ESCOLA DE GUERRA NAVAL

TECNOLOGISTA SENIOR III MAURÍCIO HAMOND REGUA

CUMPRIMENTO DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA MARINHA DO BRASIL

Rio de Janeiro
2021

TECNOLOGISTA SENIOR III MAURÍCIO HAMOND REGUA

CUMPRIMENTO DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA MARINHA DO BRASIL

Tese apresentada à Escola de Guerra Naval, como requisito parcial para conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CF (RM1) Fabiano R. Cantarino

Rio de Janeiro
Escola de Guerra Naval
2021

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por sempre permanecer ao meu lado, guiando-me, e incentivando-me, mantendo-me firme no meu objetivo.

À minha esposa Danusa Mariana e filhos, Roberta e Maurício, pelo grande carinho, apoio incondicional e compreensão de minhas ausências familiares para dedicação a este trabalho e ao Curso de Política e Estratégia Marítimas.

Aos meus pais por me darem as bases para a minha formação como ser humano, estarem presentes em cada etapa de minha vida e o apoio incondicional nos momentos difíceis.

Ao Capitão de Fragata (RM1) Fabiano R. Cantarino, meu orientador, pelo apoio acadêmico, incentivo, vibração e profissionalismo com que me orientou.

Ao Capitão de Fragata (RM1-T) Mário Roberto de Souza Lima, pela cordialidade, interesse e profissionalismo com que me concedeu as entrevistas fundamentais para o fechamento deste trabalho.

Ao Capitão de Mar e Guerra (RM1-MD) Victor Paulo Meirelles da Silva, pelo seu empenho e profissionalismo, pois sem essas competências seria impossível ter recuperado de uma forma tão rápida e positiva meu problema de saúde (para tratamento de SARS-CoV2). Ele foi não só um médico diferenciado como também um cuidador e amigo de todos os momentos, que me deu força e garantiu a vida para poder continuar nesta missão.

Aos Oficiais Alunos do Curso de Política e Estratégia Marítimas, pelos momentos de convivência e aprendizado, compartilhando conhecimentos e momentos de alegria.

Aos Instrutores pela preocupação, dedicação e compreensão.

À Escola de Guerra Naval pela excelente infraestrutura, pelo tratamento oferecido aos alunos e pela oportunidade de realizar trabalhos desta natureza em seu Curso de Política e Estratégia Marítimas de 2021.

RESUMO

A Marinha do Brasil demanda confiança na eficiência e na eficácia das informações e comunicações com as quais trabalha, para cumprir sua missão constitucional. Para tanto, cumpre um conjunto de normas de Segurança da Informação e Comunicações, assim como uma sistemática que objetiva a formação de uma mentalidade no cumprimento. Sob esse enfoque, estabelece-se este estudo de caso sobre a gestão da Segurança da Informação e Comunicações (SIC) na Marinha do Brasil, em que foram analisadas as práticas de controle, relacionados à SIC implementadas na instituição. A Segurança da Informação e Comunicações é um aspecto de extrema importância e que é tratado pela maioria das grandes organizações existentes. Sistemas eletrônicos e recursos tecnológicos utilizados atualmente como e-mails, internet, computadores, notebooks, softwares – são necessários para que as empresas e Organizações Militares se mantenham em um alto nível de produtividade e segurança. Neste trabalho, são feitas avaliações de conformidade da gestão da SIC nas Organizações Militares em relação às normas existentes na Marinha do Brasil, como também às normas ABNT NBR ISO/IEC 17799 – Tecnologia da Informação – Técnicas de segurança – Código de Prática para a Gestão da Segurança da Informação e à norma ABNT NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação. É nesse contexto que são apresentados os principais conceitos relacionados à SIC, bem como à sua gestão, fazendo uma análise/avaliação de como as práticas relacionadas ao assunto estão sendo geridas dentro das Organizações Militares e apresentando os resultados encontrados, enfatizando sua relevância, consolidando-se em uma preparação metodológica para futuros trabalhos de investigação.

Palavras-chave: Gestão da Segurança da Informação e Comunicações; Segurança da Informação e Comunicações, Tecnologia de Informação e Comunicações, Mentalidade no cumprimento das normas

ABSTRACT

The Brazilian Navy demands confidence in the efficiency and effectiveness of the information and communications with which it works, to fulfill its constitutional mission. Therefore, it complies with a set of Information and Communication Security standards, as well as a system that aims to build a compliance mentality. Under this approach, this case study is established on the management of Information and Communications Security (SIC) in the Brazilian Navy, in which the control practices related to the SIC implemented in this institution were analyzed. Information and Communications Security is an extremely important aspect that is handled by most large existing organizations. Electronic systems and technological resources currently used - such as e-mails, internet, computers, notebooks, software - are necessary for companies and Military Organizations to maintain a high level of productivity and security. In this work, conformity assessments of the SIC management in Military Organizations are carried out in relation to the existing standards in the Brazilian Navy, as well as to the ABNT NBR ISO/IEC 17799 standards - Information Technology - Security Techniques - Code of Practice for Management of Information Security and the ABNT NBR ISO/IEC 27002 – Code of Practice for Information Security Management. It is in this context that the main concepts related to SIC are presented, as well as its management, making an analysis/evaluation of how practices related to the subject are being managed within Military Organizations and presenting the results, emphasizing its relevance, consolidating in a methodological preparation for future research work.

Keywords: Information and Communications Security Management; Information and Communications Security, Information and Communications Technology, Compliance Mindset

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
API	*Application Programming Interface*
CEO	*Chief Executive Officer*
CGCFN	Comando Geral do Corpo de Fuzileiros Navais
CIO	*Chief Information Officer*
CLTI	Centro Local de Tecnologia da Informação
CFO	*Chief Financial Officer*
CN	Comunicações Navais
COMIMSUP	Comando Imediatamente Superior
ComOpNav	Comando de Operações Navais
COO	*Chief Operating Officer*
COTEC-TI	Comissão Técnica de Tecnologia da Informação da Marinha
COTIM	Conselho de Tecnologia da Informação na Marinha
CREDSEG	Credencial de Segurança
CTIM	Centro de Tecnologia da Informação da Marinha
DCTIM	Diretoria de Comunicação e Tecnologia da Informação da Marinha
DCTIMARIST	Instruções da DCTIM
DCTIMBOTEC	Boletim Técnico da DCTIM
DGMM	Diretoria Geral de Material da Marinha
DGPM	Diretoria Geral de Pessoal da Marinha
DGN	Diretoria Geral de Navegação
DPHDM	Diretoria do Patrimônio Histórico e Documentação da Marinha
ECIBER	Espaço Cibernético
EMA	Estado Maior da Armada
GRSIC	Gestão de Riscos em Segurança da Informação e Comunicações
ISIC	Instruções de Segurança da Informação e Comunicações
ISO	*International Organization for Standardization*
HRL	Histórico da Rede Local
MB	Marinha do Brasil
MD	Ministério da Defesa
NBR	Norma Brasileira
NC	Não Conformidade

NODAM	Normas Sobre Documentação Administrativa e Arquivamento na Marinha
ODS	Órgão de Direção Setorial
OM	Organização Militar
OSIC	Oficial de Segurança da Informação e Comunicações
PAD	Programa de Adestramento
PLCONT	Plano de Contingência
PSO	Plano de Segurança Orgânica
PETIM	Plano Estratégico de Tecnologia da Informação da Marinha
RAD	Relatório de Auditoria
RAI	Registros de Acesso à Internet
RECIM	Rede de Comunicações Integrada da Marinha
REI	Registros de Envio/Recebimento de E-Mail para Internet/ Intranet
RMI	Registros de Envio/Recebimento de Mensagens Instantâneas
SGM	Secretaria-Geral da Marinha
SI	Sistemas de Informação
SIC	Segurança da Informação e Comunicações
SICRL	Segurança da Informação e Comunicações da Rede Local
SISCOM	Sistema de Comunicações da Marinha
TI	Tecnologias de Informação
TIC	Tecnologia de Informação e Comunicações
VPN	*Virtual Private Network*

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Para prover a defesa e a integração de um país com dimensões continentais, vasto litoral e extensas vias interiores navegáveis, faz-se necessário possuir uma Força Naval pronta, atuante e moderna. Nesse contexto, em que não só as informações são imprescindíveis, mas também a rapidez e a confiabilidade com que elas circulam, a Segurança da Informação e Comunicações (SIC) assume papel crucial para o êxito das atividades exercidas pela Marinha do Brasil (MB).

Neste trabalho serão apresentados uma visão global da importância da mentalidade no cumprimento das normas de SIC na MB, os aspectos a serem abordados que a justificam, bem como o objetivo principal e os secundários a serem alcançados, abarcando as questões a serem investigadas, suas delimitações e a explanação acerca do estudo de caso sobre o fortalecimento da mentalidade de SIC nas Organizações Militares (OM) da MB.

A informação é um bem de suma importância em todas as áreas da atividade social humana. Para cumprir sua missão constitucional, a MB depende destes subsídios, que devem tramitar de forma precisa, célere, autêntica, sigilosa e oportuna. A Defesa da Pátria, a Segurança do Tráfego Aquaviário, o Ensino Profissional Marítimo e a Salvaguarda da Vida Humana no Mar são exemplos abrangentes das atribuições sustentadas pela instituição que demandam informações aquilatadas com as citadas características. A responsabilidade da MB na área nuclear, com o desenvolvimento de submarinos de propulsão por energia nuclear, também demanda informações com tais qualidades, configurando-se em outro exemplo, destarte mais específico, que impulsiona o setor estratégico para o crescimento militar e social de uma Nação, alavancando outras áreas e incluindo o Brasil em um grupo seleto de países em todo o mundo.

A sociedade moderna vive a chamada Era da Informação. A revolução da tecnologia da informação, mais especificamente com o desenvolvimento da Internet, provocou o surgimento de uma nova economia informacional, global e em rede (CASTELLS, 2005; p. 119).

Se por um lado, as organizações ganharam em facilidades no acesso e na troca de informações nunca antes vistas, por outro, ficaram expostas à ação de novas e perigosas ameaças que, das mais diversas formas e motivações, podem inviabilizar ou dificultar o cumprimento dos objetivos almejados.

A segurança, ou mais apropriadamente falando a proteção da informação, é hoje um importante mecanismo de gestão que as organizações devem incorporar às suas práticas,

não só para atender à legislação em vigor e às regulamentações impostas por órgãos regulatórios, mas para sua própria sobrevivência e concomitante cumprimento de suas missões.

No âmbito de pesquisa científica, sobressai-se ainda uma particularidade, pois além da informação, há que se proteger o conhecimento produzido. Exemplos disso são os segredos industriais e a propriedade intelectual que precisam ser preservados contra utilizações indevidas.

As Normas de Tecnologia da Informação da MB (DGMM-540), principal publicação normativa da MB no assunto, foram aprovadas em 12 de agosto de 2009, detalhando a RECIM sob a perspectiva de suas três principais áreas: Infraestrutura de Redes e Serviços, SIC e Desenvolvimento de Sistemas Digitais. Ressalta-se que a referida Publicação sofreu duas revisões: a primeira em 2017 e a terceira em 2019, na qual se enfatizaram as restrições quanto ao uso de dispositivos móveis e telefones celulares na MB.

De modo geral, a Tecnologia de Informação e Comunicações (TIC) tornou-se fundamental para as estratégias de grandes organizações e, nesse dinâmico contexto, inclui-se a Marinha do Brasil, em que 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 (C^2) de Forças Navais. Nesse 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 (*pen drives, Hard Disk* externo e cartões de memória) e de dispositivos móveis inteligentes (celulares, *tablets*, câmeras fotográficas e similares), criou diversas possibilidades para a exploração de vulnerabilidades das redes de computadores e ampliação da possibilidade de vazamento de dados sigilosos das instituições.

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 isso, 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 pelo qual a informação é compartilhada ou armazenada, é fundamental que ela seja sempre protegida adequadamente.

Nesse contexto, releva-se a importância da SIC, que se caracteriza como 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 o armazenam, o processam e o trafegam.

A SIC 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 necessários, 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.

A citada norma versa sobre a grande importância da segurança da informação, contendo indicações de requisitos e melhores práticas para a gestão da segurança da informação. Nela está explícito que a gestão da segurança da informação não deve ser tratada apenas pela área de TI, mas por todas as áreas da organização, notadamente pela alta Administração Naval. Deve ser uma decisão institucional, pois se ocorrer um incidente que leve a organização a um prejuízo ou a impeça de continuar a realizar suas atividades, será a Marinha do Brasil que perderá o investimento realizado ou terá sua imagem afetada.

Essa abordagem é condizente com os propósitos de governança corporativa, além de viabilizar a conscientização em segurança da informação, fazendo com que as práticas relacionadas façam parte das atividades de seus usuários.

1.1 Problema

Nas Organizações Militares (OM) da Marinha do Brasil, têm sido observados registros recorrentes de Não Conformidades (NC)[1] de SIC, causados inicialmente por possíveis inobservâncias das normas vigentes, o que pode comprometer o cumprimento da missão constitucional ou prejudicar o acesso às informações, o sigilo das operações, a disponibilidade de sistemas/meios e a imagem da instituição. Muitos desses registros são relacionados a uma questão de mentalidade de SIC.

Apesar dos inúmeros avanços tecnológicos conquistados no âmbito militar naval brasileiro, é preciso estar atento às ameaças e possíveis vulnerabilidades associadas a constante evolução. Uma das vulnerabilidades mais exploradas é o fator humano. Para MB, sendo justamente o pessoal que compõe o seu maior patrimônio, a preocupação em desenvolver as competências de sua força de trabalho nos misteres relacionados à SIC adquire extrema relevância. Assim, a Diretoria de Comunicação e Tecnologia da Informação da Marinha (DCTIM) vem realizando uma campanha de forma a ampliar e consolidar a mentalidade de segurança, ressaltando a importância do tema.

Essa afirmação se sustenta conforme registrado no Plano Estratégico de Tecnologia da Informação da Marinha (PETIM), publicado em 2015, como sua visão de futuro:

> "Ter reconhecida, internamente, a Governança de TI da MB como necessidade imprescindível para a consecução de todas as tarefas da MB, com níveis de excelência compatíveis com as tradições da Marinha, sejam elas no campo administrativo ou no operativo, além de ser reconhecida, externamente, dentro da Administração Pública Federal, por seu avanço tecnológico e nível de excelência" (PETIM, 2015)

O uso correto da informação é parte essencial no cumprimento das missões, devendo, portanto, ser adequadamente protegido. A MB provê diversos procedimentos e ferramentas sobre a importância de se protegerem as informações digitais que são trafegadas e armazenadas na Rede de Comunicações Integradas da Marinha (RECIM), mantendo, assim, alerta todos os usuários dos recursos computacionais e dos serviços disponibilizados pela Força.

A falta de informação geralmente é o que leva as pessoas a se comportarem de

[1]Não Conformidade (NC) é o não atendimento de um requisito. Quando uma empresa não opera de acordo com um dos itens de uma norma - ABNT NBR ISO 9001: 2015.

maneira inadequada. A organização deve orientar seus usuários devidamente, para evitar comportamentos que levam a incidentes, tais como sair de sua estação de trabalho deixando o computador ligado e habilitado para uso por meio de sua identificação, passar sua senha de identificação e acesso a outro colega, utilizar internet com finalidade pessoal, deixar documentos sigilosos soltos e esquecidos na impressora, portar dados confidenciais em dispositivos móveis, dentre outros (incidentes que poderiam ser evitados mediante uma boa orientação e a criação de um código de conduta ética para preveni-los). É importante que os recursos computacionais, ferramentas básicas para agilizar negócios e mostrar confiabilidade a clientes e parceiros, sejam utilizados de forma correta e segura, para evitar a perda de produtividade dos usuários, o congestionamento na rede de dados[2] e o risco de divulgação de informações sigilosas, entre outros prejuízos que podem ser causados à imagem da MB, da Organização Militar ou do próprio usuário[3].

A MB considera esse assunto preocupante e de caráter estratégico, portanto empenha-se disponibilizando programas, normas, cursos, equipamentos e materiais específicos para as atividades de SIC. No entanto, sabe-se que é imprescindível o esforço das OM em atender as orientações para dar a integridade necessária à Força, blindando-a de ataques digitais[4], desastres tecnológicos ou falhas humanas.

Em face do exposto, a justificativa do presente trabalho vem da premente necessidade de se analisar criticamente como está sendo conduzida a gestão da SIC nas Organizações Militares da MB.

1.2 Objetivo geral

O presente trabalho visa identificar e analisar os registros de não conformidades de SIC nas OM, por meio de um estudo de caso com foco nas publicações e orientações vigentes sobre o assunto em lide e à luz dos conceitos propostos, configurando-se como uma preparação metodológica para futuros trabalhos de investigação. Em face da vasta extensão da RECIM, este estudo se debruçará sobre uma amostragem significativa, centrando a análise sobre as atividades da gestão de SIC das OM da área do Rio de Janeiro e do Complexo de

[2] Uma rede de dados tem a função de interligar computadores e/ou conectá-los a outros dispositivos, permitindo que haja a circulação de informações, comandos e recursos entre eles.

[3] Um usuário ou utilizador é um agente, tanto um agente humano (usuário final) como um agente de software, que usa um computador ou serviço de rede.

[4] Uma iniciativa mal-intencionada e deliberada que pode ser executada por um indivíduo ou por uma empresa. Geralmente, o invasor busca algum tipo de benefício ao prejudicar a rede da vítima.

Mocanguê, em Niterói/RJ.

1.3 Objetivos específicos

Para atingir o objetivo geral, listam-se os seguintes objetivos específicos:

a) Apresentar uma compilação das fontes bibliográficas atualizadas sobre SIC da MB e caracterizar sua importância;

b) Apresentar os conceitos doutrinários e vigentes das atividades de SIC das OM da MB e realizar um levantamento de suas práticas formalmente estabelecidas;

c) Identificar e descrever as possíveis não conformidades em SIC nas OM da MB, decorrentes de registros de discrepâncias de inspeções ou auditorias, realizadas internamente ou pelos Centro Local de Tecnologia e Informações (CLTI) da área de jurisdição; avaliar a aderência dessas políticas junto aos usuários em suas atividades cotidianas; e verificar com os gestores da instituição (tomadores de decisão) as necessidades e demandas pertinentes ao assunto abordado; e

d) Analisar possíveis aspectos em que os resultados dos objetivos anteriores sejam convergentes e outros em que sejam complementares, buscando propor possíveis soluções de doutrinas nas estruturas voltadas para gestão de SIC na MB.

1.4 Metodologia

Segundo Fachin (2006):

> O método científico confere ao pesquisador inúmeras vantagens, oferecendo-lhe um conjunto de atividades sistemáticas e racionais, mostrando-lhe o caminho a ser seguido e permitindo-lhe detectar erros e auxiliando nas decisões. Sua aplicação correta proporciona segurança e economia, e permite obter conhecimentos eficazes, com qualidades essenciais à sua natureza (FACHIN, 2006, p.76).

Mediante a postura tomada pelo autor em questão, não é descabido afirmar que em se tratando de uma tese, a metodologia deve responder a quais etapas serão traçadas, preferencialmente dispostas em ordem cronológica, numeradas, especificadas, comportando, pois, todos os passos a serem desenvolvidos. Assim, esse planejar nos faz dar conta de que há uma previsibilidade do tempo gasto a ser utilizado – o que vai culminar na elaboração de um

cronograma cujas etapas se tornarão passíveis de se cumprir, contribuindo para que a execução do trabalho se dê de forma plena.

1.4.1 Estudo de Caso realizado nas Organizações Militares da MB

A metodologia de trabalho a ser utilizada abarcará pesquisas documental e exploratória que versem sobre o tema, e estudo de caso.

As referidas pesquisas inicialmente abrangerão, por meio de uma revisão das publicações citadas os dados mensuráveis relacionados à gestão da SIC na MB.

O estudo de caso contemplará a coleta de dado das seguintes fontes:

a) Visitas técnicas aos Centro Local de Tecnologia da Informação (CLTI) da área Rio de Janeiro e as OM de direções especializadas responsáveis pelas orientações de SIC na MB.

b) Questionário de SIC aos CLTI e as OM da MB; e

c) Entrevistas individuais, com militares e servidores civis que têm, ou já tiveram experiência em trabalhar na área da gestão da SIC, como Encarregados dos CLTI, Oficiais de Segurança da Informação e Comunicações (OSIC), administradores de rede local das OM, pessoal técnico das áreas de Tecnologia de Informação e Comunicações (TIC) e usuários das OM.

2 SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SIC) NA MB

Conforme descrito na publicação DGMM-540 (BRASIL, 2019[b]), a Segurança da Informação e Comunicações (SIC) na Marinha do Brasil (MB) apresenta um nível elevado de maturidade, pois existe uma preocupação clara e evidente por parte de todos os setores envolvidos nas atividades das Organizações. Existe uma política de segurança bem elaborada e alinhada ao código de conduta ética dos servidores militares e civis, bem como considera todos os colaboradores. A sua elaboração teve a participação de todas as áreas técnicas que constituem a instituição e com direto apoio do Comandante da MB e suas Organizações Militares (OM), além de possuir uma diretoria especializada para tratar dos assuntos relacionados a Tecnologia da Informação e Comunicações (TIC).

A MB possui inclusive um planejamento estratégico de tecnologia que estabelece o direcionamento, ações e os recursos da área de TIC, alinhado ao planejamento estratégico da instituição (Ibidem, p. 9-1).

A MB investe altos recursos financeiros na conscientização de seus servidores militares e civis acerca da SIC e na operação e gerência correta de seus sistemas. As capacitações existentes visam à divulgação da Política de SIC, treinamentos específicos e palestras (Ibidem, p. 9-1). Existem cursos de SIC disponíveis para todos os profissionais da área no Centro de Instrução Almirante Wandenkolk (CIAW) e o Centro de Instrução Almirante Alexandrino (CIAA), com a tarefa de ministrar Cursos de Especialização e de Aperfeiçoamento, em nível de pós-graduação, e de outras modalidades, para Oficiais e Praças, respectivamente.

A Segurança da Informação e Comunicações (SIC) prevê ações que objetivam viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade de dados e informações de forma a minimizar os incidentes de segurança da informação. Adicionalmente, outras propriedades, tais como responsabilidade, não repúdio e confiabilidade podem também estar envolvidas (BRASIL, 2019 [b]).

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 garantirem os seus requisitos básicos:

a) Disponibilidade – informação digital deve estar disponível para alguém autorizado a acessá-la no momento próprio;

b) Integridade – informação digital somente pode ser modificada por alguém autorizado;

c) Confidencialidade – informação digital somente pode ser acessada por alguém autorizado; e

d) Autenticidade – capacidade da origem da informação digital ser aquela identificada.

A manutenção das propriedades e dos aspectos da informação depende do estabelecimento de uma Gestão da Segurança da Informação. Pode-se observar a relação entre o ciclo de vida da informação (um dado é gerado, permanece disponível pelo tempo necessário, passa por atualizações e, depois, ao perder sua serventia, deve ser descartado adequadamente) e suas propriedades na figura 1.

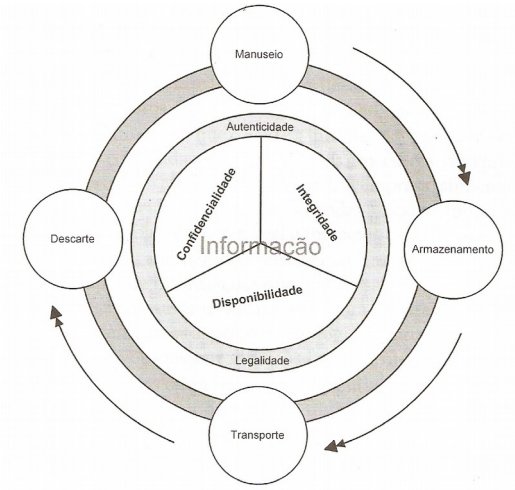


Figura 1 – Ciclo de vida da informação de acordo com Sêmola (2003).

2.1 Evolução da Segurança da Informação

No contexto da Revolução Industrial, que teve início no século XVIII na Inglaterra e alcançou seu auge no século XIX, quando se espalhou pelo mundo, desenvolveu-se o conceito de cultura de massa, em que máquinas começaram a ser usadas em atividades que antes eram feitas de forma braçal. Teve início, então, a interação em escala do homem com artefatos e engenhos autômatos, em que grande parte do trabalho humano repetitivo foi sendo gradativamente substituído por máquinas, que eram mais velozes que os seres humanos

e geravam produtos com maior qualidade. Nessa época, o ativo de maior valor era o capital, o que fez crescer o capitalismo comercial e mercantil, alavancando a disseminação de informações entre continentes e elevando a interação entre as nações. Aos poucos a informação foi ganhando valor, principalmente durante a Terceira Revolução Industrial (RED HAT, 2005), quando as indústrias e organizações comerciais começaram a vivenciar a importância de proteger suas informações, pessoais, processuais e financeiras, em prol do desenvolvimento de projetos alinhados com estratégias que colocavam as organizações ou países em vantagem competitiva no mercado.

A partir dos anos 80, com o advento da internet, começaram a ocorrer aumentos exponenciais da vulnerabilidade de acesso indevido, com diversas formas de captação das informações. Esse crescimento acelerado se deu em função do número cada vez maior de pessoas utilizando computadores e interagindo em uma rede mundial, transcendendo as barreiras geográficas e as fronteiras geopolíticas, o que impulsionou o fenômeno da globalização (o que, por sua vez, interagiu com e alterou todas as áreas de conhecimento e relacionamento humano). Isso demandou também um crescimento nas empresas dos setores de segurança da informação, levando cada vez mais as empresas e países a buscarem o fortalecimento de seus sistemas, bem como profissionais para esse setor. No escopo da segurança, desenvolveram-se o setor de coleta de informações e a inteligência competitiva, estudando os pontos fracos dos sistemas. Desde o início do século XX ficou patente a assertiva de que quem possui informação detém o poder, pois é esta que estrutura o conhecimento. Logo, quem consegue proteger de forma segura essas informações, provê vias para que as missões das instituições sejam alcançadas. Por isso, a título de exemplo, vê-se que organizações financeiras, que objetivam lucros para seus clientes e acionistas, têm o mesmo cuidado com suas informações que organizações militares, que buscam a Defesa da Pátria e dos interesses da Nação.

2.1.1 Como surgiu a Segurança em Computadores?

O filme "Jogos de Guerra"[5] tornou-se um ícone da indústria cinematográfica não por acaso. Nele, o ator Matthew Broderick faz o papel de um estudante colegial que, ao invadir o supercomputador do Departamento de Defesa dos Estados Unidos da América (*Department of Defense - DoD*), quase causa um confronto nuclear de proporções globais. No filme, Broderick acessa, via modem, o servidor do DoD e começa a brincar de jogos com o software de Inteligência Artificial que controla o computador que, por sua vez, controla todas

[5] https://www.planocritico.com/critica-jogos-de-guerra-1983/ Acesso em: 29 jul. 2021.

as bases de lançamento de mísseis nucleares. Lançado em 1983, portanto estreado durante a "Guerra Fria"[6], o filme tornou-se logo um sucesso. E inspirou muitas pessoas e grupos, mundo afora, a implementar métodos semelhantes aos utilizados pelo protagonista para acessar sistemas restritos, inclusive o que é conhecido como "*war dialing"* - um método de busca de números de telefone para conexões de modem analógicos em uma combinação de determinado prefixo de área e prefixo de telefone[7] (RED HAT, 2005).

Em fevereiro de 1995, o estadunidense Kevin Mitnick, *cracker* mais procurado do mundo, foi preso pelo FBI (*Federal Bureau of Investigation*) por ter invadido várias contas de computador e realizado acessos não autorizados, causando vultosas perdas da às empresas Nokia, NEC, Sun Microsystems, Novell, Fujitsu e Motorola, estimadas em cerca de US$ 80 milhões[8]. Na época, Mitnick, que utilizava *engenharia social* com maestria para conseguir roubar senhas e falsificar credenciais, foi proibido de usar computadores ou prestar qualquer serviço relacionado a computadores até 2003. Após cumprir sua pena, Mitnick se tornaria um requisitado consultor de segurança da informação (Ibidem, p. 1).

De acordo com Red Hat (2005), devido à crescente demanda de comunicação em rede, que levou à alta exposição de informações restritas, como pessoais e financeiras, em redes públicas, a segurança da informação teve que evoluir. O alcance da Internet foi um dos fatores mais importantes, pois exigiu que gestores e desenvolvedores despendessem um esforço intenso na segurança de dados.

Voltando aos primórdios da comunicação, encontram-se vários relatos históricos sobre a tentativa do ser humano em proteger informações. Há relatos que datam de quatro mil anos atrás sobre o uso da criptografia em inscrições na tumba de um grande chefe egípcio.[9]

Aumentando-se a necessidade de registro e comunicação de informações ao longo da História, elevaram-se também as formas de se proteger essas informações.

Buscando-se um evento de proporções mundiais, chega-se à Primeira Grande Guerra.

Em janeiro de 1917, criptoanalistas estadunidenses decifraram uma mensagem criptografada enviada pelo ministro das Relações Exteriores da Alemanha ao presidente mexicano, em que avisava que os alemães iniciariam uma guerra submarina irrestrita em fevereiro e que o México deveria, com a ajuda alemã, atacar os EUA e também convencer os japoneses a

---

[6]A Guerra Fria foi responsável pela polarização mundial e, entre 1947 e 1991, desencadeou uma série de pequenos conflitos como resultado da disputa entre EUA e URSS. Disponível em: < https://brasilescola.uol.com.br/historiag/guerra-fria.htm> Acesso em: 29 jul. 2021.

[7] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=585867 Acesso em: 29 jul. 2021.

[8]http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/ch-sgs-ov.html#:~:text=Mais%20de%2010%20anos%20depois,a%20dispositivos%2C%20que%20resultaram%20em Acesso em: 29 jul. 2021.

[9] http://www.cypher.com.au/crypto_history.htm. Acesso em: 29 jul. 2021.

fazerem o mesmo. Em abril, os então neutros EUA declararam guerra à Alemanha, que em 1918 estaria derrotada[10] (Op. cit., p. 1).

Avançando-se até a Segunda Guerra, um mecanismo eletromecânico de cifras que criptografava o texto, inicialmente criado para proteger transações bancárias, ficou famoso: a Enigma. Foi utilizado pelas Forças Armadas alemãs. O matemático britânico Alan Turing desenvolveu um método para quebrar os códigos da Enigma, possibilitando às forças aliadas desenvolver a Colossus, uma máquina que recebeu créditos por findar a guerra um ano antes[11] (Op. cit., p. 2).

Como descrito por Red Hat (2005), de forma bem sintética e exemplificadora, podem ser citados os seguintes fatos relativos às últimas quatro décadas do século XX e alvorecer do século XXI[12]:

– Nos Anos 60, o DoD criou a Rede da Agência de Projetos de Pesquisa Avançada (*Advanced Research Projects Agency Network* - *ARPANet*), advento para intercâmbio eletrônico de informações e dados acadêmicos, que logo se popularizou (gênese da Internet). Naquela década, sistemas operacionais, como o Unix, e linguagens, como o C, são desenvolvidos.

– Nos Anos 70 é desenvolvido o protocolo Telnet, uma extensão pública da ARPANet. Além disso, Steve Jobs e Steve Wozniak fundam a Apple Computer e começam a vender o computador pessoal (*Personal Computer* - PC).

– Nos Anos 80, a IBM desenvolve e comercializa PC economicamente mais acessíveis para o público em geral. Surge o protocolo combinado TCP/IP, tornando-se o padrão para toda a comunicação via Internet de hoje. Os EUA criam a Equipe de Resposta a Emergências de Computador (*Computer Emergency Response Team* - CERT), para alertar usuários das questões de segurança em redes.

– Nos Anos 90, a ARPANet é desativada, sendo seu tráfego transferido para a Internet. O Linux é criado, padrão aberto para desenvolvedores UNIX, para utilização com o sistema operacional GNU. O navegador (browser) gráfico é criado e estimula uma demanda exponencialmente alta por acesso público à Internet. *Crackers*[13] que dão golpes milionários começam a ser presos. Satélites ingleses de comunicação são tomados e controlados por

[10] *Ibidem -vocábulos de origem latina usados em notas bibliográficas e citações, de forma a evitar a repetições das fontes citadas numa primeira referência completa.*
[11] http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/ch-sgs-ov.html#:~:text=Mais%20de%2010%20anos%20depois,a%20dispositivos%2C%20que%20resultaram%20em Acesso em: 29 jul. 2021.
[12] *Ibidem - -vocábulos de origem latina usados em notas bibliográficas e citações, de forma a evitar a repetições das fontes citadas numa primeira referência completa.*
[13]Cracker, cráquer ou ciberpirata é o termo usado para designar o indivíduo que pratica a quebra de um sistema de segurança de forma ilegal ou sem ética.

criminosos desconhecidos, durante determinado tempo antes de retornarem para o controle do governo britânico.

– A partir de meados da década de 1990, a grande expectativa gerada no mundo sobre o denominado “Bug do Mlênio (Y2K)”. Os sistemas desenvolvidos no século XX guardavam e interpretavam as datas com 02 dígitos no ano e isso poderia fazer com que os sistemas reconhecessem o ano 2000 como 1900.

– No início dos Anos 2000, mais especificamente em fevereiro de 2000, um ataque de negação de serviço distribuído (*Distributed Denial of Service - DDoS*), de autoria desconhecida, afetou empresas gigantes da internet, como yahoo.com, cnn.com e amazon.com, bem como órgãos governamentais como fbi.gov e vários outros sites completamente inacessíveis para usuários normais.

Chegando-se ao novo milênio, constata-se que aproximadamente 945 milhões de pessoas usam a Internet ao redor do mundo, ao mesmo tempo (*Computer Industry Almanac*, 2004). Obviamente, o número de incidentes aumentou exponencialmente, como pode ser visto nos dados a seguir, correspondentes ao presente século:

– Em um dia qualquer de 2002, ocorriam cerca de 225 grandes incidentes de exploração de vulnerabilidades ao redor do mundo, reportados ao Centro de Coordenação da CERT, na Universidade Carnegie Mellon[14].

– O número de incidentes reportados à CERT saltou de 52.658 (em 2001) para 82.094 (em 2002). E depois para 137.529 (em 2003)[15].

– Segundo relatório da empresa McAfee, de fevereiro de 2018, o Brasil perdia US$ 10 bilhões por ano com cibercrime, cifras que colocavam o país entre os maiores centros de atividades virtuais ilícitas; e os prejuízos mundiais eram estimados em US$ 608 bilhões.

Nesse cenário, a segurança digital tornou-se uma despesa fundamental em todos os orçamentos de TI, para garantir a confiabilidade de seus sistemas, serviços e informações, que são necessários para sobrevivência e para o sucesso das empresas e instituições.

A segurança de sistemas e redes é uma tarefa difícil, que requer profissionais atualizados e cuidadosos, assim como investimento em soluções adequadas ao negócio e evolutivas. Neste escopo, a demanda pelo entendimento dos processos da empresa, a capacitação dos mantenedores e o convencimento dos colaboradores são condições primordiais para a implementação de um plano de segurança apropriado (Op. cit., p. 2).

2.2 Histórico de SIC na MB

[14]Fonte: http://www.cert.org. Acesso em: 30 jul. 2021.
[15]Fonte: http://www.cert.org/stats/ Acesso em: 30 jul. 2021.

Segundo descrito por Amaro (2010), o culto às tradições navais e à memória de personagens históricos que bem serviram ao país são traços marcantes do protocolo social da Marinha; mantendo sob harmônico equilíbrio a postura conservadora e o perfil inovador, motivado pela necessidade de uma Marinha moderna. Valores permanentes que incentivam a aquisição de conhecimento e o progresso intelectual daqueles que integram as tripulações das diferentes OM, bem como a evolução tecnológica dessas unidades organizacionais, no sentido de buscar sempre maior eficiência e qualidade no exercício das atividades-fim a elas atribuídas.

Movida historicamente por esse perfil, a Marinha tem um legado de participações relevantes no cenário nacional de tecnologia e, em particular, no contexto da TI. Na década de 60, tornou-se o primeiro órgão público da esfera federal a operar um sistema automatizado de informação, implantado na então Diretoria de Intendência da Marinha (DIM), com o propósito de processar o Sistema de Pagamento de Pessoal (SISPAG), um aplicativo desenvolvido por profissionais da própria Força e executado na plataforma *mainframe*.

Ainda de acordo com Amaro (2010), naquela época, não havia na MB nenhuma OM com a missão de orientar o emprego corporativo dos recursos de processamento de dados e, por sua iniciativa inovadora, este papel durante algum tempo foi naturalmente desempenhado pelo setor da Intendência, ramo que nas corporações militares é tradicionalmente responsável pela gestão de atividades de apoio logístico-administrativo. Voltadas para as auditorias e operações contábeis-financeiras, para o controle orçamentário, a organização documental e a provisão, armazenamento e distribuição de itens diversos de material, equipamentos e gêneros alimentícios.

Com decisões nitidamente centradas em questões de infraestrutura, o Centro de Processamento de Dados (CPD) da DIM era o ambiente de atuação característico das equipes de TI da MB (melhor dizendo, das equipes de processamento de dados) e os técnicos nele lotados tinham como foco o controle do sistema computacional e da operação dos dispositivos de hardware instalados para a execução de programas normalmente processados de modo sequencial e organizados em lotes de instruções, no estilo característico de processamento batch (AMARO, 2010).

No cenário assim configurado, os intendentes que se sucederam na função de chefe do CPD da DIM não tinham participação ativa nos processos de negócio daquela OM mas, concentrando-se em prover o suporte tecnológico para processar o SISPAG, conheciam profundamente cada aspecto da infraestrutura que operava sob sua responsabilidade.

Os sistemas – em sua maioria, soluções com perfil logístico-administrativo – eram desenvolvidos e mantidos por OM da Intendência e do setor de Pessoal, utilizando-se força de trabalho interna (analistas e programadores civis e militares da MB). Por cerca de quinze anos, esse quadro teve poucas alterações em termos de orientação corporativa da TI, em que que o surgimento de mainframes com maior capacidade de processamento e de armazenamento de dados provocou várias "ondas" de atualização para expansão das configurações utilizadas pela MB, sempre com ênfase em elementos de hardware e software, componentes da infraestrutura tecnológica.

Em paralelo, o avanço de soluções baseadas em microcircuitos e as necessidades de modernização do ambiente a bordo dos navios para subsidiar decisões de C^2 apontaram para a transformação dos navios de guerra em verdadeiras plataformas flutuantes de TI, em que cada atividade está associada a dados oriundos de equipamentos eletrônicos integrados a sistemas de informação e sensores inteligentes.

Tornou-se, então, evidente a convergência entre as soluções requeridas para o avanço tecnológico das OM da área operativa da MB e o emprego de recursos de processamento de dados (área de conhecimento que, posteriormente, viria a ser referenciada pela consagrada denominação informática). Em 1975, foi criado o Instituto de Processamento de Dados da Marinha (IPDIM), ativado sob a subordinação do EMA como a primeira OM da MB que teve missão especificamente (AMARO, 2010).

Em que pese a ausência de uma metodologia específica e a inexistência de estruturas formais de decisão, pode-se afirmar que a governança de TI da MB deu seus primeiros passos – com acertos e equívocos – a partir da estrutura assim definida. Os aplicativos construídos para atender a demandas do setor operativo somaram-se aos sistemas de emprego logístico-administrativo e o efetivo de pessoal especializado em TI aumentou de modo significativo, incluindo praças e oficiais oriundos de diferentes Corpos e Quadros da MB. Nos anos 80, estabeleceu-se um cenário em que quatro CPD da MB funcionavam interligados e com equipes dedicadas à operação dos recursos da plataforma mainframe sob a supervisão do IPDIM. As ações empreendidas por esse Instituto concentraram-se na definição de um conjunto-padrão de componentes para a infraestrutura operacional de TI (sistemas operacionais, gerenciadores de banco de dados, linguagens de programação, sistemas de rede local) e em iniciativas destinadas a padronizar o processo de desenvolvimento de software (*Ibidem, p.9*).

O IPDIM ocupava-se também em orientar o recrutamento, a seleção e a capacitação de pessoal (militares e civis) especializado em informática. Assim, a decisão de autorizar cursos de formação, especialização, mestrado e doutorado era centralizada no

IPDIM, OM orientadora técnica instituída para a área de informática.

Considerando-se os arquétipos enunciados por Weill e Ross (2006), o modelo desenhado para a governança de TI que vigorava então na MB assemelha-se ao estilo monarquia de TI, identificado pelo estágio 1 mostrado na Figura 2. Esse modelo foi caracterizado pela acentuada centralização por parte de líderes técnicos com relação à participação e à efetiva tomada de decisão concernente aos princípios de TI, à arquitetura, à infraestrutura, às aplicações e também à priorização de recursos. A visão estratégica do emprego da TI não teve um peso expressivo como direcionador da governança desta área e as unidades de negócio não tinham representatividade no correspondente processo de tomada de decisão (AMARO, 2010).

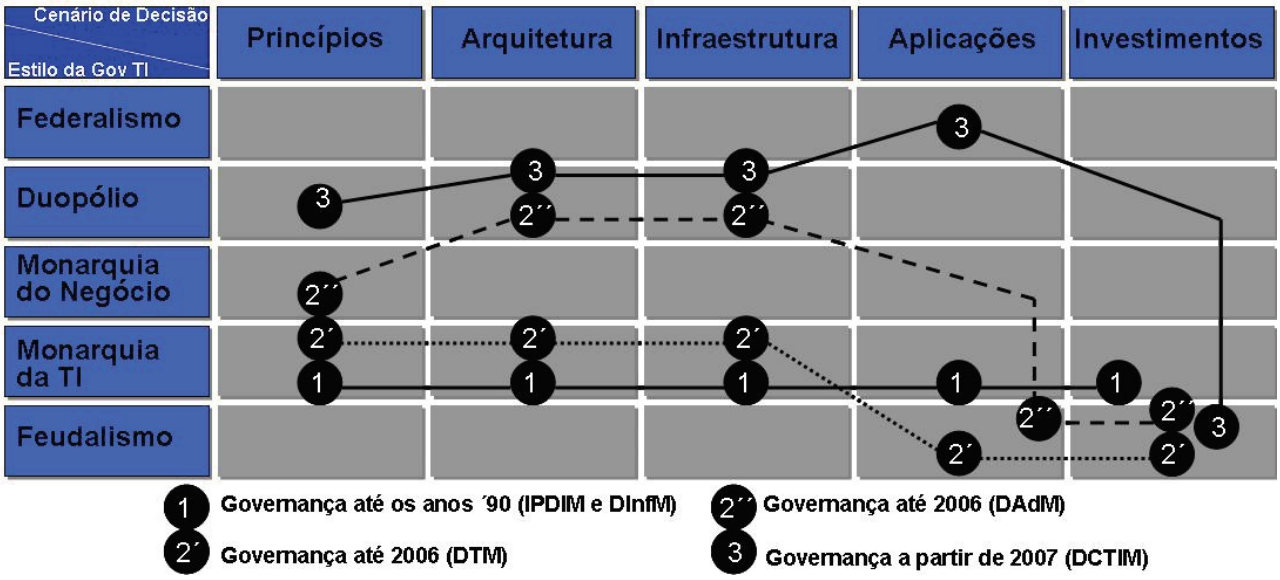


Figura 2 Mapa evolutivo dos modelos de governança de TI
Fonte: (AMARO, 2010).

No final dos anos 80, o IPDIM teve seu nome alterado para Diretoria de Informática da Marinha (DInfM), mas os estilos de governança não sofreram mudanças significativas até a década seguinte, quando a MB vivenciou uma peculiar cisão entre o que se convencionou chamar na corporação de informática administrativa e informática operativa. Explicando-se a partir de uma visão simplificada, pode-se dizer que a informática administrativa referia-se aos cenários de TI relacionados, principalmente, a necessidades ditadas por atividades-fim afetas aos setores da Intendência (ODS SGM), do Pessoal (ODS DGPM) e do Material (ODS DGMM). Em moldes semelhantes, a informática operativa dava o norte para as soluções desenvolvidas por institutos e centros de análises de sistemas pertencentes à estrutura organizacional do EMA e dos ODS ComOpNav/DGN e CGCFN (AMARO, 2010).

Em decorrência das duas formas admitidas para a TI corporativa, a DInfM foi extinta e as tarefas que então caracterizavam a governança de TI na MB saíram na esfera do EMA (nível 2 do organograma naval) e foram delegadas a duas OM do nível 4: a Diretoria de Administração da Marinha (DAdM) – subordinada ao ODS SGM – e a Diretoria de Telecomunicações da Marinha (DTM), OM criada naquela oportunidade, sob a égide do ODS DGMM. Desta forma, a DAdM, além de suas atribuições principais, ficou também responsável pela TI administrativa e à DTM coube a orientação da TI operativa, bem como a gestão dos recursos tecnológicos, serviços e projetos relacionados a necessidades requeridas para o pleno emprego das comunicações navais (redes e enlaces de dados, circuitos de voz criptografados etc).

Na tentativa de se estabelecer um conceito mais abrangente, Amaro (2010) observa que após a implantação desta nova conjuntura (correspondente aos estágios 2′ e 2′′ mostrados na Figura 2) os estilos de governança de TI até então praticados na MB foram sofrendo alterações, com algumas distinções marcantes entre os arranjos finais dos cenários definidos com ênfase nas necessidades de emprego operativo e na utilização logística-administrativa da TI. No primeiro caso (DTM como órgão de governança), o estilo monarquia de TI se manteve para as decisões da maior parte dos domínios considerados. No tocante às aplicações e aos investimentos (priorização), este regime foi substituído pelo feudalismo, reforçado pela premência por soluções locais e pela autonomia de gestão que as unidades de negócio possuem.

Com relação à governança exercida sob a coordenação da DAdM, o estilo da monarquia de TI foi gradualmente evoluindo para o duopólio nas decisões sobre arquitetura e infraestrutura e em 2005, pela primeira vez na MB, foi formalmente constituída uma comissão – denominada COPAI (Comissão Permanente para a Arquitetura da Informação) – para decidir sobre esses cenários, reunindo líderes locais de TI e representantes das OM do setor SGM.

Em razão dos excelentes resultados que esta comissão produziu ao longo dos anos, imprimindo maior sinergia entre líderes de TI de uma unidade e seus pares nas diferentes OM envolvidas, a COPAI tornou-se um padrão de fato na MB e hoje a maioria dos ODS possui comitês semelhantes a este, implantados para orientar a tomada de decisão da TI setorial.

Contudo, até a adoção dessa estrutura pelos demais ODS, a discussão sobre temas relevantes para a TI corporativa restringia-se a equipes da DAdM e da DTM e o posicionamento dos gestores de TI (setoriais e locais) refletia uma perspectiva predominantemente operacional, desviada da estratégia traçada para suas OM e pouco atenta ao comportamento que seus usuários esperavam da TI local (*Ibidem*).

Com autonomia para usar recursos financeiros a fim de adquirir ou desenvolver soluções próprias de TI, a maior parte das OM, mesmo incentivadas no sentido de adotar estruturas mistas para compartilhar as decisões entre a TI e o negócio e adequarem-se ao modelo instituído como prática de governança no setor SGM, continuavam a decidir de modo feudal e descentralizado, notadamente sobre os investimentos e aplicações de TI necessárias para suportar sua atividade-fim.

Apesar da evolução observada quanto ao entendimento comum acerca da contribuição que a TI pode prestar às diversas atividades-fim definidas para a MB e do sucesso de iniciativas promovidas pelo setor logístico-administrativo (ODS SGM), o estilo feudal de governança permaneceu inalterado nas decisões de aplicações e investimentos, tanto para o emprego administrativo da TI, como para sua aplicação no contexto das necessidades operativas da Marinha. O setor SGM perseverou no esforço de estabelecer uma arquitetura de dados comum e implantou na Diretoria de Finanças da Marinha (DFM) a primeira instalação Centro de Dados operada na MB com base nas orientações *Information Technology Infrastructure Library* (ITIL) e destinada ao uso compartilhado da infraestrutura, decisão típica do estilo federalista.

Segundo descreve Amaro (2010), atenta às dificuldades trazidas pela fragmentação da TI em administrativa e operativa, que gerou conflitos de responsabilidade e estabeleceu algumas áreas de indefinição quanto à competência normativa, a Alta Administração Naval determinou, em 2007, a criação de um grupo de trabalho no âmbito do EMA reunindo representantes de todos os ODS com o propósito de elaborar um estudo visando preparar a Marinha para a implantação de uma estrutura de governança de TI de abrangência corporativa, à qual cada ODS e respectivas OM subordinadas deveriam se adequar. O próximo tópico descreve o funcionamento dessa estrutura. Pela comparação visual com as estruturas anteriores, mostradas na Figura 3, observa-se que a evolução dos modelos de governança de TI reposicionou no segundo nível mais alto da organização o arranjo responsável pelas decisões da TI corporativa (COTIM). A ilustração mostra também as principais unidades de negócio que no estágio atual desenvolvem ou mantém sistemas de informação (*Ibidem*).

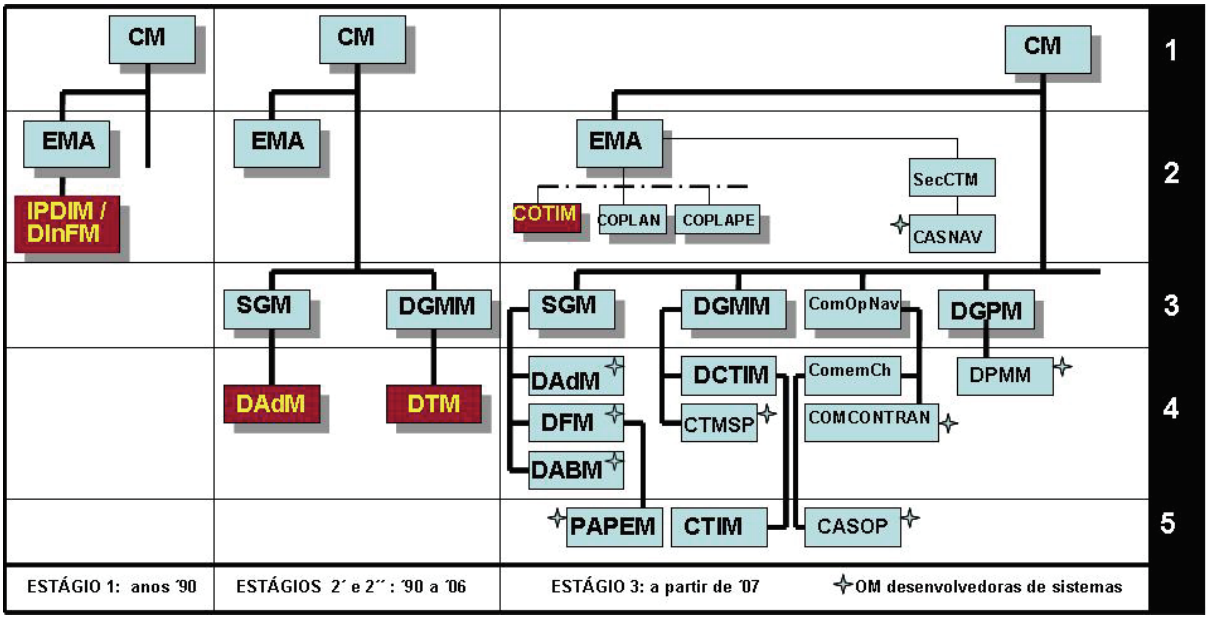


Figura 3 Comparação entre estruturas de governança de TI da Marinha do Brasil
Fonte: (AMARO, 2010).

3 GESTÃO DE SIC NA MB

Este capítulo foi concebido com o propósito de apresentar uma extensa reunião de dados, sobre a consciência situacional e a regulamentação de Gestão da Segurança da Informação e Comunicações da Marinha do Brasileira. Como constatado, não podemos alegar falta de gestão de normas e documentos regulatórios endereçada as suas Organizações Militares da MB e sua assertividade no gerenciamento.

3.1 Estrutura Organizacional e de proteção de TI

O organograma mostrado na Figura 4 transmite a noção da complexidade organizacional da Marinha. No topo da hierarquia (nível 1), situa-se o Comandante da Marinha (CM), assistido diretamente por seu gabinete de comando (GCM) e estruturas como o Centro de Inteligência da Marinha (CIM), a Procuradoria Especial da Marinha (PEM), a Secretaria da Comissão Interministerial para Recursos do Mar (SECIRM) e o Centro de Comunicação Social da Marinha (CCSM).

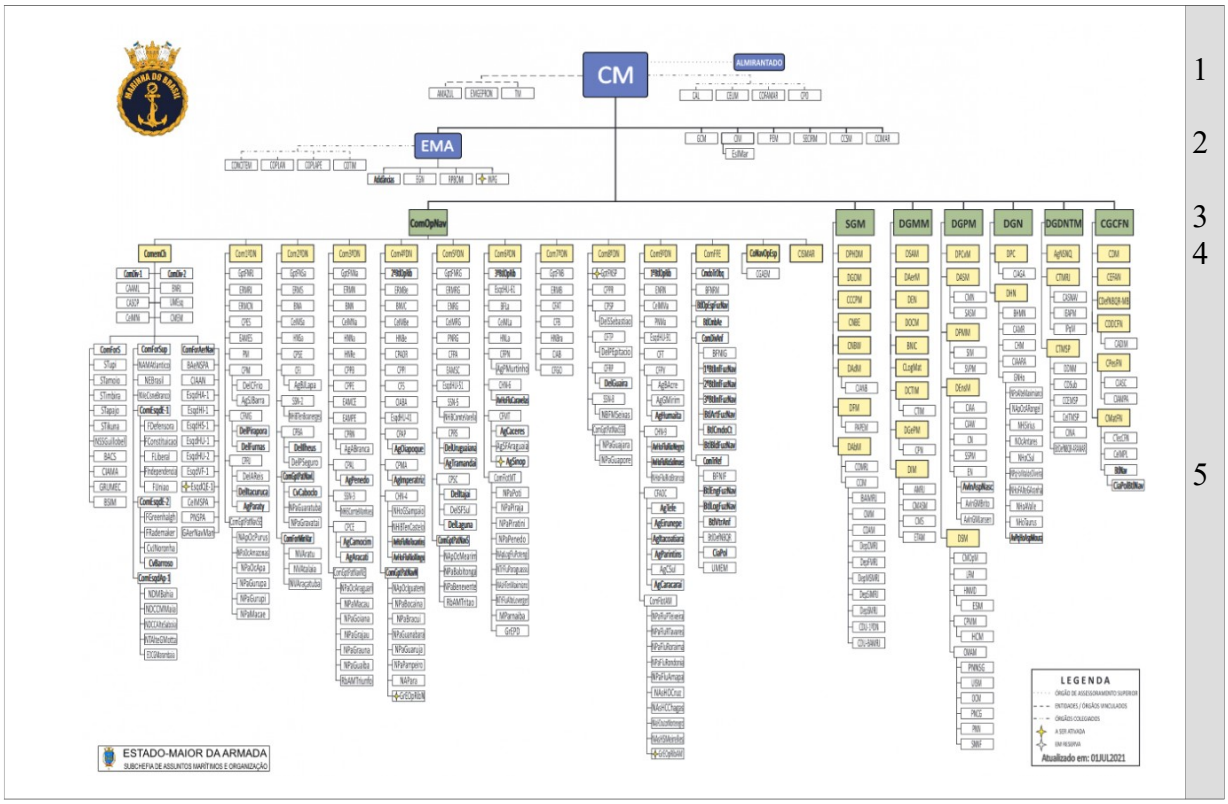


Figura 4 Organograma da Marinha do Brasil
Fonte: https://www.marinha.mil.br/sites/default/files/orgmb01jul2021.pdf. Acesso em: 12 jul. 2021.

No segundo nível do organograma, estão o Estado-Maior da Armada (EMA) e o Almirantado, órgãos que exercem funções, respectivamente, de direção geral e de assessoramento superior ao Comandante da Marinha.

No nível imediatamente seguinte, encontram-se os sete Órgãos de Direção Setorial (ODS) que, sob a direção geral do EMA são responsáveis pela orientação, coordenação e controle das atividades desenvolvidas nas diferentes áreas de atuação da MB, como mostrado na Quadro 1.

ODS	Foco de Atuação
Comando de Operações Navais(ComOpNav)	operações das Forças Navais, Aeronavais e de Fuzileiros Navais
Secretaria-Geral da Marinha (SGM)	apoio logístico para atividades corporativas de abastecimento, administração, pagamento de pessoal, documentação e gestão arquivística, controle interno e construção habitacional para o contingente militar da MB
Diretoria-Geral do Material da Marinha (DGMM)	especificação, catalogação e diretrizes de uso de materiais em obras, sistemas e serviços relacionados à construção/reparo/manutenção de equipamentos, sensores e meios navais; a sistemas de comunicação; e a sistemas de armas
Diretoria-Geral do Pessoal da Marinha (DGPM)	administração dos recursos humanos da MB
Diretoria-Geral de Navegação (DGN)	assuntos marítimos, segurança da navegação, hidrografia, oceanografia e meteorologia
Diretoria-Geral de Desenvolvimento Nuclear e Tecnológico da Marinha (DGDNTM)	planejará, orientará, coordenará e controlará as atividades nucleares, científicas, tecnológicas e de inovação, atuando como órgão central executivo do Sistema de Ciência, Tecnologia e Inovação da Marinha (SCTMB)
Comando-Geral do Corpo de Fuzileiros Navais(CGCFN)	preparo e mobilização específicos para emprego das forças e grupamentos de Fuzileiros Navais

Quadro 1 Órgãos de Direção Setorial da Marinha do Brasil

Os ODS, em conjunto com o EMA e com o Almirantado, são as instâncias hierárquicas diretamente envolvidas nas decisões estratégicas definidas para a corporação, sendo que o titular do ComOpNav, braço operativo da organização que responde pelo aprestamento das Forças Navais, Aeronavais e de Fuzileiros da Esquadra, exerce também o comando do ODS DGN (AMARO, 2010).

Cerca de 70% de todas as OM da MB – estruturadas na forma de Comandos de Forças Navais e respectivos meios flutuantes subordinados (fragatas, corvetas, submarinos, navios de apoio e demais meios de guerra), Esquadrões, Divisões, Batalhões, Grupamentos, Bases Navais e Aeronavais, Estações-Rádio (responsáveis pela manutenção da rede que suporta as comunicações navais), Capitanias dos Portos, Delegacias e Agências – estão sob o comando do ComOpNav, condição que o identifica, para a TI corporativa, como um cliente interno diferenciado, não apenas por seu volume de usuários mas também pela vinculação dos recursos e soluções de TI com atividades-fim atinentes ao setor operativo da Marinha (AMARO, 2010).

Os demais ODS, por seu turno, coordenam Diretorias Especializadas, serviços e centros de emprego específico (nível 4 mostrado na Figura 1) responsáveis pela direção executiva de várias OM posicionadas na ponta mais baixa da estrutura corporativa (nível 5).

Essas OM correspondem às unidades de negócio da MB e são responsáveis pela execução direta de atividades técnicas, administrativas e de apoio a elas atribuídas pelos escalões superiores, bem como pela utilização dos recursos alocados (AMARO, 2010). Todas as OM da MB, a despeito do escalão ao qual pertençam, possuem estrutura administrativa independente e executam suas tarefas com autonomia de gestão, o que implica em dizer que os respectivos titulares dessas unidades têm, sob a supervisão de seus comandos superiores, liberdade de ação para tomar decisões e administrar recursos financeiros provisionados na forma de crédito contábil, em favor de suas OM.

Conforme Amaro (2010), organizado, portanto, de forma federada quanto à disponibilidade de recursos financeiros e à autonomia de gestão, esse conjunto de unidades de negócio demanda necessidades bem diversificadas com relação ao emprego e aos requisitos de soluções de tecnologia da informação. Essas soluções são destinadas a suportar um amplo espectro de atividades-fim, que variam desde missões de cunho logístico-administrativo.

Temos como exemplo de atividades-fim: pagamento de pessoal, controle de bens patrimoniais, distribuição de suprimentos, gestão arquivística de documentos e gestão de hospitais e ambulatórios do sistema naval de saúde – até atividades associadas à elaboração de previsões meteorológicas, desenho de cartas náuticas, controle da navegação marítima (comercial e de navios de guerra), pesquisas científicas, projeto de sistemas de armas e desenvolvimento e manutenção de aplicativos utilizados em cenários operativos de combate.

3.2 Funcionamento da Estrutura de Governança de TI

De acordo com Amaro (2010), a implantação da governança de TI na MB definiu uma estrutura que concentra a tomada de decisão no Conselho de Tecnologia da Informação da Marinha (COTIM), organismo cujo desenho segue o padrão estabelecido para arranjos semelhantes que já existem na organização e deliberam, em colegiado, sobre assuntos corporativos. Assim estão organizados, por exemplo, o Conselho Financeiro e Administrativo (COFAMAR), o Conselho do Plano Diretor (COPLAN) e o Conselho de Planejamento de Pessoal (COPLAPE), que reúnem Almirantes-de-Esquadra que dirigem diferentes setores da Marinha.

O COTIM é um órgão consultivo, deliberativo, de caráter permanente, que tem como propósito assessorar o Comandante da Marinha no trato dos assuntos de alto nível relacionados à Governança de TI na MB (Estado-Maior da Armada [EMA], 2007; Diretoria-Geral de Material da Marinha [DGMM], 2009). Este Conselho tem a seguinte constituição:

– Presidente: Chefe do Estado-Maior da Armada;

– Membros permanentes: titulares dos ODS da Marinha;

– Membro assessor: Diretor de Comunicações e Tecnologia da Informação da Marinha; e

– Secretário: Subchefe de Logística e Mobilização do Estado-Maior da Armada.

Para assessorar o COTIM, a estrutura de governança inclui a Comissão Técnica de Tecnologia da Informação (COTEC-TI), composta da seguinte forma:

– Coordenador: Subchefe de Logística e Mobilização do EMA;

– Membros permanentes: representantes técnicos designados por cada ODS; e

– Assessores: a critério de cada ODS, de acordo com a natureza do assunto a ser tratado.

Compete ao COTIM, em linhas gerais:

– coordenar a implantação das atividades de Governança de TI na Marinha;

– aprovar diretrizes e normas doutrinárias elaboradas sobre Governança de TI na MB;

– deliberar sobre a priorização dos projetos de TI na MB;

– aprovar o Programa de Trabalho da COTEC-TI; e

– deliberar sobre outros assuntos pertinentes à Governança de TI na MB, apresentados por iniciativa do Presidente ou de qualquer de seus membros.

O Chefe do Estado-Maior da Armada, presidente do COTIM, é a autoridade de TI da MB e responde pela formulação e disseminação corporativa dos princípios que orientam o emprego da TI.

As seguintes atribuições principais cabem à COTEC-TI:

– elaborar e propor a aprovação de diretrizes e normas doutrinárias sobre Governança de TI na MB;

– preparar e encaminhar, previamente, aos membros do COTIM, pareceres com o posicionamento técnico dos ODS e das entidades relacionadas com as matérias que serão apreciadas e decididas por aquele Conselho; e

– cumprir outras atribuições que lhe forem conferidas por delegação do COTIM.

Enquanto no nível decisório o COTIM desempenha seu papel de Governança assessorado pela COTEC-TI, no nível de coordenação gerencial cabe à DCTIM tornar efetivas as deliberações emanadas daquele Conselho e ratificadas pelo Comandante da Marinha. Sob a supervisão funcional do ODS DGMM, essa Diretoria Especializada tem uma extensa relação de atribuições em razão da centralização, em uma única OM, das principais responsabilidades pela consecução dos objetivos definidos para a Governança de TI na MB (AMARO, 2010).

Como exemplos de atribuições que cabem à DCTIM, destacam-se (BRASIL, 2019[b]):

– coordenar as atividades e o cumprimento das melhores práticas de governança de TI na MB;

– coordenar a utilização da infraestrutura de rede de dados corporativa da MB (RECIM);

– executar os processos de verificação de conformidade e homologação de sistemas de informação, definindo a melhor arquitetura, autorizando (ou não) seu uso na RECIM e recomendando (ou não) a hospedagem em ambientes de Centro de Dados;

– orientar a padronização de tecnologias de Informação e de Telecomunicações;

– administrar acordos administrativos para a obtenção, em escala corporativa, de ativos de informação;

– assessorar o Diretor-Geral do Material da Marinha na obtenção de recursos financeiros atinentes às atividades concernentes ao emprego das Comunicações e da TI;

– 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);

– coordenar, executar e analisar todos os projetos que impliquem em alterações e ampliações da RECIM, bem como na oferta de serviços de TI que a utilizem;

– coordenar, executar e analisar todos os projetos que impliquem atividades de segurança da informação digital e de guerra cibernética; e

– gerenciar a capacitação dos profissionais de TI de toda a MB.

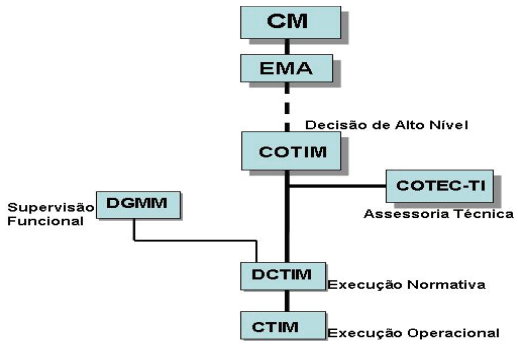


Figura 5 Estrutura de governança de TI vigente na Marinha do Brasil

O Presidente e os membros permanentes do COTIM (atualmente cinco membros, pois os ODS ComOpNav e DGN são comandados pelo mesmo titular) reúnem-se, normalmente, duas vezes ao ano, por convocação do Presidente ou por solicitação dos Membros Permanentes do Conselho, em datas preferencialmente agendadas próximas a sessões plenárias programadas para o COPLAN, COFAMAR ou COPLAPE, de vez que os Almirantes-de-Esquadra que compõem tais Conselhos são os mesmos que participam do COTIM (AMARO, 2010).

Na sequência, o Presidente do COTIM submete as resoluções do Conselho à apreciação do Comandante da Marinha e aquelas ratificadas são, então, disseminadas tempestivamente pelos ODS e encaminhadas à DCTIM, OM incumbida de implementá-las na MB.

Seguindo as informações sobre a sistemática, exposta por Amaro (2010), a COTEC-TI reúne-se, pelo menos, três vezes ao ano, podendo ocorrer convocações extraordinárias, por iniciativa de seu Coordenador. Em geral, essas plenárias ocorrem com seis a quinze participantes e, dependendo da complexidade dos temas, demandam um ou dois dias de apresentações e discussões. O Programa de Trabalho elaborado para essa Comissão é formalmente aprovado pelo COTIM e revisado a cada dois anos e serve de pauta para os debates, com vistas a subsidiar deliberações do COTIM. Alterações nesse planejamento são admitidas, desde que as propostas correspondentes observem o trâmite e os prazos devidamente estabelecidos para tal.

Em sua descrição das estruturas de Gestão da TI na Marinha, mostrando como se hierarquizam e interagem, Amaro (2010) relaciona os principais participantes da estrutura de governança de TI da MB, assim como os respectivos papéis por eles desempenhados e a equivalência de sua posição hierárquica a cargos de chefia e/ou comando, conhecidos no meio civil como executivos do nível C (funções “C-level”). Essas informações podem ser verificadas na Quadro 2 a seguir.

Contexto da MB	Posição Hierárquica Equivalente	Vínculo com a Gov TI
Comandante da Marinha (CM)	CEO: titular máximo, que responde publicamente pelas decisões e posições assumidas pela organização e estabelece as diretrizes estratégicas a serem seguidas	emite orientações para o negócio, que são observados na formulação dos princípios da TI de modo a se produzir valor agregado
Chefe do Estado-Maior da Armada (CEMA)	reporta-se diretamente ao CEO e responde pela articulação das ações dos dirigentes setoriais, presidindo diferentes Conselhos intersetoriais	autoridade de TI na MB; preside o COTIM
CON (cargo do titular dos ODS ComOpNav e DGN)	COO: dirigente setorial responsável pelas áreas diretamente ligadas à missão da organização	membro do COTIM
SGM (Comandante de todo o setor logístico-administrativo)	o CFO reporta-se diretamente a este dirigente setorial	membro do COTIM, assessorado pelo CIO setorial
Comandantes dos demais ODS	dirigentes setoriais	membros do COTIM
Diretor de Comunicações e TI da Marinha (DCTIM)	CIO corporativo	diretor corporativo de TI
Diretor de Finanças da Marinha (DFM)	CFO: executivo responsável pela administração financeira, contábil e orçamentária da organização; reporta-se ao dirigente do setor logístico-administrativo e tem assento em Conselhos corporativos como o de Planejamento Estratégico; o Financeiro e Administrativo; o Conselho de Coordenação e o Conselho de Ciência e Tecnologia	OM que "herdou" atribuições da antiga Diretoria de Intendência e responde, há mais de 20 anos, pela operação de ambientes corporativos de TI; implantou, em 2006, o primeiro Centro de Dados da MB e desde então presta serviços de TI para todo o setor SGM e também para algumas OM de outros setores
Gerente responsável pela TI de cada ODS	CIO setorial	membro da COTEC-TI e assessor do dirigente de seu setor nas decisões do COTIM; normalmente, preside o comitê/comissão da TI setorial
Encarregados locais da TI de um ODS	líderes de TI nas unidades de negócio de um determinado setor	membros de comitês/ comissões setoriais
Diretor do Centro de TI da Marinha	gestor da instalação de TI que opera supervisionada pela diretoria corporativa	membro da COTEC-TI, como assessor do DCTIM; o CTIM opera o Centro de Dados implantado em 2008 na MB,

		voltado para serviços de suporte à rede corporativa

Quadro 2 Principais Atores da Governança de TI na Marinha do Brasil

3.3 Documentação e Instruções Normativas

Neste item são apresentadas as principais normas contidas na Marinha do Brasil que norteiam as orientações de Tecnologia de Informação e Comunicações (TIC) e algumas definições e aspectos relacionados ao entendimento das Organizações Militares (OM) neste assunto, além de fazer uma análise do contexto atual dessas OM no que se refere ao cumprimento da Gestão da Segurança da Informação e Comunicações (SIC).

Ao se tratar da gestão de SIC, faz-se necessário tomar conhecimento e analisar a extensa bibliografia normativa da MB sobre o assunto, em virtude não apenas de seu caráter doutrinário mas também pela excelência que os autores atingiram dentre os estudiosos do tema, tornando-se referências dentro e fora do âmbito militar naval.

Destarte, a principal fonte de consulta será a publicação EMA-416 - Doutrina de Tecnologia da Informação da Marinha (Rev. 1), com o intuito de melhor se entender e se analisar conceitos, princípios básicos e diretrizes, englobando: Conceitos e Definições; Propósitos e Fundamentos; Responsabilidades e Atribuições; Governança de TI; Segurança da Informação Digital; e Normas para o COTIM e para a COTEC-TI (BRASIL, 2007).

Será consultada também a publicação EMA-414 - Normas para a Salvaguarda de Materiais Controlados, Dados, Informações, Documentos e Materiais Sigilosos na Marinha (Rev. 1), que tem o propósito de estabelecer as normas para a salvaguarda de materiais controlados, informações, documentos e materiais sigilosos na MB, bem como das áreas e instalações onde tramitam, incluindo os procedimentos das Comissões Permanentes de Avaliação de Documentos Sigilosos, visando a sua prorrogação, renovação, reavaliação, reclassificação, desclassificação e autorização de acesso (BRASIL, 2013 [a]).

Ainda atinente ao assunto, será utilizada também a publicação DGMM-540 - Normas de Tecnologia da Informação da Marinha (Rev.3), por ser a norma que estabelece sob um viés estratégico as orientações primordiais na gestão da SIC da MB, com suas definições e conceitos (BRASIL, 2019 [b]).

Em contraponto à bibliografia da MB relacionada à SIC, recorrer-se-á também a autores renomados na área de SIC, cujos textos servirão para comparação dos conceitos das publicações da MB. Tendo o intuito de preservar a essência das principais características da

informação, dando fluidez no cumprimento dos objetivos, Dantas (2011) menciona que a informação é útil quando mantidos seus pilares: confidencialidade, integridade e disponibilidade. Não menos importante, será analisado o capítulo 20 (Documentos Digitais) da publicação SGM-105 - Normas Sobre Documentação Administrativa e Arquivamento na Marinha (NODAM – Rev.4) (BRASIL, 2013 [b]).

Para se alcançar um entendimento mais abrangente da consolidação das orientações citadas nas publicações, serão consultadas outras normas, como: circulares, notas técnicas, DCTIMARINST, DCTIMBOTEC e as normas internas obrigatórias nas OM, disponíveis em: <http://www.marinha.mil.br/dctim/>, que serão descritas a seguir.

3.3.1 Notas Técnicas:

O Quadro a seguir apresenta uma compilação de Notas Técnicas, documento elaborado por técnicos especializados da DCTIM em assunto atinentes a Tecnologia da Informação, devendo ser criada quando identificada a necessidade de fundamentação formal ou informação específica da área responsável pela matéria sobre o assunto:

I) 10/2014	Utilização de Celulares Particulares à bordo (OSTENSIVO): Esta Nota Técnica tem o propósito de analisar a legalidade da utilização de celular particular a bordo da OM de forma indiscriminada.
II) 14/2020	Extrato de Normas que demonstram a existência de enquadramento legal que consideram como ilícito o vazamento de informações (OSTENSIVO): Esta Nota Técnica tem o propósito de em função de vazamentos de informações sigilosas que podem acarretar elevada repercussão na mídia e comprometimento da segurança das informações da Marinha do Brasil, a Comissão Técnica de Tecnologia de Informação e Comunicações da Marinha (COTEC-TIC) procurar identificar se as normas legais citadas na Nota Técnica nº 14/2016 desta Assessoria, que consideram o vazamento de informações como ilícito, permanecem em vigor.
III) 20/2020	Estudo sobre crimes de informática (OSTENSIVO): Esta Nota Técnica tem o propósito de orientar sobre o uso dos computadores em rede é o meio de comunicação que mais impacto vem causando na história da humanidade. Entretanto, esse mundo virtual não é sinônimo de mundo ideal, vale dizer, a par de representar inegável progresso tecnológico, carrega também potencialidades, indesejáveis à segurança das informações digitais, quando o ambiente computacional é mal utilizado. Assim sendo, tal progresso gerou o aparecimento de novos tipos de crimes ou novas formas de praticar os já conhecidos tipos penais. No desempenho de sua missão esta Diretoria (DE) verifica a necessidade de estudar os acontecimentos e desafios trazidos pela evolução tecnológica, antecipando-se ao problema, buscando solidificar, interpretar a legislação em vigor e fornecer subsídios para o aperfeiçoamento da condução da investigação dos delitos de informática apurados nos procedimentos administrativos de Sindicância e do Inquérito Policial Militar.

Quadro 3 – Notas Técnicas

3.3.2 DCTIMBOTEC:

O Quadro a seguir apresenta uma compilação sobre os Boletins Técnicos da DCTIM sobre o assunto:

I) 30/001/2008	Acessibilidade – Orientações para atendimentos ao nível de Prioridade 1 (OSTENSIVO): Este Boletim Técnico tem o propósito de estabelecer procedimentos para dotar de acessibilidade os sítios eletrônicos da MB em conformidade ao modelo de acessibilidade do Governo Eletrônico (E-MAG).
II) 32/002/2011	Normas de uso do mecanismo de busca na RECIM (OSTENSIVO): Este Boletim Técnico tem o propósito de divulgar as Normas Técnicas para uso do mecanismo de busca na RECIM.
III) 30/009/2016	Padronização de tecnologias, linguagens e ferramentas para o desenvolvimento de Sistemas Digitais (SD) a serem empregados pela MB (OSTENSIVO): Este Boletim Técnico tem o propósito de padronizar as tecnologias, linguagens e ferramentas a serem empregadas, no âmbito da MB, no desenvolvimento de Sistemas Digitais (SD), visando a redução do custo associado à capacitação de pessoal e o aumento da produtividade.
IV) 31/006/2017	Configuração do Serviço de Árvore de Diretórios em Software Livre (OSTENSIVO): Este Boletim Técnico tem o propósito de padronizar e divulgar o ambiente e parâmetros mínimos de segurança para a configuração do Serviço de Árvore de Diretório utilizando aplicações baseadas em Software Livre sem gerar custo de licenciamento na MB e impactos na segurança digital da MB.
V) 32/001/2017	Procedimentos para uso do Sistema de Comunicações Integradas “Cisco Jabber”, no âmbito da Marinha do Brasil (OSTENSIVO): Este Boletim Técnico tem o propósito de orientar tecnicamente a instalação e utilização do Serviço de Comunicações Integradas “Cisco Jabber”.
VI) 33/008/2017	Padronização de Sistema Operacional de Servidores na MB (OSTENSIVO): Este Boletim Técnico tem o propósito de estabelecer e divulgar as configurações de sistemas operacionais de servidores para uso na MB, com a finalidade de facilitar a administração dos recursos de Tecnologia de Informação, o controle de licenças, o planejamento das OM, a redução de custos e o aumento da segurança digital na MB.
VII) 30/002/2018	Procedimentos Operacionais para elaboração do Relatório de Inteligência de Ameaças Cibernéticas (RIAC) (OSTENSIVO): Este Boletim Técnico tem o propósito de estabelecer procedimentos operacionais sobre a elaboração do relatório executivo unificado e periódico denominado Relatório de Inteligência de Ameaças Cibernéticas (RIAC), a partir de conhecimentos coletados das ferramentas de gerenciamento e segurança de redes de computadores adotadas pela MB como Firewalls, Intrusion Detection System (IPS), Data Loss Prevention (DLP), Web Gateway, Security Information and Event Management (SIEM), ePolicy Orchestrator (ePO), Antivírus e em fontes abertas na Internet. Assim, visa-se identificar as possíveis vulnerabilidades, ameaças internas e externas imediatas à RECIM e os riscos associados, a fim de manter uma consciência situacional cibernética, propor a mitigação das vulnerabilidades detectadas e alterações dos níveis de alarmes cibernéticos vigentes na RECIM.
VIII) 30/003/2018	Estação de Trabalho Padrão da MB (OSTENSIVO): Este Boletim Técnico tem o propósito de divulgar as configurações de Estações de Trabalho (ET) e aplicativos homologados para uso nas referidas estações, a fim de direcionar a gestão efetiva dos recursos de Tecnologia de Informação (TI), o controle de licenças, os planos de TI das OM, a economia de recursos e a segurança da informação digital no âmbito da MB.
IX) 32/001/2018	Procedimentos para Utilização da Plataforma Webex (OSTENSIVO): Este Boletim Técnico tem o propósito de orientar tecnicamente a utilização da plataforma de colaboração “Webex”.
X) 32/002/2018	Procedimentos para uso de videoconferência na MB (OSTENSIVO): Este Boletim Técnico tem o propósito de orientar tecnicamente a instalação e utilização do sistema de videoconferência na MB.
XI) 33/001/2018	Padronização do Domino e configuração do correio eletrônico Lotus Notes na MB (OSTENSIVO):

	Este Boletim Técnico tem o propósito de padronizar versão do servidor da plataforma do Domino do Lotus Notes e o ambiente (versões do software nos clientes, de navegadores, templates e servidores), a ser configurado nas OM para permitir a utilização do correio eletrônico Lotus Notes, de modo funcional e seguro
XII) 33/002/2018	Padronização dos Endereços Eletrônicos da Marinha (OSTENSIVO)
XIII) 31/002/2020	Recomendações e Requisitos Mínimos de Segurança da Informação (OSTENSIVO): Este Boletim Técnico tem o propósito de estabelecer e divulgar recomendações e requisitos mínimos de segurança para a homologação de Sistemas Digitais (SD) na MB.
XIV) 31/005/2020	Configuração para Conexão Remota segura a Servidores (OSTENSIVO): Este Boletim Técnico tem o propósito de estabelecer e divulgar parâmetros mínimos de segurança para a configuração do serviço de Secure Shell (SSH) em servidores Linux que realmente tenham necessidade de acesso remoto, com a finalidade de facilitar a administração de servidores com sistema operacional Linux e incrementar a segurança digital na MB.
XV) 33/001/2020	Procedimentos para criação de máquina virtual para simulação de plataforma Windows em estações de trabalho com sistemas operacionais Linux instalados (OSTENSIVO): Este Boletim Técnico tem o propósito de possibilitar a instalação e execução de aplicações, desenvolvidas exclusivamente para funcionamento na plataforma Windows XP e Windows 7, em estações de trabalho padrão (ET) com Linux instalado

Quadro 4 – DCTIMBOTEC

3.3.3 DCTIMARINST:

O quadro a seguir apresenta uma compilação sobre as Instruções da DCTIM sobre o assunto:

I) 10-01A	Emprego Operacional dos Terminais do Sistema de Comunicações Militares por Satélite (SISCOMIS) e Convênio MB-INSS (RESERVADO)
II) 10-02E	Visita Técnico-Funcional (OSTENSIVO): Esta instrução tem o propósito de estabelecer os procedimentos para a realização das Visitas Técnico-Funcionais (VISITEC), a serem observados pela DCTIM e as OM da MB.
III) 10-03A	Boletins de Ordens e Notícias BONO (OSTENSIVO): Esta instrução tem o propósito de estabelecer normas e procedimentos para a publicação de matérias no BONO.
IV) 10-04A	Exercício de Ativação de Recursos de Comunicações Próprios da MB (RESERVADO)
V) 10-05	Exercício de Dupla Criptografia (RESERVADO)
VI) 20-01	Construção na área de influência das Estações Radiogoniométricas de Alta Frequência (ERGAF) (OSTENSIVO): Esta instrução tem o propósito de orientar as Estações Radiogoniométricas de Alta Frequência (ERGAF) da Marinha, seus respectivos Distritos Navais, a Base Aeronaval de São Pedro da Aldeia (BAeNSPA) e as Prefeituras Municipais das áreas limítrofes às ERGAF quanto ao processo administrativo para autorização de construção em área de influência das ERGAF, por meio da padronização e trâmite dos expedientes e do estabelecimento de normas específicas sobre o assunto.
VII) 20-02	Equipamentos de comunicações dos Navios da Esquadra (RESERVADO)
VIII) 20-04	Condições de operações dos principais equipamentos dotados nas Estações Rádio (RESERVADO)
IX) 20-06	Manutenção de Terminais Móveis Navais (MN) e Terminais Táticos Transportáveis (TT) do SISCOMIS (RESERVADO)
X) 30-04D	Portal de Serviços da MB (OSTENSIVO): Esta instrução tem o propósito de estabelecer os procedimentos para o acesso e utilização do

	Portal de Serviços da MB (Portal MB) – Anexo: Termo de Responsabilidade.
XI) 30-06C	Controle de conteúdo dos sítios acessados na Internet, via RECIM (OSTENSIVO): Esta instrução tem o propósito de estabelecer as políticas e procedimentos de controle de conteúdo dos sítios acessados na internet, via Rede de Comunicações Integradas da Marinha (RECIM), pelos usuários da MB.
XII) 30-08B	Uso Institucional e não Institucional de mídias e redes sociais extra-MB pelo pessoal da MB (OSTENSIVO): Esta instrução tem o propósito de estabelecer e divulgar normas para o uso Institucional e não Institucional de mídias e redes sociais pelo pessoal da MB.
XIII) 30-09C	Centros Locais de Tecnologia da Informação (CLTI) (OSTENSIVO): Esta instrução tem o propósito de estabelecer o propósito, a lotação, a estrutura organizacional, as tarefas, e a área de atuação dos Centros Locais de Tecnologia da Informação (CLTI).
XIV) 30-10	Proteção elétrica de Sistemas de Tecnologia de Informação e Comunicações (TIC) contra os efeitos indiretos decorrentes das descargas atmosféricas e manobras realizadas no sistema de alimentação elétrica (OSTENSIVO): Esta instrução tem o propósito de orientar as Organizações Militares (OM) quanto à importância da proteção elétrica de sistemas de TIC contra os efeitos indiretos decorrentes das descargas atmosféricas, por meio da instalação de um Sistema Interno de Proteção Contra Descargas Atmosféricas (SiPDA). Esta Norma não engloba o Sistema Externo de Proteção Contra Descargas Atmosféricas (SePDA), responsável pela proteção das estruturas contra as descargas diretas, sejam elas prediais, compostas ou não por elementos que possam atuar como captores naturais de raios.
XV) 30-11A	Serviço de Diretórios para Gerenciamento de Redes Locais (OSTENSIVO): Esta instrução tem o propósito de orientar, devido aos recentes cenários econômicos de restrição orçamentária e para atender aos objetivos do Plano Estratégico de TI da Marinha (PETIM) de 2016 a 2019, surgiu a necessidade de se pesquisar soluções baseadas em Software Livre para que o projeto do Serviço de Diretórios não fosse paralisado. Após a fase de testes, a DCTIM homologou a solução baseada no SAMBA 4, que atende tanto aos requisitos técnicos quanto os financeiros, para a continuidade do projeto. O SAMBA 4 é um software livre e aberto, compatível com o Serviço de Diretório da Microsoft, que permite a integração de usuários com sistemas operacionais LINUX e WINDOWS, sem nenhum custo de licenciamento.
XVI) 30-12A	Gerenciamento dos registros de eventos computacionais relevantes (logs) (OSTENSIVO): Esta instrução tem o propósito de estabelecer os procedimentos para geração, armazenamento, verificação da integridade e gerenciamento dos registros de acesso aos serviços e sistemas de Tecnologia da Informação (TI) disponibilizados aos usuários, assim como das falhas de acesso aos mesmos, a fim de permitir a detecção de atividades não autorizadas ou maliciosas.
XVII) 30-13A	Uso de Rede Sem Fio na MB (OSTENSIVO): Esta instrução tem o propósito de estabelecer normas e procedimentos para o uso de redes sem fio seguras no âmbito da MB.
XVIII) 30-14	TI Verde e Sustentabilidade (OSTENSIVO): Tem o propósito de apresentar orientações sobre a inclusão de critérios de sustentabilidade ambiental nos processos de aquisição de equipamentos de Tecnologia da Informação (TI), bem como definir procedimentos para seu uso e posterior descarte, de acordo com o conceito de TI Verde.
XIX) 30-15B	Instrução de Emprego de correio eletrônico na MB (OSTENSIVO): Esta instrução tem o propósito de estabelecer e divulgar a instrução de emprego de correio eletrônico (e-mail) na MB, incluindo as regras para a criação de caixas postais e as restrições inerentes ao uso desse serviço no âmbito da RECIM e externo à MB em complemento às regras e orientações previstas na DGMM-540 (3ª Revisão).
XX) 30-16	Autoridade Certificadora Reserva do Ministério da Defesa (AC RESERVA) (RESERVADO)
XXI) 30-18	Uso Institucional de listas de e-mail (*mailing lists*) (OSTENSIVO): Esta instrução tem o propósito de estabelecer regras de utilização de lista de e-mail (*mailing list*) na MB. Esta Instrução Normativa aplica-se a listas de e-mail, com mais de 1.000 contatos, criadas por meio de aplicações/scripts desenvolvidos pelas OM (OMSOL) e destinadas ao envio automático de notas, comunicados ou e-mail marketing a contatos dentro ou fora da MB.
XXII) 31-02B	Forense Computacional e de Dispositivos Móveis, Registros de Acesso à Internet, Registros de Envio/Recebimento de e-mail para Internet e Registros de Envio/Recebimento de

	Mensagens Instantâneas (OSTENSIVO): Esta instrução tem o propósito de disciplinar as atividades de forense computacional na MB, bem como incrementar sua eficiência, as instruções que se seguem estabelecem procedimentos para realização de perícias em recursos computacionais da MB e disciplinam a divulgação interna de registros de acesso à Internet, registros de envio/recebimento de e-mail para Internet e registros de envio/recebimento de mensagens instantâneas, por meio dos canais disponibilizados pela MB para tal.
XXIII) 31-04A	Utilização de Recursos Criptográficos na Marinha (RESERVADO)
XXIV) 31-05	Utilização de certificados digitais emitidos pela AC Defesa no âmbito da MB (OSTENSIVO): Esta instrução tem o propósito de orientar a adoção de certificados digitais emitidos pela Autoridade Certificadora de Defesa (AC Defesa) no âmbito da Marinha do Brasil (MB).
XXV) 31-06	Plano de Gestão de Incidentes Cibernéticos (OSTENSIVO): Esta instrução tem o propósito de normatizar as atividades atinentes ao Tratamento de Incidentes em Redes de Computadores da Marinha do Brasil, regulamentar a estrutura organizacional da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da MB e estabelecer os demais processos de forma consonante às diretrizes exaradas nos documentos emanados pelo Gabinete de Segurança Institucional da Presidência da República (GSI-PR) relacionados a Normas de Tecnologia da Informação da Marinha, garantindo a uniformidade de procedimentos a serem cumpridos pelas Equipes envolvidas nas atividades de Tratamento de Incidentes em Redes de Computadores e assegurar o emprego conjunto de esforços em prol da Segurança da Informação (SI) na MB.
XXVI) 32-01A	Normas para Cabeamento Estruturado em Redes de Dados em Edificações nas OM de Terra (OSTENSIVO): Esta instrução tem o propósito de estabelecer critérios e recomendações mínimas para elaboração e execução de projetos de cabeamento estruturado nas áreas administrativas das Organizações Militares (OM) de terra.
XXVII) 32-02	Compartilhamento de Arquivos da MB (OSTENSIVO): Esta instrução tem o propósito de estabelecer os procedimentos para o acesso e a utilização do repositório disponibilizado para o compartilhamento de arquivos entre usuários da RECIM.
XXVIII) 32-03C	Serviço de Comunicações Integradas (OSTENSIVO): Esta instrução tem o propósito de estabelecer e divulgar normas para o acesso, instalação e utilização do Sistema de Comunicações Integradas.
XXIX) 33-04C	Uso institucional do ambiente de colaboração Rede Marinha (OSTENSIVO)
XXX) 33-05B	Gestão de Sítios Eletrônicos de Internet de propriedades da MB (OSTENSIVO): Esta instrução tem o propósito de estabelecer os procedimentos destinados a orientar o cumprimento do ciclo de vida dos sítios eletrônicos de Internet das OM da MB, em cumprimento aos documentos em referência.
XXXI) 33-06B	Norma sobre Conformidade, Homologação e Hospedagem de Sistemas Digitais (SD) na MB (OSTENSIVO): Esta instrução tem o propósito de estabelecer a sistemática para verificação da conformidade, homologação e hospedagem de Sistemas Digitais (SD) na MB.
XXXII) 33-07	Correio Móvel da MB (OSTENSIVO): Esta instrução tem o propósito de orientar normatizar sobre e-mail móvel da MB, uma solução de Tecnologia da Informação (TI) que permite o acesso ao correio eletrônico funcional, em telefones celulares, padrão *"smartphone"*, bem como *"tablet"*, via serviço celular de internet ou *"Wi-Fi"*.
XXXIII) 50-01	Controle de Material do Símbolo de Jurisdição "NOVEMBER" (SJ-N) (OSTENSIVO): Esta instrução tem o propósito de estabelecer os procedimentos a serem cumpridos pelas OM que possuem sob a sua responsabilidade o material do Símbolo de Jurisdição "NOVEMBER" (SJ-N), além de divulgar conceitos e normas para o estabelecimento, bem como alterações de dotações de equipamentos e sobressalentes, sob a administração da DCTIM."

Quadro 5 – DCTIMARINST

3.3.4 PUBLICAÇÕES:

O quadro a seguir apresenta as publicações da MB, em mais alto nível, sobre o assunto:

I) EMA- 414	Normas para a Salvaguarda de Materiais Controlados, Informações, Documentos e Materiais Sigilosos na Marinha: Tem o propósito de estabelecer as normas para a salvaguarda de materiais controlados, informações, documentos e materiais sigilosos na Marinha do Brasil, bem como das áreas e instalações onde tramitam, incluindo os procedimentos das Comissões Permanentes de Avaliação de Documentos Sigilosos, visando a sua prorrogação, renovação, reavaliação, reclassificação, desclassificação e autorização de acesso.
II) EMA – 416	Doutrina de Tecnologia da Informação da Marinha: Esta publicação tem o propósito de estabelecer a Doutrina de Tecnologia da Informação da Marinha, enunciar seus conceitos, princípios básicos e diretrizes.
III) DGMM-540	Normas de Tecnologia da Informação da Marinha - 3ª Revisão: Esta publicação tem o propósito de orientar sobre as Normas de Tecnologia da Informação da MB (DGMM-540) 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 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, 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.

Quadro 6 – Publicações

3.4 Mentalidade de Segurança

Conforme descrito na publicação DGMM-540 (Rev.3), para se proteger as informações, os ambientes computacionais devem ser considerados seguros (BRASIL,

2019[b]). 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.

A figura a seguir ilustra, de forma cômica (mas que pode desencadear desfechos trágicos), uma cena que capta várias negligências quanto à proteção das informações no ambiente de trabalho, o que compromete a mentalidade de segurança.

Figura 6 Mentalidade de Segurança
Fonte: https://www.marinha.mil.br/com5dn/sites/www.marinha.mil.br.com5dn/files/01_Com5DN-Simposio%20v12.pdf

A Segurança da Informação e Comunicações (SIC) é 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, a processam e a trafegam. Em conformidade com a DGMM-540 (Rev3), 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.

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. Essas

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. (BRASIL, 2019[b])

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. Isso 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. Vale lembrar que segurança na utilização da Internet, por exemplo, 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.

Ainda de acordo com a DGMM-540, Rev. 3 (BRASIL, 2019[b]), o presente assunto demanda a ampliação e o detalhamento das atribuições basilares de órgãos e integrantes da estrutura organizacional da MB para a condução das atividades mentalidade de SIC, o que se vê no extrato da publicação constante no quadro a seguir:

> "À Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) compete promover e fomentar o incremento progressivo da mentalidade de SIC, por meio de ferramenta de gestão do conhecimento, palestras, seminários, simpósios e cursos.
> Ao Centro de Tecnologia da Informação da Marinha (CTIM) compete, sob a coordenação da DCTIM, a realização de auditorias de SIC nas OM, composta por uma Equipe de Auditoria (EA) designada previamente, com o objetivo de verificar o fiel cumprimento das normas de SIC, bem como estabelecer possíveis ações de correção e divulgação da mentalidade de SIC.
> Aos Centros Locais de Tecnologia da Informação (CLTI) compete, sob a orientação da DCTIM, elaborar um programa de adestramento (PAD) anual para as OM apoiadas, que dissemine e incorpore a mentalidade de SIC; e zelar pelo fortalecimento da mentalidade de segurança, junto as OM apoiadas.
> Aos Titulares das OM compete, zelar pelo fortalecimento da mentalidade de segurança e 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."
>
> Extrato da DGMM-540, Rev. 3 (BRASIL, 2019[b])

Pode-se verificar, nesse extrato, a estruturada competência hierárquica funcional

na MB sobre condução da SIC.

3.5 Consciência Situacional

Segundo descreve Guimarães (2018), a consciência situacional envolve a condição de se estar ciente daquilo que está acontecendo ao redor para entender como a informação, os eventos e as próprias ações impactarão metas e objetivos, tanto imediatamente como no futuro próximo.

Embora venha ocorrendo uma evolução do setor cibernético das nações ao longo dos anos, as ameaças ao Espaço Cibernético (ECiber)[16] vêm gradativamente incrementando a sofisticação e a complexidade dos ataques, sendo necessário um maior esforço durante um possível conflito cibernético. Antes que as ações de Proteção Cibernética possam ser executadas, é preciso se obter e manter uma Consciência Situacional (CS) do ambiente operacional cibernético, denominada Consciência Situacional Cibernética (CSCiber), que permita identificar, compreender e antecipar a evolução dessas ameaças.

3.5.1 A Definição de Consciência Situacional na Literatura

Apesar das diferentes interpretações de CS identificadas na literatura (STANTON *et al*., 2001, p. 3), a definição amplamente utilizada, em função da sua divisão em níveis, é aquela que a descreve como: “a percepção dos elementos no ambiente, dentro de um volume de tempo e espaço; a compreensão de seu significado; e a projeção de seu status no futuro próximo” (ENDSLEY, 1995, p. 36). Com base nessa definição, a CS é composta pelos nível 1 (percepção), nível 2 (compreensão) e nível 3 (projeção), que se alimentam diretamente do ciclo de decisão e ação, denominado Modelo de Endsley, conforme ilustrado pela figura 7. (GUIMARÃES, 2018).

[16] Termo que foi idealizado por William Gibson, em 1984, referindo-se a um espaço virtual composto por cada computador e usuário conectados em uma rede mundial.

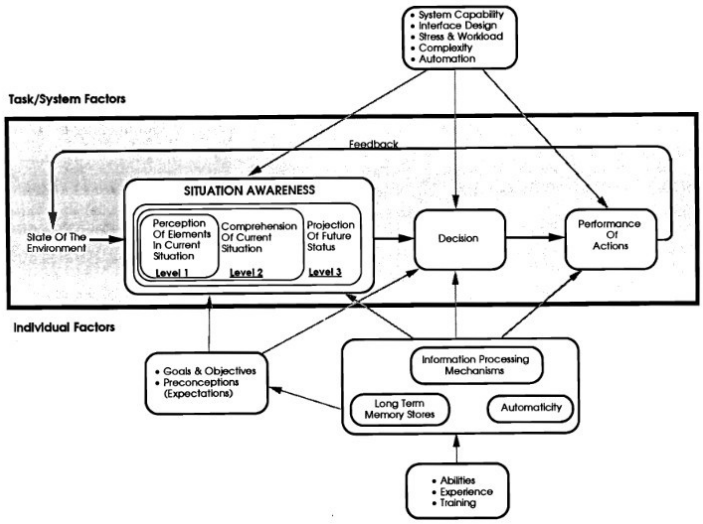


Figura 7 Modelo de Endsley

Fonte: ENDSLEY, 1995, p. 35

A Percepção envolve a detecção sensorial de informações significativas sobre o ambiente em que se está operando. Considerando o ambiente cibernético, os analistas de proteção precisam perceber as alterações relevantes no ECiber, seja de forma manual ou automática, incluindo a percepção dos nós[17] críticos da rede, protocolos[18] e logs[19].

A Compreensão envolve a assimilação do significado ou da importância dessas informações em relação aos objetivos a serem alcançados. Esse nível é denominado de Entendimento da Situação e envolve o "e daí?" das informações percebidas. Considerando o ambiente cibernético, os analistas de proteção precisam entender as causas que tornam um nó da rede vulnerável, entender a assinatura de um ataque[20], quais eventos isolados podem estar inter-relacionados, o efeito de um determinado evento nas operações atuais e a priorização correta de eventos concorrentes.

Ainda em concordância com Guimarães (2018), a Projeção, o nível mais alto de CS, consiste no planejamento das informações adiante no tempo, determinando como elas afetarão os estados futuros do ambiente operacional. Considerando o ambiente cibernético, os analistas de proteção precisam projetar o impacto de uma atividade identificada como maliciosa sobre outros sistemas ou sua consequência ao se propagar através da rede.

Além dos níveis de Percepção, Compreensão e Projeção, previstos no Modelo de Endsley, foi proposta a inclusão do nível de Resolução (MCGUINNESS; FOY, 2000), visando

[17] Ativo de informação conectado à rede de computadores.

[18] Convenção ou padrão que controla e possibilita uma conexão, comunicação ou transferência de dados entre dois sistemas computacionais.

[19] Registro histórico das atividades de um dispositivo computacional.

[20] Tráfego de pacotes de dados com conteúdo que utiliza padrões específicos de bytes, podendo ser comparado com um padrão já conhecido como malicioso.

identificar qual o melhor método a seguir para alcançar a mudança de estado da situação em que se encontra para uma situação desejada.

Logo, uma vez que o conceito de CS não depende do tipo do ambiente operacional, julga-se apropriada a adequação dos seus níveis ao ambiente operacional cibernético, estabelecendo uma CSCiber. Por conseguinte, pode-se representar a CSCiber como a percepção, compreensão, projeção e resolução inerentes ao ambiente operacional cibernético, contribuindo para o processo de tomada de decisão, nas ações de proteção cibernética.

3.5.2 A Consciência Situacional Cibernética no Âmbito do Ministério da Defesa

Considerando as operações conjuntas e a manutenção da CS, todos os níveis decisórios do MD são permeados pelos sistemas de TIC, visando assegurar o fluxo de informações e contribuir para a interoperabilidade entre as FA. A importância da CSCiber é destacada no Livro Verde de Segurança Cibernética, na Doutrina de Operações Conjuntas, na Política de Defesa Cibernética e na Doutrina Militar de Defesa Cibernética (GUIMARÃES, 2018).

O Livro Verde de Segurança Cibernética (MANDARINO JUNIOR; CANONGIA, 2010, p.44) previa a necessidade de desenvolvimento de um programa de inclusão digital que incorporasse a CSCiber sobre ameaças e segurança cibernética, no curto e médio prazos.

A Doutrina de Operações Conjuntas (BRASIL, 2020, p. 77), considerando o ambiente operacional cibernético, definiu CSCiber como a percepção precisa e atualizada do ECiber no qual se atuará, e no reconhecimento da importância de cada elemento percebido em relação à missão atribuída. É a perfeita sintonia entre a situação percebida e a situação real, proporcionando ao Comandante melhores condições para decidir. Destacou-se também que, considerando o ambiente cibernético, a obtenção e a manutenção da CSCiber por parte do Comando é proporcionada pela informação fornecida por meios adequados, pelas pessoas certas, no momento oportuno e de conteúdo relevante e preciso, agregando valor à atividade de C^2 (*Idem*, p. 177). Conforme a publicação, pode-se estabelecer que o Comandante Operacional de uma Operação Conjunta tem a atribuição de servir de interlocutor com os escalões superiores, zelando pela manutenção da CSCiber naquilo que seja relevante aos níveis de decisão estratégico e político (*Idem*, p. 179).

A Política Cibernética de Defesa (BRASIL, 2012, p. 15) atribuía as tarefas de

identificar as infraestruturas críticas de informação associadas ao setor cibernético, visando a formação da CSCiber necessária à Defesa Cibernética, em proveito da diretriz de assegurar, de forma conjunta, o uso efetivo do ECiber pelas FA. Também se atribuiu a tarefa de identificar as ameaças internas e externas, reais ou potenciais, de forma a contribuir com a formação da CSCiber necessária às atividades de Inteligência (*Idem*, p. 16).

Por fim, a Doutrina Militar de Defesa Cibernética (BRASIL, 2014, p. 23) estabeleceu a ação de Exploração Cibernética, visando a produção de conhecimento ou a identificação de vulnerabilidades no ECiber de interesse, a fim de se obter uma CSCiber, atribuindo as ações de busca ou coleta.

3.5.3 O Estabelecimento de uma CSCiber na MB

Para Guimarães (2018), a Proteção Cibernética depende da combinação de conhecimento sobre técnicas de defesas efetivas e técnicas de ataques reais, de modo a preveni-los, rastreá-los ou mitigá-los.

Considera-se que deva haver uma proatividade, onde as ações defensivas não se limitem a somente impedir um comprometimento inicial do ECiber, mas que também possam detectar os Ativos Informacionais já comprometidos, que reduza a superfície de ataque, implemente as configurações de defesa dos dispositivos e estabeleça uma capacidade adaptativa e contínua de defesa e resposta que possa ser mantida e melhorada.

Os analistas de proteção cibernética da MB possuem a função principal de empreender as atividades de detecção, identificação e resposta às ações conduzidas contra o ECiber-MB, empregando geralmente uma arquitetura de defesa em profundidade[21]. Porém, considerando o contexto de proteção, podem-se empregar ações de Ataque ou Exploração cibernética, introduzindo testes de vulnerabilidades[22] e testes de invasão[23], para avaliar o grau de resiliência dos sistemas de informação (BRASIL, 2017, p. 4-3). Assim, considera-se que manter uma CSCiber sobre a ampla variedade de eventos e quantidades de dados gerados seja um desafio analítico.

Continuando com Guimarães (2018), para minimizar este desafio, propõe-se que um analista de proteção cibernética da MB utilize um modelo mental (PAUL; WHITLEY,

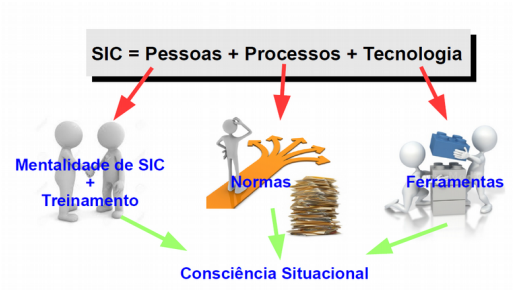
[21] Múltiplas camadas de proteção a fim de reduzir a probabilidade de sucesso de um ataque.
[22] Análise de vulnerabilidades utilizando scanners e banco de dados de vulnerabilidades para detectar falhas.
[23] Métodos que avaliam a segurança de um sistema de computador ou de uma rede, simulando ataques de uma fonte maliciosa.

2013, p. 145), baseado em questões a serem respondidas, durante o curso de evento de segurança de rede[24], para direcionamento de uma CSCiber. O modelo é composto por uma taxonomia de questões de CSCiber centradas no usuário, derivadas de uma série de atividades de pesquisa dos autores, sendo divididas em duas categorias: Detecção de Eventos e Orientação do Evento. A primeira, com questões que os analistas devem responder antes e durante um evento, visa o desenvolvimento da percepção da situação. A segunda aborda questões em proveito da compreensão do estágio de análise da situação.

A categoria de Detecção de Eventos é dividida nas seguintes subcategorias: *baseline*[25] da rede, quando funcionando em um estado "normal"[26]; detecção de alterações, capacidade de comparar estados da rede identificando diferentes tendências; e atividade de rede, refletindo uma mudança de um estado "normal" para "anormal", atuando como uma sugestão para que o analista estreite sua atenção para uma análise mais aprofundada.

A categoria de Orientação do Evento é dividida nas subcategorias: identificação, para uma análise detalhada de um evento a fim de identificar quem, o que, quando, onde e por que e o ataque está acontecendo e possivelmente o vincule à uma ameaça; impacto na missão, de forma a priorizar a importância de uma ameaça identificada; e avaliação de danos, para informar uma resposta à uma ameaça identificada.

A Consciência Situacional, formada pelos níveis de Percepção, Compreensão, Projeção e Resolução, é amplamente citada nas publicações do âmbito do MD, destacando-se sua importância no contexto da Proteção Cibernética. Considerando-se a complexidade do ambiente cibernético da MB, buscou-se minimizar este desafio analítico por meio da proposta de utilização do modelo mental (PAUL; WHITLEY, 2013, p. 145), baseado em questões voltadas para o analista. No entanto, julga-se que seja um obstáculo para esse modelo quantificar qualquer degradação ou melhoria alcançada do ambiente cibernético, dado que as respostas possam ser subjetivas. Para se obter uma percepção mais precisa da CSCiber, propõe-se ainda estabelecer métricas significativas, que possam representar as características quantitativas da condição de proteção de um ECiber (GUIMARÃES, 2018).



[24] Ocorrência identificada em um sistema, serviço ou rede, que indique uma possível violação da política de SIC ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a SIC.
[25] Configuração de referência.
[26] Condição sob um nível aceitável de operação.

Figura 8 Consciência Situacional
Fonte: https://www.marinha.mil.br/com5dn/sites/www.marinha.mil.br.com5dn/files/01_Com5DN-Simposio%20v12.pdf

3.6 Aplicabilidade das instruções de Segurança da Informação e Comunicações nas Organizações Militares da MB.

3.6.1 Propósito

I - 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.

II - Estabelecer normas e procedimentos que garantam os requisitos básicos de Segurança da Informação e Comunicações (SIC) nas OM, com a finalidade de garantir a segurança e a integridade dos Sistemas Computacionais, em que estão armazenados em meio eletrônico os conhecimentos ou dados de interesse da MB.

Ainda de acordo com a aplicabilidade das ISIC nas OM, em conformidade com a publicação DGMM-540, Rev. 3 (BRASIL, 2019[b]), são descritos a seguir as principais orientações:

3.6.2 Qualificações e Responsabilidades

3.6.2.1 Titular da OM

A Segurança dos Sistemas de Informações, bem como as medidas destinadas a implementá-las no âmbito da OM, é de inteira e exclusiva responsabilidade do Comandante/Diretor, sendo assessorado diretamente pelo Oficial de Segurança da Informação e Comunicações Digitais (OSIC).

Suas atribuições estão descritas no Anexo A, publicação em referência.

3.6.2.2 Oficial de Segurança da Informação e Comunicações (OSIC)

Será nomeado formalmente por Ordem de Serviço do Comandante/Diretor da OM, devendo possuir conhecimentos mínimos de redes locais de computadores, sistemas operacionais de rede, protocolos de comunicação, serviços disponibilizados pela rede (intranet, correio eletrônico e assinaturas digitais) e conhecimento em auditoria de redes, preferencialmente ser o Encarregado do Setor de Tecnologia da Informação.

Suas atribuições estão descritas no Anexo A, publicação referência.

3.6.2.3 Administrador da Rede Local (ADMIN)

Será nomeado formalmente por Ordem de Serviço do Comandante/Diretor da OM, devendo ter capacitação em Administração de Rede de Computadores e, se possível, certificação para os sistemas operacionais que são utilizados na OM, assim como conhecimentos mínimos em auditoria de sistemas computacionais, preferencialmente servindo no Setor de Tecnologia da Informação da OM. Por questões de segurança, as funções de ADMIN e de OSIC não poderão ser acumuladas.

Suas atribuições detalhadas estão descritas no Anexo A deste trabalho.

3.6.2.4 Usuário

Os usuários dos equipamentos de Tecnologia da Informação (TI), principalmente os interligados à rede local, seja militar, servidor civil ou prestador de serviço, deverão estar cientes das suas responsabilidades sobre Segurança da Informação e Comunicações (SIC).

Para garantir o atendimento desse requisito, os mesmos deverão assinar o Termo de Responsabilidade Individual (TRI). Dessa forma, ficando cientes das normas de SIC e autorizados a acessarem os sistemas disponibilizados. Caso tenham a necessidade de receber uma Estação de Trabalho, também deverão assinar o Termo de Recebimento de Estação de Trabalho (TRE), que deverão estar arquivados no Setor de Tecnologia da Informação.

Esses termos e as atribuições dos usuários estão detalhados nos Apêndices C e D e Anexo A deste trabalho.

3.6.3 Recursos Computacionais Críticos (RCC)

São os recursos, equipamentos ou serviços, inclusive de manutenção, que se danificados ou interrompidos, afetarão de alguma forma os requisitos básicos de SIC do Centro, quais sejam: sigilo, autenticidade, integridade e disponibilidade.

3.6.3.1 Classificação dos RCC em Níveis de Importância

Para as classificações abaixo, entende-se que os usuários com Credencial de Segurança (CREDSEG) em qualquer grau de sigilo cumprirão rigorosamente o item 9.2.5 da DGMM-540, que estabelece normas para a guarda e armazenamento de documentos sigilosos em meio eletrônico ou digital.

Os RCC das OM são classificados nos seguintes níveis:

a) NÍVEL 1: Equipamentos servidores; switchs, equipamentos (discos rígidos e outras mídias) que armazenam informações digitais sigilosas; e os sistemas de cópias de segurança (“backup”). São os RCC de alta importância que, quando atingidos, interrompem ou degradam o funcionamento da rede local da OM ou tornam expostas informações digitais sigilosas, causando prejuízo à SIC por comprometimento do assunto sigiloso;

b) NÍVEL 2: Equipamentos de conectividade (“switches”, “hubs” e modems) e os meios físicos de tráfego, localizados em alguns compartimentos da OM. Correspondem aos RCC de média importância, que, quando atingidos, degradam apenas superficialmente o funcionamento da rede local da OM ou tornam expostas apenas informações digitais não sigilosas; e

c) NÍVEL 3: Estações de Trabalho, localizadas em alguns compartimentos da OM, equipamentos portáteis, instalações elétricas, sistemas de refrigeração e sistemas de controle de acesso físico. Corresponde aos RCC de baixa importância que, quando atingidos, não causam prejuízo direto à SIC ou ao funcionamento da rede local da OM, mas requerem atenção, pois podem comprometer outros RCC de nível de importância superior.

Todos os RCC deverão ser identificados conforme o seu respectivo nível, por meio de uma etiqueta, antes da disponibilização e utilização.

O detalhamento sobre RCC está descrito no Anexo A deste trabalho.

3.6.4 Perímetros de Segurança Física das Informações Digitais

3.6.4.1 A OM deverá listar em sua ISIC os seus perímetros de segurança,

Não é permitida a entrada ou a saída do perímetro de segurança de mídias ou de qualquer outro dispositivo armazenador de informações digitais sigilosas, sem autorização do encarregado do compartimento correspondente e do OSIC.

Os visitantes destes compartimentos deverão possuir CREDSEG para acesso a esses locais e serão identificados e registrados na sua entrada, com registro de data, hora e razão da visita. O acesso será limitado ao propósito da visita e supervisionado enquanto esta durar. O visitante receberá instruções mínimas estabelecidas pelo OSIC sobre os procedimentos de SIC e assinar o Termo de Responsabilidade Individual (TRI).

3.6.4.1 Utilização de dispositivos móveis (celulares, smartphone, tablets etc):

a) Áreas em que se abrirá exceção para utilização ou porte de dispositivos móveis

a.1) autorizados a utilizar seus dispositivos móveis pessoais:

a.2) autorizados a portar seus dispositivos móveis pessoais, desde que desligados:

a.3) não autorizados a ENTRADA dos dispositivos móveis pessoais:

b) Haverá, fixado no portaló e nos corredores aviso indicando sua proibição de utilização, e nos compartimentos não autorizados sua entrada serão fixados dentro dos mesmos aviso indicando sua proibição de portar. .

Demais orientações sobre dispositivos móveis estão descritas no Anexo A deste trabalho.

3.6.5 Requisitos Mínimos de Proteção dos Perímetros de Segurança Física

3.6.5.1 Segurança Física das áreas

Os compartimentos possuirão sistema de alarme, monitorização e controle de entrada e saída do pessoal, inclusive para o período fora do expediente normal, bem como controle de chaves. Além disso, todos os equipamentos servidores utilizam permanentemente, descanso de tela (“screen saver”) protegido por senha, de acordo com a política de senhas constante nas publicações vigentes da MB.

3.6.5.1 Segurança Física dos Dispositivos de Conectividade, Servidores e Estações de trabalhos

As “switches”, dispositivos de conectividades instaladas na OM, são protegidas com a utilização de gabinetes com chaves e lacres numerados. Os Servidores da OM estão confinados em gabinetes próprios e com chave e as Estações de Trabalho desse Centro, possuem somente lacres numerados, para assegurar o controle de sua configuração e segurança dos dados.

Cada um desses dispositivos possuirá um livro próprio para que seja efetuado o controle das chaves e dos lacres utilizados.

Demais orientações estão descritas no Anexo A deste trabalho.

3.6.6 Relação dos Documentos de SIC

3.6.6.1 Plano de Contingência (PLCONT)

O PLCONT tem grau de sigilo Reservado e tem 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 os requisitos básicos de SIC. O PLCONT será elaborado pelo ADMIN e revisto pelo OSIC, no máximo, a cada um ano.

3.6.6.2 Histórico da Rede Local (HRL)

O HRL tem grau de sigilo Reservado e tem por objetivo manter os registros de transações normais e anormais (incidentes) que possam afetar de alguma forma a SIC na rede local da OM, bem como atividades de rotina e controles do Setor de Tecnologia da Informação. O documento é confeccionado na forma de Livro e sua elaboração, controle e a manutenção do HRL são de responsabilidade do ADMIN e seus registros serão realizados pelo pessoal do Setor de Tecnologia da Informação.

3.6.6.3 Relatório de Auditoria (RAD) de SIC

O RAD é um documento Reservado que tem por objetivo formalizar os resultados apurados por auditoria de SIC e indicar possíveis soluções aos problemas levantados na rede local em relação aos aspectos de SIC.

As normas para a realização de auditoria interna estão descritas no item 3.6.9.

3.6.6.4 Plano de Adestramento de SIC

Documento ostensivo que visa ações de adestramento de temas de SIC para a tripulação da OM (sejam militares, servidores civis ou prestadores de serviço).

O programa de Adestramento (PAD) de SIC se resume na apresentação de uma palestra anual para todo o pessoal (militares e civis) da OM e uma, quando necessário, para todo o pessoal recém-embarcado (militares e civis), pessoal prestador de serviço e pessoal envolvido em irregularidade/incidente (usuário que deixou de cumprir as normas de SIC – geralmente constatada em auditorias regulares internas).

A elaboração deste documento é de responsabilidade do OSIC.

3.6.6.5 Controle de Entrada e Saída de Dispositivos de Informações Digitais

Este documento é confeccionado na forma de Livro, ostensivo, que registra a entrada e a saída de qualquer dispositivo que possa armazenar informações digitais, tais como: Estações de Trabalho (de mesa ou portáteis), discos rígidos, disquetes, CD-ROM, DVD e outros dispositivos de armazenamento portáteis. Para cada ocorrência de entrada ou saída devem ser registrados: data, hora, responsável, origem, destino e a identificação do dispositivo.

O controle será efetuado na entrada da OM e compete ao pessoal de serviço da mesma o correto cumprimento e preenchimento. A elaboração da documento é de responsabilidade do OSIC.

3.6.6.6 Controle de Acesso Físico aos Perímetros de Segurança

Este relatório é ostensivo e registra a entrada e a saída de qualquer visitante (qualquer pessoa estranha ao perímetro, mesmo servidor civil ou militar da OM) nos perímetros de segurança física das informações digitais da OM.

O relatório é retirado pelo encarregado do compartimento.

3.6.6.7 Registro dos Termos de Destruição de Recursos Computacionais Críticos

Este controle é reservado e tem por propósito registrar a sistemática de

recolhimento e destruição dos Recursos Computacionais Críticos (RCC) da OM que possuam características de armazenamento de informações digitais sigilosas.

3.6.7 Segurança Lógica das Estações de Trabalho

Deverão ser observados todos os procedimentos constantes da publicação DGMM-540 a fim de garantir a SIC.

3.6.7.1 Cópia de segurança (backup):

A Política de “Backup”, incluindo a execução e o armazenamento de suas cópias de segurança, deverão estar descrita em um documento próprio atendendo as orientações mínimas constantes da publicação DGMM_540.

3.6.7.2 Porta USB nas Estações de Trabalho:

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. Esses dispositivos serão habilitados somente quando for estritamente necessário ao serviço, com autorização do Comandante/Diretor da OM e anuência do OSIC

Relembra-se que essa autorização se limita ao emprego de dispositivos de memória móveis funcionais (pendrive, HD externo e cartão de memória) para atender exclusivamente necessidade de serviço.

3.6.7.3 Utilização Segura do PenDrive:

A utilização de dispositivos Pen Drives, vem aumentando o risco em infectar e transmitir arquivos maliciosos através das portas USB.

Relembra-se que somente está autorizada a utilização de Pen Drives adquiridos pela OM e de forma comedida dentro do contexto da MB.

3.6.7.4 Privilégio mínimo:

Retirar do usuário o poder de administrador das estações de trabalho.

3.6.7.5 Controle da Manutenção dos RCC, das Estações de Trabalho e Discos Rígidos

A manutenção dos RCC é considerada crítica e sofrerá uma atenção especial sob o aspecto da SIC.

Todas as informações digitais sigilosas armazenadas em quaisquer meios digitais deverão ser mantidas criptografadas por meio de recursos criptológicos definidos e gerenciados pela DCTIM. Quando a Estação de Trabalho necessitar de manutenção preventiva ou corretiva, o Setor de Tecnologia da Informação transfere a mesma para o Setor de Tecnologia da Informação que, com a supervisão e anuência do usuário, providenciará a devida manutenção.

3.6.8 Procedimentos para Acesso à Rede Local

O OSIC é responsável pelo controle das autorizações de acesso à rede local.

O ADMIN é responsável pelo controle do cadastro no sistema dos usuários autorizados e participará qualquer cancelamento ou novo cadastro ao OSIC.

Os procedimentos para cadastramento dos usuários no ambiente computacional da OM e a definição de seus privilégios seguirão as regras descritas na publicação DGMM-540.

3.6.8.1- Senhas Seguras:

a) as senhas serão sempre individuais e os responsáveis observarão as seguintes orientações: não utilizar nomes próprios, nome do cônjuge, data de aniversário ou outros de fácil associação; não utilizar sequência fácil ou óbvia de caracteres, que facilite a sua descoberta; não utilizar palavras existentes em dicionários; utilizar aleatoriamente letras minúsculas, letras maiúsculas, números e caracteres especiais; não escrevê-la em lugares visíveis, de fácil acesso ou em claro, mantendo-a em sigilo; utilizar extensão mínima de seis caracteres; e utilizar o tempo de validade de senha de, no máximo, dois meses;

b) senhas para acessos privilegiados serão trocadas com uma frequência de trinta dias.

c) não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros;

d) as senhas utilizadas no ambiente computacional da OM, não devem ser transferidas, divulgadas ou conhecidas por terceiros; e

e) não compartilhar o uso de senha com outros usuários.

3.6.9 Normas para as Auditorias Internas

As auditorias de SIC na OM têm por propósito verificar o fiel cumprimento das normas de SIC, bem como estabelecer possíveis ações de correção juntamente a uma contínua divulgação da mentalidade de SIC.

Os seguintes procedimentos serão observados para a realização das Auditorias de SIC Internas:

a) Serão realizadas com autorização formal do Comandante da OM e sob o controle do OSIC e possuirão grau de sigilo, no mínimo, Reservado;

b) Será realizada por pessoal da OM formalmente designado por Ordem de Serviço e que possua o credenciamento adequado ao grau de sigilo estabelecido para ela;

c) Na impossibilidade de realizar auditorias internas de SIC exclusivamente com seu pessoal, a OM somente poderá utilizar algum apoio de pessoal de outra OM após obter uma autorização formal da DCTIM/CTIM. Nesse caso, a solicitação da OM, via COMIMSUP, deverá incluir a respectiva justificativa para análise da DCTIM/CTIM. 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;

d) As auditorias internas serão realizadas na periodicidade, ao menos, uma a ano;

e) A Equipe de Auditoria Interna (EAI) será constituída para cada auditoria de SIC a ser realizada, sendo composta por dois ou três membros, na qual o mais antigo será designado Chefe da Equipe de Auditoria Interna;

f) Os componentes da EAI serão designados formalmente, por Ordem de Serviço do Comandante. Somente poderá ser designado para compor a EAI o pessoal devidamente qualificado; e

g) Compete à EAI, após sua designação formal, as seguintes atividades:

1) obter as listas e questionários de verificação apropriados na página da DCTIM/CTIM, na Intranet;

2) realizar as atividades de auditoria com a preparação plena de todo o material necessário;

3) planejar as atividades específicas da auditoria a que foi designada;

4) executar, de forma imparcial, soberana e independente, as atividades de auditoria;

5) garantir o sigilo de toda informação obtida pela auditoria;

6) elaborar o RAD conforme as normas vigentes e submetê-lo à aprovação

do Comandante no prazo estabelecido; e

7) não divulgar os resultados de auditoria.

3.6.10 Controle do Uso dos Recursos Computacionais e do Acesso à Rede por Pessoal Extra-MB/Estrangeiro

Os seguintes procedimentos serão observados pelo OSIC, ADMIN e pessoal do Setor de Tecnologia da Informação por ocasião de pessoal extra-MB/estrangeiro eventualmente embarcados, destacados, cursando, participando de exercícios, visitando ou efetuando qualquer atividade na OM: estabelecimento de barreiras lógicas, realização de vigilância e todas as medidas que se façam necessárias para impedir o acesso desses usuários às informações sensíveis.

O acesso a qualquer RCC da OM por parte de pessoal extra-MB/estrangeiro somente poderá ser realizado após autorização Comandante e anuência do OSIC, com a devida assinatura da TRI.

Visando cumprir as orientações supra, os setores/departamentos deverão informar ao OSIC os nomes e propósito da atividade, com antecedência mínima de 48 horas.

3.6.11 Disposições Complementares

O pessoal do Setor de Tecnologia da Informação é responsável por manter um controle da elaboração de cópias de segurança e dos respectivos testes de recuperação com a periodicidade estabelecida no PLCONT.

Deverão ser observadas, em especial, as recomendações detalhadas descritas nos Apêndices C e D e Anexo A deste trabalho, bem como as demais orientações contidas na publicação DGMM-540.

3.7 Gestão de Riscos em Segurança da Informação e Comunicações

Conforme descrito na publicação DGMM-540, Rev 3 (BRASIL, 2019[b]), a MB já utiliza a Gestão de Riscos de forma consolidada no nível organizacional, aplicando-a no Planejamento Estratégico Organizacional (PEO) de todas as Organizações Militares (OM), (em consonância com a SGM-107 7ª Revisão – Normas Gerais de Administração), e no nível operacional, aplicado nos Planos de Segurança Orgânica (EMA-352 1ª Revisão – Princípios e

Conceitos da Atividade de Inteligência) e nos Planos de Prevenção de Acidentes Aeronáuticos (DGMM-3010 - Manual de Segurança de Aviação), dentre outros.

A Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC) é uma abordagem sistemática para apoio à decisão dos Titulares de OM que visa priorizar as medidas que contribuam para aumentar a eficiência da Segurança da Informação e Comunicações (SIC) e das Comunicações Navais (CN).

Essa Gestão é um processo contínuo que deve possuir contextos definidos de forma a 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. Nesse 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. Desta forma, o processo de GRSIC deve ser aplicado com metodologia própria, sendo essencial na identificação das necessidades da Marinha do Brasil (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.

3.7.1 Definições

As seguintes definições e conceitos que aplicam-se a GRSIC, serão apresentadas no quadro 7 a seguir:

Definições	Conceitos
Ameaça	conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização
Análise de riscos	uso sistemático de informações para identificar fontes e estimar o risco
Análise/avaliação de riscos	processo completo de análise e avaliação de riscos
Ativos de Informação	os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso

Autenticidade	propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade
Avaliação de riscos	processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco
Comunicação do risco	troca ou compartilhamento de informação sobre o risco entre o decisor e outras áreas da OM e/ou da MB
Confiança	é a garantia de que as comunicações expedidas, e somente elas, alcançarão o destinatário com sua origem perfeitamente definida e de que o pensamento do remetente (conteúdo da mensagem) não será alterado no encaminhamento
Controle	Medidas corretivas ou preventivas que visam se contrapor às ameaças, corrigindo vulnerabilidades identificadas nos ativos de informação e que representam as ações a implementar em um processo de tratamento do risco
Disponibilidade	propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade
Estimativa de riscos	processo utilizado para atribuir valores à probabilidade e consequências (impactos) de um risco
Evitar risco	uma forma de tratamento de risco na qual a autoridade competente decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco
Flexibilidade	é um requisito que deve ser considerado em todos os planejamentos de comunicações. Caracteriza-se pela possibilidade real de utilização de meios alternativos que permitam manter os enlaces de comunicações
Gestão de Riscos de SIC	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
Identificação de riscos	processo para localizar, listar e caracterizar elementos do risco. O propósito da identificação de riscos é determinar eventos que possam causar uma perda potencial e indicar onde e por quais motivos podem ocorrer
Incerteza	falta de certeza absoluta decorrente da existência de mais de uma possibilidade de resultado final
Integração	é a capacidade de um sistema poder ter acesso a outros sistemas de interesse e permitir ser acessado por estes
Integridade	propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental
Rapidez	é a garantia de que a comunicação entre o origem e o destinatário ocorra em tempo hábil, de modo a contribuir para que se alcance o efeito desejado
Reduzir risco	uma forma de tratamento de risco na qual a autoridade competente decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco
Reter risco	uma forma de tratamento de risco na qual a autoridade competente decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado
Risco	perigo ou possibilidade de sofrer um dano ou perda e diz respeito ao desvio de um ou mais resultados futuros do seu valor esperado. O risco é resultante de um estado de incerteza, onde algumas das possibilidades que envolvem perda, catástrofe ou desfecho indesejável são consideradas
Riscos de SIC	potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo na missão da OM ou da MB
Segurança	é a garantia de que as comunicações serão preservadas contra violações ou revelações não desejadas de informações de qualquer espécie
Sigilo (Confidencialidade)	propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado

Transferir risco	uma forma de tratamento de risco na qual a autoridade competente decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco
Tratamento dos riscos	processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco
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 digital ou de comunicações

Quadro 7 Definições e conceitos de GRSIC

3.7.2 Procedimentos

Para execução da metodologia, uma sequência de procedimentos, descritos nos itens a seguir, deve ser observada. Esse processo é composto pelas etapas de:

- Definições preliminares;
- Análise e avaliação dos riscos;
- Plano de tratamento dos riscos;
- Aceitação ou não dos riscos;
- Implementação do plano de tratamento dos riscos;
- Monitoração e análise crítica;
- Melhoria do processo de GRSIC; e
- Comunicação do risco.

A figura a seguir ilustra o processo de GRSIC.

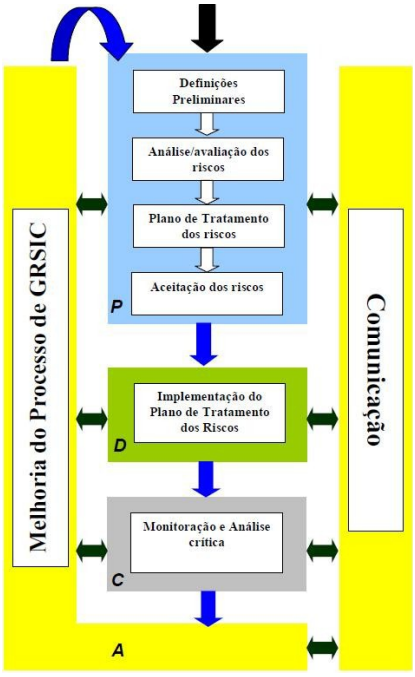


Figura 9 Processo de Gestão de Riscos de SIC.
Fonte: Marinha do Brasil. Secretaria-Geral da Marinha. SGM-107. Normas Gerais de Administração (Rev. 7). Brasília, DF, 2019 [c]

3.7.3 Análise e avaliação dos riscos

Nesta fase, são identificados os riscos, levando-se em consideração as ameaças e as vulnerabilidades associadas aos ativos de informação para que, em seguida, sejam estimados os níveis de risco para avaliação e priorização. Para tal, deve-se:

– Identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido;

– Identificar os riscos associados ao escopo definido, considerando as ameaças envolvidas, as vulnerabilidades existentes nos ativos de informação e as ações de Segurança da Informação e Comunicações (SIC) já adotadas;

– Estimar os riscos levantados, considerando a probabilidade de ocorrência e o impacto associado ao risco quanto à perda dos requisitos de SIC e das CN (disponibilidade, integridade, sigilo (confidencialidade) e autenticidade, bem como a confiança, segurança, rapidez, flexibilidade e integração) nos ativos considerados;

– Avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos; e

– Relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos.

Ameaça	Descrição
Violação de propriedade intelectual	Violação de leis reguladoras de direito autoral, direito de propriedade industrial, importação/exportação ilícita de algoritmos criptográficos implantados em software ou em hardware, que provocam processos legais, multas, prisões etc.
Vazamento de Informação	Divulgação não autorizada de informações, obtida por meio de acesso não autorizado, que representa revelação de planos, segredos de negócio, estratégias etc., que provoca perda de propriedade intelectual, vantagem a concorrente, exposição negativa etc.
Serviços diferentes das expectativas originais	Resultados ineficazes, ineficientes ou inefetivos, decorrentes de processos obsoletos ou controles que não resolvem deficiências conhecidas, que podem provocar desalinhamento com os objetivos de negócios ou organizacionais definidos.
Sanções Administrativas	Penalidade disciplinar administrativa (não judicial) imposta por atos indevidos (inobservância a regulamentações, políticas internas e outras normas).
Repúdio	Negativa no reconhecimento da autoria de uma ação; irretratabilidade. OBS.: não deve ser confundida com a dificuldade em se comprovar a autoria de uma ação, que corresponde à Perda de Rastreabilidade.
Queda de performance	Excesso de utilização de recursos de comunicação ou processamento, ou sobrecarga de tráfego, que provocam queda de performance, perda de produtividade etc.
Perda de Satisfação do Cliente.	Perda de Satisfação do Cliente

Perda de rastreabilidade	Redução da possibilidade de se verificar eventos de segurança importantes, tais como acessos não autorizados, erros, omissões etc., ou de se buscar os respectivos agentes causadores. É provocada por falta ou inconsistência de registros de eventos, por exemplo, os existentes nos logs de auditoria de software, nos livros de ocorrências etc., podendo resultar em repúdio dos usuários, acusação imprópria, recorrência de incidentes ou outras consequências.
Perda de qualidade do serviço	Queda na qualidade do serviço
Perda de Produtividade	Perda de Produtividade
Perda de expertise na organização	Perda de expertise na organização
Não-atendimento à regulamentação	Inobservância ou pontos em desacordo com leis, normas ou regulamentos de entidades reguladoras, que podem provocar penalidades administrativas, financeiras ou legais.
Multas, indenizações ou sanções legais	Penalidade financeira ou criminal, imposta por atos ilícitos (violações legais, regulamentares ou contratuais).
Inviabilidade Financeira	Inviabilidade Financeira
Interrupção da prestação do serviço	Paralisação temporária ou permanente nas atividades contratadas junto a fornecedor, decorrente de falhas administrativas, operacionais ou contratuais, ou ainda por eventos inesperados e não controlados, que pode provocar insatisfação em clientes, sanções administrativas e indenizações por conta de processos judiciais.
Interferência eletromagnética	Relâmpagos, emissões magnéticas ou cargas eletrostáticas que provocam danos ou interferências nas linhas de comunicação, perda de integridade ou apagamento dos dados armazenados em mídias, falhas em equipamentos, queima de equipamentos etc.
Indisponibilidade de serviços ou informações	Impedimento do acesso autorizado à informação ou a ativos de informação, através de ações como a desabilitação de redes ou sistemas, furto ou roubo de informação ou outras, que provocam retardamento ou interrupção de operações etc.
Incêndio	Danos por ação de fogo, que provocam perda de patrimônio, de informações, de mão-de-obra, ou falta de condições de trabalho etc.
Impossibilidade de auditoria da organização	Impossibilidade de auditoria da organização
Furto ou roubo	Crime contra o patrimônio cometido por pessoa que subtrai coisa alheia, com intenção ilegítima de apropriação, provocando perda de patrimônio, indisponibilidade de mídias com informações etc.
Funcionário Insatisfeito	Funcionário Insatisfeito.
Fraude ou sabotagem	Caracterizam-se por ações de escrita ilícita ou trapaça, por meio de ações enganosas de usuários ou técnicos autorizados - normalmente familiarizados com o sistema alvo – como métodos falsos, fornecimento de dados incorretos, adulteração de informações, manipulação premeditada de ambientes ou equipamentos etc., visando tirar proveito próprio ou de outrem ou provocar prejuízos financeiros, decisões equivocadas etc.
Fenômenos por ação da água	Tempestade, inundação, granizo, alagamento, ou outros fenômenos, em galpões, salas ou demais ambientes com risco potencial, que provocam danos a instalações, equipamentos, mídias etc.
Falta de mão-de-obra essencial	Greve, piquete, demissão, sequestro, epidemia, distúrbio civil etc., que provocam bloqueio de acesso a indivíduos ou equipes, ou indisponibilidade de mão de obra.
Falta de Apoio Interno	Falta de Apoio Interno
Falha em meios de comunicação	Interrupção de linhas, interferências etc. provocando perda de comunicação de dados ou voz.
Falha de software	Código ineficaz, fora de especificação, incompatível com outros módulos de software ou de hardware, ou falhas provocadas por parâmetros configurados

	indevidamente, que provocam perda da integridade de dados, falhas de processamento, perda de sincronismo, erros de transmissão ou outras falhas na comunicação de dados ou voz, paralisação de sistemas etc.
Falha de hardware	Falha mecânica ou eletrônica causada por stress, desgaste ou fim da vida útil de componentes ou outras causas intrínsecas ao equipamento, que provocam indisponibilidade de sistemas, erros de transmissão ou outras falhas na comunicação de dados ou voz, perda de performance, incêndios etc. Em caso de falhas em dispositivos de segurança, há exposição do ambiente a novas vulnerabilidades.
Falha de energia	Falta de suprimento, flutuações ou picos de tensão que provocam desligamento de equipamentos, travamento de sistemas, queima de equipamentos, falta de refrigeração, perda de comunicação etc.
Extremos de temperatura ou umidade	Excesso de calor, frio ou umidade, por ação direta em mídias de armazenamento ou equipamentos, que provocam deterioração das mídias, redução da vida útil dos equipamentos, travamentos de sistemas etc.
Erros, omissões ou uso indevido	Erros de entrada de dados ou omissão de controles, causados por usuários, administradores, operadores de sistema ou programadores sem o devido preparo, desatentos ou descuidados, que provocam resultados incompatíveis, travamento de sistemas, retrabalho, contaminação de backup etc. Incluem-se falhas na instalação ou configurações inseguras de sistemas, ou erros de manutenção, permitindo o aparecimento de novas vulnerabilidades.
Dano à imagem da organização	Perda de credibilidade perante o mercado
Dano a pessoas	Perigo de vida causado por desconhecimento, obstrução de acesso ou de escape, fogo, explosões, contaminações etc.
Dano a instalações	Acidentes, choques de veículos, desabamentos, trepidações, explosões, ações de vandalismo, terrorismo, guerrilhas ou outras, que provocam dano ou destruição das instalações, equipamentos, sistemas, documentos, mídias de armazenamento etc.
Custos acima do esperado	Custos acima do esperado
Contaminação ambiental	Contaminação do ar, partículas, poeira, fumaça, gases, ruído, produtos químicos ou biológicos, fungos ou outros agentes que provocam perda de informações armazenadas, deterioração de mídias, curto-circuitos em equipamentos, falta de condições ambientais de trabalho etc.
Ação de código malicioso	Contaminação eletrônica por vírus ou worms, ou outros códigos que afetam sistemas de forma não autorizada, como cavalos-de-tróia, exploits, bombas lógicas etc., que provocam perda de produtividade, desconfiança, constrangimento na troca de informação, retrabalho, perda de dados etc.
Atraso na entrega do serviço	Atraso na entrega do serviço
Atraso de Entrega	Atraso de Entrega
Acesso lógico não autorizado	Acesso a programas, sistemas, redes ou ativos de TI por usuários, por meio de ações ilícitas (escuta, interceptação de mensagens, infiltração, análise de tráfego, vazamentos, espionagem etc.), que provocam revelação não autorizada de informações proprietárias ou segredos de negócio.
Acesso indevido a informações confidenciais	Acesso de informações confidenciais pelos competidores
Acesso físico não autorizado	Acesso a ambientes, pessoas, equipamentos ou dispositivos de controle físico por pessoas não-autorizadas, que provocam vazamento de informações, desativação de controles etc.

Quadro 8 Tipos de ameaças em GRSIC

3.7.4 Plano de Tratamento dos Riscos

O Plano de Tratamento dos Riscos visa determinar as formas de endereçar os riscos, considerando as opções de:

- Reduzir;
- Evitar;
- Transferir ou
- Reter o risco.

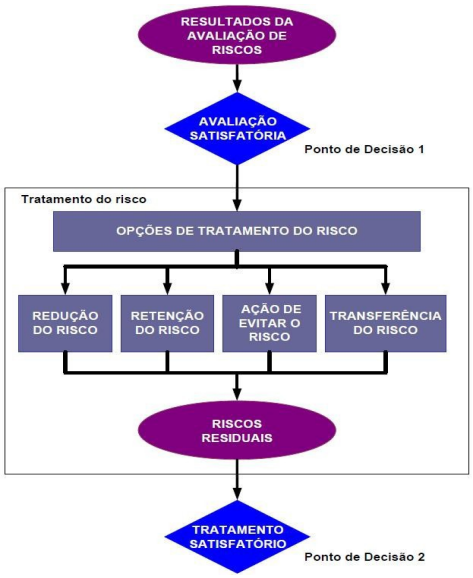


Figura 10 Atividade de tratamento do risco dentro do processo de GRSIC.

Deve-se observar, independentemente da opção de tratamento do risco, a eficácia das ações de Segurança da Informação e Comunicações (SIC) já existentes; as restrições organizacionais, técnicas e estruturais; os requisitos legais e a análise custo/benefício.

3.7.5 Responsabilidades

Caberá a DCTIM 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.

O CTIM coordenará a implantação e o gerenciamento de ferramenta de software,

homologada pela DCTIM, para o processo de GRSIC a ser utilizado na MB.

Os OSIC das OM, no âmbito de suas atribuições, são responsáveis pela coordenação da GRSIC em suas OM.

3.8 Documentos de Gestão da Segurança da Informação e Comunicações

A Gestão da Segurança da Informação e Comunicações na MB é norteada pela publicação DGMM-540 Rev.3, que estabelece os documentos e registros que devem ser criados para que tal gestão esteja documentalmente respaldada, conforme se constata a seguir.

3.8.1 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 apresentadas no quadro 9 a seguir:

Ações	Descrição
planejamento	ações que visam a preparação do ambiente da rede local para prevenção de possíveis ameaças ou riscos às informações digitais
histórico	ações para descrição da estrutura da rede local e registro de ocorrências do ambiente computacional da OM
análise	ações para avaliação de vulnerabilidades, riscos ou incidentes que possam ocorrer no ambiente da rede local, auxiliando ações preventivas, corretivas e de planejamento
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
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
adestramento	ações que visam adestrar o pessoal quanto aos documentos, aos procedimentos e às demais ações de SIC

Quadro 9 Ações de Segurança

3.8.2 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.

3.8.3 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 elaboração da ISIC, as seguintes regras básicas devem ser seguidas:

– 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.

3.8.4 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.

3.8.5 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) Descrição da Rede;

b) Atividades de Rotina; e

c) Incidentes.

3.8.6 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.

3.8.7 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 dessa análise, os riscos em relação aos incidentes de segurança serão reduzidos, permitindo que a RECIM esteja em um nível de segurança adequado.

3.8.8 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).

a) 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, com data-hora e período de conexão.

b) 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, com assunto e data-hora da mensagem.

c) 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, com data-hora e período de comunicação.

3.8.9 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.

3.8.10 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 a este e aos três itens anteriores possuem grau de sigilo, no mínimo, RESERVADO e estão voltados às ações de Forense Computacional.

3.8.11 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 apresentados no quadro10 a seguir, que podem ter um Plano de Adestramento de SIC específico:

Nº	Exemplos de Temas
1	Adestramento básico de SIC (para o pessoal recém chegado à OM)
2	Conceitos Gerais de SIC

3	ISIC da OM
4	Recursos de SIC
5	Legislação, Normas e Documentos de SIC
6	Ativação dos Planos de Contingência da OM (teoria e prática)
7	Segurança Orgânica, no que se refere à SIC
8	Normas para a salvaguarda de materiais controlados, dados, informações, documentos e materiais sigilosos
9	Recursos Criptológicos
10	Engenharia Social
11	Crimes de Informática

Quadro 10 Temas de um Plano de Adestramento SIC

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

O controle dos 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.

3.8.12 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.

4 ESTUDO DE CASO COMO ESTRATÉGIA DE PESQUISA NA ÁREA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA MARINHA DO BRASIL

4.1 Levantamentos de Requisitos e Não Conformidades da Gestão da Segurança da Informação e Comunicações nas Organizações Militares da MB

Foram formulados questionários verificadores de conformidade com as publicações da Marinha do Brasil, principalmente a DGMM-540, que norteia a gestão da Segurança da Informação e Comunicações (SIC) da MB, presentes nos Apêndices deste trabalho, com base nas Listas de Verificações contidas na publicação DCTIMARIST 10-02B.

Além da pesquisa bibliográfica sobre o assunto, assentou na recolha de dados efetuada através de questionários estruturados (APÊNDICES A e B), totalizando 133 questionamentos, tendo sido disponibilizado por meio de encaminhamento de canais formais da MB, o qual esteve disponível entre os dias 01 de maio de 2021 e 15 de junho de 2021. O pedido de resposta aos questionários foi efetuado por meio de uma mensagem de correio eletrônico criptografada, que teve como destinatários os administradores de rede das OM e os encarregados dos CLTI da MB.

Avaliaram-se os objetivos de SIC, por amostragem, nos CLTI e OM, perfazendo-se 112 colaboradores/OM, destes 23 são encarregados de CLTI e 89 administradores de rede de OM. Os dois questionários contêm o total de 123 perguntas (113 do administrador de rede e 10 do CLTI). As respostas apresentadas abaixo como “sim” significa que os controles de dado objetivo estão sendo atendidos e “não” significa que o controle não estão sendo atendido.

Os dados e informações coletados através destes questionários, relativos à política e à gestão de Segurança da Informação e Comunicações (SIC) na MB, foram utilizados unicamente para subsidiar quantitativamente (análise de cálculos percentuais e estatísticos) uma pesquisa acadêmica, do Curso Política e Estratégia Marítimas (C-PEM) da Escola de Guerra Naval (EGN). As informações serão apresentadas preservando a identificação dos respondedores e das Organizações Militares.

Nas Tabelas 1 e 2, abaixo disponibilizadas, serão apresentados somente os resultados percentuais das respostas aos questionários encaminhados aos encarregados de CLTI e OM de administradores de rede e, posteriormente, no item 4.4 serão analisados e

avaliados:

I . Respostas dos questionários aos Administradores (Admin) das Organizações Militares da MB

Obs: Os itens descritos no campo "Nº" da tabela abaixo, correspondem aos mesmos números dos questionamentos encaminhados aos colaboradores.

Nº	Descrição dos questionamentos aos ADMIN das OM	Respostas %	
1.0	**Adestramento**	**SIM**	**NÃO**
1.1	O Programa de Adestramento de SIC foi autorizado pelo Titular da OM?	**96%**	**4%**
1.2	Os Planos de Adestramentos de SIC englobam o conjunto mínimo de temas previstos no artigo 10.11 da DGMM-0540?	**100%**	**0%**
1.3	Os meios de controle de presença nos adestramentos de SIC são efetuados?	**100%**	**0%**
1.4	A função do Administrador da Rede Local está como encargo colateral ou figura na estrutura organizacional (Depto, Divisão etc) da OM?	**56%**	**44%**
1.5	O OSIC possui formação na área de TI (Curso Superior na área de TI)?	**74%**	**26%**
1.6	O ADMIN possui formação na área de TI (Curso Superior ou Técnico na área de TI)?	**73%**	**27%**
1.7	O ADMIN possui o curso de C-Exp-AdRedes (Oficiais) ou C-Sup-Linux (Praças)? Qual ano de sua realização?	**47%**	**53%**
1.8	O OSIC possui o curso de habilitação (C-Exp-AdRedes do CIAW)? Qual ano de sua realização? (citar o ano no campo de Obs)	**100%**	**0%**
1.10	São divulgadas notas da Instrução de Segurança da Informação e Comunicações (ISIC) em Plano do Dia (PD)?	**100%**	**0%**
1.11	Os usuários foram orientados sobre a proibição do uso de MODEMS em Estações de Trabalho e Servidores?	**100%**	**0%**
1.12	Os usuários foram orientados sobre a importância de se realizarem CÓPIAS DE SEGURANÇA (backup) das informações digitais armazenadas em suas Estações de Trabalho (ET)?	**100%**	**0%**
1.13	Os usuários foram orientados sobre a determinação de se utilizarem senhas e medidas de segurança em arquivos e pastas com informações sigilosas que estejam armazenados em suas Estações de Trabalho (ET)?	**100%**	**0%**
1.14	Os usuários foram orientados sobre as regras mínimas de segurança na utilização do CORREIO ELETRÔNICO e sua destinação exclusiva para fins corporativos?	**100%**	**0%**
1.15	Os usuários foram orientados sobre os possíveis ataques envolvendo técnicas de ENGENHARIA SOCIAL?	**99%**	**1%**
1.16	A mentalidade de segurança vem sendo mantida e passada para os usuários?	**100%**	**0%**
1.17	Todo o pessoal recém-embarcado recebe adestramento Básico de SIC?	**90%**	**10%**
2.0	**Administração da Rede.**		
2.1	O OSIC supervisiona a elaboração e a manutenção do Histórico da Rede Local (HRL) pelo ADMIN?	**98%**	**2%**
2.2	O ADMIN realiza as atualizações dos sistemas existentes no ambiente computacional e rede local da OM?	**100%**	**0%**
2.3	O ADMIN possui rígido controle e realiza a manutenção periódica das contas e dos direitos dos usuários?	**96%**	**4%**
2.4	O ADMIN mantém uma rotina de BACKUP dos dados dos servidores?	**87%**	**13%**
2.5	O ADMIN verifica periodicamente a integridade dos backups com testes de recuperação?	**79%**	**21%**

2.6	Os servidores e ET adotam a política de Regras Básicas de SENHA FORTE (mínimo 12 caracteres, usando caracteres especiais, números, letras maiúsculas e minúsculas) para o login de acesso e trocas periódicas dessas senhas?	**98%**	**2%**
2.7	Os servidores possuem instalados apenas softwares padronizados pela DCTIM e necessários à sua funcionalidade?	**96%**	**4%**
2.8	O acesso remoto aos servidores estão desabilitados?	**87%**	**13%**
2.9	Apenas as portas lógicas necessárias às atividades dos servidores estão habilitadas?	**97%**	**3%**
2.10	Os programas e sistemas operacionais instalados nos servidores estão atualizados com as últimas versões disponibilizadas?	**93%**	**7%**
2.11	Todos os Recursos Computacionais Críticos (RCC) nível 1, possuem senhas de configuração fortes e diferentes do fabricante?	**100%**	**0%**
2.12	Estão registrados no HRL, todos os acesso aos servidores através de conexão remota?	**96%**	**4%**
2.13	Todos os servidores possuem o antivírus instalado e atualizado?	**96%**	**4%**
2.14	Todos os programas das ET necessários para uso em Rede Local (RL) foram homologados e previamente autorizados pela DCTIM?	**90%**	**10%**
2.15	O acesso de ESTRANGEIROS à Rede Local é rigidamente controlado?	**100%**	**0%**
2.16	Os acessos de estrangeiros à Rede local da OM foram reportados formalmente à DCTIM?	**99%**	**1%**
2.17	A utilização de rede sem fio na OM foi homologada pela DCTIM?	**100%**	**0%**
2.18	O sistema de monitoramento por CFTV da OM está segregado da RECIM?	**88%**	**12%**
2.19	Todas as Estações de Trabalho estão de acordo com a DCTIMBOTEC 30/003/2018?	**67%**	**33%**
3.0	**Documentação**		
3.1	O OSIC foi formalmente nomeado por meio de Ordem de Serviço do Titular da OM?	**99%**	**1%**
3.2	O ADMIN foi formalmente nomeado por meio de Ordem de Serviço do Titular da OM?	**100%**	**0%**
3.3	A ISIC foi estabelecida e divulgada através de Ordem Interna da OM?	**97%**	**3%**
3.4	A ISIC é revisada periodicamente pelo OSIC e pelo ADMIN (em caso afirmativo, favor lançar em Obs qual a periodicidade)?	**98%**	**2%**
3.5	O Intervalo de revisão da ISIC está definido no corpo do documento?	**85%**	**15%**
3.6	O ADMIN auxilia o OSIC na divulgação da ISIC da OM?	**96%**	**4%**
3.7	O ADMIN mantém o registro da realização das cópias de segurança (BACKUP), e dos respectivos testes de recuperação dos backups, no histórico da rede local (HRL)?	**85%**	**15%**
3.8	Todos os usuários da OM assinaram o Termo de Responsabilidade Individual (TRI)?	**100%**	**0%**
3.9	O TRI é assinado por pessoal externo à OM que seja autorizado a executar serviços na Rede Local?	**88%**	**12%**
3.10	Todos os usuários da OM que receberam ET assinaram o Termo de Recebimento de Estação de Trabalho (TRE)?	**99%**	**1%**
3.11	Na Ordem Interna (OI) sobre o emprego de dispositivos móveis, consta(m):		
a)	as pessoas autorizadas a utilizarem tais dispositivos?	**92%**	**8%**
b)	os dispositivos autorizados (número de série)?	**65%**	**35%**
c)	os locais e compartimentos de utilização dos dispositivos?	**94%**	**6%**
d)	a finalidade de uso dos dispositivos?	**81%**	**19%**
e)	o horário autorizado?	**48%**	**52%**
3.12	O OSIC realiza Auditoria Interna na OM uma vez por ano?	**94%**	**6%**
3.13	A equipe de Auditoria Interna foi designada formalmente pelo Titular da OM?	**94%**	**6%**

3.14	O OSIC emitiu um Relatório de Auditoria (RAD) após a realização da Auditoria Interna?	**89%**	**11%**
3.15	O RAD é classificado como RESERVADO e guardado em local compatível com seu grau de sigilo?	**96%**	**4%**
3.16	O ADMIN elabora, controla e mantém atualizado o HRL?	**99%**	**1%**
3.17	O RAD foi arquivado no HRL?	**88%**	**12%**
3.18	O HRL está classificado com grau de sigilo RESERVADO?	**99%**	**1%**
3.19	O ADMIN registra nos TRE a lista dos programas instalados, incluindo os referentes à SIC homologados pela MB?	**99%**	**1%**
3.20	Nos Perímetros de Segurança, existe a proibição de entrada de dispositivos armazenadores de informações, contemplando tripulação e visitantes?	**96%**	**4%**
3.21	Por ocasião de cada visita a um Perímetro de Segurança é registrada data, hora, responsável na OM e razão da visita?	**89%**	**11%**
3.22	Os acessos físicos aos Perímetros de Segurança são monitorados/controlados?	**100%**	**0%**
3.23	Os Perímetros de Segurança estão demarcados localmente?	**99%**	**1%**
3.24	Os Perímetros de Segurança estão devidamente ilustrados no HRL?	**89%**	**11%**
3.25	Os Perímetros de Segurança estão claramente definidos na ISIC?	**96%**	**4%**
3.26	Os RCC estão identificados por um dos níveis de classificação de acordo com sua importância?	**98%**	**2%**
3.27	O ADMIN elaborou o Plano de Contingência (PLCONT)?	**92%**	**8%**
3.28	O PLCONT é revisado pelo ADMIN e OSIC anualmente?	**90%**	**10%**
3.29	O PLCONT foi classificado com o grau de sigilo RESERVADO?	**94%**	**6%**
3.30	Caso o usuário possua direito de administrador, o ADMIN registra no TRI do usuário?	**88%**	**12%**
3.31	O ADMIN mantém atualizados no Histórico de Rede Local (HRL) os Perfis e os Privilégios dos usuários?	**96%**	**4%**
3.32	O ADMIN efetua a remoção ou bloqueio de logins por motivo de desembarque dos usuários?	**100%**	**0%**
3.33	O HRL possui as 3 PARTES componentes?	**98%**	**2%**
3.34	As exceções quanto a proibição de dispositivos armazenadores de informações são controladas e registradas por meio de Ordem Interna ou de Ordem de Serviço?	**91%**	**9%**
3.35	Os usuários e o pessoal servindo no Setor de TI da OM estão cientes das publicações/normas de SIC emanadas pela MB?	**99%**	**1%**
4.0	**Estações de Trabalho**		
4.2	Os dispositivos de entrada/saída, tais como, portas USB, Modens, gravadores de CD/DVD e impressoras locais estão desabilitados nas ET?	**88%**	**12%**
4.3	O ADMIN possui as senhas de configuração (setup) de todas as ET da OM?	**100%**	**0%**
4.4	As ET possuem senha de inicialização (boot) de uso exclusivo do usuário que a utiliza?	**96%**	**4%**
4.5	O compartilhamento de arquivos e impressoras está desabilitado em todas as ET?	**94%**	**6%**
4.6	As ET possuem antivírus e demais programas de proteção individual homologados pela DCTIM, atualizados?	**99%**	**1%**
4.7	Nas ET estão instalados apenas os programas homologados pela DCTIM para criptografia de arquivos?	**99%**	**1%**
4.8	As ET possuem atualizações automáticas de patches dos Sistemas Operacionais e ferramentas de segurança (antivírus, antispyware e firewall pessoal)?	**100%**	**0%**
4.9	As ET possuem o agente do antivírus em vigor na MB instalado e funcionando corretamente?	**99%**	**1%**

4.10	Os equipamentos trazidos por pessoal externo à OM são verificados pelo ADMIN antes de serem utilizados na Rede Local?	**87%**	**13%**
4.11	Apenas usuários que possuam justificativa formal e autorização do Titular da OM, possuem privilégios de administrador da ET?	**85%**	**15%**
4.12	As ET são configuradas com privilégios mínimos pelo ADMIN antes de serem entregues aos usuários?	**99%**	**1%**
4.13	Todas as ET da OM possuem política de tela de login com senha e proteção de tela por inatividade (screensaver) com senha?	**99%**	**1%**
4.14	Sistemas legados são mantidos apenas através do uso de Máquinas Virtuais (VM)?	**84%**	**16%**
5.0	**Incidentes**		
5.1	Os INCIDENTES de SIC ocorridos foram reportados à DCTIM, com informação ao COMIMSUP?	**98%**	**2%**
5.2	As ET apreendidas para realização de forense computacional possuem Termo de Apreensão lavrado e assinado?	**100%**	**0%**
5.3	As ET apreendidas para realização de investigações são lacradas, isoladas e armazenadas em local seguro?	**100%**	**0%**
6.0	**Segurança Física**		
6.1	Estabilizadores/No-breaks que alimentam RCC 1 estão devidamente protegidos?	**96%**	**4%**
6.2	Os compartimentos não guarnecidos que contenham RCC 1 possuem segurança física reforçada, sistema de alarme, lacre e controle de entrada e saída?	**93%**	**7%**
6.3	Os gabinetes de proteção dos equipamentos de conectividade possuem controle rígido das chaves e dos lacres numerados?	**96%**	**4%**
6.4	Equipamentos RCC1 estão afastados de equipamentos geradores de interferência eletromagnética?	**100%**	**0%**
6.5	Equipamentos RCC 1 são alimentados por sistema de energia estabilizado e com proteção em caso de emergência (no-breaks)?	**97%**	**3%**
6.6	As mídias contendo o Backup são armazenadas em locais distintos ao dos equipamentos que contém as informações originais?	**88%**	**12%**
6.7	As mídias contendo o Backup são salvaguardadas em locais com proteção contra incêndio e alagamento?	**81%**	**19%**
6.8	As mídias contendo o Backup são classificadas com o mesmo grau de sigilo atribuído às informações nelas armazenadas?	**94%**	**6%**
6.9	Existe um acompanhamento constante do pessoal externo que encontra-se realizando serviço a bordo?	**100%**	**0%**
6.10	A OM possui locais apropriados, definidos em Ordem Interna, para acondicionar os dispositivos móveis pessoais e funcionais?	**97%**	**3%**
7.0	**Conformidades**		
7.1	Existe algo que impeça ou dificulte o atendimento das orientações normativas de SIC ou a consolidação de sua mentalidade pelo setor de Tecnologia da Informação e Comunicação ou pelos usuários?	**18%**	**82%**
7.2	O setor de Tecnologia da Informação e Comunicações (TIC) participa de Reuniões de Gestão da OM?	**79%**	**21%**
7.3	As decisões relacionadas com a Segurança da Informação e Comunicações são tomadas exclusivamente pela área de TIC (sim) ou em conjunto com o setor responsável pelas decisões estratégicas da OM (não)?	**58%**	**42%**
7.4	O setor de Tecnologia da Informação e Comunicações (TIC) elabora um Plano de Gestão de Riscos de SIC?	**54%**	**46%**
7.5	A OM possui no seu quadro de pessoal de apoio à Tecnologia da Informação e	**48%**	**52%**

	Comunicações (TIC), o número adequado de militares/civis para exercer de forma eficiente as atividades de suporte técnico aos serviços de TIC?		
7.6	O setor de TIC da OM disponibiliza para os usuários uma pesquisa de satisfação, por meio de questionários, para avaliar a percepção quanto a qualidade dos suportes técnicos realizados, assim como, identificar as possibilidades de melhoria dos serviços prestados de TIC?	**43%**	**57%**
7.7	O setor de TIC da OM aplicou alguma ação restritiva de segregação, contenção, suspensão de provisão de produtos e serviços, após a identificação de Não Conformidade (não atendimento) dos requisitos regulamentários ou de incidentes de SIC?	**4%**	**96%**
7.8	Qual o Nível de cumplicidade e comprometimento dos usuários da OM, quanto a Gestão de Segurança da Informação e Comunicações (SIC)? ( ) Baixo (não) ( ) Médio (não) ( ) Alto (sim)	**53%**	**47%**
8.0	**Inspeções/auditorias - Centro Local de Tecnologia da Informação (CLTI)**		
8.1	São verificados nas inspeções pelo CLTI, todos os pontos das normas de SIC?	**99%**	**1%**
8.2	O CLTI utiliza todo o tempo destinado para realização das suas inspeções/auditorias?	**98%**	**2%**
8.3	Nas inspeções/auditorias pelo CLTI são realizadas verificações nas Estações de Trabalho dos usuários?	**98%**	**2%**
8.4	Qual o grau de criticidade utilizado nas inspeções/auditorias pelo CLTI? ( ) Baixo (não) ( ) Médio (não) ( ) Alto (sim)	**74%**	**26%**

Obs: Os itens descritos no campo "Nº" da tabela abaixo, correspondem aos mesmos números dos questionamentos encaminhados aos colaboradores.

No	Descrição dos questionamentos aos ADMIN das OM	Valor retirado dos questionários	Valor contido na Publicação MB	Valor referente nas empresas privadas
1.9	Quantidade de pessoas que servem nos setores de TIC (suporte) das OM colaboradoras?	**429**	**7**	**5,1**
4.1	Quantidade de Estações de Trabalho (ET)/Servidores que as OMs colaboradoras possuem?	**34095**	**750**	**100**
1.9 e 4.1	**Relação** média do número de pessoas do setor de TIC das OM, que prestam suporte aos usuários, pelo número de Estações de Trabalho (ET) / Servidores das OMs:	**1/28**	**1/107**	**1/20**

Tabela 1: Resultados dos Questionários Estruturados Admin (Apêndice A)

II. Respostas dos questionários aos Centro Locais de Tecnologia e Informática (CLTI)

Obs: Os itens descritos no campo "Nº" da tabela abaixo, correspondem aos mesmos números dos questionamentos encaminhados aos colaboradores.

No	Descrição dos questionamentos aos CLTI	Respostas %	
		SIM	NÃO
4	Nas inspeções/auditorias realizadas é verificado o fiel cumprimento de todos os pontos das normas de Segurança da Informação e Comunicações (SIC)?	100%	0%
5	Os inspecionados têm o mínimo de conhecimento técnico e das normas de Segurança da Informação e Comunicações (SIC)?	91%	9%
8	As OM consideram a política e a gestão da Segurança da Informação e Comunicações (SIC) como questão estratégica?	78%	22%

9	Existe uma conscientização da Gestão da Segurança da Informação e Comunicações (GSIC) por parte das OM?	96%	4%
10	As OM mantêm um Plano de Gerenciamento de Riscos de SIC?	70%	30%
11	As OM possuem no seu quadro de pessoal de apoio à Tecnologia da Informação e Comunicações (TIC), o número adequado de militares/civis para exercer de forma eficiente as atividades de suporte técnico aos serviços de TIC?	52%	48%
12	A Marinha do Brasil possui todas as publicações necessárias a fim de atender a SIC?	83%	17%
13	Existe de forma explícita um conjunto de publicações, orientações normativas e regulamentos que as OM são obrigadas a seguir?	100%	0%
14	O CLTI aplicou alguma ação restritiva de segregação, contenção, suspensão de provisão de produtos e serviços nas OM, após a identificação de Não Conformidade (não atendimento) dos requisitos regulamentários ou de incidentes de SIC?	35%	65%
15	Existe algo que impeça ou dificulte o atendimento das orientações normativas de SIC ou a consolidação de sua mentalidade pelas OM da MB?	35%	65%

Obs: Os itens descritos no campo "Nº" da tabela abaixo, correspondem aos mesmos números dos questionamentos encaminhados aos colaboradores.

No	Descrição dos questionamentos aos CLTI	Valor retirado dos questionários	Valor contido na Publicação MB
1	Qual a quantidade de pessoas de TI que trabalhão nos CLTI colaboradores?	**248**	**7**
2	Qual a quantidade de Estações de Trabalho (ET)/Servidores apoiadas pelos CLTI colaboradores?	**34095**	**750**
1 e 2	**Relação** média do número de pessoas do setor de TIC dos CLTI, que prestam suporte as OM, pelo número de Estações de Trabalho (ET) / Servidores das OMs apoiadas:	**1/137**	**1/107**
7	**Relação** do número de OM sob jurisdição dos CLTI colaboradores pelo número de discrepâncias de SIC das OM, que foram observadas nas inspeções/ verificações de TIC, nos anos de 2018 e 2019:	**1/3**	

Tabela 2: Resultados dos Questionários Estruturados CLTI (Apêndice B)

4.2 Análise e avaliação das Demandas Apontadas nas Não Conformidades dos objetivos da Gestão da Segurança da Informação e Comunicações nas Organizações Militares da MB

Além da atual situação da gestão de SIC na MB, o estudo de caso proposto neste trabalho através dos questionários verificadores de conformidade com as publicações da MB, constatou outros pontos sobre os quais pode-se atuar para melhorar a segurança da informação, que serão citados no item 4.5 Considerações Finais.

A análise dos dados deste estudo permitiu concluir que, de uma forma geral, os usuários apresentam-se como uma proteção para a SIC das OM, pelo fato de assumirem comportamentos e atitudes corretas na maioria dos procedimentos de segurança recomendados pelas publicações vigentes da MB. Como positivo, no comportamento e atitude

revelados pelos usuários, destacamos os seguintes 25 questionamentos (20,33% do total dos questionamentos), com 100% de atendimento:

Obs: Os itens descritos no campo "Nº" da tabela abaixo, correspondem aos mesmos números dos questionamentos encaminhados aos colaboradores.

Nº	Descrição dos questionamentos aos ADMIN das OM	Respostas %	
1.0	**Adestramento**	**SIM**	**NÃO**
1.2	Os Planos de Adestramentos de SIC englobam o conjunto mínimo de temas previstos no artigo 10.11 da DGMM-0540?	**100%**	**0%**
1.3	Os meios de controle de presença nos adestramentos de SIC são efetuados?	**100%**	**0%**
1.8	O OSIC possui o curso de habilitação (C-Exp-AdRedes do CIAW)? Qual ano de sua realização? (citar o ano no campo de Obs)	**100%**	**0%**
1.10	São divulgadas notas da Instrução de Segurança da Informação e Comunicações (ISIC) em Plano do Dia (PD)?	**100%**	**0%**
1.11	Os usuários foram orientados sobre a proibição do uso de MODEMS em Estações de Trabalho e Servidores?	**100%**	**0%**
1.12	Os usuários foram orientados sobre a importância de se realizarem CÓPIAS DE SEGURANÇA (backup) das informações digitais armazenadas em suas Estações de Trabalho (ET)?	**100%**	**0%**
1.13	Os usuários foram orientados sobre a determinação de se utilizarem senhas e medidas de segurança em arquivos e pastas com informações sigilosas que estejam armazenados em suas Estações de Trabalho (ET)?	**100%**	**0%**
1.14	Os usuários foram orientados sobre as regras mínimas de segurança na utilização do CORREIO ELETRÔNICO e sua destinação exclusiva para fins corporativos?	**100%**	**0%**
1.16	A mentalidade de segurança vem sendo mantida e passada para os usuários?	**100%**	**0%**
2.0	**Administração da Rede.**		
2.2	O ADMIN realiza as atualizações dos sistemas existentes no ambiente computacional e rede local da OM?	**100%**	**0%**
2.11	Todos os Recursos Computacionais Críticos (RCC) nível 1, possuem senhas de configuração fortes e diferentes do fabricante?	**100%**	**0%**
2.15	O acesso de ESTRANGEIROS à Rede Local é rigidamente controlado?	**100%**	**0%**
2.17	A utilização de rede sem fio na OM foi homologada pela DCTIM?	**100%**	**0%**
3.0	**Documentação**		
3.2	O ADMIN foi formalmente nomeado por meio de Ordem de Serviço do Titular da OM?	**100%**	**0%**
3.8	Todos os usuários da OM assinaram o Termo de Responsabilidade Individual (TRI)?	**100%**	**0%**
3.22	Os acessos físicos aos Perímetros de Segurança são monitorados/controlados?	**100%**	**0%**
3.32	O ADMIN efetua a remoção ou bloqueio de logins por motivo de desembarque dos usuários?	**100%**	**0%**
4.0	**Estações de Trabalho**		
4.3	O ADMIN possui as senhas de configuração (setup) de todas as ET da OM?	**100%**	**0%**
4.8	As ET possuem atualizações automáticas de patches dos Sistemas Operacionais e ferramentas de segurança (antivírus, antispyware e firewall pessoal)?	**100%**	**0%**
5.0	**Incidentes**		
5.2	As ET apreendidas para realização de forense computacional possuem Termo de Apreensão lavrado e assinado?	**100%**	**0%**

5.3	As ET apreendidas para realização de investigações são lacradas, isoladas e armazenadas em local seguro?	**100%**	**0%**
6.0	**Segurança Física**		
6.4	Equipamentos RCC1 estão afastados de equipamentos geradores de interferência eletromagnética?	**100%**	**0%**
6.9	Existe um acompanhamento constante do pessoal externo que encontra-se realizando serviço a bordo?	**100%**	**0%**

Nº	**Descrição dos questionamentos aos CLTI**	**Respostas %**	
		SIM	**NÃO**
4	Nas inspeções/auditorias realizadas é verificado o fiel cumprimento de todos os pontos das normas de Segurança da Informação e Comunicações (SIC)?	100%	0%
13	Existe de forma explícita um conjunto de publicações, orientações normativas e regulamentos que as OM são obrigadas a seguir?	100%	0%

Tabela 3: Resultados dos Questionários Estruturados com 100% de atendimento

A MB é uma instituição que sempre primou pela organização e segurança. Com isso, não se espera que uma auditoria resulte num aumento de eficiência ou eficácia maior do que 5 a 10%. Mas é justamente com esse constante e gradual crescimento que a MB vem vencendo a “guerra contra o desgaste natural do tempo”, mantendo seus navios e OM organizados e seguros, e contornando as sérias restrições orçamentárias.

Dessa forma, com relação aos resultados obtidos por meioda aplicação dos questionários, somente foram avaliados os objetivos/questionamentos, que obtiveram valores acima de 10% de Não Conformidades, correspondendo a 40% do total dos questionamentos.

I. Avaliação das respostas dos questionários aos Administradores (Admin) das Organizações Militares da MB

No	**Descrição dos questionamentos aos Administradores das OM**	**SIM**	**NÃO**
1.4	A função do Administrador da Rede Local está como encargo colateral ou figura na estrutura organizacional (Depto, Divisão etc) da OM?	**56%**	**44%**

Foram considerados quatro cargos ou vínculos hierárquicos: colateral, departamento de administração, departamento técnico ou assessoramento do comando (56% correspondem aos encargos colateral e departamento de administração, e 44% aos cargos de assessoramento e departamento técnico). Esse questionamento será comentado no item 4.5 Considerações Finais.

1.5	O OSIC possui formação na área de TI (Curso Superior na área de TI)?	**74%**	**26%**

A análise permite verificar que 26% dos respondentes estão em desacordo com o

Artigo 8.6 da DGMM-0540, que orienta que o Oficial ou civil assemelhado tenha, preferencialmente, formação nível superior e realizado o curso do SEN necessário para auditoria em redes locais.

1.6	O ADMIN possui formação na área de TI (Curso Superior ou Técnico na área de TI)?	**73%**	**27%**

De acordo com o observado, 27% dos respondentes estão em desacordo com o Artigo 8.8 da DGMM-0540, não tendo 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.

1.7	O ADMIN possui o curso de C-Exp-AdRedes (Oficiais) ou C-Sup-Linux (Praças)? Qual ano de sua realização?	**47%**	**53%**

Como se pode observar pelos dados, a grande maioria dos respondentes (53%) está em desacordo com o Artigo 8.8 da DGMM-0540, não possuindo capacitação em Administração de Rede de Computadores e para os sistemas operacionais que estejam sendo utilizados dentro da OM, assim como conhecimentos mínimos em auditoria de sistemas computacionais.

1.17	Todo o pessoal recém-embarcado recebe adestramento Básico de SIC?	**90%**	**10%**

Tendo em atenção os valores obtidos, este questionamento mostra que 90% estão de acordo com o Artigo 9.9.1 da DGMM-0540, podendo considerar que os usuários apresentam comportamentos e atitudes aceitáveis quanto a todo pessoal recém-embarcado receber um adestramento básico de SIC antes de iniciar o desempenho de qualquer atividade.

2.4	O ADMIN mantém uma rotina de BACKUP dos dados dos servidores?	**87%**	**13%**

De acordo com os dados observados, 13% estão em desacordo com o Inciso 9.5.10 da DGMM-0540, que prescreve que as OM devem melhorar o seu comportamento e atitude, procurando ser mais prudentes, e verificar a execução e atendimento a periodicidade de realização das cópias de segurança, em relação às informações digitais armazenadas nos equipamentos servidores da rede local.

2.5	O ADMIN verifica periodicamente a integridade dos backups com testes de recuperação?	**79%**	**21%**

Cerca de 21% das OM estão em desacordo com o inciso 9.5.10 da DGMM-0540, isto é, não estão verificando periodicamente a integridade das cópias de segurança e nem efetuando testes de recuperação de informações digitais armazenadas. Como no

questionamento anterior (2.4) e pela sua importância(2.4), os administradores de rede, devem melhorar o seu comportamento e atitude, procurando ser mais prudentes.

2.8	O acesso remoto aos servidores estão desabilitados?	**87%**	**13%**

Os respondentes mostraram que 13% estão em desacordo com o Inciso 9.5.2 da DGMM-0540, revelando estar com os terminais de acesso remoto habilitados. Dessa forma, expõem uma vulnerabilidade preocupante, pois há possibilidade de acesso remoto aos RCC nível 1 da OM, sem prévia autorização da DCTIM.

2.14	Todos os programas das ET necessários para uso em Rede Local (RL) foram homologados e previamente autorizados pela DCTIM?	**90%**	**10%**

Como se pode observar, 10% das OM estão em desacordo com o Inciso 9.5.14 da DGMM-0540 neste questionamento. Reforçando que 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.

2.18	O sistema de monitoramento por CFTV da OM está segregado da RECIM?	**88%**	**12%**

Nesse questionamento, 12% das OM estão em desacordo com o Inciso 4.13.2 do CGCFN-315, revelando ter um comportamento e uma atitude não recomendados, comprometendo segurança da Rede de Dados da MB (RECIM), por não estar segregada.

2.19	Todas as Estações de Trabalho estão de acordo com a DCTIMBOTEC 30/003/2018?	**67%**	**33%**

Cerca de 33% das OM estão em desacordo com a DCTIMBOTEC 30/003/2018, revelando que as configurações das Estações de Trabalho (ET) Padrão e respectivos aplicativos (softwares) para utilização no âmbito da MB não estão sendo atendidas e, dessa forma, podem comprometer a SIC.

3.5	O Intervalo de revisão da ISIC está definido no corpo do documento?	**85%**	**15%**

Segundo os respondentes, 15% das OM estão em desacordo com o Artigo 10.3 da DGMM-0540, pois revelam não descrever o intervalo entre as revisões da ISIC no seu próprio corpo – que não deveria ser superior a 2 (dois) anos, comprometendo a atualização de novas orientações.

3.7	O ADMIN mantém o registro da realização das cópias de segurança (BACKUP), e dos respectivos testes de recuperação dos backups, no histórico da rede local (HRL)?	**85%**	**15%**

De acordo com o observado, 15% das OM estão em desacordo com a Alínea “e”

do inciso 9.5.10 da DGMM-0540, que estabelece que se deve manter um controle da elaboração de cópias de segurança e dos respectivos testes de recuperação, controle que deve ser regulado na ISIC da OM, no HRL. Relembra-se que os administradores de rede devem providenciar esses registros para manter um controle da execução.

3.9	O TRI é assinado por pessoal externo à OM que seja autorizado a executar serviços na Rede Local?	**88%**	**12%**

A maioria dos respondentes, 88% das OM, está de acordo com o Inciso 9.4.6 da DGMM-0540, reconhecendo a importância de que o pessoal externo envolvido na realização desses serviços realizem a assinatura do Termo de Responsabilidade Individual (Apêndice C)". Esse procedimento alerta os usuários dos seus deveres e direitos de SIC dentro da OM.

3.11	Na Ordem Interna (OI) sobre o emprego de dispositivos móveis, consta(m):		
b)	os dispositivos autorizados (número de série)?	**65%**	**35%**
d)	a finalidade de uso dos dispositivos?	**81%**	**19%**
e)	o horário autorizado?	**48%**	**52%**

Neste questionamento, constata-se que cerca de 35% das OM (média) estão em desacordo com o inciso 12.4.2 da DGMM-0540, que estabelece orientações sobre a utilização dos dispositivos móveis. Nesse caso, todas as exceções deverão ser registradas por meio de Ordem Interna. Esse procedimento exige máxima atenção por parte dos usuários, para que não adotem comportamentos de risco para SIC.

3.14	O OSIC emitiu um Relatório de Auditoria (RAD) após a realização da Auditoria Interna?	**89%**	**11%**

Como se pode observar, 11% das OM está em desacordo com a Alínea "e" do Artigo 8.7 da DGMM-0540, que estabelece a necessidade de elaboração do Relatório de Auditoria (RAD), conforme as normas vigentes, e sua submissão à aprovação da DCTIM no prazo estabelecido. Relembra-se a importância do documento, que descreverá todos os registros de vulnerabilidade de SIC ad OM.

3.17	O RAD foi arquivado no HRL?	**88%**	**12%**

Neste procedimento, 12% das OM estão em desacordo com a Alínea "j" do Artigo 8.6 da DGMM-0540, que estabelece que, após a emissão do Relatório de Auditoria (RAD), o mesmo deverá ser arquivado no HRL.

3.21	Por ocasião de cada visita a um Perímetro de Segurança é registrada data, hora, responsável na OM e razão da visita?	**89%**	**11%**

Como se pode observar, 11% das OM estão em desacordo com a Alínea "a" do

Inciso 9.4.1 da DGMM-0540, que determina que os visitantes de perímetros de segurança devem ser identificados na sua entrada, com registro de data, hora e razão da visita. Enfatize-se que o não cumprimento desse procedimento pode expor os Sistemas de Tecnologia da Informação da MB.

3.24	Os Perímetros de Segurança estão devidamente ilustrados no HRL?	**89%**	**11%**

De acordo com os resultados, 11% das OM estão em desacordo com o Inciso 9.4.1 da DGMM-0540, pois os perímetros de segurança não estão claramente definidos na "Instrução de Segurança da Informação e Comunicações" (ISIC) da OM, ilustrados no seu Histórico da Rede Local (HRL) e demarcados localmente. Relembra-se a importância dessa ação, a fim de serem demarcadas as áreas que contêm informações sensíveis, para que possam ser atribuídos os tratamentos devidos.

3.28	O PLCONT é revisado pelo ADMIN e OSIC anualmente?	**90%**	**10%**

Como se pode observar, 10% das OM estão em desacordo com a Alínea "g" do Artigo 8.6 e Alínea "c" do Artigo 10.4 da DGMM-0540, que estabelece que o administrador da rede deve supervisionar a elaboração e a manutenção do Plano de Contingência (PLCONT). Esse Plano é fundamental par que sejam tomadas as medidas cabíveis na inoperância dos serviços de TI.

3.30	Caso o usuário possua direito de administrador, o ADMIN registra no TRI do usuário?	**88%**	**12%**

Em face desses resultados, verifica-se que 12% das OM estão em desacordo com a Alínea "p" do Artigo 8.8 da DGMM-0540, que determina 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. Esse procedimento é de vital importância, para que as Estações de Trabalho sejam devidamente controladas e não venham a ser um meio de acesso a rede local da MB.

4.2	Os dispositivos de entrada/saída, tais como, portas USB, Modens, gravadores de CD/DVD e impressoras locais estão desabilitados nas ET?	**88%**	**12%**

Pela observação dos resultados, 12% das OM estão em desacordo com a Alínea "f" do inciso 9.5.4 da DGMM-0540, que obriga 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. O setor de TI das OM tem que ter consciência do perigo do não cumprimento deste procedimento e adequar o seu comportamento, de acordo com o recomendado, para não colocar em risco a segurança dos

Sistemas de Informação da MB.

4.10	Os equipamentos trazidos por pessoal externo à OM são verificados pelo ADMIN antes de serem utilizados na Rede Local?	**87%**	**13%**

Da análise, 13% das OM estão em desacordo com a Alínea "t" do Artigo 8.8 da DGMM-0540, que estabelece 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, configurado para que o usuário criado não tenha privilégios de administrador de sistemas e sem arquivo ou documento pertencente a MB no equipamento.

4.11	Apenas usuários que possuam justificativa formal e autorização do Titular da OM, possuem privilégios de administrador da ET?	**85%**	**15%**

Como se pode observar, 15% das OM estão em desacordo com a Alínea "p" do Artigo 8.8 da DGMM-0540, que permite atribuir privilégios de administrador nas estações de usuários àqueles devidamente autorizados pelo Titular da OM, com as respectivas justificativas. Os administradores da rede, junto do OSIC deverão atender conforme orientações contidas no questionamento supra 3.3.

4.14	Sistemas legados são mantidos apenas através do uso de Máquinas Virtuais (VM)?	**84%**	**16%**

De acordo com o observado, 16% das OM estão em desacordo com a DCTIMBOTEC 33/001/2020, que versa sobre os procedimentos para a instalação do software Oracle VM VirtualBox em uma ET, para uso exclusivo dos sistemas incompatíveis com os homologados pela MB e suportados pelos fabricantes. O não atendimento desta orientação deixa as Estações de Trabalho vulneráveis e, consequentemente, expostas a incidentes, devido a não atualizações dos seus softwares pelos fabricantes.

6.6	As mídias contendo o Backup são armazenadas em locais distintos ao dos equipamentos que contém as informações originais?	**88%**	**12%**

Nesse procedimento, e segundo o ilustrado, 12% das OM estão em desacordo com a Alínea "f" do inciso 9.5.10 da DGMM-0540, que orienta para uma maior segurança das informações digitais e contingência, armazenar as cópias de segurança (*backup*), sempre que possível, em prédio distinto ao do equipamento servidor do qual foi feita a respectiva cópia de segurança.

6.7	As mídias contendo o Backup são salvaguardadas em locais com proteção contra incêndio e alagamento?	**81%**	**19%**

Nesse questionamento, 19% das OM estão em desacordo com a Alínea "f" do

inciso 9.5.10 da DGMM-0540, que determina acondicionar uma das cópias de segurança em compartimentos ou armários com proteção contra incêndio e alagamento.

7.1	Existe algo que impeça ou dificulte o atendimento das orientações normativas de SIC ou a consolidação de sua mentalidade pelo setor de Tecnologia da Informação e Comunicação ou pelos usuários?	**18%**	**82%**

Como se pode observar, 18% das OM estão em Não Conformidade. Nesse caso, as respostas em "SIM" denotam o não atendimento ao questionamento. A avaliação da resposta deste questionamento será comentada no item 4.5 Considerações.

7.2	O setor de Tecnologia da Informação e Comunicações (TIC) participa de Reuniões de Gestão da OM?	**79%**	**21%**

Como se pode observar, 21% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

7.3	As decisões relacionadas com a Segurança da Informação e Comunicações são tomadas exclusivamente pela área de TIC (sim) ou em conjunto com o setor responsável pelas decisões estratégicas da OM (não)?	**58%**	**42%**

Como se pode observar, 58% das OM em Não Conformidade. Nesse caso as respostas em "SIM" denotam o não atendimento ao questionamento. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

7.4	O setor de Tecnologia da Informação e Comunicações (TIC) elabora um Plano de Gestão de Riscos de SIC?	**54%**	**46%**

Como se pode observar, 46% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

7.5	A OM possui no seu quadro de pessoal de apoio à Tecnologia da Informação e Comunicações (TIC), o número adequado de militares/civis para exercer de forma eficiente as atividades de suporte técnico aos serviços de TIC?	**48%**	**52%**

Como se pode observar, 52% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

7.6	O setor de TIC da OM disponibiliza para os usuários uma pesquisa de satisfação, por meio de questionários, para avaliar a percepção quanto a qualidade dos suportes técnicos realizados, assim como, identificar as possibilidades de melhoria dos serviços prestados de TIC?	**43%**	**57%**

Como se pode observar, 57% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

7.7	O setor de TIC da OM aplicou alguma ação restritiva de segregação, contenção,	**4%**	**96%**

	suspensão de provisão de produtos e serviços, após a identificação de Não Conformidade (não atendimento) dos requisitos regulamentários ou de incidentes de SIC?		

Como se pode observar, 96% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

7.8	Qual o Nível de cumplicidade e comprometimento dos usuários da OM, quanto a Gestão de Segurança da Informação e Comunicações (SIC)? ( ) Baixo (não) ( ) Médio (não) ( ) Alto (sim)	**53%**	**47%**

Como se pode observar, 47% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

8.4	Qual o grau de criticidade utilizado nas inspeções/auditorias pelo CLTI? ( ) Baixo (não) ( ) Médio (não) ( ) Alto (sim)	**74%**	**26%**

Como se pode observar, 26% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

No	Descrição dos questionamentos aos ADMIN das OM	Valor retirado dos questionários	Valor contido na publicação MB	Valor referente das empresas privadas
1.9	Quantidade de pessoas que servem nos setores de TIC (suporte) das OM colaboradoras?	**429**	**7**	**5,1**
4.1	Quantidade de Estações de Trabalho (ET)/Servidores que as OMs colaboradoras possuem?	**12.219**	**750**	**100**
1.9 e 4.1	**Relação** média do número de pessoas do setor de TIC das OM, que prestam suporte aos usuários, pelo número de Estações de Trabalho (ET) / Servidores das OMs:	**1/28**	**1/107**	**1/20**

A avaliação da resposta deste questionamento será comentada no item 4.5 Considerações.

II. Avaliação das respostas dos questionários aos Centro Locais de Tecnologia e Informática (CLTI)

No	Descrição dos questionamentos aos CLTI	SIM	NÃO
8	As OM consideram a política e a gestão da Segurança da Informação e Comunicações (SIC) como questão estratégica?	**78%**	**22%**

Como se pode observar, 22% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações.

10	As OM mantêm um Plano de Gerenciamento de Riscos de SIC?	**70%**	**30%**

Como se pode observar, 30% das OM em Não Conformidade com o capítulo 11

da SGM-107. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações, levando também em consideração o questionamento 7.4.

11	As OM possuem no seu quadro de pessoal de apoio à Tecnologia da Informação e Comunicações (TIC), o número adequado de militares/civis para exercer de forma eficiente as atividades de suporte técnico aos serviços de TIC?	**52%**	**48%**

Como se pode observar, 48% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações, levando também em consideração o questionamento 7.5.

14	O CLTI aplicou alguma ação restritiva de segregação, contenção, suspensão de provisão de produtos e serviços nas OM, após a identificação de Não Conformidade (não atendimento) dos requisitos regulamentários ou de incidentes de SIC?	**35%**	**65%**

Como se pode observar, 65% das OM em Não Conformidade. A avaliação da resposta desse questionamento será comentada no item 4.5 Considerações, levando também em consideração o questionamento 7.7.

15	Existe algo que impeça ou dificulte o atendimento das orientações normativas de SIC ou a consolidação de sua mentalidade pelas OM da MB?	**35%**	**65%**

Como se pode observar, 35% das OM em Não Conformidade. Nesse caso as respostas contidas na coluna “SIM” denotam o não atendimento ao questionamento. A avaliação da resposta desse questionamento será comentada no item 4.5 “Considerações” deste trabalho, em consonância a resposta do questionamento 7.1.

No	**Descrição dos questionamentos aos CLTI**	**Valor retirado dos questionários**	**Quantidade contida na Publicação MB**
1	Qual a quantidade de pessoas de TI que trabalhão nos CLTI colaboradores?	**248**	**7**
2	Qual a quantidade de Estações de Trabalho (ET)/Servidores apoiadas pelos CLTI colaboradores?	**34.095**	**750**
1 e 2	**Relação** média do número de pessoas do setor de TIC dos CLTI, que prestam suporte as OM, pelo número de Estações de Trabalho (ET) / Servidores das OMs apoiadas:	**1/137**	**1/107**

A avaliação das respostas desse questionamento será comentado no item 4.5 Considerações.

7	Relação do número de OM sob jurisdição dos CLTI colaboradores pelo número de discrepâncias de SIC das OM, que foram observadas nas inspeções/ verificações de TIC, nos anos de 2018 e 2019:	**1/3**

A avaliação das respostas desse questionamento será comentado no item 4.5 Considerações.

4.3 Considerações

Em face do presente estudo, listam-se a seguir algumas considerações sumarizadas, derivadas da análise e avaliação dos principais cenários de decisão, estruturas e mecanismos de governança de SIC, identificados nos contextos organizacionais observados:

1. Estudos de caso, semelhante ao realizado neste trabalho, relativo à gestão da SIC na MB, podem inclusive ser utilizados para preparar e orientar organizações para que estejam em conformidade com os requisitos e políticas de SIC aos quais estão sujeitas. Assim sendo, pode-se utilizar estudos como este como forma de preparação para auditorias, com o intuito de identificar eventuais falhas e adequações necessárias.

2. Os usuários são um dos elementos que podem provocar vulnerabilidades e eventuais danos nos SI, pelo que é pertinente verificar se estão sensibilizados para a utilização de práticas corretas e seguras no desempenho das suas tarefas.

3. Para Dhillon (2001), os problemas relacionados com a segurança ocorrem devido à ausência de medidas de segurança da informação na organização. Até pode existir uma estrutura de medidas na organização, no entanto, é preciso transmiti-la corretamente aos colaboradores através dos canais de comunicação adequados.

4. Desenvolver um conjunto de políticas de segurança da informação é o primeiro e mais importante passo para preparar a organização contra eventuais ataques, quer tenham origem interna ou externa.

A segurança da informação envolve uma construção multifacetada e a sua gestão exige que tenham que ser consideradas questões não apenas técnicas, mas também organizacionais, estruturais, comportamentais e aspetos sociais (Dhillon, 2004).

5. Neste trabalho foram considerados quatro cargos ou vínculos hierárquicos do setor de TI/Administrador da Rede Local: colateral; departamento de administração; departamento técnico; e assessoramento do comando (56% correspondem aos encargos colateral e departamento de administração e 44% aos cargos de assessoramento/Comando e departamento técnico). Uma hierarquia bem estruturada é importante para uma empresa se

manter no caminho certo dentro do seu negócio. Por isso, seria de suma importância que as atividades de TI/administrador da rede fiquem diretamente subordinadas ao Chefe de Estado-Maior/Imediato/Vice-Diretor ou a um Departamento de TI, pelo fato de que suas tarefas repercutem em toda OM e em face da sua importância estratégica.

6. Necessidade de um planejamento, com o propósito de elaborar um documento, que identificaria a necessidade a ser atendida pelos profissionais de TI, gerenciando a capacitação dos profissionais de TI de toda a MB nas tecnologias utilizadas e treinamento. Enfatize-se a importância da definição das atividades necessárias para capacitação e desenvolvimento de competências que vão apoiar as atividades de TI na OM. Portanto, é essencial que a capacitação seja planejada e implementada com a devida importância e em sua plenitude, a fim de que o pessoal treinado esteja disponível para atender todas as necessidades de SIC. Considera-se requisito para a OM que se propõe a interagir com as atividades de SIC, ter um mínimo de conhecimento técnico para esse fim. 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.

7. Os aspectos positivos também devem ser destacados, com a ressalva de que o fato de uma OM estar organizada e segura é algo normal e rotineiro na MB. Por isso, deve ser considerado como positivo quando em uma auditoria for verificado que uma OM possui organização e/ou esteja dentro das condições de SIC acima da média encontrada nas OM da MB.

8**.** As OM devem, além dos mecanismos de SIC definidos na publicação DGMM-540, dar ênfase às seguintes medidas de segurança:

- Aplicar as atualizações de segurança recomendadas
- Utilizar e atualizar com frequência os programas antivírus e antispyware
- Realizar cópias de segurança com regularidade
- Utilizar senhas robustas e diferentes em cada aplicação
- Armazenar/enviar/transferir a sua informação de forma encriptada
- Não partilhar a informação do seu computador com outros
- Não compartilhar ou divulgar as suas senhas com os outros
- Ser responsável e cuidadoso na utilização da Internet e do correio eletrônico
- Ser cuidadoso na utilização de equipamentos de armazenamento externos
- Informar ao setor TI, no caso de incidentes com vírus, roubos ou perdas de

informação

– Estar ciente que todos os atos praticados têm consequências

– Bloquear/desligar o computador quando se ausentar

– Não utilizar software ilegal/não homologados ou de compartilhamento de arquivos.

9. Quanto aos valores médios obtidos dos questionamentos 7.1 (18% de atendimento) e o 15 (35% de atendimento), é oportuno enfocar algumas opiniões dos respondentes:

– "Conscientização dos titulares das OM da importância do cumprimento das orientações de SIC e de conscientização dos seus militares subordinados"

– "O desconhecimento das normas de SIC, dificultando sua implementação e manutenção, por parte das OM, além da rotatividade e quantitativo de pessoal"

– "O número de ET associado ao pouco número de pessoas no CLTI, dificultam a cobrança e melhoria dos serviços"

– "A MB deveria investir em cursos básicos de SIC que permitam a conscientização dos profissionais da MB na SIC. Além disso, a estrutura de apoio à SIC está subdimensionada para a MB, faltam pessoal qualificado, faltam ferramentas que permitam um maior e melhor controle das atividades realizadas nas ET vinculadas à rede interna da MB. Além disso falta pessoal qualificado nas ferramentas de SIC disponibilizadas na MB.

Soma-se ao comentário anterior o fato da rotatividade de pessoal, uma constante em uma organização como a MB, e a falta de padronização de mão de obra, fruto que eventuais substitutos designados que, por vezes, não possuem os conhecimentos suficientes, sendo necessário investir em treinamento extra-MB para que o militar possa exercer sua função."

– "A não gerência de alguns softwares, impede a ação imediata do CLTI, sendo necessário solicitar apoio da CTIM"

10. Com relação à GRSIC, a Não Conformidade de 46%, no questionamento 7.4, apenas ressalta a importância do fiel cumprimento das medidas objetivamente voltadas para o pessoal da MB, definidas no item 10.1 da DGMM-540, que 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 às ações para avaliação de vulnerabilidades, riscos ou incidentes que possam ocorrer no ambiente da rede local, auxiliando ações preventivas, corretivas e de planejamento.

Ressaltam-se, como fator preponderante para o não cumprimento da GRSIC, os cancelamentos observados: do encaminhamento dos Relatórios de Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC), preconizado na antiga e também cancelada DCTIMARINST 31-03; e posteriormente, o acesso direto à ferramenta de Gestão de Riscos utilizada para geração do relatório consolidado de GRSIC. Ambas as metodologias que visavam permitir a otimização do mapeamento de Riscos.

Pikos (2015) identificou os seguintes fatores que são responsáveis pelo sucesso da implementação da GRSIC: suporte da alta gerência; comunicação, engajamento e comprometimento; setor específico para tratar de gestão de riscos; liderança; comunicação interna; conhecimento e capacitação; mudança cultural e resistência; e continua melhoria do processo, que são interdependentes. maiores esclarecimentos estão descrito no item 3.5 deste estudo.

11. Quanto à avaliação das OM (questionamento 7.5 com 52% para o não atendimento) e do CLTI (questionamento 11 com 48% para o não atendimento) possuírem no seu quadro de pessoal de apoio à Tecnologia da Informação e Comunicações (TIC), o número adequado de militares/civis para exercer de forma eficiente as atividades de suporte técnico aos serviços de TIC. Pode-se perceber que os dados referentes à relação média do número de pessoas do setor de TIC pelo número de Estações de Trabalho (ET) / Servidores, com 1/137 ao CLTI (questionamentos 1 e 2) e 1/28 as OM (questionamentos 1.9 e 4.1), são considerados muito próximos do ideal.

Conforme a publicação DCTIMARINST Nº 30-09C, a relação ideal estabelecida será de 1/107 para os serviços prestados pelos CLTI e de acordo com (REZENDE, 2021) a relação média entre técnicos de TI e o total de usuários de uma empresa (estações de trabalho) é de 5,1 por 100. Isto é, uma relação de 1/20 para os serviços prestados pelas OM.

12. Atendendo os questionamentos 7.2 e 7.3 com 21% e 42% para o não atendimento, respectivamente, e mediante ao propósito das reuniões do Conselho de Gestão – presente em todas as OM da Marinha que executam recursos públicos, têm por finalidade assessorar o Comando ou a Direção da OM na administração econômico financeira e gerencial e no desenvolvimento organizacional, pode-se ressaltar a importância da participação do setor de TI nessas reuniões. Dessa forma, assessorando sobremaneira com questões atinentes de estratégica de TI, gerenciamento de riscos, Segurança da Informação e Comunicações, aquisições de material e serviços de TI etc.

13. Com relação ao nível de cumplicidade e comprometimento dos usuários da OM, quanto à Gestão de SIC, com 47% de não atendimento no questionamento 7.8, ressalta-se a importância do fiel cumprimento e do reforço das medidas objetivamente voltadas aos adestramentos e disseminação das orientações da mentalidade de SIC. De acordo com a publicação DGMM-540, deve se buscar a "mentalidade de segurança incutida em todo o pessoal", ou seja, deve-se desenvolver e manter a conscientização do nosso pessoal quanto à importância desse assunto.

14. Ressalta-se a importância do fiel cumprimento do questionamento 7.6, que houve 57% de não atendimento, no sentido de assegurar o fortalecimento da mentalidade de SIC. Conforme publicado por MILLDESK (2020), Métricas, dados são essenciais em qualquer segmento. É justamente no setor da TI que dados e métricas possuem um papel fundamental. Afinal, como saber o quanto os clientes estão satisfeitos com os serviços, se há falhas em processos ou se há necessidade de correções no produto, serviço, atendimento, se isso não vier respaldado por números? Um dos meios de fazer isso é utilizando a pesquisa de satisfação em TI que ajuda a apontar melhorias que devem ser feitas. Por meio dessa, haverá métricas para realizar análises de dados do atendimento prestado pela equipe de suporte. E partindo dos resultados coletados: poderá agir de modo enfático e corrigir erros e pontos falhos; reforçar seus pontos fortes ao receber *feedback* positivo; melhorar os indicadores internos; mensurar e avaliar a eficácia de seus processos e de suas operações; e aplicar ações corretivas e de rumo para o negócio.

15. Quanto ao questionamento 7 para o CLTI, que trata da quantidade de discrepâncias de SIC, por OM, que foram observadas nas inspeções de SIC, nos anos de 2018 e 2019 (último período de normalidade antes do período COVID 2020 e 2021), podemos levantar que a relação desse dado pelo número de OM sob jurisdição dos CLTI colaboradores (DCTIMARINST Nº 30-09C) foi de 1/3. Dessa forma, temos 3 discrepâncias anotadas em dois anos por OM. Considerando que temos mais de 200 itens diretos a serem verificados nas inspeções, esse valor de 1/3 se torna baixo para uma avaliação criteriosa. Porém, ele vai ao encontro ao questionamento 8.4 das OM, que estabelece um grau de criticidade baixo de 26% utilizado nas inspeções/auditorias pelos CLTI.

16. Em face dos resultados dos questionamentos 7.7 da OM e o 14 do CLTI, que tratam da aplicação de ação restritiva de segregação, contenção, suspensão de provisão de produtos e serviços, após a identificação de Não Conformidade (não atendimento) dos

requisitos regulamentários ou de incidentes de SIC, com 96% e 65% de não atendimento, respectivamente, ressalta-se a importância do fiel cumprimento da publicação DCTIMARINST 31-06, que preconiza a retirada da Estação de Trabalho da Rede Local por quaisquer tipo de incidentes que comprometa a sua integridade. Nesse caso, assegurando à Segurança da RECIM e o fortalecimento da mentalidade em SIC.

Em face desse cenário, os usuários têm que estar cientes do perigo que representam estes comportamentos, devendo ser cautelosos e adotar as medidas necessárias de modo a garantir a integridade e segurança dos Sistemas de informações. Ou seja, é necessário sensibilizar os usuários para a importância das orientações de SIC.

5 Conclusão

Por meio deste trabalho, foi possível realizar uma avaliação do cumprimento da gestão e das práticas de SIC, observando seus controles e à luz das normas e legislações inerentes ao tema às quais o pessoal da MB está sujeito. Percebeu-se que a gestão da SIC na MB é uma questão já bem desenvolvida, inclusive por contar com uma política de SIC bem definida e de acesso a todos os usuários, embora ainda não exista uma conscientização plena desta política. Por se tratar de uma Força Armada, que lida com informações sensíveis cotidianamente, muitas de alto valor estratégico para o cumprimento de sua missão e concomitante defesa dos interesses da Nação, o conhecimento da política de segurança das OM deve ser de conhecimento de todos os seus integrantes.

Em face das lacunas apresentadas, colhidas na análise dos questionários analisados, faz-se necessário uma melhor prática da instituição, visando o fomento, em seu pessoal, da mentalidade no cumprimento das normas de SIC na MB.

Pôde-se observar que a Alta Administração Naval, através de seu planejamento estratégico e políticas orçamentárias, considera prioritariamente as questões relacionadas à infraestrutura de tecnologia, o orçamento direcionado aos recursos de TI e a Segurança da Informação e Comunicações.

Outra observação importante, contudo negativa, é o fato de as OM não disporem atualmente de um plano bem definido de análise de riscos.

A análise dos dados deste estudo também permitiu concluir que, de uma forma geral, os usuários apresentam-se como uma proteção para a SIC nos SI das OM, pelo fato de assumirem comportamentos e atitudes corretas na maioria dos procedimentos de segurança recomendados pelas orientações vigentes de SIC.

A realização deste trabalho teve, naturalmente, algumas limitações. A principal foi a escassez de estudos sobre os comportamentos e as atitudes dos usuários nas OM, para se poder fazer algum tipo de comparação com o presente estudo.

A principal ameaça à segurança é a falta de consciencialização dos usuários para esta questão, uma vez que existem medidas de segurança disponíveis que podem ser aplicadas, mas alguns as ignoram, propiciando vulnerabilidades para que sejam perpetrados ataques e violações à segurança dos SI nas OM.

Um dos grandes desafios na condução das atividades de segurança reside, justamente, na conscientização de que todos os integrantes de um determinado órgão ou tripulação de uma OM contribuem para que o nível de segurança esteja em maior ou menor

grau. O primeiro equívoco a ser combatido é a ideia de que a segurança é responsabilidade exclusiva do pessoal de SIC.

Para que essa conscientização possa ser alcançada é indispensável que o Comando ou a Direção da OM prestigie as iniciativas para aperfeiçoamento da SIC, determinando a realização de instruções e adestramentos frequentes, visando o perfeito entendimentos de todos sobre as ameaças existentes, os bens e informações a proteger, os riscos envolvidos e de que forma as pessoas podem ser afetadas no caso de concretização de uma determinada ameaça, além, evidentemente, das atribuições que cada um tem em proveito da segurança.

A assimilação dessa mentalidade não ocorre de forma instantânea, ela demanda um longo e contínuo trabalho, Sua gradativa incorporação deve ser objeto de ensino nos cursos de formação e de carreira, além do adestramento contínuo nas OM, constituindo-se em um constante doutrinamento.

Sendo assim, e levando-se em conta que a MB já possuí um farto conjunto de legislações, normas, instruções e procedimentos de SIC que devem ser do conhecimento de todos, torna-se claro que as deficiências de SIC identificadas no estudo poderão ser minimizadas também com a aplicação de ações como:

– aumento das publicações sistemáticas de notas de forma a alcançar todos os seus integrantes, como: Boletim de Ordens e Notícias (DCTIM/CTIM); e Planos do Dia (OM);

– incremento de programas de auditorias por parte das OM e visitas técnicas específicas de SIC nas OM da MB, aplicando sempre um grau de criticidade elevado de inspeção;

– ampliação dos adestramentos por meio dos PAD das OM, para todos os seus integrantes;

– contratação de cursos e/ou palestras extra-MB sobre o tema (preferencialmente, ministradas à bordo);

– participação do setor de TI em reuniões do Conselho de Gestão e Técnico, assessorando sobremaneira com questões atinentes a estratégica de TI;

– aplicação da pesquisa de satisfação em TI;

– aplicação de ação restritiva nas ET de segregação, contenção, suspensão de provisão de produtos e serviços, após a identificação de alguma Não Conformidade (não atendimento); e

– restabelecimento do encaminhamento obrigatório dos Relatórios de GRSIC pelas OM aos órgãos competentes.

Em termos de investigações futuras, entende-se que seria oportuno fazer o

cruzamento das informações presentes nesta base metodológica com outras variáveis de caracterização, como: o perfil das OM, o gênero ou a idade dos usuários, recursos empregados, patente do militar etc. A posterior análise objetivaria a verificação do impacto de conduta no cumprimento das orientações de SIC.

REFERÊNCIAS

AMARO, Marisa de Oliveira Santos. **Evolução da Governança de Tecnologia da Informação na Marinha do Brasil**. Disponível em: < http://www.anpad.org.br/diversos/ down_zips/53/adi2262.pdf>. Acesso em: 12 jul. 2021.

_____. Marinha do Brasil. Estado-Maior da Armada. EMA-416. **Doutrina de Tecnologia da Informação da Marinha**. Rev.1. Brasília, DF, 2007.

_____. Ministério da Defesa. MD30-M-01, Vol I: **Doutrina de Operações Conjuntas (Conceitos Doutrináveis)**. Brasília, DF, 2020. 215 p.

_____. Ministério da Defesa. MD31-P-02: **Política Cibernética de Defesa**. Brasília, DF, 2012. 24p. Disponível em: <http://idciber.eb.mil.br/images/documentos/doutrina manual_pol_nac_def.pdf>. Acesso em: 17 jun. 2021.

_____. Marinha do Brasil. Conselho de Tecnologia da Informação da Marinha. PETIM 2016-2019. **Plano Estratégico de Tecnologia da Informação da Marinha.** Rio de Janeiro, RJ, 2015.

_____. Marinha do Brasil. Estado Maior da Armada. EMA-414. **Normas para a Salvaguarda de Materiais Controlados, Dados, Informações, Documentos e Materiais Sigilosos na Marinha**. Rev.1. Brasília, DF, 2013 [a].

_____. Marinha do Brasil. Secretaria-Geral da Marinha. SGM-105. **Normas sobre Documentação Administrativa e Arquivamento na Marinha** (NODAM). (Rev. 41). Brasília, DF, 2013 [b].

_____. Ministério da Defesa. MD31-M-07: **Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014. 38 p. Disponível em: <http://www.defesa.gov.br/ arquivos/ legislacao/ emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 12 jul. 2021.

_____. Marinha do Brasil. Estado Maior da Armada. EMA-353. **Manual de Inteligência da Marinha**. Rev.1. Brasília, DF, 2016 [a].

_____. Marinha do Brasil. Estado Maior da Armada. EMA-411. **Manual de Publicações da Marinha**. Rev.6. Brasília, DF, 2016 [b].

_____. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. EB70-MC-10.232: **Manual de Campanha, Guerra Cibernética**. Brasília, DF, 2017. 45 p. Disponível em: <http://bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf>. Acesso em: 17 jul. 2021.

_____. Marinha do Brasil. Diretoria-Geral do Material da Marinha. DGMM-510. **Normas para Criptografia da Marinha**. Rev.1. Rio de Janeiro, RJ, 2019 [a].

_____. Marinha do Brasil. Comando-Geral do Corpo de Fuzileiros Navais. CGFFN-315. **Manual de Segurança de Áreas e Instalações de Interesse da Marinha do Brasil** (Volume II – Técnicas e Procedimentos). 1ª edição. Rio de Janeiro, RJ, 2020.

_____. Marinha do Brasil. Diretoria-Geral do Material da Marinha. DGMM-540. **Normas de Tecnologia da Informação da Marinha**. Rev.3. Rio de Janeiro, RJ, 2019 [b].

_____. Marinha do Brasil. Secretaria-Geral da Marinha. SGM-107. **Normas Gerais de Administração** (Rev. 7). Brasília, DF, 2019 [c].

_____. Marinha do Brasil. Diretoria de Comunicações e Tecnologia da Informação da Marinha. DCTIMARINST Nº 30-09C. **Centros Locais de Tecnologia da Informação (CLTI).** Rio de Janeiro, RJ, 2018.

_____. Marinha do Brasil. Conselho de Tecnologia da Informação da Marinha. **Plano Estratégico de Tecnologia da Informação da Marinha** (2016-2019). Brasília, DF, 2015.

CASTELLS, M. **A sociedade em rede** - A era da informação: economia, sociedade e cultura (volume 1). 8a. ed. São Paulo, S.P.: Paz e Terra, 2005.

DANTAS, Marcus. **Segurança da informação**: Uma Abordagem Focada em Gestão de Riscos, Olinda: Livro Rápido, 2011.

DHILLON, G. (2001). ***Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns*.** Computers & Security, 20 (2), 165-172.

DHILLON, G. (2004). ***Realizing benefits on an information security program***. *Business Process Management Journal*, 10 (3), 260-261.

ENDSLEY, M.R. Human Factors and Ergonomics Society. ***Toward a theory of situation awareness in dynamic systems***, 1995. Disponível em: <http://www.realtechsupport.org/UB/I2C/SituationAwarenessTheory_1995.pdf> Acesso em: 19 jul. 2021.

ESTADO-MAIOR DA ARMADA. Anexo (7), da Portaria n 110 de 4 de maio de 2017 **[Gestão de Risco]**. Brasília, DF, 4 maio 2017.

FACHIN O. **Fundamentos de metodologia**. 5 ed. São Paulo: Saraiva, 2006.

FERNANDES, Aguinaldo A.; ABREU, Vladimir F. de. **Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços**. 4.ed. Brasport, 2014.

GUIMARÃES, Flávio de Queiroz. **Possibilidades e Limitações de Emprego da Guerra Cibernética na Mb: Métricas Para Estabelecimento de uma Consciência Situacional Cibernética Do Eciber-Mb.** Rio de Janeiro, 2018. Disponível em <https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/CC%20Flavio%20de%20Queiroz%20Guimaraes%20-%20POSSIBILIDADES%20E%20LIMITACOES%20DE%20EMPREGO%20DA%20GUERRA%20CIBERNETICA%20NA%20MB.pdf>. Acesso em: 19 jul. 2021.

KNAPP, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). ***Information security policy: An organizational-level process model.*** *Computers & Security*, 28 (7), 493-508.

MANDARINO JUNIOR, R.; CANONGIA, C. **Livro Verde: Segurança Cibernética no Brasil**. Brasília, DF: [s.n.], 2010. 63 p. Disponível em: <http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 19 jul. 2021.

MCGUINNESS, B.; FOY, J.L. ***A subjective measure of SA: The crew awareness rating scal (cars)***. *Proceedings of the first human performance, situation awareness, and automation conference*, Savannah, Georgia, USA, 2000.

MILLDESK, **Pesquisa de satisfação em TI: não é sobre tecnologia, é sobre pessoas!** Disponível em: <https://www.milldesk.com.br/blog/pesquisa-de-satisfacao-tim>. Acesso em: 10 ago. 2021.

PAUL, C.; WHITLEY, K. A *Taxonomy of Ciber Awarebness Questions for the User-Centered design of Cyber Situation Awareness*. Lecture Notes in Computer Science, pp.145-154 Springer, 2013 Disponível em: <https://pdfs.semanticscholar.org/0ba6/8b5f0ef35ef94fa23827 5e2f571bce446538.pdf>Acesso em: 10 jun. 2021.

PEIXOTO, Mário César Pintaudi. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro, Brasport, 2006.

PIKOS, **A.** ***Introduction of risk management into municipal offices across Poland as an example of organizational change.*** *Management and Business Administration*, v. 23, n. 4, p. 74-97, 2015. Disponível em: <https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q= Introduction+of+risk+management +into+municipal+offices+ across+Poland+as+an+example+of+organizational+change.&btnG=> Acesso em: 10 ago. 2021.

RED HAT. Red Hat Enterprise Linux 4: **Guia de Segurança Segurança da Informação (TI)**. 2005. Disponível em: < http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/ch-sgs-ov.html>. Acesso em 12 jul. 2021.

REZENDE, Rafael. **Qual é o tamanho ideal de uma equipe de TI?** Disponível em <https://pt.scribd.com/doc/22719689/Qual-e-o-tamanho-ideal-de-uma-equipe-de-TI>. Acesso em: 10 ago. 2021.

SEMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. Rio de Janeiro, Campus, 2003.

STANTON, N.A.; CHAMBERS, P.R.G.; PIGGOTT, J. ***Situational Awareness and Safety,*** 2001 Safety Science 39 189-204.

WEILL, P., ROSS, J. W. **Governança de tecnologia da informação.** São Paulo: M. Books do Brasil, 2006.

WORKMAN, M.; BOMMER, W. H.; STRAUB, D. (2008). ***Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior,*** 24 (6), 2799-2816.

APÊNDICE A - QUESTIONÁRIO ESTRUTURADO – CLTI

(Instrumento de Pesquisa a ser respondido pelo Encarregado do Centro Local de Tecnologia da Informação (CLTI))

Os dados e informações coletados através deste questionário, relativos à política e à gestão de Segurança da Informação e Comunicações (SIC) na MB, serão utilizadas unicamente para subsidiar quantitativamente (análise de cálculos percentuais e estatísticos) uma pesquisa acadêmica, do Curso Política e Estratégia Marítimas (C-PEM) da Escola de Guerra Naval (EGN). As informações serão apresentadas preservando a identificação dos respondedores e das Organizações Militares.

Nome do CLTI:	
Nome do Encarregado do CLTI:	
Área de jurisdição (Listar OM):	
Data do preenchimento:	

Política e Gestão de Segurança da Informação e Comunicações

1. Qual a quantidade de pessoas que servem no CLTI? Quais os Postos/Graduações/especialidades e suas respectivas funções?

Resp:

2. Qual a quantidade de Estações de Trabalho (ET)/Servidores apoiadas pelo CLTI?

Resp:

3. Quais os tipos de inspeções/verificações de SIC que são realizadas nas OM de sua jurisdição e a quantidade realizada ao ano por OM?

Resp:

4. Nas inspeções/auditorias realizadas é verificado o fiel cumprimento de todos os pontos das normas de Segurança da Informação e Comunicações (SIC)?

( ) Sim ( ) Não

5. Os inspecionados têm o mínimo de conhecimento técnico e das normas de Segurança da Informação e Comunicações (SIC)?

( ) Sim ( ) Não

6. Enumerar as discrepâncias de SIC que foram observadas nas inspeções/verificações realizadas nas OM de sua jurisdição, no que tange principalmente as orientações sobre Segurança da Informação e Comunicações – SIC, nos anos de 2018 e 2019:

Discrepância de SIC	Tipo		Ano	
	IAM	CAVSO	2018	2019

7. Descrever as quantidades de discrepâncias de SIC, por OM, que foram observadas nas inspeções/ verificações realizadas nas OM de sua jurisdição, no que tange principalmente as orientações sobre Segurança da Informação e Comunicações – SIC, nos anos de 2018 e 2019:

OM	QTDE de Discrepâncias de SIC	
	2018	2019

8. As OM consideram a política e a gestão da Segurança da Informação e Comunicações (SIC) como questão estratégica ?

( ) Sim ( ) Não

9. Existe uma conscientização da Gestão da Segurança da Informação e Comunicações (GSIC) por parte das OM?

( ) Sim ( ) Não

10. As OM mantêm um Plano de Gerenciamento de Riscos de SIC?

( ) Sim ( ) Não

11. As OM possuem no seu quadro de pessoal de apoio à Tecnologia de Informação e Comunicações (TIC), o número adequado de militares/civis para exercer de forma eficiente as atividades de suporte técnico aos serviços de TIC?

( ) Sim ( ) Não

12. A Marinha do Brasil possui todas as publicações necessárias a fim de atender a SIC?

( ) Sim ( ) Não

13. Existe de forma explícita um conjunto de publicações, orientações normativas e regulamentos que as OM são obrigadas a seguir?

( ) Sim ( ) Não

14. O CLTI aplicou alguma ação restritiva de segregação, contenção, suspensão de provisão de produtos e serviços nas OM, após a identificação de Não Conformidade (não atendimento) dos requisitos regulamentários ou de incidentes de SIC?

Caso sim, descrever no campo “Obs” a quantidade e o(s) anos de sua(s) ocorrências(s)

(desde 2018).

( ) sim ( ) não

Obs:

15. Existe algo que impeça ou dificulte o atendimento das orientações normativas de SIC ou a consolidação de sua mentalidade pelas OM da MB?

Caso sim, comentar no campo de observação, de forma sucinta e em tópicos.

( ) Sim ( ) Não

Obs:

APÊNDICE B - QUESTIONÁRIO ESTRUTURADO – ADMIN

(Instrumento de Pesquisa a ser respondido pelo Administrador da Rede Local (ADMIN))

Os dados e informações coletados através deste questionário, relativos à política e à gestão de Segurança da Informação e Comunicações (SIC) na MB, serão utilizadas unicamente para subsidiar quantitativamente (análise de cálculos percentuais e estatísticos) uma pesquisa acadêmica, do Curso Política e Estratégia Marítimas (C-PEM) da Escola de Guerra Naval (EGN). As informações serão apresentadas preservando a identificação dos respondedores e das Organizações Militares.

Nome da OM:	
Perfil da OM:	( ) Administrativo ( ) Tecnológico ( ) Operativo ( ) Outras
Nome do CLTI subordinado:	
Administrador da Rede Local (ADMIN):	
Oficial de SIC (OSIC) da OM:	
Data do preenchimento:	

Política e Gestão de Segurança da Informação e Comunicações

1.0 - Adestramento.

1.1 - O Programa de Adestramento de SIC foi autorizado pelo Titular da OM?
Ref.: Alínea e do Art. 8.5 da DGMM-540.
( ) Sim ( ) Não
Obs.:

1.2 - Os Planos de Adestramentos de SIC englobam o conjunto mínimo de temas previstos no artigo 10.11 da DGMM-540?
( ) Sim ( ) Não
Obs.:

1.3 - Os meios de controle de presença nos adestramentos de SIC são efetuados?
Ref.: Inciso 9.9.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

1.4 - A função do Administrador da Rede Local está como encargo colateral ou figura na estrutura organizacional (Depto, Divisão etc) da OM? Caso esteja na estrutura organizacional, qual o nome do setor e a quem está vinculado?
Resp:

1.5 - O OSIC possui formação na área de TI (Curso Superior na área de TI)?
Ref.: Artigo 8.6 da DGMM-540.
( ) Sim ( ) Não

Obs.:

1.6 - O ADMIN possui formação na área de TI (Curso Superior ou Técnico na área de TI)?
Ref.: Artigo 8.8 da DGMM-540 .
( ) Sim ( ) Não
Obs.:

1.7 - O ADMIN possui o curso de C-Exp-AdRedes (Oficiais) ou C-Sup-Linux (Praças)? Qual ano de sua realização?
( ) Sim ( ) Não
Obs.:

1.8 - O OSIC possui o curso de habilitação (C-Exp-AdRedes do CIAW) ? Qual ano de sua realização? (citar o ano no campo de Obs)
( ) Sim ( ) Não
Obs.:

1.9 - Quantas pessoas servem no setor de TIC da OM? Relacionar os Postos/Graduações/especialidades/tempo e suas respectivas funções?
Resp:

1.10 – São divulgadas notas da Instrução de Segurança da Informação e Comunicações (ISIC) em Plano do Dia (PD) com que periodicidade?
Ref.: Artigo 9.9 da DGMM-540.
( ) Divulgam-se sem periodicidade definida (quando OSIC/ADMIN julgam importante)
( ) Divulgam-se constantemente
( ) Divulgam-se raramente
( ) Não se divulgam
Obs.:

1.11 - Os usuários foram orientados sobre a proibição do uso de MODEMS em Estações de Trabalho e Servidores?
Ref.: Incisos 5.4.2 e 9.5.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

1.12 - Os usuários foram orientados sobre a importância de se realizarem CÓPIAS DE SEGURANÇA (backup) das informações digitais armazenadas em suas Estações de Trabalho (ET)?
Ref.: Inciso 9.5.10 da DGMM-540.
( ) Sim ( ) Não
Obs.:

1.13 - Os usuários foram orientados sobre a determinação de se utilizarem senhas e medidas de segurança em arquivos e pastas com informações sigilosas que estejam armazenados em suas Estações de Trabalho (ET)?
Ref.: Inciso 8.9 da DGMM-540.
( ) Sim ( ) Não
Obs.:

1.14 - Os usuários foram orientados sobre as regras mínimas de segurança na utilização do CORREIO ELETRÔNICO e sua destinação exclusiva para fins corporativos?

Ref.: Artigo 6.5 e inciso 9.5.15 da DGMM-540.
( ) Sim ( ) Não
Obs.:

1.15 - Os usuários foram orientados sobre os possíveis ataques envolvendo técnicas de ENGENHARIA SOCIAL?
Ref.: Alínea j do artigo 10.11 e inciso 8.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

1.16 - A mentalidade de segurança vem sendo mantida e passada para os usuários? (indicar, na observação, de que maneira)
Ref.: Artigo 9.9 da DGMM-540.
( ) Sim ( ) Não
Obs.:

1.17 - Todo o pessoal recém-embarcado recebe adestramento Básico de SIC?
Ref.: Artigo 9.9.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.0 - Administração da Rede.
2.1 - O OSIC supervisiona a elaboração e a manutenção do Histórico da Rede Local (HRL) pelo
ADMIN?
Ref.: Alínea f do art 8.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.2 - O ADMIN realiza as atualizações dos sistemas existentes no ambiente computacional e rede local da OM?
Ref.: Artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.3 - O ADMIN possui rígido controle e realiza a manutenção periódica das contas e dos direitos dos usuários?
Ref.: Alínea k do artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.4 - O ADMIN mantém uma rotina de BACKUP dos dados dos servidores?
Ref.: Inciso 9.5.10 da DGMM-540.
( ) Sim ( ) Não
Obs.:
2.5 - O ADMIN verifica periodicamente a integridade dos backups com testes de recuperação?
Ref.: Alínea d do inciso 9.5.10 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.6 - Os servidores e ET adotam a política de Regras Básicas de SENHA FORTE (mínimo 12

caracteres, usando caracteres especiais, números, letras maiúsculas e minúsculas) para o login de acesso e trocas periódicas dessas senhas?
Ref.: Inciso 9.5.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.7 - Os servidores possuem instalados apenas softwares padronizados pela DCTIM e necessários
à sua funcionalidade?
Ref.: Artigo 4.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.8 - O acesso remoto aos servidores estão desabilitados?
Ref.: Inciso 9.5.2 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.9 - Apenas as portas lógicas necessárias às atividades dos servidores estão habilitadas?
Ref.: Inciso 9.5.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.10 - Os programas e sistemas operacionais instalados nos servidores estão atualizados com as últimas versões disponibilizadas?
Ref.: Inciso 9.5.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.11 - Todos os Recursos Computacionais Críticos (RCC) nível 1, possuem senhas de configuração fortes e diferentes do fabricante?
Ref.: Inciso 9.5.3 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.12 - Estão registrados no HRL, todos os acesso aos servidores através de conexão remota?
Ref.: Inciso 9.5.2 da DGMM-540.
( ) Sim ( ) Não ( ) Não Aplicável
Obs.:

2.13 - Todos os servidores possuem o antivírus instalado e atualizado?
Ref.: Inciso 9.5.7 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.14 - Todos os programas das ET necessários para uso em Rede Local (RL) foram homologados e previamente autorizados pela DCTIM?
Ref.: Inciso 9.5.14 da DGMM-540.
( ) Sim ( ) Não
Obs.:

2.15 - O acesso de ESTRANGEIROS à Rede Local é rigidamente controlado?

Ref.: Inciso 9.5.11 da DGMM-540.
( ) Sim ( ) Não ( ) Não há estrangeiros utilizando a RL
Obs.:

2.16 - Os acessos de estrangeiros à Rede local da OM foram reportados formalmente à DCTIM?
Ref.: Inciso 9.5.11 da DGMM-540.
( ) Sim ( ) Não ( ) Não Aplicável
Obs.:

2.17 - A utilização de rede sem fio na OM foi homologada pela DCTIM?
Ref.: Inciso 9.6.2 da DGMM-540.
( ) Sim ( ) Não ( ) Não Aplicável

2.18 - O sistema de monitoramento por CFTV da OM está segregado da RECIM?
Ref.: Inciso 4.13.2 do CGCFN-1-15.
( ) Sim ( ) Não ( ) Não Aplicável
Obs.:

2.19 - Todas as Estações de Trabalho estão de acordo com a DCTIMBOTEC 30/003/2018? (Caso
Negativo, favor especificar a quantidade de ET em desacordo e qual o percentual que este quantitativo representa do total)
( ) Sim
( ) Não. Quantidade em desacordo: ___, que equivale a ___ % do total de ET
Obs.:

3.0 - Documentação.
3.1 - O OSIC foi formalmente nomeado por meio de Ordem de Serviço do Titular da OM?
Ref.: Artigo 8.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.2 - O ADMIN foi formalmente nomeado por meio de Ordem de Serviço do Titular da OM?
Ref.: Artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.3 - A ISIC foi estabelecida e divulgada através de Ordem Interna da OM?
Ref.: Artigo 10.3 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.4 - A ISIC é revisada periodicamente pelo OSIC e pelo ADMIN (em caso afirmativo, favor lançar em Obs qual a periodicidade)?
Ref.: Artigo 10.3 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.5 - O Intervalo de revisão da ISIC está definido no corpo do documento?
Ref.: Artigo 10.3 da DGMM-540.
( ) Sim ( ) Não

Obs.:

3.6 - O ADMIN auxilia o OSIC na divulgação da ISIC da OM?
Ref.: Artigo 8.8 da DGMM-540.
( ) Sim ( ) Não

3.7 - O ADMIN mantém o registro da realização das cópias de segurança (BACKUP), e dos respectivos testes de recuperação dos backups, no histórico da rede local (HRL)?
Ref.: Alínea e do inciso 9.5.10 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.8 - Todos os usuários da OM assinaram o Termo de Responsabilidade Individual (TRI)?
Ref.: Alínea x do Artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.9 - O TRI é assinado por pessoal externo à OM que seja autorizado a executar serviços na Rede Local?
Ref.: Inciso 9.4.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.10 - Todos os usuários da OM que receberam ET assinaram o Termo de Recebimento de Estação de Trabalho (TRE)?
Ref.: Alínea z do Art. 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.11 - Na Ordem Interna (OI) sobre o emprego de dispositivos móveis, consta(m):
Ref.: Inciso 12.4.2 da DGMM-540.
a) as pessoas autorizadas a utilizarem tais dispositivos?
( ) Sim ( ) Não
b) os dispositivos autorizados (número de série)?
( ) Sim ( ) Não
c) os locais e compartimentos de utilização dos dispositivos?
( ) Sim ( ) Não
d) a finalidade de uso dos dispositivos?
( ) Sim ( ) Não
e) o horário autorizado?
( ) Sim ( ) Não
Obs.:

3.12 - O OSIC realiza Auditoria Interna na OM uma vez por ano? (caso seja mais que uma, favor lançar a quantidade no campo “Obs”)
Ref.: Alínea j do Art. 8.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.13 - A equipe de Auditoria Interna foi designada formalmente pelo Titular da OM?
Ref.: Alínea c do Artigo 11.2 da DGMM-540.
( ) Sim ( ) Não

Obs.:

3.14 - O OSIC emitiu um Relatório de Auditoria (RAD) após a realização da Auditoria Interna?
Ref.: Alínea e do Artigo 8.7 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.15 - O RAD é classificado como RESERVADO e guardado em local compatível com seu grau
de sigilo?
Ref.: Artigo 10.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.16 - O ADMIN elabora, controla e mantém atualizado o HRL?
Ref.: Alínea d do artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.17 - O RAD foi arquivado no HRL?
Ref.: Alínea j do Artigo 8.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.18 - O HRL está classificado com grau de sigilo RESERVADO?
Ref.: Artigo 10.5 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.19 - O ADMIN registra nos TRE a lista dos programas instalados, incluindo os referentes à SIC homologados pela MB?
Ref.: Item II do Apêndice II ao Anexo A da DGMM-540.
( ) Sim ( ) Não
Obs.:
3.20 - Nos Perímetros de Segurança, existe a proibição de entrada de dispositivos armazenadores de informações, contemplando tripulação e visitantes?
Ref.: Inciso 9.4.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.21 - Por ocasião de cada visita a um Perímetro de Segurança é registrada data, hora, responsável
na OM e razão da visita?
Ref.: Alínea a do Inciso 9.4.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.22 - Os acessos físicos aos Perímetros de Segurança são monitorados/controlados?
Ref.: Inciso 9.4.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.23 - Os Perímetros de Segurança estão demarcados localmente?
Ref.: Inciso 9.4.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.24 - Os Perímetros de Segurança estão devidamente ilustrados no HRL?
Ref.: Inciso 9.4.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.25 - Os Perímetros de Segurança estão claramente definidos na ISIC?
Ref.: Inciso 9.4.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.26 - Os RCC estão identificados por um dos níveis de classificação de acordo com sua importância?
Ref.: Inciso 9.2.5 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.27 - O ADMIN elaborou o Plano de Contingência (PLCONT)?
Ref.: Alínea q do artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.28 - O PLCONT é revisado pelo ADMIN e OSIC anualmente?
Ref.: Alínea g do Artigo 8.6 e Alínea c do Artigo 10.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.29 – O PLCONT foi classificado com o grau de sigilo RESERVADO?
Ref.: Artigo 10.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.30 - Caso o usuário possua direito de administrador, o ADMIN registra no TRI do usuário?
Ref.: Alínea p do Artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.31 - O ADMIN mantém atualizados no Histórico de Rede Local (HRL) os Perfis e os Privilégios
dos usuários?
Ref.: Artigo 8.8 da DGMM-540 .
( ) Sim ( ) Não
Obs.:

3.32 - O ADMIN efetua a remoção ou bloqueio de logins por motivo de desembarque dos usuários?
Ref.: Alínea k do Artigo 8.8 da DGMM-540.

( ) Sim ( ) Não
Obs.:

3.33 - O HRL possui as 3 PARTES componentes?
Ref.: Artigo 10.5 da DGMM-540.
( ) Sim ( ) Não
Obs.:

3.34 - As exceções quanto a proibição de dispositivos armazenadores de informações são controladas e registradas por meio de Ordem Interna ou de Ordem de Serviço?
Ref.: Inciso 12.4.2 da DGMM-540.
( ) Sim ( ) Não

3.35 – Os usuários e o pessoal servindo no Setor de TI da OM estão cientes das publicações/normas de SIC emanadas pela MB?
( ) Sim ( ) Não

4.0 - Estações de Trabalho.
4.1 – Qual a quantidade de Estações de Trabalho (ET)/Servidores que a OM possui?
Resp.:

4.2 - Os dispositivos de entrada/saída, tais como, portas USB, Modens, gravadores de CD/DVD
e impressoras locais estão desabilitados nas ET? (em caso negativo, favor lançar em Obs a justificativa)
Ref.: Alínea f do inciso 9.5.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.3 - O ADMIN possui as senhas de configuração (setup) de todas as ET da OM?
Ref.: Alínea h do inciso 9.5.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.4 - As ET possuem senha de inicialização (boot) de uso exclusivo do usuário que a utiliza?
Ref.: Alínea i do inciso 9.5.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.5 - O compartilhamento de arquivos e impressoras está desabilitado em todas as ET?
Ref.: Alínea j do inciso 9.5.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.6 - As ET possuem antivírus e demais programas de proteção individual homologados pela DCTIM, atualizados?
Ref.: Inciso 9.5.7 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.7 - Nas ET estão instalados apenas os programas homologados pela DCTIM para criptografia

de arquivos?
Ref.: Alínea g do Artigo 8.9 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.8 - As ET possuem atualizações automáticas de patches dos Sistemas Operacionais e ferramentas de segurança (antivírus, antispyware e firewall pessoal)?
Ref.: Alínea a e b do inciso 9.5.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.9 - As ET possuem o agente do antivírus em vigor na MB instalado e funcionando corretamente?
Ref.: Inciso 9.5.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.10 - Os equipamentos trazidos por pessoal externo à OM são verificados pelo ADMIN antes de serem utilizados na Rede Local?
Ref.: Alínea t do Artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.11 - Apenas usuários que possuam justificativa formal e autorização do Titular da OM, possuem privilégios de administrador da ET?
Ref.: Alínea p do Artigo 8.8 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.12 - As ET são configuradas com privilégios mínimos pelo ADMIN antes de serem entregues aos usuários?
Ref.: Alínea o do Artigo 8.8 e alínea e do Inciso 9.5.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.13 - Todas as ET da OM possuem política de tela de login com senha e proteção de tela por inatividade (*screensaver*) com senha?
Ref.: Artigo 8.9 da DGMM-540.
( ) Sim ( ) Não
Obs.:

4.14 - Sistemas legados são mantidos apenas através do uso de Máquinas Virtuais (VM)?
Ref.: DCTIMBOTEC 33/001/2015.
( ) Sim ( ) Não
Obs.:

5.0 - Incidentes.
5.1 - Os INCIDENTES de SIC ocorridos foram reportados à DCTIM, com informação ao COMIMSUP?
Ref.: Artigo 8.5 da DGMM-540.
( ) Sim ( ) Não ( ) Não Aplicável
Obs.:

5.2 - As ET apreendidas para realização de forense computacional possuem Termo de Apreensão
lavrado e assinado?
Ref.: Subitem 4.4 da DCTIMARINST 31-02A
( ) Sim ( ) Não ( ) Não Aplicável
Obs.:

5.3 - As ET apreendidas para realização de investigações são lacradas, isoladas e armazenadas em local seguro?
Ref.: Subitem 4.4 da DCTIMARINST 31-02A
( ) Sim ( ) Não ( ) Não Aplicável

6.0 - Segurança Física.
6.1 - Estabilizadores/No-breaks que alimentam RCC 1 estão devidamente protegidos?
Ref.: Alínea b do inciso 9.4.3 da DGMM-540.
( ) Sim ( ) Não
Obs.:

6.2 - Os compartimentos não guarnecidos que contenham RCC 1 possuem segurança física reforçada, sistema de alarme, lacre e controle de entrada e saída?
Ref.: Alínea d do inciso 9.4.3 da DGMM-540.
( ) Sim ( ) Não
Obs.:

6.3 - Os gabinetes de proteção dos equipamentos de conectividade possuem controle rígido das chaves e dos lacres numerados?
Ref.: Alínea c do inciso 9.4.3 da DGMM-540.
( ) Sim ( ) Não
Obs.:

6.4 - Equipamentos RCC1 estão afastados de equipamentos geradores de interferência eletromagnética?
Ref.: Inciso 9.4.4 da DGMM-540.
( ) Sim ( ) Não
Obs.:

6.5 - Equipamentos RCC 1 são alimentados por sistema de energia estabilizado e com proteção em caso de emergência (no-breaks)?
Ref.: Inciso 9.4.5 da DGMM-540.
( ) Sim ( ) Não
Obs.:

6.6 - As mídias contendo o Backup são armazenadas em locais distintos ao dos equipamentos que contém as informações originais?
Ref.: Alínea f do inciso 9.5.10 da DGMM-540.
( ) Sim ( ) Não
Obs.:

6.7 - As mídias contendo o Backup são salvaguardadas em locais com proteção contra incêndio e alagamento?
Ref.: Alínea f do inciso 9.5.10 da DGMM-540.

( ) Sim ( ) Não
Obs.:

6.8 - As mídias contendo o Backup são classificadas com o mesmo grau de sigilo atribuído às informações nelas armazenadas?
Ref.: Alínea g do inciso 9.5.10 da DGMM-540.
( ) Sim ( ) Não
Obs.:

6.9 - Existe um acompanhamento constante do pessoal externo que encontra-se realizando serviço a bordo?
Ref.: Inciso 9.4.1 e 9.4.6 da DGMM-540.
( ) Sim ( ) Não
Obs.:

6.10 - A OM possui locais apropriados, definidos em Ordem Interna, para acondicionar os dispositivos móveis pessoais e funcionais?
Ref.: Inciso 12.4.1.1 da DGMM-540.
( ) Sim ( ) Não
Obs.:

7.0 – Conformidades:
7.1 - Existe algo que impeça ou dificulte o atendimento das orientações normativas de SIC ou a consolidação de sua mentalidade pelo setor de Tecnologia de Informação e Comunicações ou pelos usuários?
Caso sim, comentar no campo de observação, de forma sucinta e em tópicos.
( ) Sim ( ) Não
Obs:

7.2 – O setor de Tecnologia de Informação e Comunicações (TIC) participa de Reuniões de Gestão da OM?
( ) Sim ( ) Não
Obs.

7.3 - As decisões relacionadas com a Segurança da Informação e Comunicações são tomadas exclusivamente pela área de TIC ou em conjunto com o setor responsável pelas decisões estratégicas da OM?
Resp:

7.4 – O setor de Tecnologia de Informação e Comunicações (TIC) elabora um Plano de Gestão de Riscos de SIC?
( ) Sim ( ) Não
Obs.

7.5 - A OM possui no seu quadro de pessoal de apoio à Tecnologia de Informação e Comunicações (TIC), o número adequado de militares/civis para exercer de forma eficiente as atividades de suporte técnico aos serviços de TIC?
( ) Sim ( ) Não

7.6 - O setor de TIC da OM disponibiliza para os usuários uma pesquisa de satisfação, por meio de questionários, para avaliar a percepção quanto a qualidade dos suportes técnicos realizados, assim como, identificar as possibilidades de melhoria dos serviços prestados de

TIC?
( ) sim ( ) não
Obs:

7.7 - O setor de TIC da OM aplicou alguma ação restritiva de segregação, contenção, suspensão de provisão de produtos e serviços, após a identificação de Não Conformidade (não atendimento) dos requisitos regulamentários ou de incidentes de SIC?
Caso haja, descrever no campo "Obs" a quantidade e o(s) anos de sua(s) ocorrências(s). (desde 2018).
( ) sim ( ) não
Obs:

7.8 - Qual o Nível de cumplicidade e comprometimento dos usuários da OM, quanto a Gestão de Segurança da Informação e Comunicações (SIC)?
( ) Baixo ( ) Médio ( ) Alto

8.0 – Inspeções/auditorias - Centro Local de Tecnologia da Informação (CLTI):
8.1 – São verificados nas inspeções pelo CLTI, todos os pontos das normas de SIC?
( ) Sim ( ) Não

8.2 – O CLTI utiliza todo o tempo destinado para realização das suas inspeções/auditorias?
( ) Sim ( ) Não

8.3 – Nas inspeções/auditorias pelo CLTI são realizadas verificações nas Estações de Trabalho dos usuários?
( ) Sim ( ) Não

8.4 – Qual o grau de criticidade utilizado nas inspeções/auditorias pelo CLTI?
( ) Baixo ( ) Médio ( ) Alto

APÊNDICE C - MODELO DO TERMO DE RESPONSABILIDADE INDIVIDUAL
(DGMM-540 Rev 3)

MARINHA DO BRASIL
(NOME DA OM)
TERMO DE RESPONSABILIDADE INDIVIDUAL

(Local: cidade), _____ de _____ de _____

Pelo presente instrumento, eu, (**nome completo, NIP ou n o 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 conseqüências decorrentes da não observância do acima exposto e da legislação vigente.

Assinatura

Nome Completo, NIP ou no da identidade

APÊNDICE D - MODELO DO TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO (DGMM-540 Rev 3)

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 n o da identidade) , perante a Marinha do Brasil, doravante denominada MB, na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, declaro 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

ANEXO A

EXTRATO DA DGMM-540, REV. 3 (BRASIL, 2019[B])

Parte III - Segurança da Informação e Comunicações:

CAPÍTULO 8
RESPONSABILIDADES E ATRIBUIÇÕES
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)
9.1.1 - 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-guarnecidos 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 viceversa.
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 INFORMAÇÂO 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 estiver 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 placamãe 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 sobrescrito 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.
9.9.2 - 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.

9.12 - 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.

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
11.2 - 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 edivulgado, 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.
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. Adocumentação 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.
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

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

12.2.1 - 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 contrainteligência. 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 e 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) capitanias, 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 permitam 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.