais

Os ataques às informações digitais são classificados de:

- a) acidentais: aqueles não associados à intenção premeditada;
- b) intencionais: aqueles associados à intenção premeditada;
- c) passivos: aqueles que, quando realizados, não resultam em qualquer modificação nas informações digitais contidas em um sistema, como, por exemplo, uma interceptação;
- d) ativos: aqueles que envolvem interrupção, modificação ou fabricação de informações digitais contidas no sistema, ou alteração do estado ou da operação do próprio sistema;
- e) externos: aqueles praticados por usuário externo à RECIM que, embora sem autorização de acesso, conseguiu vencer as barreiras de proteção existentes; e/ou
- f) internos: aqueles praticados por usuários internos à RECIM, com ou sem autorização de acesso, ou por usuários externos à RECIM que tenham autorização de acesso.

9.2.3 - Princípio do Privilégio Mínimo

Este princípio preconiza que nenhum privilégio, acesso, programa, dispositivo de entrada ou saída, porta ou serviço devem estar disponível na estação de trabalho, a não ser que seja realmente necessário e autorizado especificamente pelo Titular da OM.

9.2.4 - Separação das Funções e Responsabilidades

Prática comum e eficiente para se evitar que as medidas e mecanismos de segurança sejam burladas. Quando a administração ou a responsabilidade dos sistemas digitais ou dispositivos de segurança é dividida por mais de uma pessoa, nenhuma pessoa ou processo possui privilégio suficiente para realizar atividades maliciosas significante ou burlar os controles de segurança impostos.

9.2.5 - Recursos Computacionais Críticos (RCC)

No ambiente computacional integrado por uma rede local, alguns recursos ou equipamentos são considerados críticos em relação aos riscos de segurança aos quais são expostos, pois suas vulnerabilidades afetarão diretamente os requisitos básicos de SIC. Os principais RCC são: estações de trabalho, servidores, roteadores, equipamentos de conectividade, equipamentos de segurança da informação (firewalls, detectores de intrusão ou outros), meios físicos de tráfego, sistemas de armazenamento das informações digitais, equipamentos (discos rígidos e outras mídias) que armazenam informações digitais sigilosas e os sistemas de cópias de segurança (backup), assim como as instalações elétricas e os sistemas de refrigeração, sistemas de combate a incêndio, sistemas de controle de acesso físico e outros sistemas ou recursos das áreas que abrigam equipamentos computacionais. Os serviços de manutenção dos RCC também são considerados críticos, merecendo uma atenção especial sob o aspecto da SIC.

De acordo com a sua importância para a SIC, cada RCC ou grupo de RCC com características semelhantes pode ser classificado nos seguintes níveis:

- NÍVEL 1: corresponde aos RCC de alta importância, isto é, aqueles que, quando atingidos, interrompem ou degradam severamente o funcionamento da rede local da OM ou RECIM, tornam expostas informações digitais sigilosas ou causam prejuízo à SIC por comprometimento de um dos requisitos básicos;
- NÍVEL 2: corresponde aos RCC de média importância, isto é, aqueles que, quando atingidos, degradam apenas superficialmente o funcionamento da rede local da OM ou RECIM, tornam expostas informações digitais não sigilosas ou não causam prejuízo à SIC por comprometimento de um dos requisitos básicos; e

- NÍVEL 3: corresponde aos RCC de baixa importância, isto é, aqueles que quando atingidos não causam prejuízo direto à SIC ou ao funcionamento da rede local da OM ou RECIM, mas que requerem atenção, pois podem permitir que o ataque ou ameaça escale, comprometendo outros RCC de nível de importância superior.

9.3 - SEGURANÇA ORGÂNICA

A Segurança Orgânica, conforme definido em publicação do EMA que rege o assunto, compreende a adoção de um conjunto de medidas voltado para a prevenção e a obstrução das ações ou ocorrências adversas de qualquer natureza que possam comprometer a salvaguarda de conhecimentos de interesse da MB ou do País. A Segurança Orgânica desdobra-se em:

- Segurança do Pessoal;
- Segurança da Documentação e do Material;
- Segurança da Informação Digital (SID);
- Segurança das Comunicações; e
- Segurança das Áreas e Instalações.

Esta norma tem como propósito apresentar os procedimentos vinculados à Segurança da Informação e Comunicações. Entretanto, ressalta-se que as medidas que fazem parte dos demais segmentos da Segurança Orgânica também concorrem para consecução daquela, e vice-versa.

Assim, e para efeito de conformidade com as normas estabelecidas pelo Governo Federal, a apresentação que se segue das medidas de Segurança Orgânica voltadas à Segurança da Informação e Comunicações está dividida em quatro partes, que tratam, respectivamente, das Seguranças física, lógica, de tráfego e criptológica das Informações Digitais.

9.4 - SEGURANÇA FÍSICA DA INFORMAÇÃO E COMUNICAÇÕES

A Segurança Física corresponde a todos os procedimentos e dispositivos utilizados para assegurar a integridade física dos RCC.

Concorre diretamente para a sua consecução os conjuntos de medidas de Segurança orgânica, definidos no EMA-353 (Rev.1) para implementação em todas as OM.

Com relação à Segurança do Pessoal, esta norma apenas ressalta a importância do fiel

cumprimento das medidas objetivamente voltadas para o pessoal da MB, definidas no EMA-353 (Rev.1), no sentido de assegurar comportamentos adequados à salvaguarda de conhecimentos sigilosos, que, conforme preconizado na publicação supracitada, para efeito de aplicação, estão agrupadas em três tipos:

- segurança no processo seletivo;
- segurança no desempenho da função; e
- segurança no desligamento.

No que diz respeito à Segurança das Áreas e Instalações e à Segurança da Documentação e do Material, entretanto, são emitidas nesta norma instruções específicas, em complemento ao previsto no EMA-353 (Rev.1), tal como a utilização, pelas OM, de perímetros de segurança para proteger áreas que contenham RCC importantes para a continuidade das suas atividades, conforme abaixo especificado.

9.4.1 - Perímetro de Segurança

Um perímetro de segurança é uma separação física que estabelece uma barreira de proteção (como por exemplo: paredes, salas, cofres, salas-cofre, etc), cujas vias de acesso possuam controle eletrônico ou sejam vigiadas por pessoal de serviço (ou ambos), dependendo do resultado da análise de risco elaborada. Cada uma destas barreiras representa um perímetro ou camada física de segurança que melhora a proteção total. Os perímetros de segurança devem ser claramente definidos na “Instrução de Segurança da Informação e Comunicações” (ISIC) da OM, ilustrados no seu Histórico da Rede Local (HRL) e demarcados localmente. O acesso físico a cada perímetro de segurança existente na OM necessita ser controlado, identificando-se todo visitante e permitindo o acesso aos perímetros de segurança que contenham RCC somente ao pessoal autorizado. Além disso, cada visitante deverá estar sempre acompanhado por uma pessoa autorizada. A entrada ou a saída do perímetro de segurança de dispositivos periféricos de armazenamento, tais como disquetes, pendrives e discos externos, ou de quaisquer outros dispositivos armazenadores de informações digitais ou dispositivos móveis inteligentes, tais como celulares, tablets, impressoras e notebooks assim como quaisquer outros equipamentos eletrônicos com capacidade de registro de informações deve ser proibida. Exceções devem ser autorizadas pelo OSIC, além de controladas e registradas por meio de Ordem Interna ou de Ordem de Serviço da própria OM.

Cada OSIC deve elaborar normas e procedimentos de controle de acesso físico aos perímetros de segurança estabelecidos nas OM, observando os seguintes aspectos:

- a) os visitantes de perímetros de segurança devem ser identificados na sua entrada, com registro de data, hora e razão da visita. O acesso deve ser limitado ao propósito da mesma e supervisionado enquanto durar a visita. O visitante deve receber instruções mínimas estabelecidas pelo OSIC sobre os procedimentos de SIC e não deve portar qualquer equipamento eletrônico;
- b) o acesso aos perímetros de segurança deve ser controlado e permitido somente aos militares e servidores civis autorizados, de acordo com as respectivas CREDSEG; e
- c) a revisão das normas e procedimentos de controle de acesso físico aos perímetros de segurança deve ser feita regularmente pelo OSIC, em conjunto com o Oficial de Segurança Orgânica da OM, com periodicidade não superior a 12 (doze) meses.

9.4.2 - Segurança Física dos RCC Nível 1

Os locais de guarda dos RCC nível 1 (de alta importância, como, por exemplo, os equipamentos servidores e os roteadores) devem possuir segurança física compatível. Para tanto, a segurança física desses locais deve ser reforçada, estabelecendo mecanismos de controle e registro (preferencialmente eletrônicos) de entrada e saída do pessoal e mecanismos de segurança para o período fora do expediente normal, como sistema de alarme e lacre numerado. Além disso, todo equipamento servidor deve utilizar, permanentemente, senha forte para proteção de acesso físico ao servidor.

9.4.3 - Segurança Física dos Dispositivos de Conectividade

Os roteadores e switches são elementos ativos de conectividade. O contato com um equipamento deste tipo, além de permitir um acesso indevido à RECIM, pode possibilitar a manipulação imperceptível (cópia, alteração, inserção ou destruição) das mensagens que ali trafegam. Assim, é fundamental:

- a) proteger todos os equipamentos de conectividade, utilizando gabinetes com chave e lacre numerado;
- b) proteger devidamente os estabilizadores elétricos dos equipamentos de conectividade;

- c) estabelecer controle rígido das chaves e dos lacres numerados dos gabinetes de proteção dos equipamentos de conectividade;
- d) reforçar a segurança física de compartimentos não-guarnevidos que contenham equipamentos de conectividade, estabelecendo sistema de alarme de abertura da porta, controle de entrada e saída de pessoal e mecanismos de verificação para o cadeado da porta, como lacre numerado; e
- e) configurar as switches com filtro de MAC address.

9.4.4 - Proteção Contra Interferências Eletromagnéticas

As informações digitais armazenadas magneticamente são muito suscetíveis a campos ou interferências eletromagnéticos. A fim de impedir que este tipo de ameaça possa afetar algum dos requisitos básicos da SIC, deve se evitar a instalação de RCC nas proximidades de equipamentos elétricos de alta potência e rádio transmissores ou vice-versa.

9.4.5 - Proteção da Alimentação Elétrica dos Equipamentos

A alimentação elétrica dos equipamentos também requer cuidado, pois sua falha pode impactar o requisito básico de disponibilidade. Para tal, é desejável que todos os RCC estejam protegidos por fontes estabilizadas e sistemas de alimentação em emergência (nobreaks). Caso não seja possível a implementação destas proteções em todos os equipamentos, pelo menos os RCC Nível 1 devem possuir proteções contra falhas de alimentação elétrica.

9.4.6 - Realização de Serviços na Rede Local

A execução de quaisquer serviços (implementações, instalações, configurações, correções, verificações, medições, substituições, interligações, elaborações de projetos, suporte técnico, manutenções, etc.) nas redes locais por pessoal externo à OM (de outras OM ou de empresa contratada), principalmente em RCC nível 1, pode afetar os requisitos de SIC da OM e de toda a MB, devido a sua interligação à RECIM. Assim, tais serviços não devem ser efetuados sem análise e autorização prévias do CLTI, que poderá efetuar consulta à DCTIM.

A análise prévia permitirá ao CLTI avaliar os serviços a serem executados, não só quanto aos aspectos de SIC, mas também quanto a outros aspectos (da sua área de atuação) que possam ser afetados, como estrutura física (cabeamento), topologia, capacidade de tráfego, conectividade, endereçamento, configuração da rede local etc. Quanto ao pessoal externo envolvido na realização desses serviços, a OM deverá, além de exigir a assinatura do Termo de Responsabilidade Individual (Apêndice I do Anexo A), cumprir o previsto no PSO da OM em consonância com o EMA-353 (Rev.1), sobre a Segurança do Pessoal.

9.5 - SEGURANÇA LÓGICA DA INFORMAÇÃO E COMUNICAÇÕES

9.5.1 - Segurança Lógica dos Equipamentos Servidores

As vulnerabilidades lógicas normalmente encontradas nos equipamentos servidores são inerentes aos protocolos utilizados e à configuração implementada, decorrentes da falta de atualização dos programas ou pela não instalação das correções, disponibilizadas pelos fabricantes ou distribuidores dos sistemas operacionais e dos aplicativos em uso. Para mitigar essas vulnerabilidades, é fundamental a instalação das versões atualizadas dos programas existentes nos servidores, bem como de todas as correções disponibilizadas pelos respectivos fabricantes e distribuidores. Adicionalmente, todos os serviços não necessários devem ser desabilitados, observando o princípio do privilégio mínimo, desinstalando-se todos os programas e aplicativos desnecessários e fechando-se todas as portas lógicas que não estiverem efetivamente em uso. Estes dispositivos serão habilitados somente quando for estritamente necessário ao serviço.

Para reforçar a segurança lógica dos equipamentos servidores, os Administradores da Rede Local (ADMIN) devem acompanhar continuamente as circulares, DCTIMARIST e Listas de Verificação de SIC, entre outros documentos, disponibilizadas pela DCTIM, e providenciar o seu cumprimento.

9.5.2 - Acesso Remoto à Configuração dos Equipamentos Servidores

Os terminais de acesso remoto permitem aos equipamentos servidores serem configurados remotamente, sem o acesso físico à máquina. Isso é particularmente útil no caso de suporte à distância, quando técnicos podem, por exemplo, efetuar reparos emergenciais nas configurações de um equipamento servidor sem a necessidade de se deslocarem até o local onde o mesmo se encontra.

No entanto, por segurança, esses terminais de acesso remoto devem permanecer sempre desabilitados, pois ninguém externo à OM deve ter acesso remoto aos RCC nível 1 da OM sem prévia autorização da DCTIM, em virtude do comprometimento que isso pode proporcionar à RECIM. No caso da eventual necessidade de se utilizar os terminais de acesso remoto, deverá ser solicitada a devida autorização. Caso seja autorizado pela DCTIM, os terminais de acesso remoto deverão ser habilitados somente no período em que efetivamente for efetuado o reparo à distância, com a utilização de senha de acesso e protocolos seguros, baseados em criptografia (se disponíveis na máquina), e mediante a supervisão contínua do ADMIN do servidor avariado. Devem ser efetuados, também, os devidos registros na parte de Incidentes do Histórico da Rede Local (HRL), conforme previsto no Capítulo 10, indicando o quê, como, onde, quando e porque foi feito, quem fez, quem acompanhou e outras informações pertinentes ao caso.

9.5.3 - Segurança Lógica dos Dispositivos de Conectividade

Os dispositivos de conectividade, como os roteadores e os switches, possuem grande parte de sua segurança lógica amparada na configuração do equipamento. No entanto, esses dispositivos vêm de fábrica com configurações padrões (incluindo as senhas de acesso) e de conhecimento irrestrito. Esse fato é amplamente explorado por atacantes, que conhecem as senhas padrões de fábrica e as vulnerabilidades das configurações não seguras. Torna-se necessário, portanto, que os equipamentos de conectividade, ao serem instalados, sejam sempre alterados para uma configuração segura, diferente da original de fábrica. Suas senhas devem ser alteradas não só por ocasião da instalação, mas periodicamente, utilizando doze (12) ou mais caracteres, letras minúsculas, letras maiúsculas, números e caracteres especiais.

9.5.4 - Segurança Lógica das Estações de Trabalho

Por corresponder ao tipo de equipamento em maior quantidade no conjunto de RCC existentes na RECIM, as estações de trabalho - portáteis ou não - requerem maior atenção em relação à SIC.

A estação de trabalho não pode disponibilizar nenhum serviço, nem acesso remoto, pois não é um equipamento servidor, sendo, desta forma, apenas um meio para acessar os serviços e programas disponibilizados e homologados pela DCTIM.

Para este RCC, a maior vulnerabilidade está no próprio usuário. Desta forma, para se mitigar os efeitos da ação maliciosa, intencional ou não, dos usuários e proteger a RECIM, as seguintes configurações mínimas devem ser implementadas:

- a) utilização dos programas de proteção de estação de trabalho, com gerenciamento centralizado pelo CTIM, contra atividades e programas maliciosos e homologados pela DCTIM, tais como antivírus e anti-spyware;
- b) atualização dos Sistemas Operacionais através dos serviços disponibilizados pelo CTIM;
- c) orientação da sua configuração segundo o princípio do privilégio mínimo;
- d) ter somente os programas homologados pela DCTIM instalados e todas as portas e serviços desnecessários desabilitados;
- e) retirar do usuário o poder de administrador das estações de trabalho. Nas estações com sistema operacional Windows, o usuário é configurado, por padrão de instalação, como administrador da estação de trabalho. Esta configuração padrão potencializa a propagação de programas maliciosos, uma vez que estes podem vir a assumir os privilégios do usuário;
- f) desabilitar ou desinstalar, sem prejuízo das funções inerentes ao usuário, qualquer dispositivo de entrada e saída de dados, tais como gravadores de CD/DVD, portas USB e impressoras locais. Estes dispositivos serão habilitados somente quando for estritamente necessário ao serviço;
- g) submeter as estações de trabalho a um serviço de diretório, gerenciado pelo ADMIN e não permitir acesso aos serviços disponibilizados pela RECIM sem o registro de acesso do usuário neste serviço;
- h) cada máquina deverá ter uma senha de configuração (setup), de conhecimento exclusivo do ADMIN, a fim de evitar que o próprio usuário ou qualquer pessoa não autorizada altere a configuração da máquina; esta senha, portanto, não poderá ser de conhecimento do usuário da máquina ou de qualquer outra pessoa além do ADMIN;
- i) cada estação de trabalho deverá ter uma senha de inicialização (boot), de conhecimento exclusivo do usuário da máquina, a fim de evitar que outras pessoas acessem o disco rígido dessa máquina; esta senha, portanto, não poderá ser de conhecimento do ADMIN ou de qualquer outra pessoa além do usuário da máquina; e

j) É vedada a configuração e a disponibilização de discos, diretórios ou arquivos compartilhados nas estações de trabalho, mesmo que se configure seu acesso por senha, em virtude da vulnerabilidade desses compartilhamentos e do comprometimento que isso pode proporcionar à segurança da RECIM. Deve ser utilizado um servidor de arquivos ou outra solução homologada pela DCTIM para suprir tal necessidade.

9.5.5 - Realização de gerenciamento da Rede Local

A gestão dos recursos das redes locais das OM deverá ser centralizada a partir de serviço de diretório estabelecido pela DCTIM. Um serviço de diretório é um componente importante de um Sistema Operacional de Rede (SOR) e serve para armazenar, organizar, localizar, gerenciar e administrar informações sobre os recursos de rede, que podem incluir volumes, pastas, arquivos, impressoras, usuários, grupos, dispositivos e outros objetos, permitindo aos administradores da rede gerenciar o acesso de usuários e sistemas a esses recursos.

Uma das maiores utilidades de um serviço de diretórios é permitir a centralização da gestão dos recursos da rede, visando simplificar sua administração, seu backup e sua replicação, incrementando desta forma sua disponibilidade e confiabilidade, enquanto diminui o tempo despendido pelos ADMIN em tarefas básicas. A centralização do gerenciamento das redes locais visa facilitar a governança da SIC a partir da padronização de políticas a serem empregadas pelos ADMIN e OSIC.

9.5.6 - Regras Básicas para a confecção e o uso de senhas

Toda e qualquer senha é sempre individual e intransferível, devendo seu responsável:

1. nunca compartilhá-la;
2. não utilizar sequência fácil ou óbvia de caracteres, que facilite a sua descoberta;
3. não utilizar palavras existentes em dicionários;
4. utilizar aleatoriamente letras minúsculas, letras maiúsculas, números e caracteres especiais, cumprindo a política de configuração e de tamanho de senhas que estiverem em vigor nos programas e serviços em uso;
5. não escrevê-la em lugares visíveis, de fácil acesso ou em claro;

6. proceder às devidas precauções para mantê-la em sigilo, conforme previsto também no Termo de Responsabilidade Individual (Apêndice I do Anexo A); e
7. cumprir a política de tempo de validade de senhas que estiver em vigor nos programas e serviços em uso, trocando-a regularmente.

9.5.7 - Uso de Antivírus e outros Programas de Proteção Individual

Devido ao caráter dinâmico, rápido e agressivo dos programas maliciosos e de outras ameaças, as configurações de uso e de atualização dos programas de proteção individuais devem ter seu gerenciamento centralizado pelo CTIM, permitindo o sincronismo, velocidade de reação e atualização, fundamentais para a proteção de uma rede.

Ressalta-se que somente devem ser utilizados os programas homologados e previamente autorizados para uso na MB. O emprego de programas não homologados pode impactar negativamente o desempenho e a segurança da rede, além de possibilitar o surgimento de novas vulnerabilidades.

Por serem aplicativos voltados à SIC, a análise prévia da DCTIM se torna imprescindível, pois o uso indevido ou a configuração incorreta podem, além do acima citado, causar uma falsa impressão de segurança e facilitar determinados tipos de ataque.

9.5.8 - Uso de Modem em Estações de Trabalho e Equipamentos Servidores

Não é permitida a instalação de modem de nenhuma espécie, inclusive os 3G/4G, em equipamento interligado à rede local da OM. No caso de equipamento que utilize placa-mãe com modem “onboard”, este deverá ser desabilitado e, se possível, fisicamente removido. No caso da eventual necessidade de se utilizar modem 3G/4G como solução de acesso, o Projeto deverá ser apreciado e homologado pela DCTIM.

9.5.9 - Eliminação Segura de Arquivos

Para se eliminar de forma segura um determinado arquivo sigiloso, armazenado em mídia magnética, o conteúdo do mesmo deve ser sobreescrito com um texto aleatório, para evitar sua recuperação posterior e/ou devem ser utilizadas ferramentas e técnicas homologadas pela DCTIM.

9.5.10 - Cópias de Segurança (Backup)

As cópias de segurança (backup) das informações digitais servem para restabelecer a condição anterior, ou a mais próxima disso, quando a integridade das informações digitais houver sido afetada.

Essas cópias devem ser gravadas em mídias específicas, como fitas magnéticas, e devem ser armazenadas adequadamente, evitando sua deterioração ou acesso indevido.

Em relação às informações digitais armazenadas nos equipamentos servidores da rede local, a periodicidade de realização das cópias de segurança, tarefa sob controle do ADMIN, deve seguir as orientações mínimas abaixo apresentadas:

- a) realizar 1(uma) cópia parcial (apenas das informações digitais alteradas) diária ao final do expediente e manter as cópias parciais diárias efetuadas na semana vigente;
- b) realizar 1(uma) cópia completa semanal e manter as cópias completas semanais efetuadas no mês vigente;
- c) realizar cópia completa a cada mês e manter as cópias completas mensais efetuadas no bimestre vigente;
- d) verificar periodicamente a integridade das cópias de segurança, efetuando testes de recuperação de informações digitais armazenadas; e
- e) manter um controle da elaboração de cópias de segurança e dos respectivos testes de recuperação, controle este que deve ser regulado na ISIC da OM.
- f) Local de Guarda das Cópias de Segurança dos Equipamentos Servidores - As cópias de segurança dos equipamentos servidores da rede local devem ser guardadas em local determinado pelo OSIC e controlado pelo ADMIN. Para uma maior segurança das informações digitais, este local de guarda deverá estar situado, sempre que possível, em prédio distinto ao do equipamento servidor do qual foi feita a respectiva cópia de segurança. Na impossibilidade de se utilizar local de guarda em prédio distinto para armazenamento das cópias de segurança, devem ser utilizados compartimentos afastados e com proteção contra incêndio e alagamento.
- g) Grau de Sigilo das Cópias de Segurança - As cópias de segurança têm o mesmo grau de sigilo das informações digitais que armazenam e, por isso, devem ser protegidas pelas medidas de segurança correspondentes.

9.5.11 - Acesso à Rede Local por Estrangeiros

O acesso à rede local por estrangeiros deve ser reportado à DCTIM, com informação ao seu COMINSUP, EMA, ComOpNav e CIM. A DCTIM analisará a situação e as necessidades para definir barreiras lógicas, procedimentos de vigilância e outras medidas que se façam necessárias para impedir o acesso dos estrangeiros às informações sensíveis

disponíveis na rede local da OM e, consequentemente, à RECIM, e para adestrar o pessoal da OM quanto aos dispositivos e procedimentos a serem adotados.

Devem ser estabelecidas, na ISIC, normas para o controle do uso de recursos computacionais e de acesso à rede local por estrangeiros eventualmente embarcados, destacados, cursando, participando de exercícios, visitando ou efetuando qualquer atividade na OM. O princípio do privilégio mínimo deve ser observado e o estrangeiro só pode ter acesso aos recursos necessários à realização das suas funções e/ou de acordo com a sua missão no Brasil.

9.5.12 - Listas de Verificação de SIC

A DCTIM disponibiliza, na sua página da Intranet, as Listas de Verificação de SIC, com as práticas e normas complementares de segurança indicadas para os principais sistemas operacionais em uso na MB. Essas listas são constantemente atualizadas, para acompanhar o contínuo desenvolvimento tecnológico dos sistemas computacionais e incorporar as últimas ferramentas na área de segurança digital.

9.5.13 - Instalação de Programas, Equipamentos ou Dispositivos de SIC

É vedada a instalação de qualquer programa, equipamento ou dispositivo voltado à segurança de rede local, ou de estação de trabalho, sem análise e autorização prévias da DCTIM.

Por serem mecanismos voltados à SIC, a análise prévia da DCTIM se torna imprescindível, pois o uso indevido ou a configuração incorreta podem, além de impactar negativamente o desempenho e a segurança da rede, causar uma falsa impressão de segurança e facilitar determinados tipos de ataque.

9.5.14 - Instalação de Programas para Uso em Rede

É vedada a instalação de qualquer programa para uso em rede, mesmo aqueles não voltados à SIC, sem análise e autorização prévias da DCTIM, pois esta instalação e o uso em rede podem impactar negativamente o desempenho e a segurança da rede.

Para otimizar a utilização de recursos, a OM deve consultar a DCTIM antes da aquisição do programa. No caso de programas especialmente desenvolvidos (tanto por empresa contratada quanto por uma OM) para uso em rede na MB, é necessário que a consulta à

DCTIM seja realizada anterior ao início ou ainda na fase inicial desse desenvolvimento, de modo a possibilitar os eventuais ajustes necessários.

9.5.15 - Correio Eletrônico

O correio eletrônico corresponde ao serviço de troca de mensagens por meio da rede local, tanto entre usuários internos à OM, quanto entre estes e usuários externos. As mensagens de correio eletrônico também podem transportar arquivos digitais em anexo. Pela sua eficiência como meio de comunicação, a propagação de ameaças e ataques pelo serviço de correio eletrônico é rápida e muitas vezes avassaladora, como, por exemplo, propagação de um ataque por vírus.

Para minimizar possíveis ameaças à SIC, que podem vir tanto no corpo da mensagem quanto em seus anexos, as seguintes regras devem ser seguidas por todos os usuários:

- a) o uso do correio eletrônico da MB é restrito para o interesse do serviço, é vedado o seu uso para transmissão de qualquer mensagem que não seja de serviço;
- b) não é permitida a transferência de arquivo que pertença a MB por “e-mail” para caixa postal externa, exceto no interesse de serviço;
- c) as máquinas utilizadas como servidores de correio eletrônico devem ser instaladas em compartimentos de acesso restrito e controlado;
- d) não devem ser executados, copiados ou retidos arquivos recebidos em anexo à mensagens de correio eletrônico sem uma prévia análise ou varredura por programas específicos de controle e verificação de ataques, como por exemplo programas antivírus;
- e) se houver qualquer dúvida quanto à origem de mensagem recebida, esta ocorrência deve ser notificada ao ADMIN e ao OSIC, para análise, antes da abertura dessa mensagem;
- f) É vedado o uso de correio eletrônico por meio de páginas específicas da Internet (webmail);
- g) devem ser utilizados os programas certificados pela DCTIM para assinatura digital, cujo uso deve ser incentivado em todas as correspondências eletrônicas internas à rede local da OM;
- h) é proibido o uso de programas para criptografia de arquivos e mensagens que não sejam os controlados pela DCTIM, de acordo com instruções próprias; e

i) conforme indicado no Termo de Responsabilidade Individual (Apêndice I do Anexo A), toda informação processada, armazenada ou em trâmite no ambiente computacional da OM pode ser auditada, incluindo o correio eletrônico.

9.5.16 - Bases de Dados

Uma base de dados corresponde ao conjunto de informações digitais armazenado em determinados recursos computacionais. As bases de dados podem estar integradas pela rede local ou podem estar localizadas em redes externas, tais como a Internet. Os serviços de acesso à base de dados incluem transferência de arquivos e acessos à diretórios específicos da rede que contenham informações digitais de interesse.

As autorizações para acesso à base de dados ou diretórios constitui uma concessão de privilégios, que deve ser controlada pelo OSIC.

Todas as informações digitais contidas em bases de dados ou em diretórios específicos devem atender às seguintes regras mínimas de segurança:

- a) as informações digitais sigilosas não podem ser mantidas em texto claro nos RCC. Devem ser criptografadas como preconizado na doutrina vigente e somente utilizando recursos criptológicos disponibilizados pela DCTIM;
- b) não é permitido que diretórios de qualquer equipamento servidor interligado pela rede local possuam compartilhamento de livre acesso. Caso seja necessário algum tipo de compartilhamento, este deverá ser restrito a usuários específicos da rede local e utilizar registro (logs) dos acessos;
- c) as configurações dos arquivos de registro (logs) dos acessos de leitura ou escrita à base de dados ou diretórios da rede devem ser mantidas no Histórico da Rede Local (HRL), possibilitando a realização de análises e estudos estatísticos; e
- d) conforme indicado no Termo de Responsabilidade Individual (Apêndice I do Anexo A), toda informação processada, armazenada ou em trâmite no ambiente computacional da OM pode ser auditada, incluindo o histórico dos acessos e das modificações das bases de dados.

9.6 - SEGURANÇA DO TRÁFEGO DA INFORMAÇÃO E COMUNICAÇÕES

Esta segurança compreende todas as medidas colocadas em prática para impedir a obtenção não autorizada das informações digitais quando estas estiverem trafegando em uma rede local e suas conexões.

9.6.1 - Enlace entre Instalações Afastadas da Rede Local

Caso haja a necessidade de se interconectar duas instalações afastadas fisicamente de forma a constituir uma mesma rede local, deverão ser tomadas as devidas medidas de proteção às informações digitais que trafegam entre as mesmas. Quando o enlace não for controlado pela MB, como no caso dos enlaces contratados de empresas de telecomunicações, os dados deverão trafegar por meio de uma Rede Privada Virtual (VPN—Virtual Private Network). Relembra-se que os dados sigilosos somente podem trafegar criptografados. Os projetos de implementação de VPNs devem ser submetidos à aprovação da DCTIM.

9.6.2 - Quanto ao uso de Redes Sem Fio

É vedado o uso de redes sem fio para a interligação de equipamentos na rede local da OM. Em casos excepcionais, as OM da MB interessadas em instalar redes sem fio deverão encaminhar seu pedido formal à DCTIM, de acordo com norma específica daquela Diretoria, a fim de obter parecer favorável e autorização. Nenhum dispositivo de rede sem fio deve ser implementado sem análise e autorização prévias da DCTIM.

9.6.3 - Quanto ao uso de redes Ponto a Ponto (P2P)

É vedado o uso de redes P2P nas estações de trabalho da RECIM. Atualmente os principais problemas relacionados às redes ponto-a-ponto estão relacionados à segurança, já que não é feito um controle sobre o conteúdo (vídeos, livros, músicas, softwares e etc.) liberado nessas redes. A ausência de um servidor central, típico desses sistemas, determina uma rede livre, onde uma estação de trabalho se conecta a outro computador diretamente e, desta forma, qualquer tipo de material, incluindo programas maliciosos, arquivos corrompidos e de conteúdo proibido na RECIM, pode vir a ser disseminado.

9.7 - SEGURANÇA NA UTILIZAÇÃO DE MÍDIAS E REDES SOCIAIS

As Mídias e Redes Sociais são aplicações ou serviços de Tecnologia da Informação (TI) que disponibilizam informações acessíveis publicamente, via Internet, compartilhando-as em ambientes computacionais ou sítios que não são de propriedade e não são operados ou controlados pela MB. Tais aplicações ou serviços incluem ferramentas colaborativas de compartilhamento de informações inseridas nestes serviços por usuários comuns ou organizações. Exemplos de aplicações ou serviços: Facebook, Youtube, Flickr, Instagram, Twitter, Google Apps, Blogs, Slideshare, Foruns de Discussões, dentre outros.

9.7.1 - Uso Institucional de Mídias e Redes Sociais

Consiste na realização, pela MB, de atividades oficiais de Relações Públicas (RP), conduzidas em mídias ou redes sociais. Essas presenças Institucionais da MB na Internet devem funcionar como extensão ou complemento aos sítios oficiais da MB, e não em substituição aos mesmos.

9.7.2 - Uso Não Institucional de Mídias e Redes Sociais

Consiste na publicação ou divulgação de qualquer conteúdo (informação) relacionado à MB em qualquer Mídia ou Rede Social, por militares ou servidores civis, da ativa ou da reserva, da MB, de forma pessoal e não institucional. O conteúdo inclui (não estando limitado a): fotos, imagens, vídeos, textos ou sons. São publicações não institucionais, não endossadas pela MB e portanto não submetidas a qualquer processo interno de aprovação. O autor da publicação possui total responsabilidade pelo conteúdo publicado.

9.7.3 - Quanto ao uso de Mídias e Redes Sociais em estações de trabalho conectadas à RECIM

É vedado o uso de redes sociais, tais como, Facebook, Instagram, WhatsApp e Twitter a partir de estações de trabalho conectadas à RECIM, por esta ser uma rede para fins operativos e administrativos da MB. Os usuários que, de acordo com o seu exercício funcional e a missão da OM, tiverem a necessidade de acesso às mídias e redes sociais a partir de estações de trabalho conectadas à RECIM, deverão ter autorização concedida pelo Titular da OM, de acordo com os procedimentos definidos em norma específica da DCTIM, a partir do tipo de acesso à Internet definido para cada usuário.

9.7.4 - Quanto ao uso de Mídias, Redes Sociais, e-mail pessoal e serviço de mensageria particular em estações de trabalho e dispositivos móveis pessoais não conectados à RECIM

É vedado o uso de Mídias e Redes Sociais, assim como e-mail pessoal e serviço de mensageria particular, como WhatsApp, para trafegar dados cujo teor estejam relacionados a assuntos de serviço, especialmente os sigilosos, ou aqueles com potencial de macular, de alguma forma, a imagem da Instituição ou de seus integrantes.

9.8 – SEGURANÇA CRIPTOLÓGICA DA INFORMAÇÃO E COMUNICAÇÕES

A segurança criptológica consiste no emprego de processos de codificação ou cifração para alterar-se o conteúdo original da informação, de modo a torná-lo incompreensível quando examinado sem o uso dos mesmos códigos ou cifras.

As informações digitais sigilosas devem trafegar e ser armazenadas cifradas, utilizando-se os recursos criptográficos em vigor na MB e observando-se o preconizado nas publicações do EMA e da DGMM referentes, respectivamente, às Normas para a Salvaguarda de Materiais Controlados, Dados, Informações, Documentos e Materiais Sigilosos na Marinha e às Normas para a Criptologia da Marinha.

9.8.1 - Quanto ao uso de dispositivos criptográficos

É vedada a utilização de quaisquer dispositivos criptográficos que não os previamente autorizados e homologados pela DCTIM para uso na MB.

9.8.2 - Quanto ao local das Estações de Trabalho com recursos criptográficos definidos para tráfego de mensagens e expedientes entre OM

As Estações de Trabalho que contenham recursos criptográficos definidos para tráfego de mensagens e expedientes entre OM devem ser alojadas nos Camarins de Criptografia do tipo exclusivo, de acordo com o artigo 2.1, da DGMM-0510 (RES) - Normas para a Criptologia da Marinha.

9.9 - MENTALIDADE DE SEGURANÇA

O esforço para as atividades de SIC deve ser de todos e não somente do pessoal diretamente envolvido com o setor de informática da OM. O fator mais importante para a SIC é a existência de uma mentalidade de segurança incutida em todo o pessoal. Pouco adiantará o estabelecimento de rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver delas perfeita consciência. As OM devem, portanto, envidar esforços para desenvolver e manter um alto nível de conscientização do pessoal quanto à SIC. Isto pode ser feito, por exemplo, por meio de notas em Plano do Dia e de palestras, adestramentos, exercícios internos e outras atividades cabíveis, englobando publicações, normas e procedimentos afetos ao assunto. Além disso, dentro do Programa de Adestramento de cada OM, devem ser formalmente estabelecidos e continuamente cumpridos adestramentos que abordem todos os aspectos de SIC.

9.9.1 - Adestramentos de SIC

As OM devem prever, dentro do seu Programa de Adestramento, o contínuo adestramento de SIC para todo o seu pessoal, de modo a auxiliar a manutenção e a garantia de uma elevada mentalidade de segurança.

Consequentemente, também deve haver um controle do cumprimento desses adestramentos, indicando qual o pessoal adestrado e o tipo de adestramento ministrado a cada militar, funcionário civil ou prestador de serviço, de modo a possibilitar o planejamento e a manutenção dos níveis mínimos de adestramento de SIC da OM. O Programa de Adestramento, conforme normas específicas, deve ser documentado e ter seu respectivo cumprimento controlado por meio dos Planos de Adestramentos. Para possibilitar que o Programa de Adestramento da OM englobe todos os aspectos de SIC, os assuntos devem ser divididos em pequenas partes, cada uma direcionada a um tema específico, de acordo com o conteúdo da Parte III desta Norma, de modo que os adestramentos tenham conteúdo conciso (facilitando a assimilação por quem está sendo adestrado) e sejam de curta duração (facilitando ajustá-los à rotina da OM). Como regra fundamental, todo pessoal recém-embarcado deverá receber um adestramento básico de SIC antes de iniciar o desempenho de qualquer atividade.

9.9.2 - Engenharia social

A Engenharia Social corresponde ao conjunto de técnicas para se obter ou comprometer informações sobre uma organização ou seus sistemas computacionais, utilizando-se como ferramenta de ataque a interação humana ou as habilidades e fragilidades sociais do ser humano.

A Engenharia Social deve ser tratada por todos da OM como uma ameaça à SIC, onde toda informação sobre as características da OM e de sua rede local é considerada sigilosa, exigindo o tratamento adequado de segurança.

Para minimizar a probabilidade de estranhos à OM obterem sucesso na aplicação de tais técnicas pelos meios de comunicação disponíveis, devem ser seguidas, no mínimo, as seguintes orientações:

- a) não passar informações de nomes, telefones e outras informações pessoais de qualquer servidor civil ou militar da OM;
- b) não confirmar a estranhos a existência de determinada pessoa na OM;
- c) não atender uma chamada telefônica, não se identificar sem que antes o interlocutor, que efetuou a ligação, tenha se identificado;

- d) não passar a estranhos nenhuma informação sobre os sistemas utilizados na rede local, tais como: sistemas operacionais, aplicativos, serviços disponibilizados, endereços de rede, computadores, roteadores, servidores, localizações físicas, topologia da rede, sistemas de segurança, entre outros; e
- e) não passar a estranhos informações a respeito da rotina e dos procedimentos internos da OM.

9.10 - FORENSE COMPUTACIONAL E REGISTROS DE ACESSO

A contínua evolução tecnológica dos sistemas de informação, redes de computadores e plataformas computacionais como os dispositivos móveis inteligentes e celulares vêm transformando rapidamente o modo de se comunicar e de execução das tarefas cotidianas. No entanto, também é crescente as possibilidades de falhas de segurança nas novas tecnologias, procedimentos e pessoas. Portanto, juntamente com essas facilidades, surgem ambientes propícios para ocorrência de incidentes que envolvam as informações armazenadas ou processadas em dispositivos computacionais e aquelas em trâmite nas suas redes de interligação. Outro aspecto relevante está associado ao comportamento humano diante da tecnologia.

Observa-se a tendência a uma “falsa sensação de segurança” ou de “privacidade” no uso de dispositivos computacionais, especialmente os conectados em rede. Por conta desse comportamento, recursos computacionais são, muitas vezes, utilizados na prática de crimes, contravenções disciplinares e em outras atividades destoantes do interesse do serviço.

Ressalta-se que toda atividade computacional deixa registros de acesso (logs) nos dispositivos e nas redes em que trafegam.

Os dispositivos computacionais de propriedade da MB e a RECIM não são exceções a essa regra. Todo incidente em suas estações, equipamentos servidores, dispositivos periféricos de armazenamento, dispositivos móveis inteligentes e celulares deve ser avaliado pelo CTIM, possibilitando o atingimento dos requisitos básicos de segurança da informação e de operação da rede. Paralelamente, no mesmo contexto evolutivo, técnicas e equipamentos vêm sendo desenvolvidos e aplicados com sucesso na detecção e análise de vestígios decorrentes dos mencionados incidentes.

A DCTIM é responsável por normatizar os processos de Forense Computacional, a serem executados pelo CTIM, visando a contribuir para a produção de provas digitais, juridicamente válidas, em sindicâncias, IPM e processos judiciais.

Além disso, estes processos auxiliam na descoberta de vulnerabilidades e na mitigação do risco de comprometimento da informação digital de propriedade da MB.

9.11 - GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

A Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC) é uma abordagem sistemática para apoio à decisão que visa priorizar as medidas que contribuem para aumentar a eficiência da Segurança da Informação Digital e das Comunicações Navais (CN), as quais agruparemos sob o significado de Segurança da Informação e Comunicações (SIC). Faz-se necessário que as ações de SIC lidem com os riscos de maneira efetiva e no tempo apropriado, onde e quando forem necessários e que a GRSIC seja parte integrante das atividades inerentes à SIC e às CN.

A GRSIC é um processo contínuo e deve possuir contextos definidos, avaliar os riscos e tratá-los por meio de um plano de tratamento, a fim de implementar as recomendações e decisões em ordem de prioridade. Neste processo, é necessário que a gestão de riscos analise os possíveis acontecimentos e suas consequências (impacto), antes do processo de decisão, a fim de reduzir os riscos a níveis aceitáveis. Ou seja, o processo de GRSIC deve ser aplicado com metodologia própria, sendo essencial na identificação das necessidades da MB nessas áreas. Portanto, a GRSIC deve contribuir para a(o)

- a) Identificação de riscos;
- b) Análise e avaliação dos riscos em função do impacto e da probabilidade de sua ocorrência;
- c) Compreensão dos significados das probabilidades e das consequências dos riscos;
- d) Estabelecimento da ordem prioritária das ações para tratamento do risco;
- e) Envolvimento das diversas áreas partícipes do processo de gestão do risco; e
- f) Eficácia do monitoramento do tratamento do risco.

9.12 - DISPOSITIVOS PERIFÉRICOS DE ARMAZENAMENTO

As vulnerabilidades e ameaças ocasionadas pelo uso de dispositivos periféricos de armazenamento como, por exemplo, pendrives, discos externos, drives de CD e DVD, caracterizam-se pela execução de códigos maliciosos executados à partir destes dispositivos ou pelo vazamento de informações sigilosas neles gravadas.

Desta forma, recomenda-se bloquear a utilização das interfaces e portas que permitem a comunicação com estes dispositivos periféricos de armazenamento em todas as Estações de Trabalho da OM.

Caso seja necessário inserir informações contidas nestes dispositivos na rede local, os mesmos deverão ser verificados em uma estação de trabalho do Serviço de Tecnologia da Informação (STI) ou do CLTI apoiador da OM, a ser chamada de “Estação de Descontaminação”, pelo ADMIN. Deve-se certificar que esta estação esteja com Sistema Operacional e antivírus homologados e atualizados em suas últimas versões. Somente após esta verificação as informações poderão ser inseridas na rede da OM.

Em face da necessidade de prover uma maior flexibilidade na troca de informações dentro das OM (Intranet) e fora das OM (Internet), sem a utilização destes dispositivos, otimizando as tarefas diárias e reduzindo o risco de vazamento de informações sigilosas, recomenda-se:

- a) Utilizar servidor de arquivos homologado pela DCTIM em suas redes locais para o compartilhamento de arquivos no ambiente interno.
- b) Utilizar serviço de “Compartilhamento de Arquivos”, disponibilizado pela DCTIM para transmissão de arquivos no ambiente externo à OM, lembrando que NÃO é permitido compartilhar:
 - 1- Arquivos sigilosos sem estarem devidamente criptografados por recurso criptológico da MB;
 - 2 - Cópias não autorizadas de programas (pirataria); e
 - 3 - Arquivos não relacionados com o serviço da MB.

CAPÍTULO 10

DOCUMENTOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

10.1 - AÇÕES DE SEGURANÇA

Todas as ações de SIC devem estar plenamente documentadas, pois seus registros e análises possibilitarão seu contínuo aperfeiçoamento, objetivando a manutenção dos requisitos básicos de SIC. Para tanto, faz-se mister elaborar em cada OM um conjunto de documentos, voltados para as seguintes ações:

- a) planejamento: ações que visam a preparação do ambiente da rede local para prevenção de possíveis ameaças ou riscos às informações digitais;
- b) histórico: ações para descrição da estrutura da rede local e registro de ocorrências do ambiente computacional da OM;
- c) análise: ações para avaliação de vulnerabilidades, riscos ou incidentes que possam ocorrer no ambiente da rede local, auxiliando ações preventivas, corretivas e de planejamento;
- d) auditoria: ações para verificação e avaliação das condições de segurança do ambiente computacional da OM e das respectivas informações digitais que trafegam e são processadas ou armazenadas nesse ambiente;
- e) manutenção: ações preventivas ou corretivas no ambiente da rede local para proteção ou pronto restabelecimento das suas condições operacionais e dos requisitos básicos de SICRL;
- e
- f) adestramento: ações que visam adestrar o pessoal quanto aos documentos, aos procedimentos e às demais ações de SIC.

O Anexo A relaciona os documentos de SIC em vigor na MB.

10.2 - GRAU DE SIGILO DOS DOCUMENTOS DE SIC

Os documentos de SIC que contenham informações sensíveis a respeito da OM devem ser classificados como sigilosos. Neste caso, eles deverão ser corretamente marcados quanto ao seu Grau de Sigilo e deverão ser observados os procedimentos de salvaguarda cabíveis, estabelecidos nas normas e legislação em vigor.

10.3 - INSTRUÇÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (ISIC)

A ISIC de uma OM constitui um documento para gerenciamento de segurança da informação

e comunicações e é voltada às ações de planejamento. Seu objetivo é definir procedimentos que garantam os requisitos básicos de SICRL. A ISIC deve ser simples, objetiva, de fácil compreensão e aplicação e deve possuir grau de sigilo ostensivo, para que todos os usuários da rede local tenham acesso e pleno conhecimento das ações de planejamento e procedimentos nela contidos.

Para sua elaboração, as seguintes regras básicas devem ser seguidas:

- a ISIC deve ser formalizada internamente por cada OM em uma Ordem Interna;
- todo o pessoal da OM, usuários ou não de recursos ou serviços disponibilizados pela rede local, devem conhecer a ISIC; e
- as regras estabelecidas na ISIC aplicam-se, indistintamente, a todo o pessoal na OM.

A elaboração e a revisão periódica da ISIC são responsabilidades do OSIC da OM. O intervalo entre revisões da ISIC deverá estar formalizado no seu próprio corpo, não devendo ser superior a 2 (dois) anos. A ISIC deverá ser voltada ao pleno gerenciamento da SIC e considerar a operação segura da rede local como um fator crítico ao pleno funcionamento da OM. Para o detalhamento da elaboração deste documento, deve ser observada a Instrução disponibilizada pela DCTIM.

10.4 - PLANOS DE CONTINGÊNCIA (PLCONT)

Estes planos, formalizados em um documento com grau de sigilo no mínimo RESERVADO, separado da ISIC, têm por objetivo salvaguardar a continuidade operacional da rede local da OM e a plena recuperação das informações digitais em caso de qualquer interferência (causada por acidente, desastre ou ataque), garantindo, assim, os requisitos básicos de SIC. O restabelecimento operacional da rede local deve ser obtido em um tempo compatível com a missão da OM. Os PLCONT devem:

- a) ser elaborados e revistos pelo ADMIN;
- b) ser organizados de forma objetiva, possibilitando que todos os usuários credenciados tenham pleno conhecimento das ações e dos procedimentos nele contidos;
- c) ter periodicidade de revisão estabelecida pelo OSIC e formalizada na ISIC, não podendo ser superior a 1 (um) ano;
- d) ser ativados pelo ADMIN sempre que algum fato anormal impeça ou impacte a atividade de algum RCC ou uma sucessão de eventos coloque em risco processos ou informações

digitais integradas pela rede local da OM; e

- e) ser ativados periodicamente pelo ADMIN, a título de adestramento, em intervalos não superiores a 1 (um) ano.

A meta final das ações contidas nos PLCONT será sempre o restabelecimento dos RCC e das informações digitais, possibilitando a continuidade operacional da rede local da OM e garantindo os requisitos básicos de SIC. Para o detalhamento da elaboração deste documento, deve ser observada a Instrução disponibilizada pela DCTIM.

10.5 - HISTÓRICO DA REDE LOCAL (HRL)

O HRL tem por objetivo manter um memorial descritivo e o registro de todas as atividades e transações normais e de rotina que podem afetar de alguma forma a SIC. O HRL está voltado às ações de histórico, análise de incidentes, prevenção e correção. A elaboração, o controle e a manutenção do HRL são de responsabilidade do ADMIN, sob supervisão do OSIC. O HRL deve possuir grau de sigilo, no mínimo, RESERVADO e ser composto de 3 (três) partes:

- a) PARTE I : Descrição da Rede;
- b) PARTE II : Atividades de Rotina; e
- c) PARTE III : Incidentes.

10.5.1 - PARTE I: Descrição da Rede

Esta parte deve apresentar o estado atualizado da rede local e seu respectivo ambiente.

10.5.2 - PARTE II: Atividades de Rotina

Estas atividades correspondem aos eventos rotineiros de segurança da rede, explícitos e declarados na ISIC.

10.5.3 - PARTE III: Incidentes

Esta parte tem como objetivo registrar qualquer incidente que afete a SIC. Após analisar uma ocorrência e verificar que se trata de um incidente que afete RCC Nível 1, o OSIC deve participar o fato ao Titular da OM, o qual deverá enviar mensagem preferencial/reservada à DCTIM, com informação ao COMIMSUP, indicando se algum procedimento do PLCONT foi acionado e seu respectivo resultado. O relato imediato de qualquer incidente é de responsabilidade de todos os usuários da rede local. A omissão de relato, pelo usuário, de um incidente que possa afetar a SIC está sujeita a responsabilização, pois contraria a presente Norma e o previsto no Termo de

Responsabilidade Individual. O registro do incidente deve ser feito, de forma clara e objetiva e a análise do ocorrido deverá ser feita pelo OSIC.

Para o detalhamento da elaboração do HRL, deve ser observada a Instrução disponibilizada pela DCTIM.

10.6 - RELATÓRIO DE AUDITORIA (RAD) DE SIC

O RAD é um documento RESERVADO que tem por objetivo formalizar os resultados apurados por alguma auditoria de segurança e indicar possíveis soluções aos problemas levantados na rede local em relação aos aspectos de SIC. Este documento está voltado às ações de auditoria, e maiores detalhes são apresentados no Capítulo 11 desta Norma.

10.7 - RELATÓRIO DE ANÁLISE DE VULNERABILIDADES (RAV)

O Relatório de Análise de Vulnerabilidades (RAV) tem como objetivo identificar vulnerabilidades nos ativos das OM e consequentemente sugerir ações para repará-las, antes que estas sejam exploradas por atacantes. A partir desta análise, os riscos em relação aos incidentes de segurança serão reduzidos, permitindo que a RECIM esteja em um nível de segurança adequado.

10.8 - REGISTRO DE ACESSO

Os acessos e as falhas de acesso aos dispositivos, serviços e sistemas de TI poderão ser registrados em arquivos de transações (logs).

10.8.1 - REGISTROS DE ACESSO À INTERNET (RAI)

O RAI contém um conjunto de informações armazenadas do canal de comunicação entre a RECIM e a Internet, registrando origem e destino do acesso, juntamente com data-hora e período de conexão.

10.8.2 - REGISTROS DE ENVIO/RECEBIMENTO DE E-MAIL PARA INTERNET/INTRANET (REI)

O REI contém um conjunto de informações armazenadas do canal de comunicação entre a RECIM e a Internet, registrando o endereço do remetente e endereço do destinatário de mensagens de correio eletrônico, juntamente com assunto e data-hora da mensagem.

10.8.3 - REGISTROS DE ENVIO/RECEBIMENTO DE MENSAGENS INSTANTÂNEAS (RMI)

O RMI contém um conjunto de informações armazenadas do canal de comunicação do

CHAT homologado pela MB, registrando origem e destino da comunicação, juntamente com data-hora e período de comunicação.

10.9 - TERMO DE APREENSÃO

Documento que formaliza a apreensão do recurso computacional para uma perícia eficaz, preservando as evidências, evitando a adulteração ou eliminação de indícios relevantes à elucidação dos fatos.

10.10 - CADEIA DE CUSTÓDIA

Documento que mantém as atividades de coleta, armazenamento, controle, transferência e disposição física das evidências eletrônicas, registradas de maneira cronológica. O propósito da cadeia de custódia é tornar possível o rastreamento completo das atividades realizadas com as evidências desde sua coleta ou apreensão até a devolução ao encarregado da sindicância ou IPM, a fim de garantir que o laudo seja uma análise imparcial do objeto a ser estudado.

Os documentos referentes aos itens 10.7, 10.8, 10.9 e 10.10 possuem grau de sigilo, no mínimo, RESERVADO e estão voltados às ações de Forense Computacional.

10.11 - PLANOS DE ADESTRAMENTO DE SIC

Documentos ostensivos que visam às ações de adestramento de um determinado tema de SIC para todos da OM (sejam militares, funcionários civis ou prestadores de serviço), de modo que o somatório dos temas englobe todos os aspectos de SIC. Exemplos de temas que podem ter um Plano de Adestramento de SIC específico:

- a) Adestramento básico de SIC (para o pessoal que tenha recém chegado à OM);
- b) Conceitos Gerais de SIC;
- c) ISIC da OM;
- d) Recursos de SIC;
- e) Legislação, Normas e Documentos de SIC;
- f) Ativação dos Planos de Contingência da OM (teoria e prática);
- g) Segurança Orgânica, no que se refere à SIC;
- h) Normas para a salvaguarda de materiais controlados, dados, informações, documentos e materiais sigilosos;

- i) Recursos Criptológicos;
- j) Engenharia Social; e
- k) Crimes de Informática.

Os exemplos acima formam um conjunto mínimo de temas a serem abordados, podendo as OM acrescentar outros, de acordo com suas características e necessidades.

10.11.1 - Controle dos Adestramentos de SIC

Os Planos de Adestramento de SIC, parte integrante do Programa de Adestramento (PAD) da OM, devem conter seus respectivos controles de aplicação, indicando qual o pessoal adestrado e qual o tipo de adestramento fornecido a cada um, de modo a possibilitar o planejamento e a manutenção dos níveis mínimos de adestramento de SIC da OM. Ressalta-se que todo pessoal recém-embarcado deverá receber um adestramento básico de SIC antes de iniciar o desempenho de qualquer atividade

10.12 - CONTROLE DE ENTRADA NA OM DE DISPOSITIVOS ARMAZENADORES DE INFORMAÇÕES DIGITAIS

Registrar em documento próprio, ostensivo, a entrada na OM de qualquer dispositivo que possa armazenar informações digitais, tais como: microcomputadores (de mesa ou portáteis), discos rígidos, pendrives, celulares, disquetes, CD-ROM, DVD ou qualquer outro dispositivo que possa armazenar informações digitais. Para cada ocorrência de entrada de visitantes na OM, devem ser registrados: identificação do visitante, data, hora, destino, identificação do acompanhante, tipo de dispositivo e autorização. Caso não seja autorizada a entrada do dispositivo na OM, o mesmo deve ser recolhido e guardado em local indicado na OM, para posteriormente, ser devolvido ao visitante. As normas e os procedimentos para este controle deverão estar regulados na ISIC de cada OM.

CAPÍTULO 11

AUDITORIAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

11.1 - FINALIDADE DAS AUDITORIAS DE SIC

A auditoria de SIC é composta por uma Equipe de Auditoria (EA) designada previamente, cujo objetivo é verificar o fiel cumprimento das normas de SIC, bem como estabelecer possíveis ações de correção e divulgação da mentalidade de SIC.

11.2 - TIPOS DE AUDITORIAS DE SIC

Os aspectos de SIC podem ser verificados pelos seguintes tipos de auditoria:

- a) Auditoria Programada: requerida pela DCTIM, realizada por EA designada pela DCTIM em uma data previamente determinada, conforme planejamento anual, a ser divulgado pela DCTIM antecipadamente às OM a serem auditadas;
- b) Auditoria Inopinada: requerida pela DCTIM, realizada por EA designada pela DCTIM em data flexível, a ser definida conjuntamente com a OM auditada;
- d) Auditoria Solicitada: requerida formalmente pela OM ou seu COMINSUP à DCTIM, realizada por EA designada pela DCTIM. A partir da análise da solicitação, a DCTIM agendará a data e designará a EA.
- c) Auditoria Interna: realizada por pessoal interno à OM, por EA designada pelo Titular da OM, cujas regras, procedimentos e periodicidade deverão ser estabelecidos na ISIC da OM. Caso a OM não possua militares capacitados tecnicamente para efetuar a auditoria, poderá solicitar apoio ao CLTI da sua área de jurisdição.

Para quaisquer tipos de auditoria de SIC, não é autorizada a participação de EA com pessoal externo à MB.

11.3 - PLANEJAMENTO DAS AUDITORIAS DE SIC

O planejamento e o controle das auditorias de SIC, exceto as auditorias internas, são de responsabilidade da DCTIM.

a) Auditoria Programada

O planejamento das auditorias de SIC programada, para o ano N + 2, deve ser elaborado e divulgado, por aquela Diretoria, no ano N.

Para cada uma das auditorias de SIC programada, as atividades apresentadas na Tabela

11.1 deverão ser seguidas pelos respectivos responsáveis. O documento de designação da EA deverá apresentar, além da relação nominal dos componentes, as datas-limite para os eventos apresentados nessa Tabela e o grau de sigilo reservado. O planejamento das auditorias de SIC será elaborado pela DCTIM de modo a que as OM sejam submetidas pelo menos a uma delas, quer seja programada, inopinada ou solicitada, a cada dois anos.

Tabela 11.1 - Planejamento de atividades para a auditoria de SICRL programada

DATA	EVENTO	RESPONSÁVEL
(D-25)	Designação da EA	DCTIM
(D-25) A (D-10)	Elaboração do planejamento da auditoria	EA
(D-10) a (D-5)	Aprovação do planejamento e respectiva divulgação para a OM a ser auditada	DCTIM
D	Início da auditoria programada nas instalações físicas da rede local da OM	EA
(D+5)	Conclusão da auditoria na OM	EA
(D+60)	Elaboração do RAD + Aprovação do RAD	EA/DCTIM

b) Auditorias Inopinadas e Solicitadas

Realizadas a partir de um planejamento prévio conjunto entre a DCTIM e a OM a ser auditada.

c) Auditoria Interna

O planejamento e o controle das auditorias de SIC internas serão realizados pelo OSIC e formalizados na ISIC da OM.

11.4 - PROCEDIMENTOS PARA AUDITORIAS DE SIC

11.4.1 - Auditorias de SIC programadas

A auditoria de SIC programada será executada pela EA formalmente designada pela DCTIM. Sua composição e as responsabilidades da EA estão apresentadas no Capítulo 8. A EA executará a auditoria de SIC no local das instalações físicas da rede local em um período máximo de 05 (cinco) dias úteis. Para otimizar o tempo de execução dessa auditoria nas instalações físicas da rede local da OM, a EA deverá planejar e testar com a devida antecedência todo o material necessário para a sua realização. No caso de auditoria de SIC programada, estas ações de planejamento deverão ser devidamente

documentadas e efetuadas sob coordenação do Chefe da Equipe de Auditoria. A documentação do planejamento deve receber grau de sigilo, no mínimo, reservado e ser submetida à aprovação da DCTIM. A auditoria de SIC será composta por duas fases: remota e local.

Na fase remota de auditoria de SIC busca-se reduzir o tempo de execução da auditoria de SIC na OM, através atividades que possam ser efetuadas prévia e remotamente, por programas específicos. Estas atividades remotas deverão ser definidas na fase de planejamento e serão realizadas em laboratório específico nas instalações do CTIM ou em outro lugar apropriado, devidamente autorizado pela DCTIM. A fase local da auditoria de SIC é realizada nas instalações físicas da rede local da OM a partir de uma reunião de abertura entre a EA, o representante da OM auditada e o respectivo pessoal envolvido. Nesta reunião, o Chefe da EA deve apresentar os auditores, a programação e o escopo das atividades de auditoria, e o representante da OM deve apresentar o seu pessoal diretamente envolvido. O modelo de documento de programação está apresentado no Apêndice IV do Anexo A. A fase local deve se restringir à avaliação das conformidades das Listas de Verificação disponibilizadas na página da DCTIM na Intranet e ao levantamento de outras informações, por meio de programas específicos para esse tipo de auditoria, utilizados pela DCTIM e CTIM. Ao término desta fase é realizada uma reunião de encerramento, na qual a EA apresenta as principais constatações e colhe sugestões para o aprimoramento das atividades de auditoria. A DCTIM poderá autorizar, em caráter excepcional, que a Auditoria de SIC programada seja realizada por EA do CLTI de jurisdição da OM auditada. Os procedimentos para uma auditoria de SIC programada estão ilustrados no fluxograma da Figura 11.1, onde as atividades da EA se encerrarão na aprovação do RAD pela DCTIM, a ser encaminhado para a OM auditada, com cópia ao respectivo COMIMSUP.

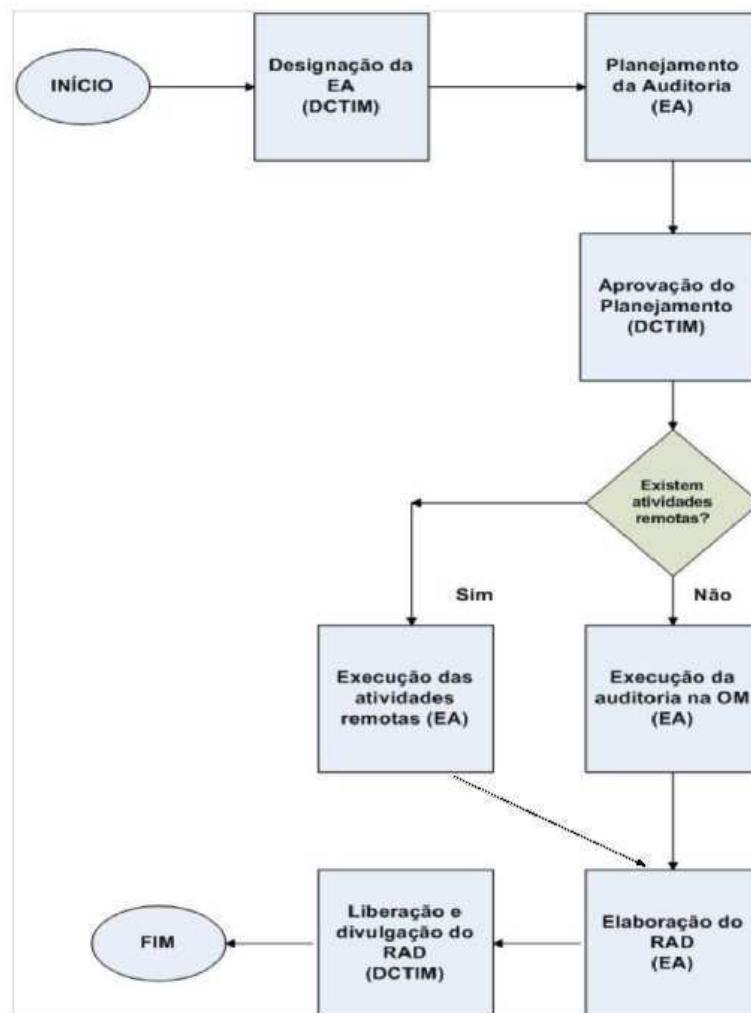


Figura 11.1 - Fluxograma dos procedimentos para uma auditoria de SIC programada

11.4.2 - Auditorias de SIC inopinadas

As auditorias de SIC inopinadas serão realizadas nas OM, em data aleatória, sem o conhecimento da OM, quando identificado um problema que possa causar alguma vulnerabilidade grave ou represente uma ameaça à RECIM. Por se tratar de uma auditoria de SIC com finalidade específica, a EA para este tipo de auditoria será designada pela DCTIM com grau de sigilo, no mínimo, reservado e cumprirá orientações específicas para sua execução. Mesmo sendo de caráter inopinado, a DCTIM deverá informar formalmente ao COMIMSUP sobre a realização da auditoria na OM. O RAD deverá ser elaborado segundo as orientações da DCTIM e conterá o ato administrativo de designação da EA. Assim como em uma auditoria de SIC programada, os trabalhos da EA da auditoria de SIC inopinada encerram-se na aprovação do respectivo RAD pela DCTIM. Após sua aprovação, o RAD será encaminhado para a OM, com cópia ao seu respectivo COMIMSUP.

11.4.3 - Auditorias de SIC solicitadas

Este tipo de auditoria será feito a partir de uma solicitação formal de uma OM ou seu COMIMSUP à DCTIM. A necessidade geradora de uma auditoria de SIC solicitada deve ser avaliada pelo Titular da OM (assessorado pelo OSIC), exceto quando oriunda do COMIMSUP.

Após receber a solicitação, a DCTIM procederá a uma análise de disponibilidade de recursos humanos e financeiros sobre a possibilidade de seu atendimento com a maior brevidade possível. Após a análise, a DCTIM programará uma data adequada e formalizará a designação da EA referente à auditoria. O documento para designação da EA deve incluir o escopo da auditoria, seu sigilo e os devidos prazos, devendo seguir os procedimentos de uma auditoria programada, conforme o fluxograma estabelecido pela Figura 11.1.

11.4.4 – Auditorias de SIC internas

Por constituir uma inspeção realizada por pessoal interno à OM, os procedimentos para realização de auditorias de SIC internas devem ser formalizados na ISIC da OM. As auditorias internas para verificação das condições de SIC da OM devem ser realizadas com autorização formal do Titular da OM e sob o controle do OSIC e possuir grau de sigilo, no mínimo, reservado. Os procedimentos para auditorias de SIC internas devem ser elaborados para que seja possível verificar se as soluções de SIC adotadas para atender as particularidades da rede local da OM são satisfatórias, como também para um contínuo aperfeiçoamento das ações e medidas de SIC por todos os usuários dos serviços prestados pela rede. A execução de uma auditoria interna de SIC deve ser feita por pessoal da OM que possua o credenciamento adequado ao grau de sigilo estabelecido para ela. Na impossibilidade de realizar auditorias internas de SIC exclusivamente com seu pessoal, a OM poderá solicitar apoio ao CLTI de sua área de jurisdição. Caso necessário, o CLTI poderá utilizar os programas específicos autorizados pela DCTIM. É vedada a realização de auditorias internas de SIC por empresas contratadas, por pessoal externo à MB ou por funcionários da OM contratados em caráter temporário. Os prazos a serem seguidos deverão ser os mesmos da Auditoria Programada.

11.5 - RELATÓRIO DE AUDITORIA (RAD) DE SIC

11.5.1 - Composição do RAD

O RAD elaborado pela EA é composto das seguintes partes:

a) Capa: Esta parte tem por finalidade apresentar os dados iniciais da auditoria de SIC realizada e de seus executores (integrantes da EA), juntamente com as assinaturas de aprovação pela DCTIM e a data de encaminhamento à OM e ao seu respectivo COMIMSUP. O modelo de “Capa” para o RAD encontra-se no Apêndice V do Anexo A.

b) Introdução: Esta parte tem por finalidade apresentar os documentos de designação da EA, as referências, os prazos envolvidos, seu tipo, sigilo e escopo, bem como o nome da OM onde foi realizada a auditoria de SIC. O modelo da parte de “Introdução” do RAD encontra-se no Apêndice VI do Anexo A. Pelo seu caráter mais específico, as auditorias inopinadas e solicitadas devem ter os aspectos a serem constatados claramente definidos na Introdução do RAD.

c) Constatações da Auditoria de SIC: Esta parte tem por finalidade apresentar as constatações da auditoria, podendo ser agrupadas sob os seguintes aspectos:

- quanto ao adestramento;
- quanto à administração da rede local;
- quanto à documentação;
- quanto às Estações de Trabalho;
- quanto aos incidentes; e
- quanto à segurança física.

Pelo seu caráter mais específico, as auditorias inopinadas e solicitadas não precisam observar todos esses seis aspectos acima. Cada item listado nesta parte do RAD deve conter os seguintes campos:

1. Constatação: este campo deve apresentar a ocorrência, a vulnerabilidade ou o fato constatado;

2. Comentário: este campo deve apresentar as possíveis consequências ou prejuízos à SIC decorrentes da constatação efetuada; e

3. Ação a empreender: este campo deve recomendar soluções para a constatação efetuada e listar os documentos, normas, publicações e outras referências nos quais as recomendações apresentadas estão fundamentadas. O modelo da parte de “Constatações da Auditoria de SIC” do RAD encontra-se no Apêndice VII do Anexo A.

d) Considerações Finais da Equipe de Auditoria de SIC: Esta parte tem por finalidade apresentar as considerações finais da Equipe de Auditoria de SIC. O modelo da parte de “Considerações Finais da Equipe de Auditoria de SIC” do RAD encontra-se no Apêndice VIII do Anexo A.

e) Assinaturas: Esta parte tem por finalidade apresentar as assinaturas dos componentes da Equipe de Auditoria, que elaboraram o RAD. O modelo da parte de “Assinaturas” do RAD também encontra-se no Apêndice VIII do Anexo A.

11.5.2 - Encaminhamento do RAD

O encaminhamento do RAD para a OM, com cópia ao seu respectivo COMIMSUP, é de responsabilidade da DCTIM, após sua devida aprovação. Caso o RAD não seja aprovado pela DCTIM, esta determinará nova auditoria de SIC e fornecerá as instruções pertinentes.

11.5.3 - Implementação das ações recomendadas pelo RAD

A partir do recebimento do RAD, a OM deverá apresentar à DCTIM e ao seu COMIMSUP, em até 45 dias, o planejamento e o cronograma de implementação das ações recomendadas (cuja data de início pode ser anterior a essa apresentação), mantendo-os informados e atualizando o HRL (conforme previsto no Capítulo 10) à medida que forem sendo concluídas as ações previstas.

CAPÍTULO 12

SEGURANÇA APLICADA AOS DISPOSITIVOS MÓVEIS E TELEFONES CELULARES

12.1 – PROPÓSITO

Disciplinar a utilização de dispositivos móveis pessoais e funcionais do tipo dispositivo periférico de armazenamento e dispositivo móvel inteligente (“smartphone”, “tablets”, telefones celulares com recursos de câmera e gravador, e “smartwatch”), bem como as facilidades provenientes de suas plataformas de operação pelos servidores civis e militares da Marinha do Brasil (MB).

12.2 - DISPOSIÇÕES GERAIS

Para auxiliar o entendimento e dirimir possíveis dúvidas, está disponibilizado no Apêndice IX do Anexo A um glossário de termos relacionados a este assunto.

12.2.1 - Introdução

A partir de 2004 foram disponibilizados os primeiros modelos de telefones com capacidades de conexão a redes, processamento e armazenamento. Devido às suas capacidades, tais dispositivos móveis foram denominados de “smartphones” ou telefones inteligentes. Ao longo do tempo, passaram a ser equipados com outras funcionalidades como câmera fotográfica, gravador de som e vídeo, editor de textos, leitor de arquivos e memória de armazenamento. Para potencializar o seu uso, as novas gerações de celulares e “smartphones” desenvolveram a capacidade de processar diversos tipos de programas e compartilhar dados em rede entre dispositivos similares, com outros computadores e em nuvem (“cloud computing”), via Internet.

Atualmente, somam-se a estes “smartphones” os dispositivos móveis do tipo “tablet” que, além das funcionalidades de telefone celular, também processam aplicativos, armazenam maior quantidade de dados e muitas vezes são utilizados como estação de trabalho, e os dispositivos móveis do tipo “smartwatch”, que é o nome dado para um relógio inteligente, ou seja, um aparelho que mistura a aparência de um relógio de pulso tradicional com as funcionalidades de um “smartphone”.

Estes dispositivos móveis podem permitir o uso de um cartão SIM (“Subscriber Identity Module”), que habilita a sua conexão com as operadoras de telefonia. Esse cartão também possui capacidade de armazenamento de pequenos dados, como números de

telefones e mensagens de SMS (“Short Message Service”).

A telefonia móvel também expandiu seu uso típico para rede de dados, passando a utilizar redes EDGE (“Enhanced Date Rates For GSM Evolution”), 3G (Terceira Geração de Telefonia Móvel) e atualmente 4G (Quarta Geração de Telefonia Móvel), além de conexões por rede sem fio (Wi-fi) e “Bluetooth”.

Os sistemas operacionais disponibilizados nestes equipamentos possuem características de modo a:

- a) impedir que o usuário tenha o controle de administração do aparelho, sem que haja a quebra de mecanismo de segurança do sistema operacional (conhecido como “jailbreak” ou “rooting”);
- b) instalar aplicativos por meio de loja proprietária do fabricante do sistema operacional;
- c) permitir a utilização de um espaço de memória na infraestrutura do fabricante do sistema operacional para armazenar cópia de segurança (armazenamento em nuvem);
- d) conectar os dispositivos em rede por meio de tecnologias de redes sem fio;
- e) servir como roteador para acesso à Internet por computadores;
- f) informar localização geográfica;
- g) estabelecer conexão direta a outros dispositivos via tecnologia “Bluetooth”; e
- h) sincronizar dados com estações de trabalho.

Com base em todos estes recursos, torna-se fundamental regular seu uso e aplicabilidade na Marinha pelos servidores civis e militares da MB assim como seus prestadores de serviços.

12.2.2 - Fundamentação Legal

Conforme disposto nas diretrizes e orientações básicas da Norma Complementar nº 12/IN01/DSIC/GSIPR e na conclusão da Nota Técnica nº 10/2014 da DCTIM, entende-se que a utilização de dispositivos móveis deva ser controlada em todas as Organizações Militares (OM) da MB. Este controle visa a garantir a Segurança das Informações e Comunicações (SIC) de todos os ativos de informação da Marinha.

12.2.3 - Tipos de dados nos dispositivos móveis

Os dispositivos móveis permitem processar, armazenar, enviar e receber diversos tipos de dados, tais como: lista de contatos pessoais, mensagens de texto, fotos, vídeos, áudio (gravações), e-mails, documentos, senhas do dispositivo e dos serviços acessados por meio dele, e posicionamento geográfico e trajetos de deslocamentos.

12.3 - AMEAÇAS E VULNERABILIDADES DOS DISPOSITIVOS MÓVEIS

São consideradas ameaças de SIC aquelas ações que possam comprometer a disponibilidade, integridade, confidencialidade e a autenticidade de dados e serviços utilizados pelos usuários da MB, por meio da exploração de alguma vulnerabilidade. Estas vulnerabilidades podem surgir, de forma intencional ou não, desde a concepção do hardware ou dos softwares embarcados, até a falta de conhecimento ou de mentalidade de SIC dos usuários e na ausência de procedimentos que expressem as boas práticas de segurança.

Os tipos de ameaças e vulnerabilidades observados no uso de dispositivos móveis podem ocorrer devido às seguintes causas:

- a) operação inadequada;
- b) perda, roubo ou furto;
- c) interceptação de voz e dados; ou
- d) execução de códigos maliciosos.

Tais ameaças e vulnerabilidades podem ocasionar o vazamento de informações sigilosas, pois, uma vez que a informação seja compartilhada na Internet, ou acessada por terceiros, não haverá mais o controle sobre suas cópias, divulgação e conteúdo.

Ressalte-se que a presença de tais dispositivos em reuniões ou em conversas interpessoais implicam no risco de gravações de áudio e vídeo sem autorização, além da captura de imagens. Outrossim, com a contínua expansão da área de cobertura e serviços de conexões de dados oferecidos pelas operadoras de telecomunicações, tais arquivos podem ser enviados imediatamente para outros locais, como as redes sociais, por meio de aplicativos instalados nestes dispositivos.

12.3.1 - Operação inadequada do dispositivo

A principal causa da operação inadequada destes dispositivos está relacionada com a

falta de conhecimento por parte do usuário das melhores configurações de segurança para os mesmos.

Normalmente, estes dispositivos são disponibilizados pelos fabricantes com diversas funcionalidades habilitadas por padrão de configuração. Tais configurações de fábrica podem habilitar o compartilhamento de documentos em nuvem, conexões “bluetooth” e coleta de informações relativas ao perfil de utilização do usuário e de seu posicionamento geográfico.

A partir da análise computacional dessas incontáveis pequenas informações sobre o usuário (metadados), é possível inferir o perfil de deslocamento, hábitos, a rede de relacionamentos interpessoais e profissionais por sistemas de monitoramento de inteligência extra MB.

Assim sendo, configurar os dispositivos móveis de acordo com as recomendações técnicas preconizadas e mantê-los desligados quando a situação exigir, minimizam os riscos de SIC e contribuem para a constrainteligência. Nesse sentido, também não devem ser armazenadas no aparelho informações sigilosas em claro.

12.3.2 - Perda, roubo ou furto do dispositivo

Na ocorrência desses eventos com dispositivos funcionais, o usuário deverá comunicar tempestivamente à sua OM para a tomada de ações de mitigação de danos, como por exemplo o bloqueio do cartão SIM, apagamento remoto do dispositivo e/ou localização do mesmo por softwares de geolocalização.

12.3.3 - Interceptação de voz e dados

Este risco é inerente ao ambiente de transmissão, considerado inseguro, que trafega por diversas infraestruturas e localidades fora do controle da MB. Para reduzir tal risco, faz-se necessário que sejam evitados o tráfego (voz e dados) de assuntos sigilosos por este canal.

12.3.4 - Execução de códigos maliciosos

Os principais sistemas operacionais para dispositivos móveis possuem suas próprias lojas de aplicativos (exemplos: Apple Store e Google Play). Por meio dessas lojas, os softwares homologados pelos fabricantes são disponibilizados para instalação. Buscar aplicativos fora desses ambientes representa um risco de inserção de códigos maliciosos

nos dispositivos móveis. Consequentemente, ações não autorizadas podem ser executadas, tais como a simulação de desligamento, realização de gravações e roubo de dados.

Manter os aplicativos e sistema operacional atualizados é indispensável, pois as vulnerabilidades descobertas podem ser corrigidas nas atualizações. Especial atenção deve ser dada no envio de equipamentos para assistência técnica especializada. Nessas ocasiões, informações armazenadas em claro podem ser acessadas e códigos maliciosos inseridos.

12.4 - POLÍTICAS DE USO DE DISPOSITIVOS MÓVEIS NA OM

O uso de dispositivos móveis no dia a dia das OM vem se tornando cada vez mais frequente, sendo considerado, atualmente, um dos principais problemas de SIC enfrentado pelas organizações em todo o mundo: BYOD (“Bring Your Own Device”). Variações de políticas de uso são comuns, dependendo do tipo de instituição e da sensibilidade de alguns setores dentro das organizações.

Apesar de tais dispositivos possibilitarem uma maior flexibilidade e mobilidade, otimizando as tarefas diárias, os riscos relacionados às ameaças e vulnerabilidades expostas no item anterior não podem ser desprezados. Portanto, torna-se necessária a criação de procedimentos que visem evitar o vazamento de informações sigilosas e sensíveis aos interesses da MB.

Assim sendo, a utilização de tais dispositivos a bordo das OM da Marinha é proibida, sendo que algumas exceções estão previstas nos itens 12.4.2, 12.4.3 e 12.4.4.

As OM devem controlar rigorosamente a entrada de dispositivos móveis (celulares, tablets, câmeras fotográficas e similares) pessoais e funcionais, que deverão ser acondicionados em locais apropriados e definidos em cada OM.

Quando for autorizado o uso de dispositivos móveis, os seguintes aspectos devem ser observados para a autorização de uso desses dispositivos:

- a) propriedade do dispositivo (Pessoal ou Funcional);
- b) necessidade do emprego;
- c) missão operativa;
- d) OM que lidam com atendimento ao público; e

e) compartimento onde tais dispositivos serão utilizados (Permitido ou Não permitido).

Recomenda-se ainda a utilização de avisos nas portas de acesso aos locais e compartimentos, ressaltando a proibição da entrada e uso desses dispositivos. Além disso, os Planos de Segurança Orgânica (PSO) e os Programas de Adestramento (PAD) devem contemplar medidas preventivas e orientadoras quanto à política de utilização de dispositivos desta natureza.

12.4.1 - Classificação da propriedade dos dispositivos móveis

Os dispositivos móveis podem ser classificados como pessoais, funcionais ou de pessoal extra-MB. Os dispositivos pessoais são aqueles de propriedade de membro da MB. Os dispositivos funcionais são aqueles de propriedade da MB. Os dispositivos de pessoal extra-MB são aqueles de propriedade de pessoas não vinculadas à MB.

Para os dispositivos pessoais e funcionais, independente da propriedade, o usuário deverá ser alertado de que o Termo de Responsabilidade Individual (TRI) assinado por ele engloba não somente as estações de trabalho, microcomputadores, ambientes computacionais e equipamentos listados naquele termo ou outros ativos de informação não mencionados, mas também os dispositivos móveis a que tiver acesso.

12.4.1.1 - Dispositivos móveis pessoais

Os militares e servidores civis das OM devem guardar seus dispositivos móveis pessoais nos locais ou compartimentos definidos pelo Titular da OM por meio de Ordem Interna. Caso se aplique, também deve ser regulado o uso de tais dispositivos pelo pessoal de serviço, considerando as suas peculiaridades e situações especiais.

A regulamentação deve ser fruto de uma análise de risco, realizada pela Titular da OM, envolvendo as ameaças e impactos da utilização dos equipamentos.

Fica proibida a conexão de dispositivos móveis pessoais na RECIM, por meio de conexões sem fio ou cabos USB, inclusive para o carregamento de sua bateria.

12.4.1.2 - Dispositivos móveis funcionais

Todo dispositivo móvel funcional deverá ser cadastrado e controlado pela OM, por meio do Termo de Recebimento de Estação de Trabalho (TRE), garantindo sua

identificação única, bem como os responsáveis pelo seu uso. Para tanto, deverá ser gerado um TRE específico para cada usuário (ou usuários, no caso de dispositivos compartilhados), para cada dispositivo móvel funcional.

Não deverão ser armazenados dados sigilosos nos dispositivos móveis. Após a homologação pela DCTIM, é recomendada a adoção de solução que garanta a proteção e o sigilo dos dados armazenados nos dispositivos para casos de extravio.

Os militares e servidores civis da MB devem ser orientados a respeito dos procedimentos de segurança acerca dos dispositivos que lhes forem disponibilizados, mediante a assinatura de Termo de Responsabilidade Individual (TRI) da OM a que pertencem, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido.

12.4.1.3 - Dispositivos móveis de propriedade de pessoal extra-MB

Para pessoal não vinculado à MB, fica vedado o uso de dispositivos móveis nas dependências das OM, exceto em situações especiais como cerimônias militares, simpósios e eventos similares. Tais procedimentos devem estar previstos em Ordem Interna e em Ordem de Serviço.

Para funcionários terceirizados serão considerados os procedimentos preconizados no item que trata de Dispositivos móveis pessoais.

As OM devem dispor de local para a guarda de tais dispositivos.

12.4.2 – Emprego de dispositivos móveis

A utilização de dispositivos móveis a bordo das OM da Marinha é proibida. Não obstante, cabe ao Titular da OM avaliar qualquer circunstância que fuja a esta regra, levando em consideração o local, período ou situação que justifique sua permissão de uso. Tais exceções devem ser registradas por meio de Ordem Interna ou Ordem de Serviço onde devem constar:

- a) as pessoas autorizadas a utilizar tais dispositivos;
- b) os dispositivos autorizados (número de série);
- c) os locais e compartimentos de utilização dos dispositivos;
- d) a finalidade de uso dos dispositivos; e

e) horário.

As OM devem definir um local para a guarda dos dispositivos (escaninhos, armários já utilizados pela tripulação para a guarda dos seus pertences ou outros). Tais locais deverão ser estabelecidos pelo titular da OM por meio de Ordem Interna.

12.4.3 - Missão Operativa

O uso de dispositivos móveis pessoais ou funcionais durante missão operativa é proibido.

Casos especiais de utilização deverão constar da respectiva Diretiva, ressaltando que o seu uso pode indicar o posicionamento geográfico do meio naval ou o registro de dados não autorizados. Portanto, em regime de viagem, devem permanecer desligados e guardados nos armários.

Recomenda-se o constante adestramento das tripulações sobre tais implicações.

12.4.4 - OM que lidam com atendimento ao público

Nas OM que lidam com atendimento ao público, as restrições ao uso de dispositivos móveis não devem impactar no cumprimento de sua missão. Por isso, nessas OM, o uso destes dispositivos é permitido. Entretanto, caberá ao Titular da OM realizar uma criteriosa análise para identificação das áreas e compartimentos onde seu uso será proibido a fim de evitar o vazamento de informações sigilosas e sensíveis aos interesses da MB. Tais locais deverão receber avisos nas suas portas de acesso que os identifique como áreas de uso proibido. As proibições devem ser registradas por meio de Ordem Interna ou de Ordem de Serviço.

As seguintes OM enquadram-se neste grupo:

- a) hospitais, policlínicas, odontoclínicas e ambulatórios ;
- b) capitarias, delegacias e agências;
- c) Arsenal de Marinha do Rio de Janeiro (AMRJ), Bases Navais e Estações Navais;
- d) Serviço de Seleção do Pessoal da Marinha (SSPM);
- e) Serviço de Identificação da Marinha (SIM);
- f) Serviço de Veteranos e Pensionistas da Marinha (SVPM); e

g) OM do Sistema de Ensino Naval (SEN).

12.5 - RECOMENDAÇÕES DE CONFIGURAÇÃO PARA DISPOSITIVOS MÓVEIS

As seguintes recomendações de segurança devem ser observadas para os dispositivos móveis funcionais e pessoais que utilizem serviço de acesso a sistemas corporativos, tais como correio eletrônico e Portal da MB:

- a) não armazenar dados, agenda, notas e contatos de pessoal da Marinha em nuvem privada (exemplos: iCloud, Dropbox, Google Drive etc.);
- b) desabilitar o serviço de localização para todos os aplicativos;
- c) não instalar qualquer aplicativo que não seja disponibilizado pela loja proprietária do fabricante do sistema operacional;
- d) não realizar o “jailbreak” (ou “rooting”) - procedimento com ferramentas não homologadas que permitem ao usuário ter o controle de administração do aparelho;
- e) desabilitar a possibilidade do dispositivo móvel se conectar a redes sem fio automaticamente;
- f) desabilitar o uso de “bluetooth”;
- g) desabilitar a função de compartilhamento de ponto de acesso a rede;
- h) habilitar a senha de proteção do dispositivo e, sempre que a tecnologia do dispositivo permitir, utilizar senhas mais complexas que 4 dígitos numéricos;
- i) habilitar a proteção de tela;
- j) habilitar o PIN (“Personal Identification Number”) do cartão SIM;
- k) instalar antivírus quando houver disponibilidade para o sistema operacional;
- l) manter o sistema operacional e as aplicações atualizados; e
- m) solicitar o apagamento seguro das informações em caso de perda, roubo ou extravio do dispositivo móvel funcional.

A DCTIM normatizará e homologará soluções de hardware e software que promovam a segurança dos dispositivos móveis na MB.

12.6 - CONSIDERAÇÕES FINAIS

O desafio de se estabelecer normas e procedimentos sobre um tema em constante evolução visa a garantir os requisitos Confiança, Rapidez, Segurança e Flexibilidade das Comunicações Navais, fator de força fundamental no cumprimento das missões.

Os titulares de OM deverão baixar normas complementares atendendo às especificidades da própria OM.

PARTE IV
SISTEMAS DIGITAIS

CAPÍTULO 13 - CATEGORIZAÇÃO, CLASSIFICAÇÃO e OM REGULAMENTADORAS

CAPÍTULO 14 - CICLO DE VIDA DE UM SISTEMA DIGITAL

CAPÍTULO 15 - FASE DE PLANEJAMENTO

CAPÍTULO 16 - FASE DE OBTENÇÃO

CAPÍTULO 17 - FASE DE PRODUÇÃO

CAPÍTULO 18 - FASE DE MANUTENÇÃO

CAPÍTULO 19 - FASE DE DESATIVAÇÃO

CAPÍTULO 20 - ADMINISTRAÇÃO DE DADOS

CAPÍTULO 21 - PROCESSOS DE APOIO

INTRODUÇÃO

1 - APRESENTAÇÃO

Atualmente, os Sistemas Digitais (SD) são amplamente utilizados nos mais diversos setores da MB, envolvendo desde aplicações triviais até sistemas críticos que suportam processos administrativos e operativos.

Esta norma baseia-se nos conceitos, métodos, ferramentas e procedimentos da engenharia de software (ES) essenciais ao pleno desenvolvimento, manutenção (evolutiva, adaptativa e corretiva) e uso dos SD, que compõem seu ciclo de vida.

O controle do ciclo de vida de um SD demanda o cumprimento de ações para promover o alinhamento aos instrumentos estratégicos em vigor na MB, como por exemplo: Plano Diretor de Tecnologia da Informação e Comunicações da MB (PDTIC), Plano Estratégico de TI da MB (PETIM) e demais normas decorrentes.

O conjunto de processos para a aquisição de um SD refere-se ao seu ciclo de vida e contemplam os fundamentos e os requisitos estabelecidos pela Doutrina de TI da Marinha (EMA-416). Os modelos esquemáticos das principais fases do ciclo de vida de um SD encontram-se no Anexo B.

2 - PROPÓSITO

Agregar os conceitos, métodos, ferramentas e procedimentos da Engenharia de Software (ES) na gestão do ciclo de vida dos SD na MB para garantir a produtividade e a qualidade dos sistemas empregados, considerando a constante evolução tecnológica, o tamanho e a complexidade dos diversos projetos.

3 - REFERÊNCIAS

Esta norma baseia-se nas melhores práticas difundidas no segmento de Engenharia de Software (ES) e na literatura e em metodologias utilizadas por órgãos e entidades da Administração Pública Federal.

CAPÍTULO 13

CATEGORIZAÇÃO, CLASSIFICAÇÃO E OM REGULAMENTADORAS

13.1 - PROPÓSITO

A Doutrina de TI da MB (EMA-416) apresenta a definição de SD, classificando-os em duas categorias: Sistemas Digitais Administrativos (SDA) e Sistemas Digitais Operativos (SDO). A partir dessas categorias, o propósito deste capítulo é apresentar as classificações complementares dos SD e OM Regulamentadoras responsáveis pelas atividades apoiadas pelos SD.

13.2 - DEFINIÇÕES

13.2.1 - Sistemas Digitais (SD)

SD são todos os sistemas que, utilizando recursos de TI, efetuam o trâmite, a geração, o desenvolvimento, o processamento ou o arquivamento de informações digitais, constituindo um conjunto de elementos inter-relacionados que executam os processos de informação, a fim de apoiar os processos de tomada de decisão.

13.2.2 - Categorias de SD

13.2.2.1 - SISTEMAS DIGITAIS ADMINISTRATIVOS (SDA)

São sistemas de informação digital projetados para apoio das atividades administrativas da MB.

13.2.2.2 - SISTEMAS DIGITAIS OPERATIVOS (SDO)

São sistemas de informação digital projetados para o emprego em operações navais ou em benefício delas.

13.2.3 - Classificação dos SD

13.2.3.1 - *Software de Prateleira ou COTS (Commercial-off-the-shelf)*

Sistema ou *software* estável com documentação e requisitos bem definidos, julgados úteis pelas OM para a consecução de suas tarefas técnicas. Suas limitações são conhecidas e não há possibilidade de adaptações ou desenvolvimento de novas funcionalidades específicas para a MB.

13.2.3.2 - *Software de Prateleira Modificável ou MOTS (Modified-Off-the-shelf)*

Os sistemas do tipo MOTS, *software* de prateleira modificável, poderão ser alterados segundo os requisitos ou demandas específicas da MB ou da OM solicitante (OM SOL) da Solução que detém o controle relativo da manutenção e das características da parte customizada, porém não possui controle sobre todas as funcionalidades presentes no *software*. Frequentemente, este tipo de solução é mais caro que um *Software* de Prateleira (COTS) e mais barato que um *Software* Desenvolvido por Demanda (FD), a seguir definido.

13.2.3.3 - FD (*Fully Developed Software*) ou Desenvolvido sob Demanda

Sistema ou *software* desenvolvido sob demanda, em atendimento às necessidades e/ou requisitos da MB ou OMSOL. Em geral é desenvolvido e implantando para uma demanda específica e, neste caso, a MB ou OMSOL, possuirá total controle sobre os processos de desenvolvimento e manutenção. Poderão ser sistemas desenvolvidos internamente na MB ou por desenvolvedores externos.

13.3 - CLASSIFICAÇÕES COMPLEMENTARES

Classificação complementar dos Sistemas Digitais na MB:

13.3.1 - Quanto à abrangência

- a) **Local:** Utilizado por usuários de uma única OM, para apoio a atividades realizadas nessa OM, segundo regras definidas por Diretoria Especializada (DE).
- b) **Corporativo:** São sistemas desenvolvidos para atender a gestão das OM da MB, trazendo integração, rapidez e confiabilidade para as informações corporativas, sendo utilizado por toda a MB em função das funcionalidades e regras de negócio. Fazem uso da RECIM e deverão ser hospedados Centro de Dados da MB.

13.4 - ORGANIZAÇÃO MILITAR REGULAMENTADORA (OMREL)

A Organização Militar Regulamentadora (OMREL) é responsável pela área de conhecimento e/ou atividade fim que o SD apoiará. Em virtude dos conhecimentos e competências de seu corpo técnico, a OMREL será responsável por ratificar, por meio de um parecer, a necessidade de desenvolvimento ou manutenção do SD proposto pela OMSOL.

CAPÍTULO 14

CICLO DE VIDA DE UM SISTEMA DIGITAL

14.1 - DEFINIÇÃO

O ciclo de vida de um SD representa o conjunto de processos para a sua implantação, que abrange desde as fases de concepção e especificação, até a sua desativação. Na MB, o ciclo de vida de um SD contempla cinco fases: o planejamento (PLA), a obtenção (OBT), a produção (PRO), a manutenção (MAN) e a desativação (RET).

14.2 - PLANEJAMENTO (PLA)

A Fase de Planejamento do SD compreende a modelagem de processos de negócios da OM e a análise e avaliação do contexto interno e externo em relação aos SD existentes ou disponíveis. Esta fase consistirá em planejar o desenvolvimento do SD em apoio aos processos da OMSOL. As demandas geradas pelos SD deverão estar alinhadas ao Plano Estratégico de TI da Marinha (PETIM) e contempladas no Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC) da OM, permitindo que diretrizes para os investimentos viabilizem a realização de soluções amplas e integradas, de acordo com as disponibilidades de orçamento e estimativas de prazos, além de aspectos relacionados à infraestrutura de TI e de pessoal. A análise quanto ao desenvolvimento ou manutenção de um SD deve ser avaliada sob os pontos de vista gerencial e técnico. A análise gerencial deverá verificar se a demanda está alinhada à governança de TIC da MB e à missão da OMSOL. Também compreenderá o parecer da OMREL para avaliar se a solução é adequada ao atendimento da demanda apresentada. Muitas vezes o problema pode ser resolvido com uma reestruturação de processos internos da OM ou redefinição de responsabilidades. A análise técnica deverá focar no estudo de viabilidade das possíveis soluções e na verificação da compatibilidade das soluções propostas. O propósito da análise técnica realizada pela DCTIM, ainda na fase de planejamento, é identificar:

- a existência de soluções disponíveis que possam atender à demanda apresentada, evitando redundâncias e desperdício de recursos da MB;
- os impactos não planejados na infraestrutura de TI da MB ou riscos de segurança de informação e comunicações gerados nas diversas fases do ciclo de vida do SD;
- o atendimento às normas em vigor na MB que regulam a gestão e o uso da TI; e
- a capacidade de manutenção (produtiva, adaptativa e evolutiva) da solução proposta.

A partir da análise de viabilidade elaborada pela OMREL e do parecer da DCTIM, caso o SD seja avaliado em conformidade, a OMSOL irá executar os procedimentos previstos na Fase de Obtenção.

14.3 - OBTENÇÃO

A Fase de Obtenção de um SD inicia-se com a elaboração das especificações e requisitos de arquitetura e infraestrutura. Nesta fase será definido se a demanda da OMSOL consistirá na atualização de um SD em produção ou na aquisição de um novo SD, de acordo com a classificação prevista no item 13.2.3 desta Norma. Caso a aquisição do SD envolva a contratação de serviços de TI, deverão ser seguidos os procedimentos para seleção dos fornecedores, critérios de avaliação e de aceitação previstos para contratações de TI na Administração Pública Federal, conforme instrumentos normativos vigentes. É importante ressaltar que o processo de conformidade deve estar concluído junto à DCTIM, antes do início da Fase de Obtenção, a fim de evitar investimentos desnecessários ou manutenções futuras.

14.4 - PRODUÇÃO

A fase de produção de um SD inicia-se após a sua homologação pela DCTIM, caracterizando-se pela atividade de implantação e do pleno funcionamento do SD em ambiente de produção, disponibilizando seus recursos para seus usuários.

14.5 - MANUTENÇÃO

A manutenção de um SD poderá ocorrer a qualquer tempo de seu ciclo de vida e até durante a fase de produção, sendo decorrente de um dos seguintes fatores:

- erros de desenvolvimento: manutenção corretiva;
- mudanças no ambiente sem alteração dos requisitos: manutenção adaptativa;
- mudanças nos requisitos: manutenção evolutiva; e
- melhoria da qualidade (programas ou base de dados): manutenção preventiva.

14.6 - DESATIVAÇÃO

A obsolescência de um SD pode ser planejada pelos seguintes motivos:

- a) necessidade de novo SD para atendimento dos requisitos com maior eficiência;
- b) necessidade de utilização de novas tecnologias;
- c) disponibilidade de um novo SD;

- d) não atendimento de novos requisitos; e
- e) relação custo x benefício para a manutenção da atual versão ou evolução do SD.

A desativação de um SD em produção deve avaliar todos os aspectos do processo de transição ou de migração para outro SD para proporcionar a preservação da informação.

CAPÍTULO 15

FASE DE PLANEJAMENTO

15.1 - DEFINIÇÃO

Nesta fase é identificada a necessidade de obtenção de um SD para atender a uma demanda de uma ou mais OM. Tal necessidade deve estar contemplada no PDTIC da OM e ser justificada tecnicamente, em conjunto com os estudos de viabilidade, evidenciando o alinhamento estratégico da proposta, visando sua avaliação pela OMREL e a subsequente verificação de conformidade pela DCTIM.

SD corporativos ou padronizados estarão sujeitos à avaliação posterior pela COTEC-TIC e COTIM, quando aplicável, em função do escopo, criticidade e recursos financeiros envolvidos. O modelo esquemático desta fase do ciclo de vida encontra-se disponível no Anexo B desta publicação. A seguir são detalhadas as atividades previstas.

15.2 - PLA01 - APRESENTAÇÃO DA NECESSIDADE DE SD

Esta atividade marca o início da Fase de Planejamento. O propósito é elaborar o Documento de Visão do Sistema (DVS). Nesse documento, a OM solicitante (OMSOL) deve identificar a necessidade a ser atendida pelo SD proposto e demais requisitos, como por exemplo:

- a) as oportunidades e benefícios que serão obtidos com a implantação do SD proposto;
- b) os processos de negócio e organizacionais que serão apoiados/atendidos e os motivos pelos quais a aquisição de um SD é a solução do problema;
- c) os projetos que eventualmente estejam relacionadas com a necessidade a ser atendida com o SD;
- d) as pessoas/funções envolvidas no ciclo de vida do SD e na utilização de suas funcionalidades;
- e) o impacto de integração do SD com a infraestrutura de TI da MB;
- f) a infraestrutura e recursos de TI necessários à implantação e sustentação do SD;
- g) a necessidade de capacitação e treinamento;
- h) a contratação de soluções de TI para apoiar todo o ciclo de vida do SD;
- i) aspectos relativos à manutenção e sustentação da solução proposta, contemplando o retorno sobre o investimento;

- j) os requisitos de segurança, de proteção e outros requisitos críticos relacionados às atividades do SD; e
- k) as restrições que devem ser consideradas para a obtenção do SD. Essas restrições permitirão avaliar a viabilidade do projeto de diversos pontos de vista: econômico, técnico e legal, diminuindo riscos que possam afetar a obtenção do SD e, consequentemente, o atendimento à necessidade da OMSOL.

Ao término da atividade PLA01, o DVS deverá ser enviado pela OMSOL à OMREL via COMINSUP. O modelo do DVS será disponibilizado em norma própria da DCTIM.

15.3 - PLA02 - AVALIAÇÃO DA NECESSIDADE DO SD PELA OMREL

A OMREL deverá, em caso de parecer favorável, ratificar o DVS, complementando-o, se for o caso, e encaminhá-lo à DCTIM, com informação para OMSOL e COMINSUP. Em caso de parecer desfavorável, restituir à OMSOL, via COMINSUP.

Esta atividade visa obter junto à OMREL a ratificação da necessidade do SD. Com base nas informações do DVS emitido pela OMSOL, a OMREL verificará a pertinência da necessidade do SD, emitindo seu parecer (favorável ou não favorável).

Caso o parecer da OMREL seja contrário (não favorável) à obtenção do SD, o DVS deve ser devolvido à OMSOL, encerrando-se o ciclo de vida do SD, iniciado em PLA01.

15.4 - PLA03 - VERIFICAÇÃO DE CONFORMIDADE DO SD PELA DCTIM

A DCTIM analisará o DVS e informará, por mensagem à OMSOL, o resultado da avaliação do SD quanto ao processo de Conformidade, classificando-o em SD Conforme ou Não Conforme. Em caso de SD corporativos ou a critério da DCTIM, o DVS será submetido à apreciação da COTEC-TIC.

A DCTIM realizará estudo técnico da solução proposta pelo SD e verificará a pertinência e impactos desse atendimento na arquitetura corporativa de TI da MB. Este estudo técnico contemplará, dentre outros aspectos, as seguintes especificidades:

a) Avaliação dos requisitos

Avaliação dos requisitos do SD e sua relação com o contexto de TI da MB.

b) Avaliação dos riscos

Avaliação de riscos para o atendimento da necessidade de SD no contexto de TI da MB.

c) Avaliação dos benefícios

Avaliação da relação custo e benefício, em função da necessidade que o originou, sob o ponto de vista técnico.

d) Avaliação de atendimento às normas da MB

Avaliação do SD quanto à conformidade aos aspectos de Governança de TI da MB.

e) Avaliação quanto a sistemas digitais já existentes

Avaliação de SD similares, outras soluções possam absorver a demanda da OMSOL ou oportunidades de reutilização de SD desenvolvidos que executem tarefas similares.

Caso o SD seja considerado em conformidade pela DCTIM e em atendimento à Governança de TIC da MB ("SD Conforme"), o ciclo de vida seguirá para o início da Fase de Obtenção (OBT).

Caso a análise do SD seja concluída pela DCTIM como "SD Não Conforme", o DVS será restituído à OMSOL, com as devidas explicações e exigências e impedimentos para a continuação do ciclo de vida do SD. Caso as discrepâncias ou restrições não sejam sanadas, encerra-se o ciclo de vida do SD.

15.5 - PLA04 - AVALIAÇÃO DA NECESSIDADE DE SD PELA COTEC-TIC

O propósito desta atividade é submeter à análise da COTEC-TIC os SD corporativos considerados em conformidade pela DCTIM.

15.6 - PLA05 - AVALIAÇÃO DA NECESSIDADE DE SD PELO COTIM

Somente os casos julgados pertinentes pela COTEC-TIC, de acordo com sua abrangência, criticidade e/ou recursos financeiros serão encaminhados para ratificação do COTIM.

CAPÍTULO 16

FASE DE OBTENÇÃO

16.1 - DEFINIÇÃO

Esta fase consiste na definição da estratégia de desenvolvimento ou no desenvolvimento do SD, encerrando-se com o processo de homologação do SD pela DCTIM. Consistirá na elaboração do Projeto Básico, na escolha da estratégia de obtenção e da metodologia para desenvolvimento do SD, os mecanismos para gerência de projetos e os demais aspectos que devem ser contemplados antes da implantação do SD.

Nesta fase devem ser observados também aspectos legais, aplicados à Administração Pública Federal, visando atender os princípios da eficiência, economicidade e do controle administrativo.

O modelo esquemático desta fase do ciclo de vida encontra-se disponível no Anexo B desta publicação. A seguir são detalhadas as atividades previstas.

16.2 - OBT01 - DESIGNAÇÃO DE UM GERENTE DE PROJETO

Esta atividade marca o início da fase de obtenção com a designação formal de um Gerente de Projeto e responsável pelo SD na OMSOL, por meio de Ordem de Serviço. Esse gerente terá como principal responsabilidade o gerenciamento do processo de obtenção para o desenvolvimento ou manutenção do SD até a atividade de Aceitação do Produto ou SD (OBT09).

Para aquisição de SD de prateleira, COTS (Commercial Off-The-Shelf), não há necessidade de designação de um gerente. A OM adquirente deve se assegurar de que os requisitos do produto, a disponibilidade de documentação e os direitos de propriedade, de uso, de autoria, de licença e de suporte futuro sejam satisfeitos, em conformidade com a atividade de Avaliação de SD (OBT08).

No caso de desenvolvimento ou manutenção de SD, a OMSOL deverá elaborar o Projeto Básico, de acordo com a atividade Elaboração do Projeto Básico do SD (OBT02).

Considerando o DVS e tendo cumprido os procedimentos previstos na Fase de Planejamento, a OMSOL deverá elaborar e encaminhar à DCTIM, com informação para a OMREL, o Documento Preliminar de Arquitetura, Infraestrutura e Sustentação do Sistema (DAIS). A elaboração do Documento de Arquitetura, Infraestrutura e Sustentação do Sistema (DAIS) deverá especificar de forma preliminar e macro, os requisitos e decisões de projeto

arquiteturais da solução e a especificação de infraestrutura que está disponível e prevista para o ambiente de produção, além do plano de sustentação e suporte que levará em consideração requisitos de hospedagem e manutenibilidade, testes e a solução do sistema. O modelo do Documento de Arquitetura, Infraestrutura e Sustentação do Sistema (DAIS) será disponibilizado em norma própria da DCTIM.

16.3 - OBT02 - Elaboração do Projeto Básico do SD

Nesta atividade, o Gerente de Projeto da OMSOL deve elaborar o Projeto Básico do SD, a partir dos critérios estabelecidos no DVS de SD. O Projeto Básico do SD deve apresentar os seguintes aspectos:

- a) definição do(s) propósito(s) ou meta(s) a ser(em) alcançado(s) com o SD (escopo do projeto);
- b) definição do modelo de ciclo de vida, com a identificação das atividades que deverão ser executadas para produzir ou alcançar cada um dos itens do escopo, magnitude e complexidades definidos, além dos recursos necessários e o tempo para sua execução;
- c) seleção e adaptação de padrões, métodos, ferramentas e linguagens para apoiar as atividades de desenvolvimento;
- d) vantagens e benefícios do SD (motivação);
- e) riscos de implementação do projeto e respectivo contingenciamento;
- f) especificação dos requisitos do sistema, descrevendo: suas funções e capacidades; requisitos de negócio, organizacionais e de usuários; requisitos de proteção (de operação, influências do ambiente e danos), de segurança (informações sigilosas), de engenharia de fatores humanos (ergonomia), de interface, de restrições e de qualificação;
- g) definição de requisitos funcionais (relacionados diretamente com o problema) e não funcionais (como tolerância a falhas, portabilidade, características físicas e condições do ambiente de execução, interfaces externas, especificação de plataformas operacionais e que auxiliam na identificação da arquitetura geral do projeto);
- h) definição de características de qualidade do SD, como: confiabilidade, manutenibilidade, usabilidade, eficiência e portabilidade;
- i) definição de dados e requisitos de bases de dados;
- l) critérios de aceitação do SD pela OMSOL; e

I) informações necessárias para avaliação da estratégia de obtenção: local de instalação do SD; arquitetura proposta; quantidade de OM usuárias do SD; frequência média de acessos; equipe coordenadora do projeto e equipe executora do projeto.

16.4 - OBT03 - AVALIAÇÃO DA ESTRATÉGIA DE OBTEÇÃO DO SD

Nesta atividade, a partir do Projeto Básico do SD, é selecionada a estratégia de obtenção mais apropriada, a fim de não comprometer a consecução do projeto, nem correr o risco de escolher uma abordagem que a MB não seja capaz de suportar. As estratégias de obtenção podem ser:

- a) aquisição de SD de prateleira, já existente no mercado, chamado componente COTS (Commercial Off-The-Shelf), que satisfaça os requisitos;
- b) desenvolvimento de SD internamente, com equipe própria da OM ou da MB;
- c) contrato de serviço para desenvolvimento do SD; e
- d) contrato de serviço para manutenção do SD.

Caso seja identificada a necessidade de contratação de serviço ou aquisição de produto, deverá ser estabelecida a estratégia de contratação, contendo:

- análise de viabilidade de contratação;
- plano de sustentação (continuidade dos serviços em eventual interrupção contratual);
- considerações de mercado e de soluções existentes no momento da licitação;
- critérios de julgamentos de propostas técnicas;
- procedimentos e critérios de mensuração dos bens e serviços, abrangendo métricas, indicadores e valores;
- metodologia de avaliação;
- quantificação ou estimativa prévia do volume de serviços demandados;
- transferência de tecnologia, quando cabível; e
- filosofia de manutenção aplicável, baseada no projeto do sistema a ser obtido.

16.5 - OBT04 - SELEÇÃO DE PRODUTOS

Esta atividade destina-se a orientar a seleção de SD para avaliação, quando a estratégia de obtenção é por aquisição de SD de prateleira (COTS). A OMSOL deverá estabelecer e

documentar, no mínimo, os requisitos essenciais, o emprego planejado, o tipo de contrato de aquisição, as responsabilidades com o fornecedor, o conceito de suporte a ser empregado e os riscos considerados.

Neste caso, a seleção deverá assegurar que:

- a) os requisitos essenciais sejam satisfeitos;
- b) a documentação esteja disponível;
- c) os direitos de propriedade, de uso, de autoria, de garantia e de licença sejam satisfeitos;
- d) o suporte futuro para o SD seja planejado.

Os requisitos não imprescindíveis, mas desejáveis ou opcionais, podem ser avaliados e pontuados para efeito de comparação com outros produtos existentes.

A identificação de candidatos viáveis à avaliação pode ser realizada, entre outras modalidades por:

I) Consulta pública para obter os fornecedores que já desenvolveram soluções anteriores para a MB; ou

II) Pesquisa sobre SD que atenda os requisitos essenciais.

Deve ser estabelecido um prazo para a seleção de produtos, evitando que os propósitos a serem alcançados possam ser comprometidos com essa pesquisa.

16.6 - OBT05 - SELEÇÃO DE FORNECEDORES

Esta atividade é necessária nos casos de aquisição de SD de prateleira ou de contratação de serviço de desenvolvimento ou de manutenção de um SD. Tem como propósito definir os critérios com os quais o fornecedor será avaliado e selecionado, considerando os requisitos do SD, as condições de mercado e as soluções existentes.

Constituem fatores que podem influenciar na escolha de um fornecedor: a localização geográfica, a equipe e a infraestrutura disponíveis para o serviço (desenvolvimento ou manutenção) do SD e, principalmente, a qualificação técnica por meio de atestados ou certificações de capacidade técnica.

Em virtude de ser uma Instituição Avaliadora (IA) do modelo MPS.Br, o CASNAV poderá ser consultado para avaliar a capacidade técnica de empresas extra-Marinha e, se necessário, a DCTIM também poderá participar do processo.

16.7 - OBT06 - CONSTRUÇÃO DO SD

Esta atividade, seja de desenvolvimento ou de manutenção de um SD, exige o uso de métodos e ferramentas e a produção de artefatos específicos.

A OMSOL deverá escolher a Metodologia de Desenvolvimento do Software (MDS), antes de iniciar, efetivamente, a construção/desenvolvimento do SD, de acordo com o que foi planejado, especificado e dimensionado. Os documentos DVS e DAIS, previstos na fase de Planejamento (PLA), serão atualizados sempre que necessário para se adequarem às novas realidades de tempo, escopo, custo e qualidade.

Deverão ser empregadas uma das Metodologias de Desenvolvimento de Software (MDS) padronizadas para uso na MB, que deverá compor a Especificação de Requisitos, o Projeto Lógico e a Arquitetura do SD. O desenvolvimento do SD poderá ser terceirizado, seguindo o estabelecido no Projeto Básico e de acordo com a atividade Avaliação da Estratégia de Obtenção do SD (OBT03), porém o código-fonte do SD deverá ser entregue à MB. Ainda na Fase de Obtenção, deverá ser definido o Plano de Testes com o propósito de testar o SD e maximizar a sua abrangência, permitindo que se identifique antecipadamente o maior número possível de problemas. O plano de testes deve contemplar:

I) testes estruturais ou de caixa branca para garantir que as funções do SD foram implementadas segundo as especificações. Esses testes são realizados pela equipe de desenvolvimento durante a Implementação; e

II) testes funcionais ou de caixa preta, a serem aplicados na Fase de Produção, quando todo o SD já foi desenvolvido para avaliar se o SD atendeu aos requisitos estabelecidos na Especificação de Requisitos.

16.8 - OBT07 - CONTRATAÇÃO DE SERVIÇOS

Nesta atividade, que ocorre quando a estratégia de obtenção é por contratação de serviço de desenvolvimento ou de manutenção de um SD, o contrato é executado e, se for o caso, a implementação do produto é monitorada. São também realizados preparativos e planos para a implantação do produto e o treinamento dos usuários. É importante estabelecer um Acordo de Nível de Serviço (ANS) como parte do contrato de prestação de serviços, visando estabelecer parâmetros para mensurar resultados de tempo e desempenho, durante a execução contratual. Deve-se observar as seguintes diretrizes:

I - estabelecer as atividades consideradas críticas e secundárias;

II - definir claramente serviços e resultados esperados;

III - estabelecer indicadores e metas de forma sistemática que possam contribuir cumulativamente para o resultado global do serviço;

IV - os indicadores devem refletir fatores sob controle do prestador de serviços;

V - identificar fatores que possam interferir no atendimento das metas; e

VI- os indicadores devem ser objetivamente mensuráveis.

16.9 - OBT08 - AVALIAÇÃO DO SD PRONTO

Esta atividade inicia-se após a atividade Construção do SD (OBT06) e destina-se a apresentar uma estratégia para elaboração de um roteiro para avaliação dos produtos, levando em consideração:

I) o atendimento às funcionalidades essenciais, desejáveis e opcionais;

II) o custo;

III) o integração com outros SD;

IV) o tempo para implantação;

V) os aspectos não previstos;

VI) a infraestrutura necessária para operação do SD; e

VII) as características do fornecedor: capacidade de suporte, de treinamento, de implantação e de manutenção.

16.10 - OBT09 - ACEITAÇÃO DO PRODUTO OU SD

É a atividade em que são avaliados os critérios de aceitação definidos no Projeto Básico, utilizando parâmetros objetivos e mensuráveis, a fim de verificar se o produto ou SD é aderente aos requisitos a serem utilizados para sua validação e seu recebimento. Esta atividade envolve a OMSOL e a OMREL, se necessário. A partir da aceitação, o SD deverá ser homologado.

A geração dos dados a serem utilizados no Teste de Aceitação do SD é uma atividade que tem como principal tarefa o desenvolvimento do Plano de Testes que consistirá:

a) na definição do pessoal encarregado de testar o sistema;

b) na elaboração de um esboço das normas e padrões para os testes;

c) no estabelecimento de um critério para determinar o término dos testes; e

d) na estimativa de tempo e demais recursos para a realização dos testes.

16.11 - OBT10 - RECEBIMENTO DO PRODUTO OU SD

A atividade de recebimento do SD ocorre tanto para a estratégia de obtenção por aquisição de SD pronto como para a contratação de serviço de desenvolvimento ou de manutenção de um SD, desenvolvidos especificamente para a OMSOL, e deve ser formalizada pelo Gerente do Projeto.

16.12 - OBT11 - HOMOLOGAÇÃO DO SD

Esta atividade destina-se a avaliar se foram atendidos os aspectos previstos no Projeto Básico, em relação à hospedagem, à conectividade à segurança. Será realizada pela DCTIM, após a atividade Recebimento do produto ou SD (OBT10).

A Homologação do SD (OBT11) será solicitada formalmente à DCTIM pela OMSOL, via OMREL. A DCTIM avaliará os aspectos previstos no DVS e DAIS em relação a requisitos, tecnologias, infraestrutura, hospedagem, conectividade e a segurança, dentre outros. A Figura 4 apresenta o fluxograma das atividades de homologação do SD. A OMSOL deverá preparar a infraestrutura necessária para atender aos requisitos do SD que entrará na fase de homologação. O ambiente de homologação deverá reproduzir o futuro ambiente de produção.

CAPÍTULO 17

FASE DE PRODUÇÃO

17.1 - DEFINIÇÃO

Nesta fase são definidas as atividades necessárias ao acompanhamento da implantação e da operação do SD aceito e homologado, conforme previsto nas atividades OBT09, OBT10 e OBT11.

O modelo esquemático desta fase do ciclo de vida encontra-se disponível no Anexo B desta publicação. A seguir são detalhadas as atividades previstas.

17.2 - PRO01 - ACORDO DE NÍVEL DE SERVIÇO (ANS) PARA HOSPEDAGEM EM CENTRO DE DADOS

Esta atividade destina-se ao estabelecimento do Acordo de Nível de Serviço (ANS) com o Centro de Dados onde o SD será hospedado. Nos casos da implantação do SD dar-se dentro da própria estrutura da OM deverá ser realizada revisão no Histórico da Rede Local (HRL) para as devidas atualizações.

17.3 - PRO02 - IMPLANTAÇÃO DO SD

Esta atividade destina-se a colocar o SD em operação, mediante o cumprimento das seguintes etapas:

1. instalação do SD no ambiente definido no Projeto Básico;
2. entrega da documentação do SD; e
3. treinamentos associados ao SD.

Na implantação do SD devem ser considerados os critérios de aceitação estabelecidos no Projeto Básico do SD e os testes definidos no Plano de Testes, a fim de não comprometer o projeto. Nessa ocasião serão validados os requisitos funcionais, verificados os requisitos não funcionais e os critérios de aceitação definidos no Projeto Básico do SD (referentes à manutenção, treinamento, instalação etc). Também serão consolidados os treinamentos estabelecidos e será entregue a documentação elaborada durante o processo de desenvolvimento ou aquisição do SD. No caso específico de aquisição do SD, deve ser mantida a conformidade com o contrato. Durante esta atividade, é importante considerar os seguintes processos fundamentais:

a) Processo de Operação

Ocorre a partir da implantação e define as atividades de operação do SD no seu ambiente de funcionamento (entrada em produção) para seus usuários.

b) Processo de Treinamento

Define as atividades necessárias para capacitação e desenvolvimento de competências que irão apoiar o ciclo de vida do SD até sua desativação. Portanto, é essencial que a capacitação seja planejada e implementado com antecedência, a fim de que o pessoal treinado esteja disponível quando o SD for implantado.

c) Processo de Documentação

Para a aceitação e entrada em operação do SD deve ser produzida, no decorrer do ciclo de vida, a documentação que registra os processos de desenvolvimento do SD, descrevendo a implementação desde a especificação dos requisitos até os testes dos processos:

- do produto, que descreve as características do SD que está sendo desenvolvido;
- de instalação, que descreve como instalar o sistema, especificando a plataforma mínima necessária;
- do usuário, que descreve a interface homem-máquina para utilização do SD;
- do administrador, que descreve informações relevantes para uma boa administração do sistema; e
- de manutenção, que identifica possíveis problemas do SD, relacionando suas causas e alternativas de soluções.

17.4 - PRO03 - ACOMPANHAMENTO DO SD EM PRODUÇÃO

Nesta atividade deve ser verificado se o SD mantém suas funcionalidades conforme previsto em projeto. Tal verificação deve ser realizada a partir de Relatórios de Avaliação de satisfação do usuário. Esses relatórios devem ser obtidos de maneira sistemática e periódica, a partir de consultas (pesquisa de satisfação) junto aos usuários e também ao setor de suporte ao SD. As pesquisas de satisfação do usuário devem contemplar os aspectos de aplicabilidade e usabilidade do SD.

CAPÍTULO 18

FASE DE MANUTENÇÃO

18.1 - DEFINIÇÃO

A manutenção de um SD consiste no processo de melhoria e otimização de um SD implantado (Manutenção Evolutiva), como também no reparo de defeitos (Manutenção Corretiva), para garantir a operacionalidade dos SD durante toda a sua vida útil na MB. A manutenção é decorrente de, pelo menos, um dos seguintes fatores:

- erros de desenvolvimento que exigem mudanças no SD para corrigir defeitos e deficiências que foram encontrados durante a utilização pelo usuário;
- mudanças no ambiente sem alteração dos requisitos;
- mudanças nos requisitos;
- novas funcionalidades para melhorar a aplicabilidade e usabilidade do SD; ou
- melhoria da qualidade (programas ou base de dados).

Esta fase não se aplica aos SD de prateleira adquiridos sem o fornecimento do código-fonte do produto.

Para facilitar o controle de versões, recomenda-se o emprego do processo de apoio: gerência de configuração (APO02). O modelo esquemático desta fase do ciclo de vida encontra-se disponível na página 5 do Anexo B desta publicação. A seguir são detalhadas as atividades previstas.

18.2 - MAN01 - MANUTENÇÃO CORRETIVA DO SD

Esta atividade ocorre quando são detectados erros de funcionamento do SD e deve ser efetuada sua manutenção corretiva.

Quando o SD encontra-se em produção, podem ser encontrados problemas para sua utilização. Tais problemas devem ser reportados ao responsável pela manutenção (definido no Contrato de Manutenção), ao qual cabe apresentar estimativa para sua correção e entrega. Corrigidos os problemas reportados, o responsável pela manutenção deve apresentar a nova versão do SD e uma breve descrição da solução adotada.

A nova versão deve ser avaliada em ambiente de teste para verificar se o problema reportado foi realmente corrigido, e se nenhum outro problema decorrente da solução adotada foi

identificado.

A descrição do problema deve detalhar os seguintes aspectos:

- a descrição do problema, relacionando-o com o que deveria ocorrer;
- o ambiente onde o SD está instalado;
- os detalhes sobre a prioridade para correção do problema; e
- o procedimento para reprodução do defeito, se possível.

A descrição da correção do problema deve conter a data da entrega do SD corrigido, a data da validação da correção efetuada no ambiente de testes e o responsável por essa validação.

18.3 - MAN02 - MANUTENÇÃO ADAPTATIVA DO SD

Esta atividade consiste nas modificações que afetam o ambiente de produção do SD, sem alteração de requisitos. Podem ocorrer alterações de configuração do hardware, sistema operacional, etc.

18.4 - MAN03 - MANUTENÇÃO EVOLUTIVA DO SD

Esta atividade consiste na adição de novas funcionalidades ou alteração das já existentes, a fim de atender às mudanças nos requisitos dos SD. Trata-se de deixar de lado pequenos ajustes e lançar uma nova versão do SD, devendo ser tratada como uma necessidade de obtenção de SD e seguindo as atividades decorrentes dessa fase.

18.5 - MAN04 - MANUTENÇÃO PREVENTIVA DO SD

Esta atividade somente deve ser iniciada após o grupo responsável pela manutenção adquirir alguma experiência em manutenção corretiva, por envolver um conjunto de medidas operacionais e testes, visando evitar possíveis problemas dos componentes do SD que possam vir a comprometer seu desempenho. Embora a manutenção preventiva seja necessária para ampliar a vida útil do SD, com a consequente redução dos custos e aumento da sua segurança e desempenho, a limitação de recursos materiais, humanos e financeiros restringe o desenvolvimento de programas de manutenção preventiva.

18.6 - MAN05 - MANUTENÇÃO PREDITIVA DO SD

Esta atividade não representa um tipo de manutenção, mas uma técnica de gerenciamento de manutenção que evita desperdícios como resultado de manutenção desnecessária ou inadequadamente realizada. Visa predizer (ou prevenir) as falhas nos SD, por meio do

acompanhamento de diversos parâmetros, permitindo a operação contínua pelo maior tempo possível. As técnicas de monitoramento na manutenção preditiva são baseadas em condições e incluem a monitoria de processo e outras técnicas de análise que, combinadas, oferecem os meios de monitoramento direto de todos os SD, principalmente os críticos, e são essenciais na busca da melhoria do processo de SD.

CAPÍTULO 19

FASE DE DESATIVAÇÃO

19.1 - DEFINIÇÃO

Nesta fase da sistemática são definidas as seguintes atividades necessárias à desativação de um SD em produção:

- a notificação aos usuários;
- o plano de descontinuação; e
- a desativação do SD.

O modelo esquemático desta fase do ciclo de vida encontra-se disponível na página 6 do Anexo B desta publicação. A seguir são detalhadas as atividades previstas.

19.2 - RET01 - ELABORAÇÃO DO PLANO DE DESATIVAÇÃO

Esta atividade deve gerar um Plano de Desativação do SD para remover o suporte ativo de um SD. O Plano de Desativação do SD deve ser elaborado pela OMSOL do projeto, conjuntamente com a OM responsável pela hospedagem do SD e deve contemplar:

- a) o propósito da desativação;
- b) a data da desativação do SD;
- c) a responsabilidade por quaisquer questões futuras de suporte residual;
- d) a transição para um novo SD, se aplicável;
- e) o Plano de Migração do SD, contendo o projeto de migração de dados;
- f) a disponibilidade de cópias de arquivos de dados;
- g) as questões de preservação das informações; e
- h) a auditoria dos dados.

19.3 - RET02 - NOTIFICAÇÃO AOS USUÁRIOS

Esta atividade consiste no comunicado aos usuários do SD sobre sua desativação. Deve ser realizada formalmente, contendo as seguintes informações:

- a) o motivo da desativação;
- b) a solução de contingência;

- c) o Plano de Migração do SD, descrito na atividade Elaboração do Plano de Descontinuação (RET01);
- d) a data da desativação; e
- f) o SD substituto, se for o caso.

19.4 - RET03 - DESATIVAÇÃO (EXCLUSÃO DO SD)

Caso os usuários não apontem problemas ou discrepâncias impeditivas para a execução da desativação, esta atividade consiste na exclusão do SD desativado. Na fase de exclusão do SD deverão ser previstas as reconfigurações em outros SD, de forma a remover os arquivos e as dependências.

19.5 - RET04 - PRESERVAÇÃO DE DADOS

As bases de dados do SD desativado, caso representarem informações relevantes para a Marinha deverão ser mantidas e permanecer acessíveis, considerando os aspectos de preservação digital durante o período de guarda, conforme o estabelecido pelas Normas de Temporalidade da Marinha.

CAPÍTULO 20

ADMINISTRAÇÃO DE DADOS

20.1 - DEFINIÇÃO

A Administração de Dados tem por propósitos conceituar, estruturar, organizar, documentar e disponibilizar os recursos dos dados. Seus principais instrumentos são: dicionários de dados, modelagem e definição de padrões. Permite, ainda, definir as estruturas de dados, identificando sua localização e seu conceito, garantindo sua reutilização e mantendo a devida integração e consistência.

20.2 - ADMINISTRAÇÃO DOS DADOS NOS SD

A administração de dados de SD é atribuição da OM responsável pelo SD, por meio do seguinte conjunto de atividades, que devem ser documentadas e exercidas rotineiramente, de acordo com as características técnicas de cada sistema:

- a) a modelagem conceitual de dados;
- b) a revisão dos modelos de dados;
- c) o gerenciamento das regras de negócio aplicadas aos dados;
- d) a integração das bases de dados existentes na OM, minimizando as redundâncias;
- e) a manutenção da integridade referencial dos dados;
- f) a criação e a manutenção de esquemas dos banco de dados;
- g) o levantamento dos modelos existentes,
- h) a atualização constante dos dicionário de dados; e
- i) a divulgação do modelo de dados conceitual e do dicionário de dados dos SD.

20.3 - ADMINISTRAÇÃO GLOBAL DE DADOS

A administração global de dados dos SD é coordenada pela DCTIM e exercida pelas OM responsáveis pelos SD. Ela visa à criação e à manutenção de um modelo de dados corporativo em cada ODS, por meio da integração entre seus SD, e compreende o seguinte conjunto de atividades:

- a) a promoção do intercâmbio de práticas de administração de dados;
- b) a definição, em conjunto com os demais ODS, de um padrão de nomenclatura e de um

glossário de termos para as bases de dados; e

c) a promoção, em conjunto com os demais ODS, da padronização dos dicionários de dados.

20.4 - PROJETO DO BANCO DE DADOS

Consiste em especificar a estrutura do banco de dados definindo os modelos de dados (conceitual, lógico e físico) e os requisitos e componentes arquiteturais do banco de dados. Os modelos poderão ser descritos utilizando linguagens textuais e/ou linguagens gráficas em diferentes níveis de abstração, porém de forma a elucidar o domínio das informações armazenadas (domínio do problema). Será composto pelo Modelo Conceitual, Modelo Lógico e Modelo Físico.

Modelo Conceitual: É a descrição formal da base de dados de forma independente de implementação ou de plataforma tecnológica. É representado pelo esquema conceitual.

Modelo Lógico: É a descrição formal da base de dados com detalhes sobre tabelas, relacionamentos, regras, metadados dentre outros. Dependente, em certo nível de abstração, do Sistema Gerenciador de Banco de Dados (SGBD) utilizado. As entidades e atributos do modelo lógico são mapeados para tabelas e colunas do modelo físico. É representado pelo esquema lógico.

Modelo Físico: É a descrição formal da base de dados, modelo de armazenamento, estrutura física, SGBD. Descrição dos objetos do banco de dados (tabelas, visões, colunas, funções, restrições, permissões, dentre outros). É dependente do SGBD utilizado e representado pelo esquema físico.

As descrições dos modelos geram os esquemas de banco de dados. Os esquemas conceituais, lógicos e físicos das bases de dados serão considerados para efeitos de conformidade, homologação e hospedagem de sistemas e são previstos no Processo de Software da MB. Os modelos dos artefatos serão definidos pela DCTIM em norma própria. Por ocasião da homologação dos SD deverão ser apresentados os seguintes artefatos:

- Para o representar o esquema conceitual: Diagrama de Contexto
- Para representar o esquema lógico e físico: Modelo Entidade-Relacionamento
- (MER), Dicionário de Dados e script para criação do banco de dados.

20.4.1 - DIAGRAMA DE CONTEXTO

Entendimento inicial do contexto do SD em relação à gestão das informações. Representa os principais dados (fluxos de dados) que trafegam entre o SD e as entidades externas (outras fontes de dados, internas ou externas à MB). Uma entidade externa atua como produtor ou como consumidor de informações e reside fora dos limites do sistema a ser modelado. Deverão ser apresentados os fluxos de dados com os sistemas externos.

20.4.2 - MODELO ENTIDADE-RELACIONAMENTO (MER)

Modelo Entidade-Relacionamento (MER) deverá representar a base de dados sob três conceitos fundamentais: Entidade, Atributo e Relacionamento. O MER poderá ser conceitual, lógico ou físico e poderá ser substituído por modelo relacional que representa tabelas, atributos e relações materializadas no banco de dados. O MER deverá conter todas as entidades que compõem o sistema.

20.4.3 - DICIONÁRIO DE DADOS

Ferramenta textual utilizada para documentar o significado de cada entidade no modelo de dados. Compõe uma fonte de informação para auxiliar e facilitar o entendimento das entidades e regras de negócios. Descreve o significado dos fluxos de dados e dos depósitos de dados. A Tabela abaixo apresenta as informações que deverão compor o dicionário de dados.

Tabela/Entidade:					
Descrição:					
Atributo/Campo	Tipo	Tam	PK	FK	Descrição

20.4.4 - SCRIPT PARA CRIAÇÃO DO BANCO DE DADOS

Todos os ambientes de BD de produção residentes no CD-MB deverão ser gerados por meio de script/template de criação. Este script deverá compor a documentação da base de dados.

20.5 - PADRONIZAÇÃO DO MODELO DE DADOS

Tem o objetivo de prover informações para formalizar a nomenclatura de objetos do banco de dados. É a padronização de nomenclatura das estruturas físicas e lógicas relacionadas com o armazenamento dos dados.

20.6 - HOSPEDAGEM DAS BASES DE DADOS NO CENTRO DE DADOS DA MB (CD-MB)

As bases de dados hospedadas no Centro de Dados da MB (CD-MB) serão administradas gerenciadas, controladas e mantidas sob responsabilidade das OMSOL, considerando as atribuições estabelecidas nos Acordos de Nível de Serviço (ANS) celebrados.

20.7 - ATRIBUIÇÃO DE RESPONSABILIDADES

À DCTIM caberá:

- I) Avaliar a documentação das bases de dados para fins de conformidade e homologação de sistemas.
- II) Homologar o banco de dados quanto aos padrões definidos nesta norma.
- III) Assessorar os processos de Governança de Dados no âmbito da MB.

Ao CTIM caberá:

- I) Disponibilizar e controlar a infraestrutura necessária à hospedagem dos servidores de bancos de dados;
- II) Realizar backup dos dados conforme ANS celebrado com a OM responsável pelo SD;
- III) Supervisionar tecnicamente o serviço;
- IV) Apoiar as OM nos problemas de acesso aos servidores e erros no ambiente do CD-MB;
- V) Administrar os servidores de bancos de dados hospedados no CD-MB; e
- VI) Gerenciar usuários com permissão de DBA para servidores de bancos de dados no CD-MB.

À OMSOL caberá:

- I) Manter atualizado o modelo de dados, de forma a acompanhar, analisar e registrar os impactos decorrentes das manutenções evolutivas e corretivas;
- II) Realizar a recuperação de dados (recovery);
- III) Controlar o crescimento do ambiente mediante acordo formalizado com o CD-MB e solicitar previamente o aumento da área utilizada, respeitando a disponibilização da área no

momento da solicitação;

IV) Administrar os servidores de banco de dados; e

V) Custear o licenciamento e o suporte do SGBD.

CAPÍTULO 21

PROCESSOS DE APOIO

21.1 - DEFINIÇÃO

São processos que permeiam todo o ciclo de vida do SD, desenvolvidos pela própria OMSOL ou por meio da contratação de serviços terceirizados, com o propósito de contribuir para seu sucesso e sua qualidade. Para efetuar a gerência do desenvolvimento do SD e garantir a conclusão do projeto, alguns processos de apoio, tais como a documentação do SD e as gerências de configuração, de riscos e de comunicações devem ser realizados.

21.2 - APO01 - DOCUMENTAÇÃO

Esta atividade visa à elaboração e à gerência da documentação do SD, definindo os procedimentos necessários para registrar as informações produzidas durante o ciclo de vida do SD. Busca a qualidade e o sucesso do projeto, com a documentação tanto das interfaces externas quanto do projeto interno do SD para futuras manutenções e aprimoramentos. O processo consiste no registro das fases do desenvolvimento e de manutenção do SD e contém documentos necessários a todas as partes interessadas (gerentes, engenheiros de software, usuários do SD etc).

21.3 - APO02 - GERÊNCIA DE CONFIGURAÇÃO

Esta atividade define a aplicação de procedimentos administrativos e técnicos por todo o ciclo de vida do SD visando:

- a) identificar e definir os itens de software no SD (associados às entregas);
- b) estabelecer suas linhas básicas (baseline), para controle do processo;
- c) controlar as modificações e liberações dos itens;
- d) registrar e apresentar a situação dos itens e dos pedidos de modificação;
- e) garantir a completude, a consistência e a correção dos itens; e
- f) controlar o armazenamento, a manipulação e a distribuição dos itens.

O resultado desse processo é o Documento de Gerência de Configuração.

21.4 - APO03 - GERÊNCIA DE QUALIDADE

Esta atividade visa à garantia da qualidade do SD, buscando alcançar:

- maior eficiência na obtenção do SD;
- melhor adaptação às mudanças;
- melhor integração de esforços; e
- maior capacidade de aprendizado.

Para alcançar esses propósitos, podem ser utilizadas ferramentas, tais como:

- pesquisas / inspeções / entrevistas;
- definição de metas e indicadores operacionais e de desempenho;
- acompanhamento dos indicadores;
- monitoramento do processo;
- gerência de requisitos;
- monitoramento das reclamações dos usuários;
- acompanhamento dos prazos de realização das atividades; e
- ferramentas estatísticas.

21.5 - APO04 - VERIFICAÇÃO

Esta atividade descreve o acompanhamento do Plano de Testes, com relação aos testes estruturais ou de caixa branca, que visam garantir que as funções do SD estão implementadas segundo as especificações. O Plano de Testes contém o planejamento de todos os testes a serem executados no SD. Porém, para a Gerência de Verificação, o foco constitui, apenas, os testes estruturais a serem executados pela equipe de desenvolvimento, durante o ciclo de vida, com o propósito de testar um SD para melhorar o seu desempenho e maximizar a sua abrangência, permitindo que se identifique, antecipadamente, o maior número possível de problemas.

21.6 - APO05 - VALIDAÇÃO

Esta atividade descreve o acompanhamento do Plano de Testes, com relação aos testes funcionais ou de caixa preta, que visam avaliar se o SD desenvolvido atende aos requisitos estabelecidos ao início do Projeto, na Especificação de Requisitos. O Plano de Testes contém o planejamento de todos os testes a serem executados no SD. Porém, para a Gerência de Validação, o foco constitui os testes funcionais aplicados na atividade de Implantação do SD (PRO01), quando todo o SD já foi desenvolvido, visam avaliar se o SD atendeu aos

requisitos estabelecidos na Especificação de Requisitos.

21.7 - APO06 - GERÊNCIA DE RISCOS

Esta atividade descreve o processo que visa identificar, analisar, tratar, monitorar e reduzir continuamente os riscos em nível organizacional e de projeto. O gerenciamento de riscos do projeto inclui os processos que tratam da realização de identificação, análise, respostas, monitoramento, controle e planejamento do gerenciamento de riscos em um projeto. O propósito do gerenciamento de riscos é aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos adversos ao projeto. Deve contemplar:

- a) o planejamento do gerenciamento de riscos – decisão de como abordar, planejar e executar as atividades de gerenciamento de riscos de um projeto;
- b) a identificação de riscos – determinação dos riscos que podem afetar o projeto e documentação de suas características;
- c) a análise qualitativa de riscos – priorização dos riscos para análise ou ação subsequente, através da avaliação e da combinação de sua probabilidade de ocorrência e de impacto;
- d) a análise quantitativa de riscos – análise numérica do efeito dos riscos identificados no propósito geral do projeto;
- e) o planejamento de respostas a riscos – desenvolvimento de opções e ações para aumentar as oportunidades e reduzir as ameaças ao propósito do projeto; e
- f) o monitoramento e o controle de riscos – acompanhamento dos riscos identificados, monitoramento dos riscos residuais, identificação dos novos riscos, execução de planos de respostas a riscos e avaliação da sua eficácia durante todo o ciclo de vida do projeto.

21.8 - APO07 - GERÊNCIA DE COMUNICAÇÕES

O gerenciamento das comunicações do projeto é a área de conhecimento que emprega os processos necessários para garantir a geração, a coleta, a distribuição, o armazenamento, a recuperação e a destinação final das informações sobre o projeto, de forma oportuna e adequada. Os processos de gerenciamento das comunicações do projeto fornecem as ligações críticas entre pessoas e informações que são necessárias para comunicações bem-sucedidas. Os gerentes de projetos podem gastar um tempo excessivo na comunicação com a equipe do projeto, partes interessadas, cliente e patrocinador. Todos os envolvidos no projeto devem entender como as comunicações afetam o projeto como um todo. Deve contemplar:

- a) o planejamento das comunicações -determinação das necessidades de informações e comunicações das partes interessadas no projeto;
- b) a distribuição das informações - colocação das informações necessárias à disposição das partes interessadas no projeto no momento adequado;
- c) o Relatório de Desempenho - coleta e distribuição das informações sobre o desempenho, incluindo o relatório de andamento, a medição do progresso e a previsão.
- d) O gerenciamento das partes interessadas - gerenciamento das comunicações para atender aos requisitos das partes interessadas no projeto e solucionar problemas.

PARTE V
SÍTIOS ELETRÔNICOS

INTRODUÇÃO

CAPÍTULO 22 - FASES DO CICLO DE VIDA DE UM SÍTIO ELETRÔNICO

INTRODUÇÃO

1 - APRESENTAÇÃO

A informação institucional de cada OM transforma-se e atualiza-se a cada dia, por meio de atividades internas e externas que, em maior ou menor escala, envolvem a MB e, até mesmo, a sociedade em geral, e que são passíveis de divulgação. A utilização adequada das potencialidades da Internet, com a disponibilização de serviços eletrônicos, integrada a uma cultura interna de universalização do acesso à informação e ao conhecimento, possibilita atingir metas com eficácia, eficiência e economia de recursos (financeiros, de pessoal, de material, de tempo, de processos e etc.) para toda a MB. A Rede de Comunicações Integradas da Marinha (RECIM), por meio do serviço World Wide Web (WWW), viabiliza às OM a divulgação de informações e serviços na Intranet e na Internet, além de tornar acessíveis sistemas corporativos de uso pelo pessoal da MB. Para utilizar esse canal de comunicação é necessário que a OM possua um sítio eletrônico. Esta parte visa orientar as ações que devem e podem ser realizadas em relação aos sítios eletrônicos de Intranet e Internet das OM da MB, estabelecendo o que deve ser feito nas fases de planejamento, estruturação, elaboração, manutenção e gestão desses sítios eletrônicos, considerando os padrões do Governo Federal (acessibilidade, intercâmbio de informações entre os sistemas do governo federal e etc.) e os aspectos da RECIM. O modelo esquemático das principais fases do ciclo de vida de um sítio eletrônico encontra-se no Anexo C.

2 - PROPÓSITO

Esta parte da norma de TI destina-se a prover um guia para os usuários da MB, estabelecendo ações que devem ser criteriosamente aplicadas para desenvolver, disponibilizar e administrar sítios eletrônicos na MB.

3 - REFERÊNCIAS

Esta Norma consolida orientações existentes no âmbito da Marinha do Brasil e do Governo Federal.

4 - DEFINIÇÕES

A seguir são apresentadas as principais definições relacionadas a sítios eletrônicos.

4.1 - Sítio Eletrônico

Sítios eletrônicos constituem um conjunto de páginas Web, com hipertextos acessíveis geralmente pelo protocolo HTTP na Internet ou na Intranet.

A estrutura organizacional dessas páginas parte do endereço da página principal na Intranet ou na Internet (endereço-base único - URL).

As páginas Web são documentos virtuais que podem conter texto, imagens e arquivos de áudio e vídeo, relacionados e interligados de forma hipertextual com outros documentos na Intranet ou na Internet.

4.2 - Ciclo de Vida de um Sítio Eletrônico

O ciclo de vida de um sítio eletrônico descreve as fases pelas quais o sítio passa, a partir do planejamento, até tornar-se indisponível para acesso na Intranet ou na Internet. A utilização da abordagem de ciclo de vida visa estabelecer procedimentos que facilitem não só o seu uso efetivo mas também sua administração. Na MB, o ciclo de vida contemplará 6 fases. Cada uma delas inclui um conjunto de atividades que devem ser realizadas pelos elementos organizacionais envolvidos. Essas fases são: planejamento, produção, implantação, administração, manutenção e desativação.

4.3 - Padrão do Sítio Eletrônico

O padrão de formatação dos sítios eletrônicos da MB deverá possuir identidade visual compatível com a do sítio oficial da Marinha do Brasil na Internet, www.marinha.mil.br. As orientações para a compatibilização com os padrões de usabilidade e acessibilidade do Governo Federal estão no sítio da DCTIM, por meio de publicação técnica específica. A adoção de meios eletrônicos para a prestação dos serviços governamentais exige que sítios e portais desenvolvidos e mantidos pela administração pública sejam fáceis de usar, relevantes e efetivos. O Governo Federal desenvolveu um projeto de Identidade Digital de Governo, que busca padronizar os portais dos órgãos públicos federais e alinhar as informações para otimizar a comunicação com o cidadão.

A fim de facilitar o desenvolvimento dos sítios de Internet, encontra-se disponível para utilização no CD-MB, o tema GOVBR para o sistema de gerenciamento de conteúdo (CMS) homologado pela DCTIM. Este tema já contempla as recomendações de estilo e formatação de páginas do Governo Federal. As OM deverão utilizar o tema GOVBR para o desenvolvimento dos seus sítios de Internet, conforme instruções definidas pela DCTIM em

norma própria.

4.3.1 - Divulgação de informações

As informações divulgadas pelas OM devem obedecer ao disposto no Manual de Comunicação Social da Marinha (EMA-860).

4.3.2 - Textos

Os textos devem estar em conformidade com os conceitos de Comunicação Social em vigor na MB. A linguagem utilizada deve ser sóbria, comprehensível, coerente e não apresentar erros gramaticais, ortográficos ou de estilo, evitando-se o emprego de gírias navais, sem a devida explicação.

4.3.3 - Link para a página da MB

As páginas deverão estar ligadas, por meio de “link”, à página da MB na Internet, usando-se a imagem do Distintivo da MB, a qual pode ser obtida na citada página, com diâmetro mínimo de dois centímetros.

4.3.4 - Segurança

Caso o sítio eletrônico hospede informações sigilosas em seu banco de dados, a OM cliente deverá manter esses dados protegidos por um mecanismo de criptografia. Para tal, podem ser utilizados os Algoritmos de Estado estabelecidos pela MB.

CAPÍTULO 22

FASES DO CICLO DE VIDA DE UM SÍTIO ELETRÔNICO

Este capítulo destina-se a fornecer as orientações para cada uma das fases do ciclo de vida de um sítio eletrônico.

22.1 - FASE DE PLANEJAMENTO

Nesta fase, a OM da MB que necessite incluir sítios eletrônicos na Internet ou na Intranet deve apresentar uma proposta para divulgação de informações, conforme o caso, que justifique a necessidade da utilização desse canal de comunicação. Para sítio na Internet, a proposta deverá ser encaminhada para o Centro de Comunicação Social da Marinha (CCSM) e para a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM). No caso de sítio na Intranet, a proposta deverá ser encaminhada para a DCTIM. Analisada a proposta pelo Órgão competente, autoriza-se ou não a continuidade do ciclo de vida do sítio eletrônico. As atividades a serem realizadas na fase de planejamento são:

22.1.1 - PLA01 - Apresentação de proposta para sítio eletrônico

O propósito desta atividade é elaborar uma proposta para sítio eletrônico na Intranet ou na Internet, na qual deve ser claramente identificado o propósito da divulgação de informações e/ou serviços pela OM solicitante (OMSOL). Para tanto, é preciso descrever:

a) O propósito do sítio eletrônico

O propósito descreve a que se destina o sítio eletrônico. A definição precisa do que se deseja alcançar com o sítio é fundamental, pois não só o restante da proposta deverá ser condizente com esse propósito, como também apoiará sua estruturação e seu desenvolvimento.

b) A abrangência do sítio eletrônico e público-alvo

O público-alvo especifica para quem se destina o sítio eletrônico. É importante categorizá-lo em grupos, a fim de nivelar, entre outros, os seguintes aspectos: o tipo de linguagem a ser utilizada, a estruturação das informações, a tecnologia a ser empregada e as facilidades de navegação. São definidos alguns grupos básicos. No entanto, essa classificação pode ser ampliada, à medida em que se pode direcionar os aspectos que serão contemplados no sítio eletrônico. Categorias de público-alvo a serem utilizados nesta publicação: cidadãos; empresas; governo; e militares da MB, ativos e/ou inativos.

c) A justificativa para a criação do sítio eletrônico

A justificativa para a criação do sítio eletrônico deve contemplar, pelo menos, os seguintes aspectos:

- relação entre o propósito para criação do sítio e a missão, projetos e tarefas da OMSOL;
- relação dos serviços oferecidos no sítio, evidenciando como as informações e os serviços propostos para o sítio eletrônico atenderão ao público-alvo; e
- benefícios que serão produzidos com a disponibilização do sítio eletrônico para o público-alvo; e benefícios para a OMSOL, para a MB e para a Administração Pública.

d) Sítios com igual propósito

Devem ser verificados e mencionados os sítios eletrônicos com propósito semelhante ao que se deseja criar.

e) Estruturação das informações e serviços disponibilizados.

A estruturação do sítio deve contemplar, principalmente, o projeto, o conteúdo, as aplicações disponibilizadas e a arquitetura da informação.

f) Os recursos humanos, técnicos e de disponibilidade financeira para o desenvolvimento e a manutenção do sítio e de seus serviços.

Ao término desta atividade, a Proposta para Sítio Eletrônico na Internet deve ser enviada via COMINSUP da OMSOL, para o CCSM. No caso da Proposta para Sítio Eletrônico na Intranet, deve ser enviada via COMINSUP da OMSOL para a DCTIM.

22.1.2 - PLA02 - Avaliação da proposta para sítio eletrônico pelo CCSM

Esta atividade visa analisar a viabilidade do atendimento da necessidade de divulgação de informações e/ou serviços da OMSOL via sítio eletrônico, definida na proposta para sítio eletrônico na Intranet ou na Internet. Com base nas informações fornecidas pela OMSOL, o CCSM/DCTIM verificará a pertinência da solicitação, no âmbito da publicação EMA-860, consolidando tais informações na avaliação da proposta para sítio eletrônico na Intranet ou na Internet. O documento de avaliação da proposta para sítio eletrônico na Intranet ou na Internet, será enviado à OMSOL, qualquer que tenha sido o parecer sobre a criação do sítio. A DCTIM deve ser comunicada da decisão no caso de sítios para Internet.

22.2 - FASE DE PRODUÇÃO DO SÍTIO ELETRÔNICO

Definido o propósito a ser alcançado com o sítio eletrônico, inicia-se a fase de produção que busca, inicialmente, detalhar os aspectos que devem ser contemplados no sítio eletrônico, tais como a identidade visual, o conteúdo, o projeto gráfico, as condições de naveabilidade, as aplicações, a arquitetura da informação e a tecnologia homologada pela DCTIM para a confecção do sítio eletrônico, a fim de que sejam observados e analisados antes de sua efetiva implementação.

22.2.1 - PRO01 - Estruturação do Sítio Eletrônico

A estruturação do sítio eletrônico visa definir as principais categorias de informação, e como elas serão organizadas. Deve ser observado o padrão de páginas de sítios eletrônicos da MB. O Governo Federal estabeleceu, por Decreto, normas gerais e critérios básicos para a promoção da acessibilidade aos portais e sítios eletrônicos da Administração Pública na Internet, visando seu uso pelas pessoas portadoras de deficiência visual, de modo que seja viável o pleno acesso às informações disponíveis. A fim de facilitar a adequação dos sítios eletrônicos de Internet da MB aos critérios de acessibilidade do Decreto, tomando-se por base o modelo de acessibilidade do Governo Eletrônico (e-MAG), a DCTIM divulga, em seu sítio na Intranet, os principais aspectos que devem ser observados na disponibilização de conteúdo na Internet. Ao término desta atividade será produzida a estrutura do sítio eletrônico, onde estarão registrados os aspectos mencionados neste tópico e que serão implementados no sítio eletrônico.

22.2.2 - Implementação do Sítio Eletrônico

Esta atividade destina-se a implementar o sítio eletrônico no ambiente de homologação do Centro de Tecnologia da Informação da Marinha (CTIM), quando se converte a estrutura do sítio eletrônico para o sítio eletrônico propriamente dito. Para essa implementação é necessário abrir um chamado na Central de Suporte da RECIM - CSRECIM, solicitando a criação de um usuário no servidor de homologação, informando o nome e a caixa postal, em formato externo (usuário@marinha.mil.br), do responsável pelo sítio eletrônico, para recebimento da senha de acesso.

22.3 - FASE DE IMPLANTAÇÃO DO SÍTIO ELETRÔNICO

A fase de implantação inicia-se quando a OM ou a empresa contratada, utiliza o ambiente de homologação do Centro de Dados da Marinha (CD-MB) e consiste no atendimento dos

requisitos de segurança, acessibilidade, identidade visual compatível com os padrões da MB e certificação digital visando sua publicação na Internet ou Intranet. O ambiente de homologação consiste em uma estrutura de sítio para a OM com configurações básicas pré-definidas. A administração será realizada, dinamicamente, por meio de uma interface de acesso *web*, permitindo ao administrador configurar, personalizar e adicionar conteúdo ao seu sítio.

22.3.1 - IMP01 - Solicitação para implantação do sítio eletrônico

Para iniciar a fase de implantação é necessário a OMSOL contactar a DCTIM, participando a prontificação do sítio eletrônico e solicitar a homologação. Este contato deve ser efetuado por mensagem da OMSOL à DCTIM, com cópia para o CTIM.

22.3.2 - IMP02 - Avaliação de usabilidade, identidade visual e acessibilidade

Esta atividade inicia-se com o recebimento da mensagem na DCTIM. Destina-se a verificar o atendimento aos aspectos de usabilidade, identidade visual do sítio eletrônico e acessibilidade, conforme padrões definidos pela DCTIM. Ao término da análise, a DCTIM enviará uma mensagem ao CTIM, com cópia para a OMSOL participando sua conclusão. Caso seja necessário, devem ser efetuados contatos com a OMSOL para correções necessárias à aprovação do sítio eletrônico.

22.3.3 - IMP03 - Avaliação de segurança, conectividade e certificação digital para publicação

Esta atividade inicia-se no CTIM com o recebimento da mensagem resultante da etapa anterior, participando a aprovação do sítio pela DCTIM. Nesta atividade, é verificado o atendimento aos aspectos de certificação digital, segurança e conectividade, atendendo aos padrões estabelecidos pela DCTIM. Ao término da atividade será elaborada mensagem para a OMSOL, com cópia para a DCTIM, participando o atendimento aos aspectos supracitados. Caso necessário, serão efetuados contatos com a OMSOL para viabilizar as verificações.

22.3.4 - IMP04 - Publicação do sítio eletrônico

Esta atividade, realizada pelo CTIM, destina-se a estabelecer formalmente aspectos relacionados à publicação e à administração do sítio eletrônico. São elas:

- a data para publicação do sítio eletrônico;
- o endereço eletrônico do sítio eletrônico na Internet ou Intranet; e

- os aspectos que deverão ser atendidos para administração do sítio eletrônico pela OM responsável.

Tais aspectos devem ser participados pelo CTIM à OM responsável pelo sítio eletrônico, por mensagem, com cópia para a DCTIM.

22.4 - FASE DE ADMINISTRAÇÃO

Com o sítio eletrônico publicado, inicia-se sua administração. Esta fase caracteriza-se por atividades que visam garantir confiabilidade às informações e aos serviços fornecidos por meio do sítio eletrônico. Essas atividades são de responsabilidade da OM responsável pelo sítio eletrônico e foram estabelecidas na fase de implantação. São características da fase de administração as seguintes atividades:

- a) alterações de conteúdo do sítio eletrônico; e
- b) alterações na disposição do menu de opções.

22.5 - FASE DE MANUTENÇÃO

A fase de manutenção caracteriza-se pelas alterações relacionadas à estrutura do sítio eletrônico: identidade visual, usabilidade etc. Caso a OM responsável pelo sítio eletrônico considere necessárias alterações do tipo das mencionadas neste tópico, deve ser iniciado novo ciclo de vida para o sítio eletrônico.

22.6 - FASE DE DESATIVAÇÃO

A fase de desativação ocorre quando o sítio não mais atende aos requisitos e tem que ser tirado do ar. Tal procedimento deve ser formalizado por meio de mensagem à DCTIM com cópia para o CTIM. Tal procedimento visa a desativação do nome de domínio associado ao sítio eletrônico.

22.7 - ESTRUTURA DOCUMENTAL RELACIONADA A SÍTIO ELETRÔNICO

Os principais documentos relacionados a sítios eletrônicos são:

- Avaliação da Proposta para Sítio Eletrônico na Intranet ou na Internet;
- Documento enviado à OMSOL, contendo o parecer do CCSM sobre a pertinência da solicitação de criação do sítio, no âmbito da publicação EMA-860;
- Padrão de Páginas de Sítios Eletrônicos da MB;

- Documento que apresenta os padrões a serem seguidos na produção de sítios eletrônicos;
- Proposta para Sítio Eletrônico na Intranet ou na Internet; e
- Documento que apresenta a proposta da OMSOL para divulgação de informações em sítio eletrônico na Intranet ou Internet.

22.8 - RESPONSABILIDADES**DCTIM:**

- Homologar os sítios, verificando se ele se enquadra nas normas da referência ao manual de diretrizes de comunicação digital do Governo Federal.

CTIM:

- Gerenciar o servidor de páginas dinâmicas da Marinha, realizando as atualizações das tecnologias homologadas;
- Prover o backup dos conteúdos;
- Apoiar as OM, que possuem sítios hospedados no servidor de páginas dinâmicas no CD-MB, em problemas de acesso ao servidor e erros no ambiente do CD-MB.(O CTIM não dará suporte ao desenvolvimento de sítios);
- Criar e disponibilizar ao “admin” da OM um usuário com perfil de “Administrador”;
- Disponibilizar em seu sítio eletrônico, as versões dos softwares em uso no servidor e instruções técnicas que auxiliem a criação/manutenção do sítio eletrônico; e
- Transferir o sítio das OM do ambiente de homologação para o ambiente de produção.

OM Cliente

- Desenvolver e administrar o seu sítio, devendo criá-lo, atualizá-lo e mantê-lo.

CCSM

- Avaliar a proposta para sítios eletrônicos.

ANEXO A**RELAÇÃO DE DOCUMENTOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**

APÊNDICE I - MODELO DE TERMO DE RESPONSABILIDADE INDIVIDUAL

APÊNDICE II - MODELO DE TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO

APÊNDICE III - MODELO DO HISTÓRICO DA REDE LOCAL

APÊNDICE IV - MODELO DE PROGRAMAÇÃO DAS ATIVIDADES DE AUDITORIA DE SICRL

APÊNDICE V - MODELO DE CAPA DO RELATÓRIO DE AUDITORIA (RAD)

APÊNDICE VI - MODELO DE PARTE DE INTRODUÇÃO DO RAD

APÊNDICE VII - MODELO DE PARTE DE CONSTATAÇÃO DO RAD

APÊNDICE VIII - MODELO DE PARTE DE CONSIDERAÇÕES FINAIS E ASSINATURA DO RAD

APÊNDICE IX - GLOSSÁRIO DE TERMOS DE SIC

APÊNDICE I AO ANEXO A

MODELO DO TERMO DE RESPONSABILIDADE INDIVIDUAL

MARINHA DO BRASIL
(NOME DA OM)

TERMO DE RESPONSABILIDADE INDIVIDUAL

(Local: cidade), ____ de _____ de _____

Pelo presente instrumento, eu, (nome completo, NIP ou nº da identidade), perante a Marinha do Brasil, doravante denominada MB, na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, **declaro estar ciente** das normas de segurança das informações digitais da OM, segundo as quais devo:

- a) tratar a informação digital como patrimônio da MB e como um recurso que deva ter seu sigilo preservado, em consonância com a legislação vigente;
- b) utilizar as informações disponíveis e os sistemas e produtos computacionais, dos quais a MB é proprietária ou possui o direito de uso, exclusivamente para o interesse do serviço;
- c) preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas;
- d) não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a minha Credencial de Segurança (CREDSEG) ou que eu não tenha autorização ou necessidade de conhecer;
- e) não compartilhar o uso de senha com outros usuários;
- f) não me fazer passar por outro usuário usando a sua identificação de acesso e senha;
- g) não alterar o endereço de rede ou qualquer outro dado de identificação do microcomputador de meu uso;
- h) instalar e utilizar em meu microcomputador somente programas homologados para uso na MB e que esta possua as respectivas licenças de uso ou, no caso de programas de domínio público, mediante autorização formal do Oficial de Segurança de Informações e Comunicações (OSIC) da OM;
- i) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer

tipo de afastamento, preservar o conteúdo das informações e documentos sigilosos a que tive acesso e não divulgá-los para pessoas não autorizadas;

- j) guardar segredo das minhas autenticações de acesso (senhas) utilizadas no ambiente computacional da OM, não cedendo, não transferindo, não divulgando e não permitindo o seu conhecimento por terceiros;
- k) não utilizar senha com seqüência fácil ou óbvia de caracteres que facilite a sua descoberta e não escrever a senha em lugares visíveis ou de fácil acesso;
- l) utilizar, ao me afastar momentaneamente da minha estação de trabalho, descanso de tela (“screen saver”) protegido por senha, a fim de evitar que alguém possa ver as informações que estejam disponíveis na tela do computador;
- m) ao me ausentar do local de trabalho, momentaneamente ou ao término de minhas atividades diárias, certificar-me de que a sessão aberta no ambiente computacional com minha identificação foi fechada e as informações que exigem sigilo foram adequadamente salvaguardadas;
- n) seguir as orientações da área de informática da OM relativas à instalação, à manutenção e ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;
- o) comunicar imediatamente ao meu superior hierárquico e ao Oficial de Segurança das Informações e Comunicações (OSIC) da OM a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de segurança estabelecidos;
- p) responder, perante a MB, as auditorias e o Oficial de Segurança das Informações e Comunicações (OSIC) da OM, por acessos, tentativas de acessos ou uso indevido da informação digital realizados com a minha identificação ou autenticação;
- q) não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação;
- r) estar ciente de que toda informação digital armazenada e processada no ambiente computacional da OM pode ser auditada, como no caso de páginas informativas (“sites”) visitadas por mim;
- s) não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;
- t) não transferir qualquer tipo de arquivo que pertença à MB para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;
- u) estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional da OM;

- v) estar ciente de que a MB poderá auditar os arquivos em trâmite ou armazenados nos equipamentos do ambiente computacional da OM sob meu uso ou responsabilidade;
- w) estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da OM deve obedecer a este preceito; e
- x) estar ciente de que a MB poderá auditar as correspondências eletrônicas originadas ou retransmitidas por mim no ambiente computacional da OM.

Desta forma, estou ciente da minha responsabilidade pelas consequências decorrentes da não observância do acima exposto e da legislação vigente.

Assinatura

Nome Completo, NIP ou nº da identidade

APÊNDICE II AO ANEXO A**MODELO DO TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO**

MARINHA DO BRASIL
(NOME DA OM)

TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO

(Local: cidade), ____ de _____ de _____

Pelo presente instrumento, eu, (nome completo, NIP ou nº da identidade), perante a Marinha do Brasil, doravante denominada MB, na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, **declarei ter recebido desta OM** uma estação de trabalho com as seguintes configurações:

I – de identificação:

- a) **endereço IP:** (especificar o endereço IP da máquina);
- b) **endereço físico de rede:** (especificar a identificação exclusiva da placa de rede da máquina); e
- c) **identificação da máquina:** (especificar o nome e outros dados de identificação da máquina).

II – de instalação de programas:

- a) (especificar cada um dos programas pré-instalados);
- b) ...

III – de senha de acesso à máquina (“boot”), inicialmente estabelecida pelo Administrador da Rede Local (ADMIN) da OM e por mim alterada, sendo agora de meu conhecimento exclusivo; e

IV – de senha de configuração (“setup”), de conhecimento exclusivo do ADMIN e à qual não devo tomar conhecimento.

Assim, quaisquer alterações ou inclusões nos dados acima são de minha inteira responsabilidade e devem ser previamente autorizadas pelo Oficial de Segurança das Informações e Comunicações (OSIC), conforme previsto nas normas de Segurança das Informações Digitais da OM.

Estou ciente que o ADMIN (**executou / não executou**) a “formatação” prévia dos discos rígidos da referida estação de trabalho e sua correspondente reconfiguração e que, a qualquer momento e sempre que julgar necessário, poderei solicitar ao ADMIN auxílio para a realização dessa “formatação”, de modo a garantir a configuração padronizada da OM e a inexistência de arquivos ou programas irregulares.

Assinatura

Nome Completo, NIP ou nº da identidade

APÊNDICE III AO ANEXO A**MODELO DO HISTÓRICO DA REDE LOCAL****- INCIDENTES -****RESERVADO****MARINHA DO BRASIL****NOME DA OM****HISTÓRICO DA REDE LOCAL****INCIDENTE NA REDE LOCAL Nº:** _____ (*a ser preenchido pelo OSIC*)**1- Responsável pela informação do incidente:**

Função: _____

2- Data e hora do Incidente: _____ / _____ / _____ - _____ horas

Data e hora do relato: _____ / _____ / _____ - _____ horas

3- Relato do incidente:*(relatar detalhadamente o incidente, utilizando quantas linhas forem necessárias)***4- Comentários, Análise sobre o Incidente e respectivas correções:***(escrever detalhadamente, utilizando quantas linhas forem necessárias)***5- Afetou algum Recurso Computacional Crítico (RCC) Nível 1? ()sim ()não**

Data: _____ / _____ / _____

Assinatura do OSIC: _____

Ratificação pelo Titular da OM: _____

RESERVADO**- nº da página -**

APÊNDICE IV AO ANEXO A**MODELO DE PROGRAMAÇÃO DAS ATIVIDADES DE AUDITORIA DE SICRL**

MARINHA DO BRASIL**NOME DA OM****PROGRAMAÇÃO DAS ATIVIDADES DE AUDITORIA DE
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES EM REDES LOCAIS****OM AUDITADA:** _____**TIPO DA AUDITORIA:** _____**REFERÊNCIAS:**

- (Portarias, ofícios, mensagens e outros documentos)

AUDTORES:

- (Nome, posto, função)
- (Nome, posto, função)
- (Nome, posto, função)

1 - PROPÓSITO**2 - PESSOAL ENVOLVIDO**

- Representante da OM auditada;
- Oficial de Segurança das Informações e Comunicações (OSIC) da OM;
- Administrador da Rede Local (ADMIN) da OM; e
- Auditores de SICRL (designados pela DCTIM);

3 - PROGRAMAÇÃO DA AUDITORIA

Local e data.

<posto/nome/função/assinatura >

Chefe da Equipe de Auditoria

- nº da página -

APÊNDICE V AO ANEXO A**MODELO DA CAPA DO RELATÓRIO DE AUDITORIA (RAD)****RESERVADO**

MARINHA DO BRASIL
DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA
DA INFORMAÇÃO DA MARINHA

RELATÓRIO DE AUDITORIA DE**SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES EM REDES LOCAIS**

OM sob Auditoria de SICRL: _____

Data da Auditoria de SICRL: ____/____/____.

Equipe de Auditoria:

1. <posto/nome> _____

2. <posto/nome> _____

3. <posto/nome> _____

Aprovação do RAD pela DCTIM em ____/____/____.

Obs: Em caso de não-aprovação, deve ser anexada a justificativa.

<posto/nome/função/assinatura>

Encaminhado à OM e respectivo COMIMSUP por meio do _____ em ____/____/____.
(documento)

RESERVADO

APÊNDICE VI AO ANEXO A**MODELO DA PARTE DE INTRODUÇÃO DO RAD****RESERVADO**

(Cont. do RAD do(a) (SIGLA da OM).....)

1 – INTRODUÇÃO**1.1 – OM sob Auditoria de SICRL:** _____**1.2 – Data da Auditoria de SICRL:** _____**1.3 – Tipo de Auditoria de SICRL:** _____**1.4 – Documento de designação da Equipe de Auditoria de SICRL:** _____**1.5 – Propósito da Auditoria de SICRL:**

1.6 – Referências:

1.7 – Prazos Limites:

- para elaboração do RAD: ____/____/____.

- para aprovação do RAD: ____/____/____

RESERVADO

APÊNDICE VII AO ANEXO A**MODELO DA PARTE DE CONSTATAÇÕES DO RAD****RESERVADO**

(Cont. do RAD do(a) (SIGLA da OM).....)

2 - CONSTATAÇÕES DA AUDITORIA DE SICRL**2.1 - QUANTO AO ADESTRAMENTO****2.1.1 - XXX (denominação do item)****CONSTATAÇÃO**

(ocorrência, vulnerabilidade ou fato constatado)

COMENTÁRIO

(possíveis consequências ou prejuízos à SIC decorrentes da constatação efetuada)

RECOMENDAÇÃO

(soluções recomendadas e referências que as fundamentam)

...

2.2 - QUANTO À ADMINISTRAÇÃO DA REDE LOCAL**2.2.1 - XXX (denominação do item)****CONSTATAÇÃO**

(ocorrência, vulnerabilidade ou fato constatado)

COMENTÁRIO

(possíveis consequências ou prejuízos à SIC decorrentes da constatação efetuada)

RECOMENDAÇÃO

(soluções recomendadas e referências que as fundamentam)

...

2.3 - QUANTO À DOCUMENTAÇÃO**2.3.1 - XXX (denominação do item)****CONSTATAÇÃO**

(ocorrência, vulnerabilidade ou fato constatado)

COMENTÁRIO

(possíveis consequências ou prejuízos à SIC decorrentes da constatação efetuada)

RECOMENDAÇÃO

(soluções recomendadas e referências que as fundamentam)

...

2.4 - QUANTO ÀS ESTAÇÕES DE TRABALHO

2.4.1 - XXX (*denominação do item*)

CONSTATAÇÃO

(*ocorrência, vulnerabilidade ou fato constatado*)

COMENTÁRIO

(*possíveis consequências ou prejuízos à SIC decorrentes da constatação efetuada*)

RECOMENDAÇÃO

(soluções recomendadas e referências que as fundamentam)

...

2.4 - QUANTO AOS INCIDENTES

2.4.1 - XXX (*denominação do item*)

CONSTATAÇÃO

(*ocorrência, vulnerabilidade ou fato constatado*)

COMENTÁRIO

(*possíveis consequências ou prejuízos à SIC decorrentes da constatação efetuada*)

RECOMENDAÇÃO

(soluções recomendadas e referências que as fundamentam)

...

2.4 - QUANTO A SEGURANÇA FÍSICA

2.4.1 - XXX (*denominação do item*)

CONSTATAÇÃO

(*ocorrência, vulnerabilidade ou fato constatado*)

COMENTÁRIO

(*possíveis consequências ou prejuízos à SIC decorrentes da constatação efetuada*)

RECOMENDAÇÃO

(soluções recomendadas e referências que as fundamentam)

...

RESERVADO

- nº da página -

APÊNDICE VIII AO ANEXO A**MODELO DA PARTE DE CONSIDERAÇÕES FINAIS E ASSINATURAS DO RAD****RESERVADO**

(Cont. do RAD do(a) (SIGLA da OM).....)

3 - CONSIDERAÇÕES FINAIS DA EQUIPE DE AUDITORIA DE SICRLa) _____
_____b) _____
_____c) _____

...

4 - ASSINATURAS

<posto/nome>

Membro da Equipe de Auditoria

<posto/nome>

Membro da Equipe de Auditoria

<posto/nome>

Membro da Equipe de Auditoria

RESERVADO

- nº da página -

APÊNDICE IX DO ANEXO A**GLOSSÁRIO DE TERMOS DE SIC**

Ativos de Informação – os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Usuário – servidor civil ou militar da MB, lotado ou não em OM da MB ou em entidade extra-MB.

Usuário Visitante – servidor civil, militar da MB ou não, que utilizam dispositivos móveis de sua propriedade, ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos e virtuais de órgãos ou entidades da MB, dos quais não fazem parte.

Dispositivos móveis – são os dispositivos periféricos de armazenamento e os dispositivos móveis inteligentes.

Dispositivos periféricos de armazenamento – consiste em equipamentos portáteis dotados de capacidade computacional de processamento e armazenamento, entre os quais se incluem: pendrives, “Hard Disk” externo e cartões de memória

Dispositivos móveis inteligentes - possuí a capacidade de usar aplicações de forma independente, conectar-se a redes, processar e armazenar dados, além de funcionalidades como câmera fotográfica, gravador de som e vídeo, editor de textos, leitor de arquivos, exemplos: “smartphones”, “tablets”, “smartwatch”.

Dispositivos móveis pessoais – são os dispositivos móveis adquiridos pelo próprio usuário. Dispositivos móveis pessoais que se submetem aos padrões corporativos de software e controles de segurança, e que são incorporados à rede de dados do órgão, serão considerados como dispositivos funcionais.

Dispositivos móveis funcionais – são os dispositivos móveis fornecidos pela MB ao usuário, ficando sob sua responsabilidade tanto para o caso de perda, roubo ou extravio quanto para os casos de divulgação de informações sigilosas da MB.

Ameaça – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Vulnerabilidade – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.





ANEXO B**MODELOS ESQUEMÁTICOS DO CICLO DE VIDA DOS SD**

B2 - FASE DE PLANEJAMENTO DE SD

B3 - FASE DE OBTENÇÃO DE SD

B4 - FASE DE PRODUÇÃO DE SD

B5 - FASE DE MANUTENÇÃO DE SD

B6 - FASE DE DESATIVAÇÃO DE SD

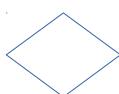
B7 - PROCESSO DE APOIO DE SD

Legenda

Atividade



Documento



Condição



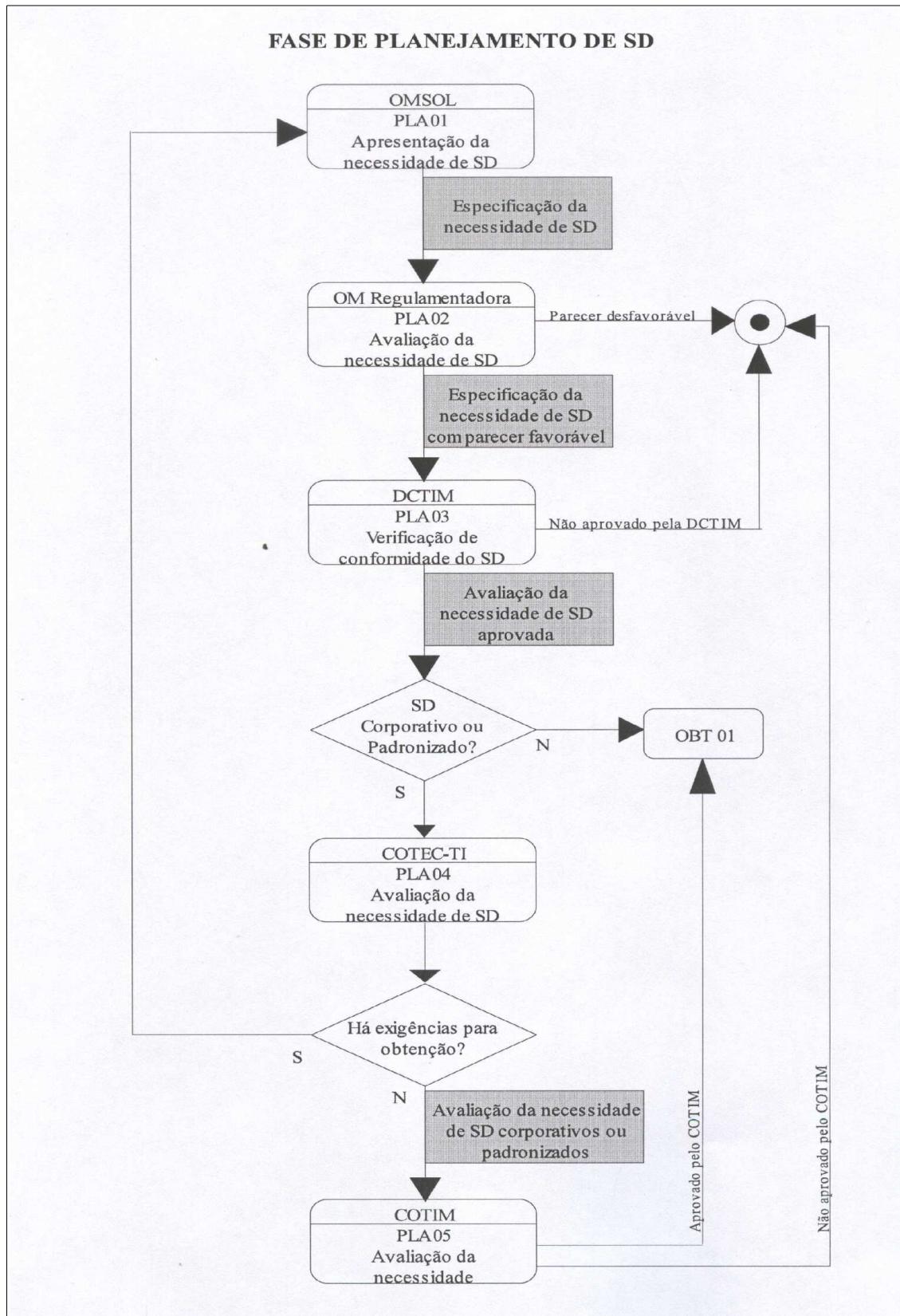
Bifurcação/junção

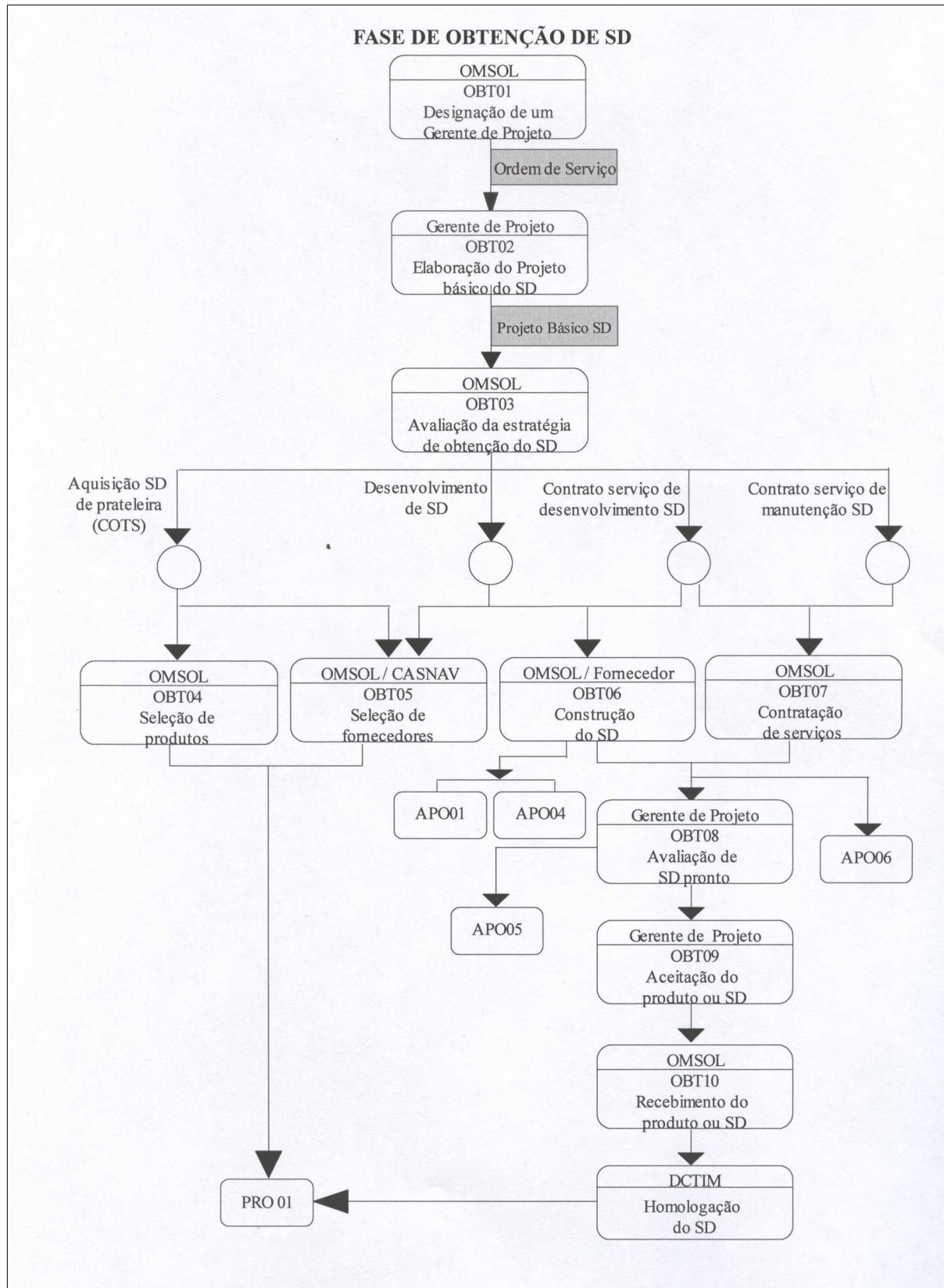


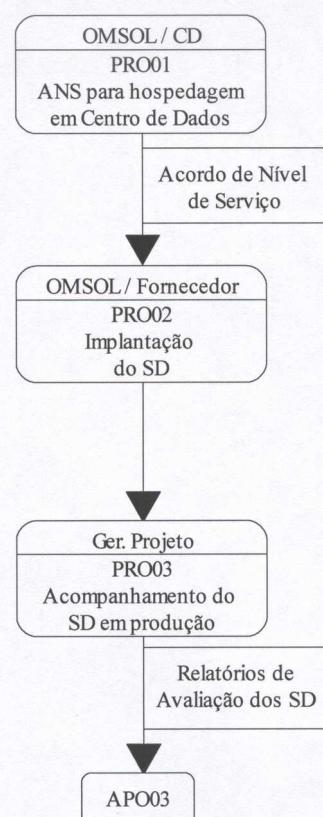
Fluxo

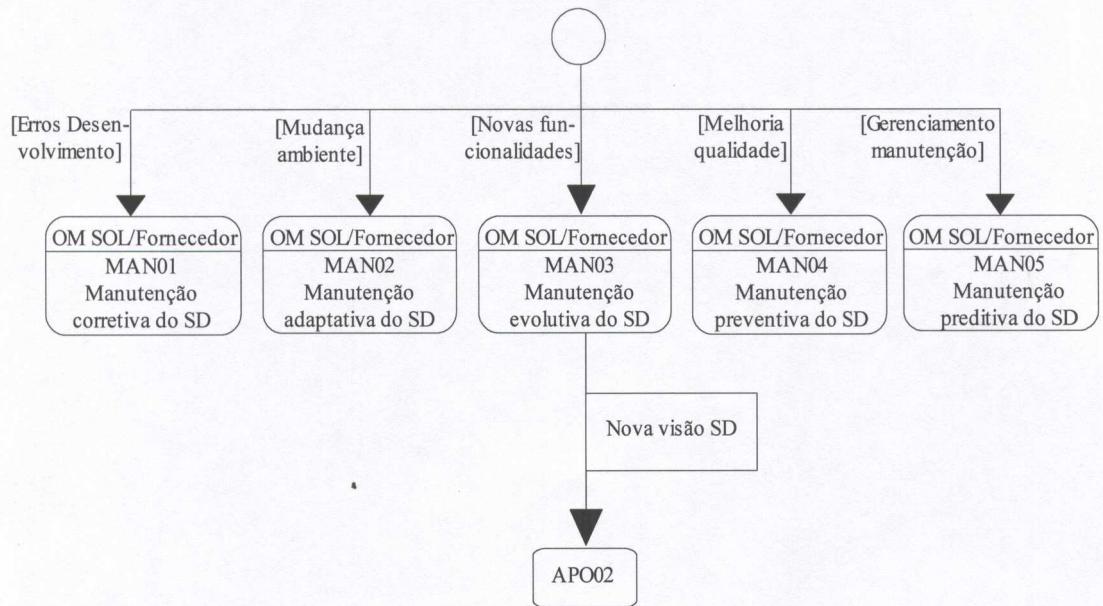


Saída



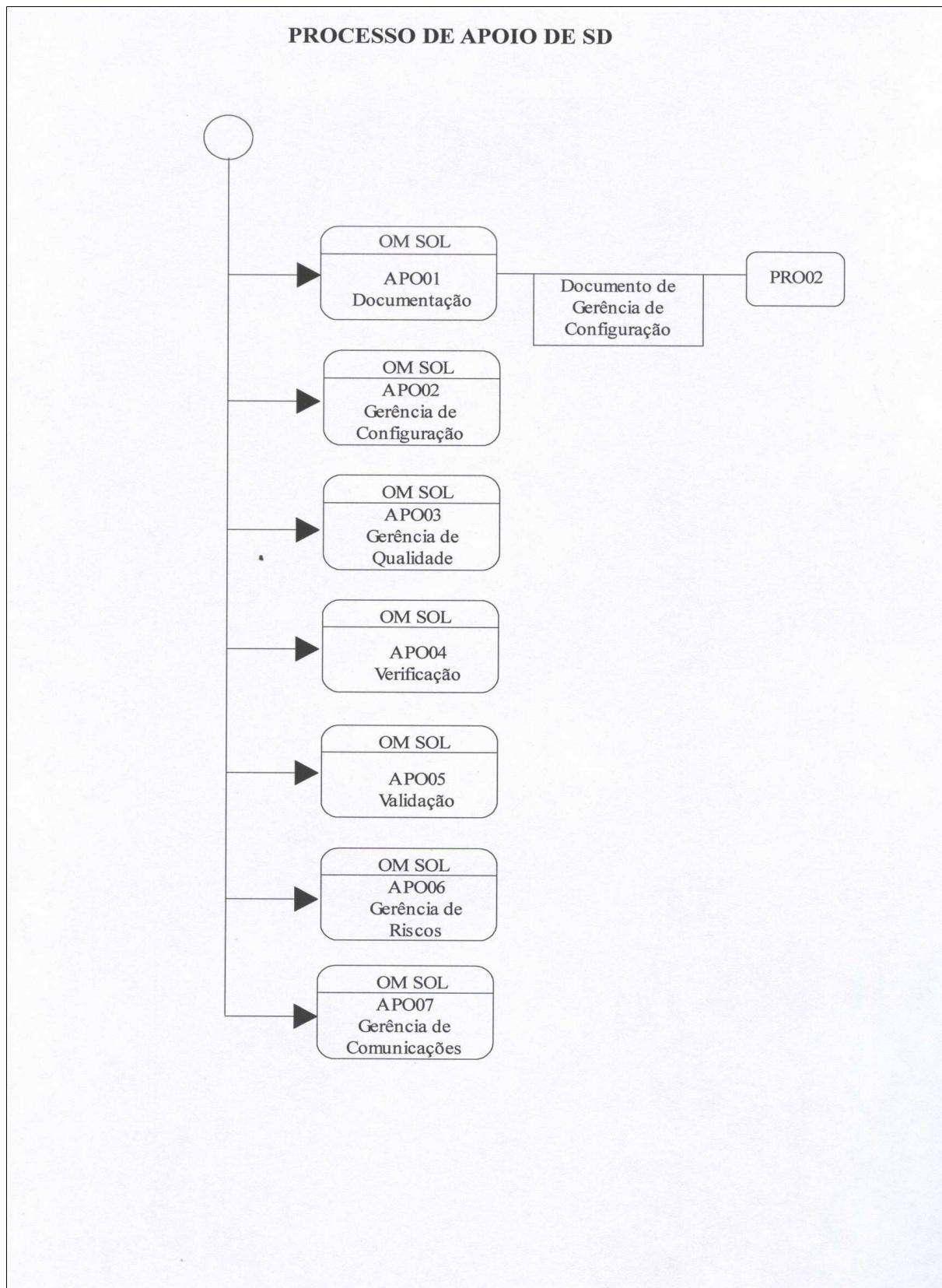


FASE DE PRODUÇÃO DE SD

FASE DE MANUTENÇÃO DE SD

FASE DE DESATIVAÇÃO DE SD





ANEXO C**MODELOS ESQUEMÁTICOS DO CICLO DE VIDA DE UM SÍTIO ELETRÔNICO**

C2 - FASE DE PLANEJAMENTO DE SÍTIOS ELETRÔNICOS

C3 - FASE DE PRODUÇÃO DE SÍTIOS ELETRÔNICOS

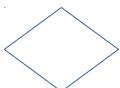
C4 - FASE DE IMPLANTAÇÃO DE SÍTIOS ELETRÔNICOS

Legenda

Atividade



Documento



Condição



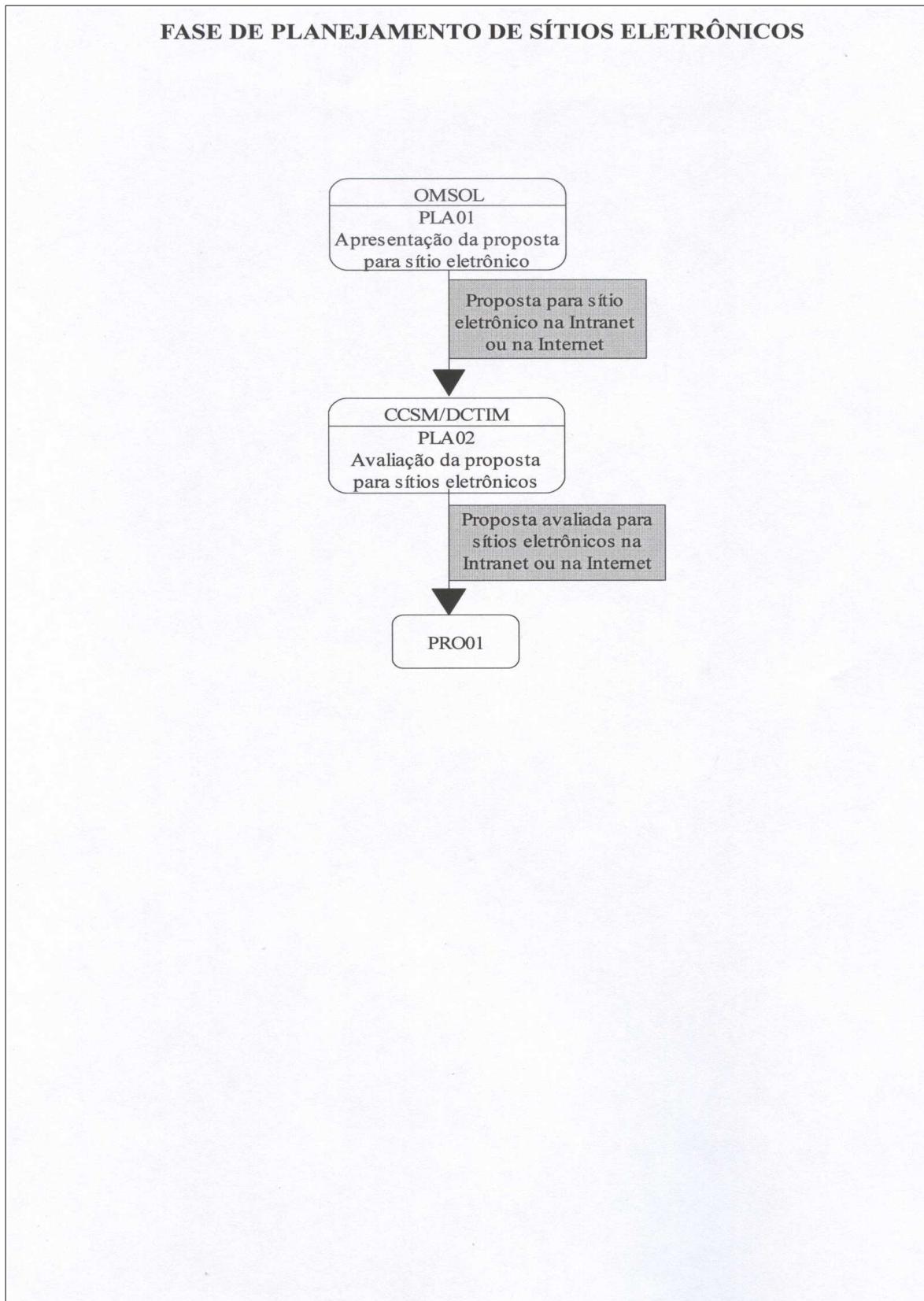
Bifurcação/junção

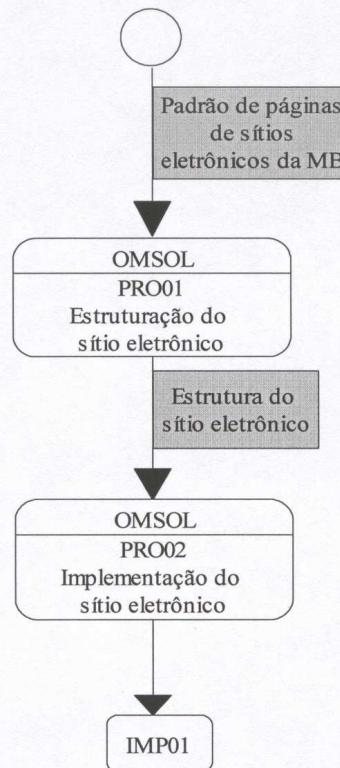


Fluxo



Saída



FASE DE PRODUÇÃO DE SÍTIOS ELETRÔNICOS

FASE DE IMPLANTAÇÃO DE SÍTIOS ELETRÔNICOS