MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM SEGURANÇA DAS INFORMAÇÕES E COMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

TREINAMENTO DE OFICIAIS E PRAÇAS DA MARINHA DO BRASIL: FERRAMENTA IMPRESCINDÍVEL PARA GARANTIR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DE EXCELÊNCIA.

1º TEN KAYO CUEVAS DE AZEVEDO SOARES TORRES

CIAW
Rio de Janeiro
2018

1T KAYO CUEVAS DE AZEVEDO SOARES TORRES

TREINAMENTO DE OFICIAIS E PRAÇAS DA MARINHA DO BRASIL: FERRAMENTA IMPRESCINDÍVEL PARA GARANTIR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DE EXCELÊNCIA.

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança Da Informação E Comunicações

Orientador

CC (EN) Patricia Amaro Rocha Arruda

CIAW

Rio de Janeiro

2018

1T KAYO CUEVAS DE AZEVEDO SOARES TORRES

TREINAMENTO DE OFICIAIS E PRAÇAS DA MARINHA DO BRASIL: FERRAMENTA IMPRESCINDÍVEL PARA GARANTIR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DE EXCELÊNCIA.

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança Da Informação E Comunicações.

Aprovada em _____

Banca Examinadora:

CMG (RM-1) HUBACK – CIAW _____

CF (RM-1 T) WAGNER – CIAW _____

CC (EN) PATRICIA ROCHA – DCTIM _____

CIAW

Rio de Janeiro

2018

Dedico esse trabalho aos militares que dioturnamente dedicam-se ao serviço da pátria.

AGRADECIMENTOS

Primeiramente agradeço a Deus, por tudo que tenho e por estar onde estou. Agradeço minha família, em especial minha mãe, que me ajudou a concluir este trabalho, sempre esteve ao meu lado nos meus desafios. A minha noiva que permanece ao meu lado me dando apoio e compartilhando das minhas vitorias. Agradeço a minha orientadora pela paciência para responder as minhas duvidas e dedicação para auxiliar no trabalho.

"The Only Easy Day Was Yesterday", "It Pays to be a Winner”(Navy SEALs)

TREINAMENTO DE OFICIAIS E PRAÇAS DA MARINHA DO BRASIL: FERRAMENTA IMPRESCINDÍVEL PARA GARANTIR UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DE EXCELÊNCIA.

Resumo

A informação é a principal matéria prima na era do conhecimento, por esta razão tem que ser tratada com a devida prioridade e relevância, enfatizando sempre sua segurança. O presente trabalho tem como objetivo reforçar a importância do treinamento de praças e oficias da Marinha do Brasil no que tange esse assunto, sendo ferramenta essencial na garantia de uma Política de Segurança da Informação de excelência. Foram analisados os documentos Portaria Normativa no 2.327 do Ministério da Defesa, Decreto no 3505 da Presidência da República, DGMM-0540, EMA-416 que ratificaram a necessidade desse treinamento específico. A metodologia adotada comportou uma pesquisa bibliográfica visando buscar os referenciais teóricos que abordam o tema em questão. Concluiu-se que o conhecimento sobre a Política de Segurança da Informação é imprescindível para todos os setores e níveis hierárquicos da Marinha do Brasil e que o treinamento do pessoal é a ferramenta que garantirá enfim uma maior conscientização e prática eficaz, minimizando ataques e possíveis vazamentos de informação.

Palavras- chave: Informação, Treinamento, Segurança da Informação, Politica de Segurança;

LISTA DE FIGURAS

LISTA DE TABELAS

LISTAS DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ADMIN	Administrador da rede local
CIAW	Centro de Instrução Almirante Wandenkolk
CLTI	Centro Locais de Tecnologia de Informação
CREDSEG	Credencial de Segurança
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DGMM	Diretoria-Geral do Material da Marinha do Brasil
EMA	Estado Maior da Armada
EUA	Estados Unidos da America
ISIC	Instrução de Segurança da Informação e Comunicações
MB	Marinha do Brasil
MD	Ministério da Defesa
NSA	National Security Agency
OM	Organizações Militares
OSIC	Oficial de Segurança da Informação e Comunicações
PAD	Programa de Adestramento
POSIC	Política de Segurança da Informação e Comunicações
P2P	Ponto-a-Ponto
RECIM	Rede de Comunicações Integrada da Marinha do Brasil

SIC	Segurança da Informação e Comunicações
SISMC2	Sistema Militar de Comando e Controle
TI	Tecnologia da informação
UNB	Universidade de Brasília

SUMÁRIO

1. INTRODUÇÃO

Nos tempos atuais a informação tornou-se o ativo mais valioso, ao mesmo tempo, passou a exigir uma proteção adequada, mas de forma assustadora e crescente, as organizações, seus sistemas de informações e suas redes de computadores, apresentam-se diante de uma série de ameaças, sendo que, algumas vezes, estas ameaças podem resultar em prejuízos irreparáveis para todo o sistema (SPANCESKI, 2004).

Um dos indicadores que podem corroborar para tal informação é a quantidade de incidentes de Segurança da Informação reportados constantemente, sinalizando a importância dessas ameaças que atentam contra a confidencialidade, a integridade e a disponibilidade das informações.

A segurança da informação visa a proteção de um grande número dessas ameaças, mas existe ainda a dificuldade de entender a sua importância e como medidas de implementação de uma série de controles tipo: novas práticas e novos procedimentos podem com certeza permitir que os objetivos específicos da segurança da informação da Marinha do Brasil sejam realmente garantidos.

Há que se ressaltar que a Segurança da Informação deixou de ser há tempos apenas uma questão banal, para ser tratada como questão de segurança nacional, por diversos países, incluindo o Brasil.

A Política de Segurança da Informação e Comunicação (POSIC) da Marinha do Brasil (MB) é definida como a doutrina a ser cumprida pela organização para orientação e apoio às medidas de implementação de segurança da Informação e comunicações. Esta Norma representa a Política de Segurança da Informação para a MB e define também os procedimentos e instruções a fim de reger o SIC da MB e deverão ser seguida e ser também do conhecimento de todo os pessoal credenciado e autorizado a operar e manusear os equipamentos conectados à Rede de Comunicações Integrada da Marinha do Brasil.

Baseado no fato que os procedimentos e instruções deveriam ser seguidos por todos os “usuários” e ratificando que ter uma preocupação com a vulnerabilidade de todo o Sistema de Informação torna-se essencial, esse trabalho tem como objetivo reforçar a importância do treinamento de oficiais e praças, a fim

de garantir profissionais conscientes, no que tange ao conhecimento das normas e procedimentos da Política de Segurança da Informação, como também deixa registrado algumas sugestões que poderão contribuir para uma melhor ação de todos os usuários.

1.1. Apresentação do Problema

Diante de um cenário cada vez mais tecnológico e inovador, onde é uma realidade o conceito de internet das coisas, a Marinha do Brasil necessita acompanhar tais evoluções e ao mesmo tempo buscar defender-se de ameaças ainda desconhecidas.

Os militares que guarnecem suas respectivas organizações militares (OM) são a interface mais importante diante das necessidades das novas estações de trabalho cada vez mais informatizadas, porém muitas vezes por falta de pessoal qualificado, algumas OM selecionam para compor a função de oficial encarregado da sessão de segurança da informação e comunicações (SIC), um militar sem a expertise na área de tecnologia da informação (TI). É importante dizer que na maioria das vezes também ocorre acúmulo de funções por parte de oficiais e praças, deixando a Marinha do Brasil mais suscetível a vazamentos de informação e falhas na segurança. Outro fato a ser levantado, que falhas repetem-se no processo de formação tanto do praça como do oficial, apesar da publicação DGMM-0540 estabelecer as atribuições dos setores responsáveis e dos usuários.

Por este motivo é necessário o treinamento de oficiais e praças na política de segurança da informação na Marinha do Brasil, verificar a maneira que os militares estão sendo doutrinados e como estes estão seguindo as leis regidas pelas publicações internas da Marinha do Brasil, do Ministério da Defesa e órgãos federais para sanar as falhas observadas neste processo.

Além de se fazer perpetuar sempre as leis que vigoram, também deve-se atentar para atualização constante das tecnologias que chegam no cenário de TI, bem como os operadores dos meios de comunicações mantendo-os motivados em vista à importância do tema em questão.

1.2. Justificativa

Com o avanço da tecnologia, o acesso à informação tornou-se cada vez mais fácil, instantâneo e eficiente fazendo com que a Marinha do Brasil por possuir

informações sigilosas e vitais para suas operações e segurança orgânica, necessite difundir a cultura de segurança das informações para conter os vazamentos “hackeamentos”, controlar e restringir os acessos à informações sigilosas dentro de suas organizações militares.

Um exemplo foi o caso ocorrido em 2013, com a agência de segurança nacional do Estados Unidos da America (NSA - sigla em inglês), onde o ex-técnico Edward Snowden tornou público um programa de espionagem executado pelo governo americano. Segundo Snowden a NSA espionava governos, governantes, empresas, empresários, de diversos países, aliados ou não, com o argumento do combate ao terrorismo. Para isso a NSA utilizava empresas comuns como Facebook, Youtube, Apple, entre outras, para atualizar o banco de dados da agência de segurança. É estimado que os recursos disponibilizados pelo governo norteamericano giravam em torno de 7 bilhões de dólares. (ARAUJO, 2014)

Fonte: (DIOGO SCHELP; 2017)

Entretanto a espionagem não é exclusiva da NSA pois diversos países também a realizam, além de igualmente existirem ataques cibernéticos por hackers. Em 6 de julho de 2013, o jornal brasileiro O Globo publicou reportagem que apontava que milhões de chamadas telefônicas e e-mails de brasileiros e estrangeiros no Brasil também foram monitorados pelo programa de vigilância norte-americano. O fato causou mal-estar entre governos brasileiros e dos Estados Unidos, uma vez que a prática feria os princípios de não-intervenção e soberania

nacional. O governo federal e o Congresso Nacional criticaram o vazamento e realizaram uma série de encontros com representantes norte-americanos para discutir o tema. (PEDROSA e MATSUKI, 2013)

Fonte: (NSA; 2016)

Para o professor da Universidade de Brasília (UnB) e especialista em Segurança da Computação, Pedro Rezende, os Estados Unidos realiza uma vigilância como argumento na luta contra o terrorismo. “Na hora de monitorar, a busca está direcionada para tudo e todos que a pretexto de encontrar uma centena de pessoas criminosas no meio de bilhões”, alerta.

A presidente Dilma Rousseff chegou a afirmar que a luta contra o terrorismo não justificava a espionagem. Uma visita da presidente aos Estados Unidos foi marcada para o dia 23 de outubro de 2013 com o objetivo de discutir o assunto "espionagem" com políticos americanos.

No dia 1º de setembro de 2013, o programa Fantástico da Rede Globo levantou novas denúncias de espionagem. O programa apresentou documentos ultrassecretos que comprovariam que os Estados Unidos monitorou comunicações da presidente Dilma Rousseff e de seus assessores próximos em 2011. Esse material fazia parte de uma apresentação privada para a agência de segurança nacional dos Estados Unidos. A reportagem é de autoria da repórter Sônia Bridge e de Glenn Greenwald, jornalista do The Guardian. Os materiais foram entregues a Greenwald pelo ex-agente da NSA, Edward Snowden. No seu conteúdo, a apresentação explica que houve interceptação de dados tanto do governo mexicano

quanto brasileiro.

Na segunda-feira 2/09/13 a presidente Dilma se reuniu com ministros para discutir as denúncias. O resultado da conversa foi externado pelos ministros da Justiça José Eduardo Cardozo e do Itaramaty, Luiz Figueiredo, que reiteraram a indignação do governo brasileiro sobre o caso. Contudo, eles evitaram mencionar futuras providências que serão tomadas contra os Estados Unidos. Cardozo e Figueiredo cobraram do governo norte-americano explicações, por escrito e formais, sobre as denúncias.

No mesmo dia, a Comissão de Relações Exteriores e de Defesa Nacional da Câmara dos Deputados convocou o ministro da Justiça, José Eduardo Cardozo, para prestar esclarecimentos sobre as denúncias. Na semana anterior, Cardozo viajou até os Estados Unidos para discutir as denúncias de espionagem com o governo norte-americano. Na ocasião, o Ministro da Justiça propôs um acordo de reciprocidade com os Estados Unidos sobre a interceptação de dados, mas a propsota foi rejeitada pelo país. Cardozo chegou a ressaltar que aceitaria a manutenção do diálogo com os norte-americanos, desde que as conversas fossem objetivas e esclareceu que as negociações não excluem uma iniciativa brasileira de levar o assunto a fóruns internacionais. No dia 8 de novembro de 2013, o Mercado Comum do Sul (Mercosul) reuniu e um dos principais temas abordados foi, exatamente. o programa de espionagem norte-americano.

A presidente Dilma Rousseff divulgou uma nota oficial dizendo que, caso a espionagem fosse confirmada, ficaria evidenciado que o motivo das tentativas de violação e de espionagem de dados do Brasil não é a segurança ou o combate ao terrorismo, mas sim interesses econômicos e estratégicos.(PEDROSA e MATSUKI, 2013)

Todos os fatos relatados acima demonstram a fragilidade e a vulnerabilidade de todo o sistema de tecnologia e controle de informação dentro e fora do Brasil.

Em contrapartida segundo a publicação DGMM-0540, sobre mentalidade de segurança no item 9.9 estabelece: "O esforço para as atividades de SIC deve ser de todos e não somente do pessoal diretamente envolvido com o setor de informática da OM. O fator mais importante para a SIC é a existência de uma mentalidade de segurança incutida em todo o pessoal. Pouco adiantará o estabelecimento de

rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver delas perfeita consciência. As OM devem, portanto, envidar esforços para desenvolver e manter um alto nível de conscientização do pessoal quanto à SIC. Isto pode ser feito, por exemplo, por meio de notas em Plano do Dia e de palestras, adestramentos, exercícios internos e outras atividades cabíveis, englobando publicações, normas e procedimentos afetos ao assunto. Além disso, dentro do Programa de Adestramento de cada OM, devem ser formalmente estabelecidos e continuamente cumpridos adestramentos que abordem todos os aspectos de SIC."

Nesse escopo, pretende-se ratificar a importância de um treinamento e qualificação frequente dos praças e oficiais, em conformidade com as normas vigentes internas, com a utilização de ferramentas que sejam eficazes do ponto de vista técnico, para garantir a confidencialidade, integridade, autenticidade e a disponibilidade das informações que trafegam pela Rede de Comunicações Integrada da Marinha do Brasil (RECIM) ou até mesmo com meios externos à Marinha do Brasil.

1.3. Relevância

As forças armadas do país detêm diversas informações garantidoras da soberania do país, portanto necessita manter controle positivo das informações, tanto quanto o sigilo, impedindo que outras fontes tenham conhecimento dessas informações.

Faz-se imprescindível que os serviços de suporte prestados pela RECIM como por exemplo: comunicações por meios físicos (radioenlaces, fibra, satélite, par metálico), comunicação por telefonia IP, conectividade, sistema operacional de rede, correio eletrônico, intranet, internet, certificação digital, aplicações de redes sem fio, aplicações de videoconferência sejam dotados de total segurança, desde a confecção das estruturas até o manuseio pelos militares.

Ao se falar no “manuseio” pelos militares levantamos a necessidade de haver um programa de treinamento de pessoal voltado para segurança da informação que transmitirá a natureza central dessa política, facilitando a aplicação da política de informação de uma forma bem-sucedida.Esse sucesso pode ser estendido ainda mais, quando ocorre o entendimento do que é a “política da informação” na sua essência.

A centralidade das políticas de segurança da informação para praticamente tudo o que acontece no campo da segurança da informação é cada vez mais evidente. Essas políticas estipularão o tipo de serviços de transmissão que devem ser permitidos, como autenticar as identidades dos usuários e como registrar eventos relevantes para a segurança. Um treinamento eficaz de segurança da informação e um esforço de conscientização, não podem ser iniciados sem definir políticas de segurança da informação, visto que elas fornecem o conteúdo essencial que pode ser utilizado em material de treinamento e conscientização. Estudantes de segurança da informação, digo oficiais e praças, equipados com habilidades no desenvolvimento e gerenciamento de políticas, poderão contribuir positivamente com qualquer intercorrência que aja, tendo uma ação mais pontual, eficaz e realmente importante evitando quaisquer intercorrências.

A política de ensino é efetivamente a base essencial de um programa eficaz de educação sobre segurança da informação, para tanto, faz-se imprescindível que os militares que compõem as organizações militares (OM) estejam motivados a ter todo o conhecimento relativo a segurança da informação e estejam atualizados através de treinamentos contínuos, pois isso com certeza garantirá maior segurança a Marinha do Brasil e menos vulnerabilidade.

1.4. Objetivos

O objetivo geral e os específicos relacionados abaixo são responsáveis por apresentar o direcionamento dessa monografia e os resultados esperados, sendo que o geral irá resumir e descrever delimitando a ideia central e os específicos os resultados que se pretende alcançar com essa pesquisa de forma detalhada.

1.4.1 Objetivo Geral

Reforçar a importância do treinamento constante de oficias e praças, a fim de garantir profissionais conscientes, no que tange a política de segurança das informações, diante dos avanços tecnológicos e das ameaças constantes, para que faça cumprir de fato os fundamentos e os requisitos estabelecidos pela Doutrina de Tecnologia da Informação da Marinha do Brasil (DGMM-0540 e EMA- 416).

1.4.2 Objetivos Específico

Analisar os documentos e as publicações relacionadas à política de segurança da informação;

Clarificar os principais conceitos de política de segurança, como importante ferramenta de informação, na formação dos militares da Marinha do Brasil;

Identificar as atribuições e responsabilidades dos diversos setores e recursos humanos envolvidos, focando principalmente na parte de mentalidade de SIC;

Salientar que a interface mais fraca é a do usuário

Promover sugestões para melhoria da política de segurança da informação da Marinha do Brasil, principalmente aquilo que diz respeito ao usuário e a mentalidade de segurança

2. REFERENCIAL TEÓRICO

Serão observados textos, dissertações e teses dos principais autores que abordaram a política de segurança da informação, bem como publicações, procedimentos e protocolos adotados pela Marinha do Brasil no que tange a política de segurança da informação.

Será realizada uma comparação entre os seguintes documentos: a portaria normativa numero 2327 do Ministério da Defesa, decreto n 3505 da Presidência da Republica, DGMM-054 e EMA-416 no que se refere ao treinamento de pessoal e a mentalidade da segurança da informação.

Na publicação internas DGMM 0540, abordou-se a política de segurança da informação bem como as atribuições e responsabilidades de todos envolvidos no que tange a procedimentos rotineiros para especialistas no assunto e usuários dos sistemas de comunicações, em âmbito interno ou na troca de informações com o meio externo também.

Na tese de SPANCESKI, F. R., Política de Segurança da Informação, a autora salienta sobre a imprescindibilidade no processo de investimento na segurança, mostrando os impactos negativos, que por muitas vezes passam por despercebidos.

3. **METODOLOGIA**

Será versado os tipos de pesquisa deixando claro a forma como foi realizado e abordado os assuntos tratados, citando de maneira detalhada os procedimentos que foram utilizados para a coleta e para análise dos dados levantados, adaptados às necessidades e objetivos do presente trabalho.

3.1. Classificação da Pesquisa

A classificação da pesquisa é realizada mediante estabelecimento de um critério e esta será classificada levando em conta o nível de profundidade do estudo. No caso abordado neste trabalho será do tipo exploratória, que tem como objetivo proporcionar maior familiaridade com objeto de estudo.

3.1.1. Quanto Aos Fins

Esta é uma pesquisa com método quantitativo através de uma pesquisa empírica e experimental, de caráter exploratório, descritivo e explicativo com observação simples, análise bibliográfica e documental, com objetivo de buscar informações pertinente relacionadas a política de segurança da informação.

3.1.2. Quanto Aos Meios

Foram realizadas uma pesquisas bibliográficas e documentais, com material proveniente da internet e dos meios acadêmicos, com destaque para outras teses anteriores que abordam o assunto em tese.

3.2. Limitações Do Método

O curso de Oficial da Segurança da Informação e Comunicações (OSIC), com os princípios descritos na DGMM-0540, estabelece as atribuições que teoricamente deveriam garantir uma atuação eficaz aos praças e oficiais da Marinha do Brasil. Na prática isso muitas vezes não é percebido e falhas no processo são identificadas, tais como a falta de domínio do assunto, o não aprofundamento do tema em questão por parte dos profissionais, a facilidade de acesso sem o real conhecimento dos riscos, falta de treinamento específico os quais poderão permitir falhas em sua atuação e também possíveis vulnerabilidade todo no processo.

O assunto por si só já é considerado reservado dentro do âmbito de qualquer força armada, desse modo houve dificuldade em se conseguir vasta quantidade de

material bibliográfico, principalmente no que se refere a materiais e métodos, que poderiam ser aplicados, para avaliar e melhorar a atuação desses profissionais.

Devido a extrema evolução das tecnologias de informações militares e civis, essa atualização tornar-se-ia necessária, fundamental e constante, mas na realidade isso não é discutido, muitas vezes deixado de lado e tratado sem a revelância necessária que merece a questão em si.

É necessário que oficiais e praças passem por um treinamento para que sua atuação possa realmente ter a eficácia que a Marinha do Brasil necessita e a segurança seja enfim garantida.

3.3. Coleta e Tratamento de Dados

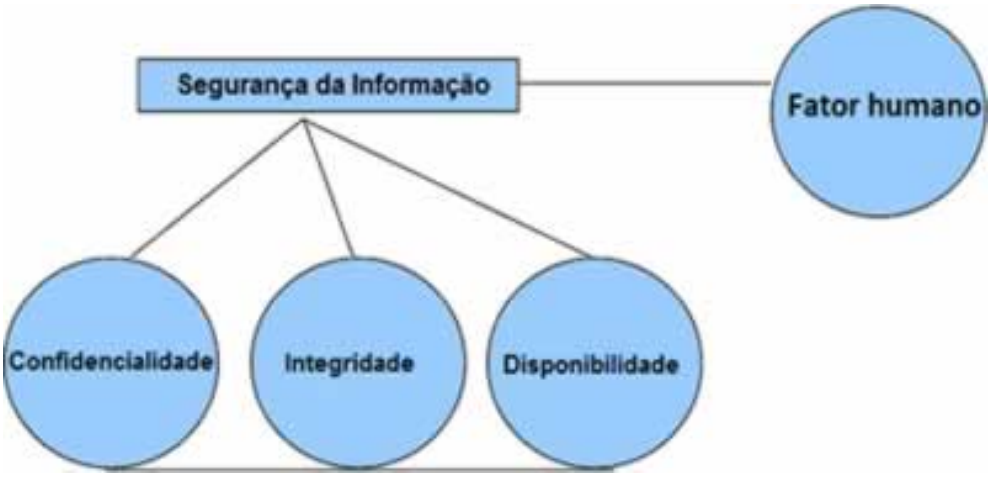
Foram estudadas as bibliografias descritas neste trabalho, provenientes da internet e dos meios acadêmicos.

As publicações, DGMM-0540, EMA-416, PORTARIA NORMATIVA número 2.327/MD do Ministério da Defesa e o decreto n 3505 da Presidência da Republica foram estudados com intuito de verificar as características similares relacionadas com a mentalidade de segurança enfatizando a importância do treinamento de pessoal.

4. DESCRIÇÃO E ANÁLISE DOS RESULTADOS.

4.1 Dgmm-0540 E Treinamento De Pessoal.

Na parte III, da DGMM-540, SIC, em sua introdução estatelece que: “A informação é um bem de valor intangível e nem sempre mensurado. Por esta razão, ela é classificada como ativo para uma organização. Como qualquer outro ativo, a informação e o seu correto uso são partes essenciais no cumprimento das missões, devendo, assim, ser adequadamente protegidos. Nos dias atuais, os maiores repositórios de informações são os ambientes computacionais, especialmente os interconectados por redes. Para proteger as informações, tais ambientes devem ser considerados seguros. Contudo, ser um ambiente seguro é um estado para dado momento, em face dos riscos inerentes, do valor do ativo, das ameaças e das vulnerabilidades. Logo, a segurança é uma busca constante do aperfeiçoamento da mentalidade de segurança, dos procedimentos e da tecnologia que envolvem o ativo informação. No cenário da MB, as redes estão cada vez mais interconectadas, chegando até aos meios navais e OM no Brasil e exterior. Com isto, a informação fica exposta a um crescente número e variedades de ameaças e vulnerabilidades inerentes aos sistemas, protocolos de rede, configurações e compartilhamento dos canais de transmissão e recepção de dados, voz e vídeo. A informação pode estar impressa em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é fundamental que ela seja sempre protegida adequadamente” (DGMM-540).



Fonte: (SILVA, M.; COSTA, 2009)

"A Segurança da Informação e Comunicações (SIC) é, portanto, um conjunto de medidas que visam garantir os requisitos de sigilo, autenticidade, integridade e disponibilidade em face dos riscos corretamente medidos em função do valor do ativo, das ameaças e das vulnerabilidades dos ambientes que a armazenam, a processam e a trafegam. Ela é obtida a partir da manutenção constante de um conjunto de normas e procedimentos adequados, incluindo políticas, processos, estruturas organizacionais, configurações de software, hardware, protocolos de redes e proteção dos enlaces de dados, voz e vídeo. Além disso, é fundamental uma permanente construção de mentalidade de segurança da informação em todos os integrantes da MB, desde os altos escalões até as escolas de formação. Outrossim, controles precisam ser estabelecidos, implementados, monitorados, analisados e aperfeiçoados, onde necessário, para garantir que os propósitos da SIC sejam atendidos. É imprescindível que tais tarefas sejam feitas em conjunto com outros processos de gestão da MB" .(DGMMM-0540).

Ao citar a importância da permanente construção de mentalidade de segurança da informação, o mesmo documento estabelece as atribuições e responsabilidades de todos envolvidos no processo, ratificando como todas essas ações podem influenciar no controle, gerenciamento e melhores resultados a serem alcançados.

Essas atribuições e responsabilidades podem ser visualizada nas tabelas abaixo:

TABELA - 1	
RESPONSABILIDADES E ATRIBUIÇÕES	
DCTIM	Promover e fomentar o incremento progressivo da mentalidade de SIC, por meio de ferramenta de gestão do conhecimento, palestras, seminários, simpósios e cursos;
CLTI	Elaborar um programa de adestramento (PAD) anual para as OM apoiadas, que dissemine e incorpore a mentalidade de SIC;
	Zelar pelo fortalecimento da mentalidade de segurança, junto as OM apoiadas;
	Alterar, propor, analisar e verificar se os requisitos de SIC das OM apoiadas estão sendo praticados em conformidade com as normas estabelecidas;

Fonte: DGMM-0540

TITULAR DA OM	Manter o fiel cumprimento das normas, procedimentos e instruções pertinentes à SIC na sua OM;
	Zelar pelo fortalecimento da mentalidade de segurança;
	Manter um programa de adestramento de SIC para todo o pessoal da OM;
	Designar o Oficial de Segurança da informação e Comunicações (OSIC) da OM;
	Designar o Administrador da rede local (ADMIN) da OM;
OSIC	Possuir conhecimentos mínimos de redes locais de computadores, serviços disponibilizados pela rede (Intranet, correio eletrônico e assinaturas digitais) e conhecimento em auditoria de redes.
	Estabelecer procedimentos para o gerenciamento da infraestrutura de SIC de acordo com as normas em vigor.
	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;
	Coordenar, junto aos demais setores da OM, o estabelecimento dos Planos de Adestramento de SIC e zelar pelo seu cumprimento;
	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;
	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;
ADMIN	Ter capacitação em Administração de Rede de Computadores e sistemas operacionais, que estejam sendo utilizados dentro da OM, assim como conhecimentos mínimos em auditoria de sistemas computacionais;
	Gerenciar a rede local de forma a mantê-la operando dentro dos seus requisitos operacionais e com todos seus serviços em funcionamento;
	Promover adestramentos periódicos aos usuários da OM quanto aos procedimentos e serviços de TI;
	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;

Fonte: DGMM-0540

DO USUÁRIO	Tratar a informação digital como patrimônio da MB e como um recurso que deva ter seu sigilo preservado;
	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;
	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;
	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;
	Não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros;
	Não alterar o endereço de rede ou qualquer outro dado de identificação de sua estação de trabalho;
	Utilizar em sua estação de trabalho somente programas homologados para uso na MB;
	Não compartilhar, transferir, divulgar ou permitir o conhecimento das suas autenticações de acesso (senhas) utilizadas no ambiente computacional da OM, por terceiros;
	Seguir as orientações da área de informática da OM relativas ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;
	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;
	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;
	Não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação;
	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;
	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;
	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;

Fonte: DGMM-0540

DO USUÁRIO	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.
	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;
	Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional da OM pode ser auditada;
	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;

Fonte: DGMM-0540

Quando observamos o quadro acima vimos que todos os setores e pessoas envolvidas são peças primordiais na garantia de uma política de segurança da informação coesa, eficaz e sólida, contudo na prática isso não vem sendo observado.

A DCTIM , o CLTI e o CIAW possuem militares capacitados e bem formados no que tange ao conhecimento e atuação de fato na área de TI. Dentre suas atribuições e responsabilidades seriam os mais aptos a realizar o treinamento aos oficias, praças ou seja "os usuários", que dentro da Marinha do Brasil tem acesso a informação digital.

O titular da OM, OSIC e ADMIN, possuem em seu rol de responsabilidades e atribuições à manutenção do programa de adestramento de SIC para todo o pessoal da OM, ratificando a importância que todos são responsáveis pela garantia do que é proposto na política de segurança da informação da Marinha do Brasil, mas isso também não acontece.

Quando interpretamos o quadro do “usuários"que são “todos” que tem acesso a informação digital, uma das suas atribuições iniciais é exatamente “tratar a informação como patrimônio da MB e como um recurso que deva ter seu sigilo preservado”, mas nem todo o real conhecimento da importância desta área de TI e são estes que mais tem acesso e podem realmente colocar em risco a segurança.

Todas essas colocações vem ratificar que o treinamento de pessoal passa ser uma ferramenta imprescíndivel na garantia de toda a política de segurança da informação da Marinha do Brasil.

4.2 Comparação Entre: Portaria No 2327, Decreto No 3505 E Dgmm-054, Ema-416

Na Tabela 2 abaixo, observa-se que os documentos elaborados pela Marinha do Brasil DGMM-0540 e EMA - 416 são bem redigidos, estruturados e completos, ressaltando o treinamento do pessoal e a mentalidade de segurança da informação, os quais são os objetivos do presente trabalho, assim como também são apresentadas as mesma preocupações no Decreto Nº 3.505 da Presidência da República e da Portaria Normativa Nº 2.327 do Ministério da Defesa.

São também observadas várias referências equiparadas que são citadas em todos os documentos quanto a capacitação, conscientização, sensibilização, especialização, formação e aprimoramento dos recursos humanos em todos os campos da segurança da informação.

Então conclui-se que a maior dificuldade da Marinha do Brasil para fortalecer a sua POSIC não se concentra nas suas publicações e sim na mudança da abordagem do tema e usar o treinamento de pessoal para tornar as POSICs uma realidade prática.

TABELA - 2

PORTARIA NORMATIVA No 2.327, 2015 DO MINISTÉRIO DA DEFESA	
CAPÍTULO II	Atributos de Segurança da Informação e das Comunicações Os atributos clássicos de *SIC*, que também se aplicam ao SISMC2, são os seguintes: confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio (irretratabilidade)
CAPÍTULO III	Promover a capacitação de pessoal para o desenvolvimento de competência científico-tecnológica em segurança da informação, no EMCFA e nas Forças Armadas, visando viabilizar a formação de cultura organizacional de segurança da informação.
	Promover cultura de *SIC* no âmbito do SISMC2, por intermédio de atividades de sensibilização, conscientização, capacitação e especialização;

DECRETO Nº 3.505, 2000 PRESIDÊNCIA DA REPUBLICA	
Art. 1º	Assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
	Criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
	Conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.
Art. 3º	Promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;
	Promover as ações necessárias à implementação e manutenção da segurança da informação;
	Promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;
Art. 4º	Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos de que trata o artigo anterior, visando garantir a adequada articulação entre os órgãos e as entidades da Administração Pública Federal;
	Estabelecer programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação;
	Orientar a condução da Política de Segurança da Informação já existente ou a ser implementada;

DGMM-0540	
PROPÓSITOS	Estabelecer a Política de Segurança da Informação e Comunicações da MB, definindo procedimentos e instruções a fim de reger as atividades relacionadas à SIC da MB, complementando as instruções contidas em outras publicações correlatas em uso, devendo ser de conhecimento de todo o pessoal credenciado e autorizado a operar e manusear equipamentos conectados à RECIM.

EMA-416	
PROPÓSITOS	Assegurar a capacitação das diversas OM para o uso eficaz da TI, enfocando os riscos que proporcionam as vulnerabilidades dos processos de informação;
	Promover a capacitação de recursos humanos na MB, para o desenvolvimento de competência científico-tecnológica em TI e criptologia, envolvendo tanto as atividades de desenvolvimento de códigos quanto as atividades de criptoanálise;
	Promover o intercâmbio entre as OM da MB especializadas em TI e criptologia com instituições públicas e privadas congêneres;
PRINCÍPIOS	A capacitação dos recursos humanos envolvidos, constituída pela qualificação do pessoal e associada à aplicação do conhecimento adquirido, é essencial para a eficácia das ações de TI;
	Uso dos Sistemas de Ensino à Distância (EAD) como ferramentas de baixo custo e grande poder de disseminação de conhecimento, para continuamente aprimorar o preparo e a indispensável atualização do pessoal;

5. CONCLUSÃO

Na sociedade da informação, ao mesmo tempo que estas são consideradas um dos principais ativos de uma organização, elas encontram-se também sobre constantes riscos. Com isso a segurança da informação tornou-se um ponto extremamente importante para sobrevivência de toda e qualquer organização seja civil ou militar.

Dentre as medidas de segurança implantadas encontramos as normas, procedimentos, ferramentas, atribuições e responsabilidades que devem ser seguidas por todos os setores e usuários de modo a garantir a total segurança da informação.

A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante e definindo desde do setor de implementação até o usuário, as regras que devem ser seguidas para utilização de maneira adequada dos recursos de informática.

O modelo de política de segurança desenvolvido visa a descrição destas regras de modo acessível ao entendimento dos usuários, mas de forma geral apesar da acessibilidade desses manuais e regras, nem todos tem ciência, por isso torna-se necessário uma política para implementação mais eficaz que envolva todos os profissionais, evitando que cada equipe tenha para si um padrão desconexo das demais.

Em decorrência do que foi exposto acima e ao verificar que o conhecimento sobre a política de segurança da informação é imprescindível, que o presente trabalho vem ratificar a importância do treinamento de pessoal em todos os setores e níveis hierárquicos para garantir enfim uma maior conscientização e prática eficaz.

5.1. Considerações Finais

Segundo Charles Wood: “Um programa de segurança da informação de qualidade começa e termina com a política”, mas para que essa política seja eficaz, é necessário o envolvimento, participação e conscientização de todos.

Algumas sugestões poderiam ser implementadas para alcançarmos tal objetivo, tais como:

- Treinar, capacitar e atualizar os oficiais e praças;

- Promover avaliação continuada dos oficiais e praças;

- Identificar as práticas adotadas na disseminação da cultura organizacional da SI, reforçando a necessidade dessa prática dentro das diversas unidades militares, através de uma ferramenta de avaliação criada para esse fim;

- Investir na disseminação da mentalidade da SIC, a fim de sanar os problemas que surjam;

- Definir para os usuários da OM, as regras que deverão ser seguidas, para utilização de maneira adequada, dos recursos de informática;

- O treinamento continuado de pessoal agregado as sugestões relatadas acima, colocadas em prática, muito contribuirão para a garantia de uma política de segurança da informação da Marinha do Brasil.

Fonte (The Trusted Toolkit,2007)

5.2. Sugestões para Futuros Trabalhos

Devido a dificuldade de se encontrar material suficiente para aprofundamento do tema, torna-se necessário maiores pesquisas para prover informações, que sejam dirigidas de forma mais rápida e segura atingindo todos os níveis hierárquicos.

É relevante que sejam realizados trabalhos complexos no estilo pesquisa de campo, para cada tipo de meio de informação, mostrando peculiaridades, principais pontos de insegurança e até mesmo as vantagens e prioridades desse conhecimento, com objetivo de garantir maior segurança para todo o SIC.

Uma pesquisa de campo em todos níveis hierárquicos quanto ao conhecimento, avaliando-se os recursos humanos que atuam direta ou indiretamente, é primordial dentro de todo o processo, a fim de direcionar as ações de uma maneira mais assertiva o problema em questão. Essa pesquisa também contribuirá para que o treinamento de pessoal seja realizado de maneira mais eficaz, resultando em condições mais satisfatórias para controle de todo o sistema.

Todos os procedimentos relacionados acima colocados em prática muito contribuirão para que falhas em todo o processo sejam identificadas e corrigidas, a fim de que ações sejam elaboradas para de fato possa melhorar e previnir qualquer vazamento no Sistema de Informação e Comunicação da MB.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002:**

_____ **Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal**: Decreto nº 3.505, de 13 de junho de 2000.

_____. MINISTÉRIO DA DEFESA: **Política de Segurança da Informação para o Sistema Militar de Comando e Controle**, Portaria Normativa nº 2.327/MD, de 28 de outubro de 2015.

_____, ESTADO MAIOR DA ARMADA (EMA). **EMA 416:** Doutrina de Tecnologia da Informação da Marinha do Brasil (Mod 2). Rio de Janeiro, 2007.

_____. DIRETORIA GERAL DE MATERIAL DA Marinha do Brasil (DGMM). **DGMM 0540:** Normas de Tecnologia da Informação da Marinha do Brasil (2a REV). Rio de Janeiro, 2017.

SPANCESKI, F. R., **Política De Segurança Da Informação. Desenvolvimento De Um Modelo Voltado Para Instituições De Ensino**, Instituto Superior Tupy. Joinville, 2004.

CRESSON WOOD, Charles, **Information Security Policies Made Easy**, Ninth Edition (2003) NetIQ Corporation p 1.

FERREIRA DE ARAUJO, Rubens, **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: Instrumento de defesa cibernética**, Escola Superior de Guerra, Rio de Janeiro 2014.

E. WHITMAN, Michael & J. MATTORD, Hebert, **Teaching Information Security Policy**, West Point, NY June 2004.

SCHELP, Diogo **A Incrível História Da Fuga De Edward Snowden**, 2017, https://veja.abril.com.br/blog/a-boa-e-velha-reportagem/a-incrivel-historia-da-fuga-de-edward-snowden/ . Acesso em: 15 de fevereiro de 2018.

NSA , **National Security Agency Insignia,** 2016, https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/insignia/nsa-insignia.shtml. Acesso em 15 de fevereiro de 2018.