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

CURSO DE APERFEIÇOAMENTO AVANÇADO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

SEGURANÇA FÍSICA DA INFORMAÇÃO E COMUNICAÇÃO NA MARINHA DO BRASIL: Comparação entre a NBR ISO/IEC 27002 e a DGMM0540

1º Ten (QC-CA) BERNARD PEREIRA DE OLIVEIRA

Rio de Janeiro
2020

1º Ten (QC-CA) BERNARD PEREIRA DE OLIVEIRA

SEGURANÇA FÍSICA DA INFORMAÇÃO E COMUNICAÇÃO NA MARINHA DO BRASIL: Comparação entre a NBR ISO/IEC 27002 e a DGMM0540.

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Sistema de comunicação e informação.

Orientadores:
Prof. Dr. Anderson Oliveira da Silva
CC(T) Patrícia Amaro Rocha Arruda

CIAW
Rio de Janeiro
2020

OLIVEIRA, Bernard Pereira.
Segurança Física Da Informação e Comunicação na Marinha do Brasil: Comparação entre a NBR ISO/IEC 27002 e a DGMM0540 / Bernard Pereira de Oliveira. Rio de Janeiro: CIAW, 2020.
Total de folhas. 41f.: il.

Orientadores: CC(T) Patrícia Amaro Rocha Arruda; Dr. Anderson Oliveira da Silva.

Monografia (Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações) — Centro de Instrução Almirante Wandenkolk. Centro de Pós-Graduação Avançada, Rio de Janeiro, 2020.

1. Segurança física da informação. 2. Segurança física da Comunicação. 3. Marinha do Brasil. 4. ISO 27000. 5. Normas da tecnologia da Marinha I. Centro de Instrução Almirante Wandenkolk. Centro de Pós-Graduação Avançada. II. Título.

1º Ten (QC-CA) BERNARD PEREIRA DE OLIVEIRA

SEGURANÇA FÍSICA DA INFORMAÇÃO E COMUNICAÇÃO NA MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Sistema de comunicação e informação.

Aprovada em _____

Banca Examinadora:

_____

CMG (RM1-EN) MSc. Gian Karlo Huback Macedo de Almeida (Banca Examinadora)

Marinha do Brasil

_____

CC (T) Patrícia Amaro Rocha Arruda (Orientador Técnico)

Marinha do Brasil

_____

Prof. Dr. Anderson Oliveira da Silva (Orientador Acadêmico)

PUC-RJ

Rio de Janeiro, 24 de abril de 2020.

Dedico esse trabalho a minha esposa Aline Rabello e a meus pais Délio Martins, Georgina Pereira, e a meu irmão Délio Filho.

AGRADECIMENTOS

Agradeço primeiramente a Deus, em seguida aminha esposa, Aline Rabello José de Oliveira, a minha mãe, Georgina Pereira de Oliveira, ao meu pai, Délio Martins de Oliveira e ao meu irmão, Délio Martins de Oliveira Filho, por me incentivarem, a meu orientador acadêmico, prof. Dr. Anderson Oliveira da Silva, pela orientação de qual norma internacional, na área da segurança da informação, usar para comparar com as normas da Marinha do Brasil, e sua visão de segurança, que auxiliou na confecção deste trabalho, e a minha orientadora técnica, CC(T) Patrícia Rocha, pelo apoio com a aquisição das normas mais atualizadas e sua visão de como o presente trabalho poderia melhorar a segurança na Marinha do Brasil, ao meu professor da matéria de metodologia, Hélios Malebranche ,pelas orientações de como formatar o trabalho e melhor apresentar os resultados ao meu coordenador do Curso de segurança da informação e Comunicação que marcou meu encontro com meu orientador técnico na DCTIM e por todo apoio geral prestado a turma para que melhor nos preparássemos para produção deste trabalho e a todos do Curso de Aperfeiçoamento Avançado, que se dispuseram a me ajudar com este trabalho.

“O sucesso é ir de fracasso em fracasso
sem perder entusiasmo.”
Winston Churchill

SEGURANÇA FÍSICA DA INFORMAÇÃO E COMUNICAÇÃO NA MARINHA DO BRASIL

Resumo

Este trabalho busca comparar a norma internacional sobre a criação e operação de sistemas de gestão de segurança da informação, NBR ISO/IEC 27002, e as normas de tecnologia da informação da Marinha do Brasil (MB), DGMM0540 com o objetivo de criar uma melhoria na segurança física da informação e comunicação na MB, buscando meios de reduzir vulnerabilidades no acesso indevido a informações através da análise dos controles de segurança encontrados na NBR ISO/IEC 27002, sugestões essas que poderão ser aplicadas a diversas organizações militares da Marinha do Brasil. É exposta uma análise da NBR ISO/IEC 27002 e da DGMM0540, para auxiliar na posterior comparação entre elas, ressaltando o que mais tem influência na segurança física da informação e comunicação, definido o que é segurança para cada uma das normas e como pode ser obtida. Neste sentido, a comparação seguiu cada seção da NBR ISO/IEC 27002, buscando uma equivalência na DGMM0540 que implementasse os objetivos apresentados e, depois de percorrer todas a seções, formou-se um quadro com cada seção tendo um capítulo equivalente e sua respectiva descrição. Por fim, concluiu-se que todos os controles analisados são implementados, e tal resultado ocorreu, pois, uma norma internacional de padrões de segurança da informação tem que ser o mais genérico possível para que possa ser aplicada na maioria das organizações do mundo, enquanto uma norma especifica pode ter algumas particularidades próprias. Além disso, cada organização opta por implementar ou não todas as recomendações da norma internacional, já que certos controles podem inviabilizar seus objetivos ou missão.

Palavras-chave: Segurança física da informação. Segurança física da Comunicação. Marinha do Brasil. ISO 27000. Normas da tecnologia da Marinha.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

LISTAS DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ACID	Autenticidade, Confiabilidade, Integridade e Disponibilidade
BS	*British Standard*
CLTI	Centro Local de Tecnologia da Informação
CN	Comunicações Navais
CTIM	Centro de Tecnologia da Informação da Marinha
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DGMM	Diretoria-Geral de Material da Marinha
DGMM0540	Normas de Tecnologia da Informação da Marinha do Brasil
DSIC	Departamento de Segurança da Informação
GRSIC	Gestão de Riscos em Segurança da Informação e Comunicações
IEC	*InternationalElectrotechnicalCommission*
IN01	Instrução Normativa n°01
ISO	*International Standard Organization*
MAC	*MultiAcessControl*
MAN	Manutenção
MB	Marinha do Brasil
OBT	Obtenção
OM	Organização Militar
OSI	*Open System Interconnection*
P2P	*Peer-to-Peer*(Ponto a ponto)
PLA	Planejamento
PLCONT	Planos de Contingência
PRO	Produção

RCC	Recurso computacional crítico
RECIM	Rede de Comunicações Integradas da Marinha
RET	Desativação
SD	Sistema Digital
SGSI	Sistemas de Gestão de Segurança da Informação
SIC	Segurança de Informação e Comunicação
TI	Tecnologia da Informação

1. INTRODUÇÃO

O presente trabalho tem ênfase na análise da segurança física da informação e comunicação na Marinha do Brasil (MB). As principais normas que serão usadas como base para este trabalho serão a norma DGMM0540 (MARINHA DO BRASIL, 2019) e a NBR ISO/IEC 27002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013), mais especificamente a parte que trata de segurança física da informação.

Em 1995, o padrão Britânico (*British Standard*) BS 7799, deu origem a série ISO 27000 (*International Standard Organization*), a qual obteve uma grande aceitação mundial. A norma BS 7799 possui três versões: código de práticas, normas para certificação e outra para análise de riscos. (SOUZA; LAUTERT, 2006)

Atualmente, as normas da família 27000, servem de base para a criação e operação de Sistemas de Gestão de Segurança da Informação (SGSI). O objetivo desta é apresentar conceitos sobre a gestão da segurança da informação e situar sobre os termos técnicos padronizados utilizados.

1.1 Apresentação do Problema

A segurança da informação é um assunto muito amplo, envolve todas as camadas do modelo OSI, como a física, enlace, rede, transporte, seção, apresentação e aplicação (TANENBAUM, A.; WETHERALL, 2011). Desta forma, para que seja delimitado um escopo, o trabalho abordará a segurança física da informação e comunicação, isto é, os recursos que fornecem a infraestrutura para o funcionamento da rede.

A Marinha do Brasil possui grande interesse no assunto por causa das informações sensíveis que trafegam em seu meio, como por exemplo, os dados provenientes de militares em missão de paz no exterior.

Para salvaguardar estas informações, são utilizados procedimentos fundamentados na DGMM0540, que apesar de não ter ferramentas especificas para solucionar todos os problemas de segurança da informação, apresenta em linhas gerais e os requisitos que os sistemas de Tecnologia da informação (TI) devem ter, semelhante à NBR ISO/IEC 27002, que também não tem soluções especificas e sim controles de segurança da informação.

A última atualização da DGMM0540, realizada em 2019, não mudou o capítulo que versa sobre segurança física da informação se comparado a última versão de 2017, apesar de

ter incluído um novo capítulo sobre dispositivos moveis nas organizações militares da Marinha. Com o intuito de estudar se seria necessária alguma revisão no capítulo que versa sobre a segurança física, a referida será comparada com a NBR ISO/IEC 27002.

A segurança física difere da segurança lógica de uma organização pois trata de problemas que são causados por adversidades físicas, e muitas vezes inesperadas, como por exemplo depredação, chuvas fortes, incêndio e descargas atmosféricas. Para reduzir os impactos destas adversidades, é importante analisar a frequência com que ocorrem tais condições climáticas, averiguar se são recorrentes e se preparar com a aplicação dos métodos de segurança física adequados para proteger as informações armazenadas nos equipamentos ou em meio físico como papel, juntamente com os recursos humanos da organização.

A implementação do controle de acesso do pessoal da organização a áreas críticas, que possuem informações sensíveis para a organização, devem ser através de mecanismos como crachá, fechadura com senha e câmeras de segurança.

Além de controle de acesso do pessoal da organização, devem-se ter métodos de controle para pessoas de fora da organização, como fornecedores e prestadores de serviço, que não devem andar sozinhos e é desejável que sejam registrados no sistema interno da organização.

A segurança física adotada tem que levar em consideração o modo como são feitas as operações da organização para que o investimento feito seja adequado a segurança. É necessário priorizar a capacidade dos funcionários de exercer suas funções antes de escolher os métodos de segurança, para que eles não impeçam que sejam atingidos os objetivos da organização. (WESTCON, 2016).

1.2Justificativa e Relevância

A Segurança física da informação e comunicação possui diferentes abordagens, como a proteção dos equipamentos físicos que armazenam a informação ou que efetuam a comunicação, ou seja, aquela que está disposta em meio digital, como em discos rígidos, que são físicos; ou em documentos em meio físico como, por exemplo, em papel. A proteção destes equipamentos e documentos envolve a proteção contra danos causados por incêndio, surtos de energia e por apropriação indevida.

Todos esses aspectos serão analisados sob a luz das recomendações de controle de acesso apresentados na NBR ISO/IEC 27002 e comparados com o que é apresentado pela DGMM0540 ao longo deste trabalho.

A segurança da informação e comunicação é de extrema importância para a Marinha do Brasil, pois no meio operacional, por exemplo, é crucial que não seja conhecida a posição dos navios; na questão estratégica, é importante manter confidencial quais as especificações dos equipamentos; e, no âmbito do pessoal militar, informações vazadas podem lhe causar muitos problemas.

Existem casos em que antes de começar a se preocupar com a segurança lógica, deve-se atentar para a segurança física, por exemplo, em uma situação em que se tenha acesso a um cabo de rede da organização onde o *switch* que o conecta à rede interna já liberou o fluxo de dados. Nenhum dos controles de segurança lógica barraria este acesso.

A segurança em qualquer nível causa *overhead*, ou seja, a comunicação e o acesso à informação seriam mais rápidos sem a segurança, então se faz necessário verificar até que nível se precisa de segurança, sendo que nunca se atingirá 100% de segurança. (OLIVEIRA, 2009)

1.3Objetivos

O objetivo a ser alcançado é propor uma melhoria na segurança física da informação e comunicação na Marinha do Brasil, a NBR ISO/IEC 27002, que discorre sobre a gestão de segurança da informação, em busca de controles de segurança que oferecem meios de reduzir vulnerabilidades no acesso indevido a informações (OSTEC, 2017) e que ainda não estejam sendo implementados pela DGMM0540 para serem aplicadas a diversas organizações militares da Marinha do Brasil.

1.3.1 Objetivo Geral

Analisar documentos que discorram sobre a segurança física da informação e comunicação (NBR ISO/IEC 27002) e militar (DGMM0540) e realizar um levantamento da situação dos controles de segurança na Marinha do Brasil.

1.3.2 Objetivos Específicos

Criação de um trabalho que possa auxiliar na segurança física da Informação e Comunicação das diversas organizações militares da Marinha do Brasil no que tange aos diversos controles que serão explorados, visando criar uma consciência que os colaboradores devem possuir com relação à segurança física.

1.3.3 A Segurança da Informação na Marinha

A Marinha vem promovendo cursos e palestras para promover a segurança da informação dentro da corporação, conforme o capitão de Mar e Guerra Antônio José da Rosa: "Hoje as informações estão concentradas na DCTIM e no CTIM e o objetivo é disseminá-las também a quem trabalha na ponta, de forma a contribuir cada vez mais para robustecer a defesa cibernética e segurança da informação na Marinha".(MARINHA DO BRASIL, 2020)
Em outubro de 2016, a DCTIM lançou a campanha *Mês da segurança da Informação Digital* cujo objetivo é a conscientização sobre a política de segurança da informação digital implementada na Marinha.

Essa campanha tinha como objetivo alertar todos os usuários sobre a importância de se proteger as informações digitais que são trafegadas na rede de comunicações integradas da Marinha.

Em junho de 2019, a DCTIM promoveu um curso de defesa cibernética. Teve como público alvo, militares que trabalham na área da Tecnologia da Informação. Essa formação contemplou assuntos como análise de vulnerabilidades e monitoramento de links e serviços, e tem como objetivo, a capacitação do pessoal em atividades como gestão de riscos cibernéticos e prevenção a incidente na rede de computadores.

2. ANÁLISE DA NBR ISO/IEC 27002

O propósito da ISO é promover normas que possam ser usadas por todos os países do mundo. É uma organização internacional que visa a padronizar as normas. O Brasil faz parte da ISO e é representado pela Associação Brasileira de Normas Técnicas (ABNT).

A série 27000 foi projetada para servir como referência na seleção de controles e na elaboração de um Sistema de Gestão da Segurança da Informação (SGSI). O conjunto destes controles aplicados corretamente, garantem a segurança da informação. (ALMEIDA, 2020)

De acordo com a NBR ISO/IEC 27002, através da implementação de controles, políticas e procedimentos é obtida a segurança da informação. Deve ser mantido um monitoramento destes controles e fazer análise de seus procedimentos criticamente para que seja garantido a segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

Figura 1 – Aplicação de um conjunto de controles

Fonte: elaborado pelo autor.

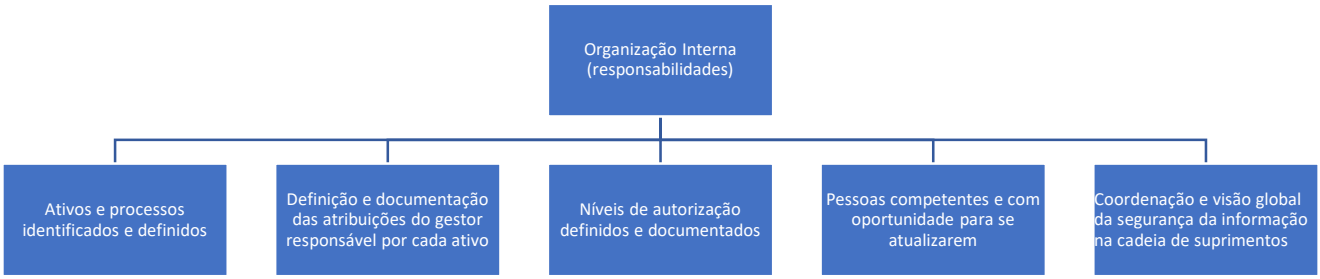
A NBR ISO/IEC 27002 possui 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles, algumas dessas seções são a que versa sobre a política de segurança da informação (seção 5), o controle de acesso (seção 9) e a segurança física e do ambiente (seção 11). A NBR ISO/IEC 27002 não é específica em suas recomendações como serão implementados os controles sugeridos para abranger vários tipos de tarefas e ser aplicada a diversas organizações diferentes.

A seleção de controles depende da organização quanto a aceitação de risco no seu tratamento, contanto que sejam sujeitos a legislações e regulamentações nacionais e internacionais. Cada seção da ISO 27002 cita um controle explicando o seu objetivo e diretrizes para apoiar a sua implementação.

Na seção 5 da NBR ISO/IEC 27002, o objetivo apresentado é o de se ter uma política de segurança da informação regulamentada por normas e padrões aprovados pela direção da organização e que essa norma seja atualizada periodicamente, o que é de crucial importância para a segurança física, pois uma norma que não é aprovada pela direção da organização não possui grande adesão por seus funcionários.

Na seção 6, é tratado a organização da segurança da informação interna e externa. Na subseção 6.1, é apresentado o objetivo de iniciar e controlar uma implementação da segurança, e, para isso, deve ser estabelecido uma estrutura dentro da organização. Este controle define que todas as responsabilidades pela segurança, que devem ser definidas, estejam de acordo com a seção 5.

Figura 2 – Diretrizes para Implementação da Subseção 6.1



Fonte: elaborado pelo autor.

A subseção 6.2 define uma política que deve ser adotada para a segurança da informação quanto aos dispositivos móveis e o trabalho remoto através do gerenciamento dos riscos no seu uso. Esse controle implica em analisar quais os riscos que podem ser gerados com este uso, onde cuidados especiais devem ser tomados para que informações do negócio não sejam comprometidas.

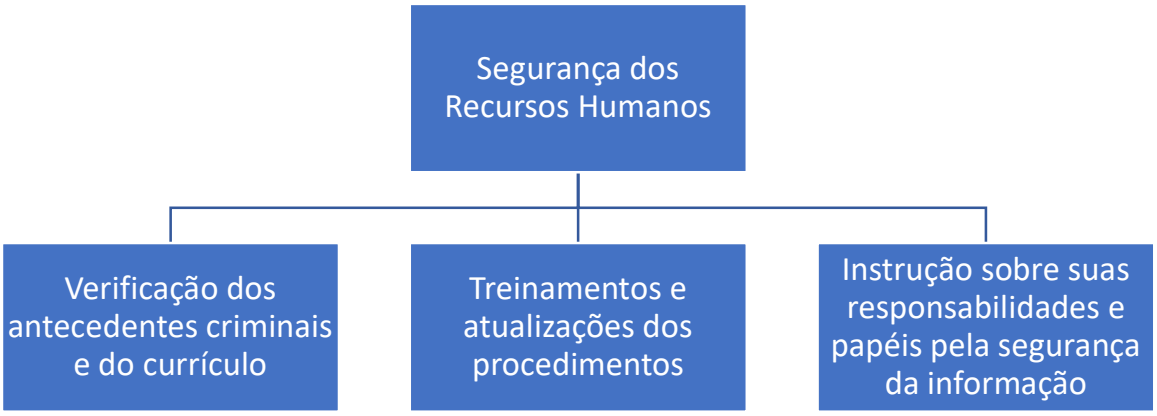
Figura 3 – Diretrizes para Implementação da Subseção 6.2

Fonte: elaborado pelo autor.

Na seção 7, é tratado a segurança em recursos humanos cuja subseção 7.1 se refere a seleção dos candidatos, quanto a verificação dos seus históricos de acordo com a ética, regulamentações e leis relevantes. Este controle é para garantir a integridade dos funcionários e verificar se estão aptos para exercerem cargos que requerem confiança e responsabilidade para manter a segurança.

A subseção 7.2 define que todos os funcionários recebam treinamentos e atualizações regulares das políticas e procedimentos organizacionais relevantes as suas funções, e que isso é responsabilidade da direção da organização.

Figura 4 – Diretrizes para Implementação da Seção 7

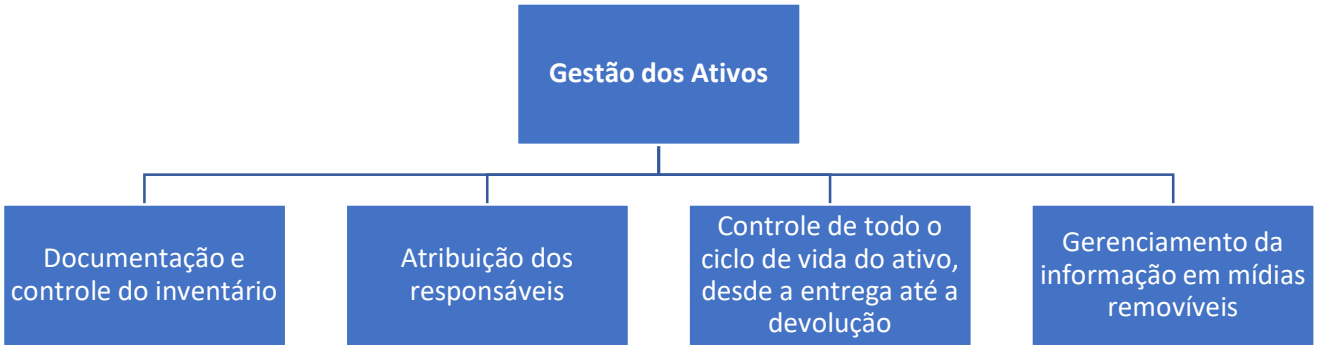


Fonte: elaborado pelo autor.

Na seção 8, é tratado a gestão dos ativos, seu objetivo é a identificação e atribuição de responsáveis para garantir a segurança destes ativos. Para isso, deverá existir um controle de inventário e que seja criado uma documentação quanto ao seu ciclo de vida.

Na subseção 8.3, há uma preocupação quanto a divulgação não autorizada da informação. Este controle define um gerenciamento de mídias removíveis. É citado algumas diretrizes, permitindo ser destruída uma informação caso ela não seja mais útil e esteja em um meio magnético reutilizável. Quanto ao seu armazenamento, deverá ser seguro em um ambiente protegido. Para informações importantes, deve ser adotado técnicas de criptografia e cópias devem ser feitas para mitigar perdas ou danos à informação.

Figura 5 – Diretrizes para Implementação da Seção 8



Fonte: elaborado pelo autor.

A Seção 9 trata sobre o controle de acesso, cujas políticas devem ser definidas e documentadas, e podem ser criados níveis de permissão para obtenção da informação de acordo com as funções dos usuários, devendo ser mantido o gerenciamento, por exemplo, sobre a entrada e saída de usuários destes níveis.

Na subseção 9.1.2, é definido o controle do acesso aos serviços da rede, apenas pessoas autorizadas poderão acessar. Devem ser especificados os procedimentos para conceder a autorização à rede e este controle deve ser monitorado para casos de alguma violação ou que este acesso não é mais de interesse à organização, para que seja revogada.

Na subseção 9.4.3, é especificado a importância de possuir um gerenciador de senhas para assegurar a qualidade delas. Esta ferramenta deverá obrigar, em intervalos regulares, a troca de senha e forçar a elaboração de uma senha de qualidade.

A seção 10 refere-se a criptografia. Para o uso correto, deverá ser elaborado uma política da criptologia para garantir a confiabilidade, autenticidade e a integridade da informação. Deve ser mantido o gerenciamento das chaves criptográficas através de uma política que abrange todo o seu ciclo de vida.

A seção 11 abrange a segurança física do ambiente cujo objetivo é prevenir o acesso físico não autorizado através da criação de perímetros de segurança que protegem áreas que processam ou que possuem informações críticas à organização.

O acesso a essas áreas protegidas deve possuir uma política onde são definidos os procedimentos na concessão de acesso e registros como entrada e saída. Esse controle também dá importância a instalações que processam informações e devem ter acesso restrito ao público.

O ambiente seguro também deve ser projetado contra desastres naturais, ataques maliciosos e acidentes além de que o trabalho em áreas seguras deve ser supervisionado. Meios de gravação nestas áreas devem ser proibidas e o conhecimento da localidade destas instalações só são reveladas em casos necessários.

Na subseção 11.1.6, é especificado que as áreas de entrega ou carregamento devem ser projetadas para que pessoas não autorizadas não tenham acesso ao resto do prédio. Os materiais entregues devem ser inspecionados para que não contenham produtos que possam prejudicar a segurança do perímetro como, por exemplo, explosivos, materiais químicos ou outros materiais perigosos.

O controle de utilidades, na subseção 11.2.2, prevê que os equipamentos sejam protegidos contra falha de energia elétrica, telecomunicações e outras interrupções por falha de uma utilidade. Estes equipamentos devem conter um sistema de alarme para avisar sobre o mau funcionamento.

A subseção 11.2.3 provê informações sobre segurança no cabeamento que transporta energia, telecomunicações ou dados quanto a interceptações, interferência ou danos. O acesso a estes painéis de conexões deve ser controlado e é necessário varreduras técnicas para verificação da integridade física.

Figura 6 – Diretrizes para Implementação da Seção 11

Fonte: elaborado pelo autor.

Na seção 12, é abordada a segurança nas operações e na garantia do processamento das informações. Os procedimentos destas operações devem ser documentados e estar disponíveis para qualquer usuário que necessite deles, visando a garantir a continuidade de um sistema em caso de erro, parada parcial ou total.

Este controle também especifica a importância de possuir ambientes separados para reduzir riscos de modificações e alterações não autorizadas. Podem ser ambientes de desenvolvimento, teste e produção, e, além disso, deve existir meios para detectar códigos maliciosos. Todos os eventos no sistema devem possuir logs para gerar evidências como por exemplo de dados, ids de usuários, data da ocorrência e o evento.

Na seção 13, é abordada a segurança das comunicações, o seu objetivo é garantir a segurança das informações na rede e nos recursos que lhe apoiam no processamento.

Um método de controlar a segurança da rede é segregando-a, ou seja, dividindo em domínios de rede, mas convém que o perímetro de cada domínio seja bem definido. Esse controle também especifica que o acesso a esses domínios deve ser gerenciado por um *gateway*. Esta segregação pode ser usada com diferentes tipos de redes físicas ou lógicas.

Na seção 14, é abordada a segurança nos processos de aquisição, desenvolvimento e manutenção de sistemas. Os requisitos de segurança do sistema são refletidos de acordo com a análise do valor da informação do negócio e o potencial impacto negativo caso falhe a segurança. Os testes de funcionalidades de segurança devem ser realizados durante o desenvolvimento.

A seção 15 aborda a segurança da informação na cadeia de suprimentos, o objetivo é manter um controle dos ativos que entram em contato com os fornecedores, que eles obedeçam às condições de segurança e que este acesso seja documentado. Deverá ser exigido a documentação dos fornecedores, definição de quais ativos eles poderão ter acesso e convém que a organização monitore e analise a entrega dos serviços executados pelos seus fornecedores.

A seção 16 trata sobre a gestão de incidentes de segurança da informação, na qual devem ser definidos responsáveis para garantir respostas rápidas na ocorrência de incidentes e estes devem ser registrados. Como por exemplo, a violação da disponibilidade e confiabilidade da informação, erros humanos e violação de acesso. Estes incidentes devem ser usados, através de uma análise, para reduzir a probabilidade de que novos incidentes ocorram futuramente.

A seção 17 especifica a gestão da continuidade da segurança da informação, caso ocorra algum incidente, para isso é necessário haver um planejamento para ter uma recuperação do desastre.

A gestão de continuidade aborda a necessidade de redundâncias dos recursos para manter o processamento das informações.

A conformidade com as obrigações legais é abordada na seção 18, onde são identificados os requisitos legislativos, contratuais e direitos de propriedade para não serem violados. Convém que os registros sejam protegidos contra roubo, perda ou destruição. Para não se perder estes registros, deve ser definido um sistema de armazenamento.

3. ANÁLISE DGMM0540

As normas da DGMM0540 foram aprovadas em agosto de 2009, com ênfase em Infraestrutura de Redes e Serviços, SIC (Segurança da Informação e Comunicação) e Desenvolvimento de SD (Sistemas Digitais).

A norma é dividida em cinco partes. A 1º parte apresenta as atribuições das estruturas da MB. A parte 2, define os serviços da RECIM (Rede de Comunicação Integrada da Marinha) e infraestrutura normatizando seus aspectos. A parte 3 visa resguardar os pilares da segurança da informação (ACID): Autenticidade, Confiabilidade, Integridade e Disponibilidade. A parte 4 aborda o ciclo de vida de um sistema digital quanto a Planejamento, Obtenção, Produção, Manutenção e Desativação. E, a parte 5 aborda normas de referentes a acessibilidade.

Sua última atualização foi aprovada em 2019 e incluiu, no capítulo 12, o tratamento que será dado aos dispositivos móveis nas OM's da MB.

A RECIM é a infraestrutura responsável por fornecer recursos e serviços de TI para todos os usuários da MB garantindo a segurança da informação, como a confiabilidade, o gerenciamento e detecção de erros.

Alguns equipamentos ou recursos são considerados críticos em relação aos riscos que são expostos e sua interrupção ou degradação pode comprometer a rede local da OM ou da RECIM.

A integridade física dos RCC (recursos computacionais críticos) será assegurada quando todos os procedimentos e dispositivos utilizados estejam de acordo com a segurança física, conforme a DGMM0540 (MARINHA DO BRASIL, 2019).

3.1 Estrutura Organizacional de TI na MB

A estrutura organizacional de TI na MB possui 3 níveis: o primeiro é composto pela DCTIM, que atua no nível estratégico; o segundo é mantido pela CTIM, que trabalha nas tarefas operacionais de toda a MB; e o terceiro é mantido pelos CLTIs, que promovem tarefas de nível operacional em um local restrito, auxiliando a CTIM quanto a coordenação das OMs através de apoio aos administradores de redes locais de sua área de jurisdição.

3.2 Atribuição dos Órgãos de TI

3.2.1 Diretoria de Comunicação e Tecnologia da Informação (DCTIM)

Como coordenador diretor da TI, tem a função de controlar e supervisionar tecnicamente, com o apoio do CTIM, toda a infraestrutura de redes da Marinha, e estabelecer normas de utilização, dentre outras funções.

3.2.2 Centro de Tecnologia da Informação (CTIM)

Como executor e coordenador da TI, sob a supervisão da DCTIM, tem a função de controlar e monitorar os recursos de TI (hardware e software), gerenciar e executar as atividades de serviços de TI dentre outras. Sem sua autorização não é permitido instalar nem atualizar nenhum software nas OM's da MB.

3.2.3 Centro Local de Tecnologia da Informação (CLTI)

O centro é um apoio a CTIM em suporte técnico de TI, otimizando os recursos humanos de tecnologia da informação e comunicação, diminuindo o tempo de atendimento à serviços prestados à Marinha.

3.2.4 Responsabilidades e Atribuições

A DCTIM é responsável pela elaboração, revisão e o gerenciamentos das normas para a SIC da MB. É de sua responsabilidade a homologação de equipamentos e programas que promovam a segurança da informação e treinamentos.

A CLTI conforme os requisitos definidos pela DCTIM, mantem o pessoal capacitado a fazer auditorias com treinamentos à OM's que estão sob sua área de jurisdição.

O responsável da OM deve manter o cumprimento das normas e procedimentos pertinentes a SIC em sua Organização Militar, assim como treinamentos. Um oficial de segurança é designado para o auxiliá-lo.

Ao oficial de segurança cabe monitorar e garantir que todo o pessoal esteja de acordo com as normas de segurança, isso se aplica também ao pessoal externo. Caso ocorra algum incidente, este oficial deverá reportar após uma análise do ocorrido.

3.3Segurança Orgânica

A segurança orgânica consiste na adoção de medidas de prevenção e a obstrução das ações ou ocorrências que comprometem a segurança dos conhecimentos de interesse da MB ou do país.

Assim, de acordo com as normas estabelecidas pelo governo Federal, as medidas de segurança orgânica voltadas à SIC estão divididas em 4 partes: segurança física, lógica, tráfego e criptológica das informações digitais.

Em relação a segurança da seleção do pessoal, são adotadas medidas para assegurar meios adequados quanto à propagação de conhecimentos sigilosos e eles estão agrupadas em três partes: no processo seletivo, garantia de aptidão para exercer a função e no cuidado no desligamento.

3.3.1 Segurança Física da Informação e Comunicações

A segurança física corresponde aos procedimentos e dispositivos utilizados assegurando a integridade física dos recursos computacionais críticos (RCC). Objetiva o comportamento adequado do pessoal da Marinha protegendo os conhecimentos sigilosos.

A segurança física possui algumas diretrizes: perímetro de segurança, segurança física dos RCC nível 1, segurança física dos dispositivos de conectividade, proteção contra interferências eletromagnéticas, proteção da alimentação elétrica dos equipamentos e realização de serviços na rede local.

O perímetro de segurança é definido como uma barreira física que separa dois ambientes, o comum e o que possui informação sigilosa.

A Segurança Física dos RCC Nível 1 é voltada para os locais onde os RCC estão instalados, por isso esses locais devem possuir uma segurança física reforçada com controle de registro de entrada e saída de pessoal, alarme e lacres numerados e uma senha forte para acessos aos equipamentos.

A Segurança Física dos Dispositivos de Conectividade como roteadores e switches possuem semelhança com a segurança do RCC nível 1, mas neste caso, possuem algumas proteções a mais como a utilização de gabinetes lacrados e com chave, inclusive para os estabilizadores, *No-Breack's*, configurar filtro de MAC *address* nos *switches* e sistema de alarme para os compartimentos que possuírem estes equipamentos e não forem guarnecidos.

A Proteção Contra Interferências Eletromagnéticas é voltada para prevenir que equipamentos de armazenamento sensíveis a campos eletromagnéticos sejam afetados provocando a perda de disponibilidade como um dos requisitos básicos da SIC.

A Proteção da Alimentação Elétrica dos Equipamentos é importante, pois sua falha impacta o requisito da disponibilidade, para evitar isso é desejável que todos os RCC sejam protegidos contra falha de alimentação.

A Realização de Serviços na Rede Local, por pessoal externo à OM, principalmente em RCC nível 1, podem afetar os requisitos de SIC de toda a MB devido a sua interligação com a RECIM. Esses serviços devem ter autorização prévia do CLTI, que poderá efetuar consulta à DCTIM.

3.3.2 Segurança Lógica da Informação e Comunicação

As vulnerabilidades lógicas são decorrentes de falta de atualizações de software e a não instalação de correções disponibilizadas pelos fabricantes. Para reforçar a segurança lógica, os administradores das redes devem ficar sempre atentos a alguma alteração nas listas de verificação da SIC que são normas disponibilizadas pela DCTIM.

3.3.3 Segurança do Tráfego da Informação e Comunicações

A segurança do tráfego compreende a prática das medidas de segurança para impedir a obtenção das informações digitais que estejam trafegando pela rede. Desta forma o uso de redes ponto a ponto (P2P) é vedado pela RECIM nas estações de trabalho já que não é feito um controle sobre o conteúdo.

3.3.4 Segurança Criptológica da Informação e Comunicações

A segurança criptológica consiste na utilização de meios para alterar a informação utilizando processos de codificação de modo a torná-lo incompreensível quando não for utilizado uma outra forma para decodificá-la.

3.4Mentalidade de Segurança

O pessoal da Marinha deve receber treinamentos de acordo com a SIC, pois o seu fator mais importante é a mentalidade de segurança. Por esse motivo, as OM's devem promover adestramentos de SIC e estabelecer um controle dos participantes para que possam ser administrados os níveis mínimos de adestramento dentro da OM.

A engenharia social abrange um conjunto de técnicas para obter ou comprometer informações, por meio delas a SIC estabelece instruções para minimizar esse tipo de ataque, como por exemplo, não oferecer informações sobre rede local da OM ou não confirmar a presença de um determinado militar ou civil a bordo.

3.5Gestão de Risco em Segurança da Informação e Comunicações

A Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC) visa priorizas meios para aumentar a eficiência da segurança da informação digital e das comunicações navais (CN).

O GRSIC é um processo contínuo e deve possuir um plano de tratamento na presença de riscos. Nesse processo é necessária uma análise dos possíveis acontecimentos e o seu impacto antes que seja tomada alguma decisão com o objetivo de reduzir o nível de risco.

3.6 Documentos de Segurança da Informação e Comunicações

Todas as ações da SIC devem estar documentadas para possibilitar o contínuo aperfeiçoamento, por isso que cada OM deverá fornecer os seus registros de adestramentos, histórico de ações de ocorrências, auditorias, ações corretivas e preventivas.

3.7 Planos de Contingência (PLCONT)

Planos de contingência são documentos cujo objetivo é garantir a continuidade operacional da rede local da OM e tais documentos devem ter grau de sigilo no mínimo de reservado.

3.8 Auditoria da Segurança da Informação e Comunicações

A auditoria da SIC tem como objetivo verificar o cumprimento fiel das normas da SIC assim como propagar a mentalidade de SIC e corrigir algumas medidas tomadas caso necessite.

3.9 Segurança aplicada aos dispositivos móveis e telefones celulares

A segurança aplicada aos dispositivos móveis e celulares visa conscientizar o uso dentro da corporação. Com base na Norma Complementar nº 12/IN01/DSIC/GSIPR e na conclusão da Nota Técnica nº 10/2014 da DCTIM, a utilização destes dispositivos deva ser controlada em todas as organizações militares (OM) visando a manutenção da SIC.

A presença destes dispositivos traz vulnerabilidades como por exemplo, em reuniões ou em conversas interpessoais existe o risco da captura e propagação da informação sem autorização. Com o avanço dos meios tecnológicos, tais arquivos podem ser enviados imediatamente para outros locais.

Portanto, a utilização de tais dispositivos a bordo das OM's da Marinha é vedada, salvo por algumas exceções que cabe o responsável da OM avaliar qual a circunstância e deverá ser registrada por meio de uma ordem interna. Algumas OM's que lidam com o público, sendo tais dispositivos não atrapalhem o cumprimento da missão, neste caso não é proibido o uso.

3.10 Ciclo de Vida de um Sistema Digital

Na Marinha o ciclo de vida de um sistema digital (SD) contempla cinco fases: o planejamento (PLA), a obtenção (OBT), a produção (PRO), a manutenção (MAN) e a desativação (RET).

A Fase de Planejamento compreende a elaboração dos processos e regras de negócios da OM, esta fase consiste no planejamento do desenvolvimento do SD.

A Fase de Obtenção inicia-se com a elaboração das especificações e requisitos de arquitetura e infraestrutura. Nesta fase é definido se será utilizado um SD vindo de uma demanda ou na aquisição de um SD no mercado de softwares.

Após a fase de obtenção a de produção inicia-se após a sua homologação pela DCTIM, é caracterizado pela implantação e a disponibilização do SD para os usuários.

A manutenção de um SD poderá ocorrer a qualquer tempo de seu ciclo de vida como o objetivo de manter o SD operando de forma correta e segura.

A Desativação de um SD pode ocorrer nos seguintes casos: quando já não atende as perspectivas dos usuários, quando surge outro para substituí-lo, ou quando a relação do custo versus benefício esteja desfavorável.

4. METODOLOGIA

Os principais métodos utilizados estão descritos neste capítulo, assim como as suas limitações.

O método científico pode ser entendido como a forma com que serão sistematicamente analisados os conhecimentos reunidos de forma clara para se alcançar um objetivo (MARCONI; LAKATOS, 2011). Com isso em mente, este trabalho irá se basear na NBR ISO/IEC 27002 para verificar se a DGMM0540 atende a todos os requisitos internacionais de segurança da informação, focando no aspecto de segurança física.

A cada controle voltado para segurança física da informação, presente na NBR ISO/IEC27002, será apontado uma recomendação da DGMM0540. Esses documentos que são de cunho ostensivo, ou seja, livres para a consulta do público em geral, mas com uma visão interna da MB.

A pesquisa bibliográfica serviu como uma base para alcançar os objetivos deste trabalho, reunindo as informações obtidas nos documentos analisados para tratar o problema a ser abordado.

4.1Classificação da Pesquisa

A classificação da pesquisa pode ser quantitativa e qualitativa, a grande diferença delas é que a quantitativa está inclinada para a análise de dados numéricos, enquanto a pesquisa qualitativa tem uma base subjetiva usando narrativas escritas.

O trabalho utilizará a classificação quanto aos dados de forma qualitativa, visto que não serão tratados dados numéricos e, sim, comparada a norma técnicas NBR ISO/IEC 27002 com a da MB, DGMM0540.

4.1.1 Quanto aos fins

A classificação quanto aos fins pode ser exploratória, descritiva, explicativa, metodológica, aplicada e intervencionista, e a metodologia classificada como metodológica é definida por Vergara (2005) como:

> Pesquisa metodológica é o estudo que se refere a instrumentos de captação ou de manipulação da realidade. Está, portanto, associada a caminhos, formas, maneiras, procedimentos para atingir determinado fim construir um instrumento para avaliar o grau de descentralização de uma organização é um exemplo de pesquisa metodológica. (VERGARA, 2005)

Desta forma será utilizada a pesquisa metodológica no trabalho para avaliar a segurança física da informação analisado os fatores que contribuem para este fim em uma norma interna da MB, a DGMM0540, através do uso de uma outra norma internacional, NBR ISSO/IEC 27002.

4.1.2 Quanto aos meios

Quanto aos meios, a metodologia que será usada no trabalho será a bibliográfica, isto é, será um estudo sobre os documentos e estudos de acesso ao público em geral. (VERGARA, 2005). Os documentos utilizados são os que versam sobre segurança da informação e esse estudo fará um comparativo entre a DGMM0540 e a NBR ISO/IEC 27002 com foco na segurança física.

4.2Limitações do Método

A limitação do método escolhido está no fato de serem analisados apenas dois documentos, a DGMM0540 e a NBR ISO/IEC 27002, sendo que existem diversos outros documentos, tais como as notas técnicas e as normas complementares, no caso da MB, e as várias outras normas da série 27000, que versa sobre o sistema de gestão da segurança da informação nas organizações.

5. COMPARAÇÃO ENTRE A NBR ISO/IEC 27002 E A DGMM0540

A seguir, cada seção da NBR ISO/IEC 27002 é comparada com a DGMM0540 e verificado quais objetivos estão implementados e de quais formas.

Na ISO27002, seção 5, subseção 5.1 – (Orientação da direção para segurança da informação), o objetivo apresentado é o de se ter uma norma aprovada pela direção da organização e que ela seja atualizada periodicamente, o que na MB é feito através da DGMM0540 que foi aprovada pela DGMM, Diretoria Geral de Material da Marinha e é atualizada periodicamente, tendo tido uma revisão em 2017 e em 2019. A vantagem de ter uma norma sendo atualizada constantemente é manter os métodos de segurança correspondentes com a atualidade, além de possuir diversas normas complementares e notas técnicas.

A seção 6, subseção 6.1 – (Organização Interna) da ISO27002, informa que deve ser definida uma estrutura para implementação das políticas da segurança da informação, onde cada componente deve ter suas responsabilidades e atribuições bem definidas. Por sua vez, a MB possui uma estrutura definida de acordo com o capítulo 8 (Responsabilidades e Atribuições) da DGMM0540 que detalha os integrantes da estrutura organizacional da MB com relação a SIC.

A subseção 6.2 – (Dispositivos móveis e trabalho remoto) da ISO27002 especifica que há riscos na utilização de dispositivos móveis portanto estes devem receber um controle. Na MB, o uso deles é permitido, mediante autorização do responsável da OM de acordo com o capítulo 12 (Segurança Aplicada aos Dispositivos Móveis e Telefones Celulares) e a DCTIMARINST 30-04D.

A seção 7 – (Segurança em Recursos Humanos) da ISO27002 descreve a importância da correta seleção dos funcionários e cita os procedimentos que devem ser adotados. Na DGMM0540, no capítulo 9 (Segurança Física da Informação e Comunicações), é abordado que uma das medidas da segurança orgânica é o processo seletivo de seu pessoal. Retrata também a importância de verificar se o candidato é apto para o serviço e o cuidado que se deve ter no seu desligamento do serviço.

Para a manutenção da segurança, a subseção 7.2 – (Durante a Contratação) da ISO27002 determina que é de responsabilidade da Organização disponibilizar as normas e procedimentos atualizados para que os seus funcionários atinjam um nível de conscientização pela segurança. Na DGMM0540, no capítulo 8 (Responsabilidades e Atribuições) informa que essa responsabilidade é da DCTIM.

Quanto ao treinamento, ainda na subseção 7.2 da ISO27002, é dito a importância de oferecer treinamentos aos funcionários e a sua conscientização. Na DGMM0540, no capítulo 8.4 (dos centros locais de tecnologia da informação - CLTI), a DCTIM elabora programas para treinamentos, mas cabe à CLTI aplicá-las encaminhando a ordem para as OM's de sua jurisdição. Cabe ao responsável da OM, incluir este treinamento de segurança ao programa de adestramentos de sua OM onde o seu oficial responsável pela segurança, possa garantir o cumprimento.

Quanto a Gestão de Ativos, seção 8 da ISO27002, o objetivo é a identificação, documentação e atribuição de responsáveis para garantir a segurança destes ativos. Na DGMM0540, no capítulo 1.2.3 (Elemento Organizacional de Apoio – CLTI), a CLTI tem como uma de suas funções, manter um inventário atualizado dos recursos de TI da OM da sua área de jurisdição.

A subseção 8.3 (Tratamento de Mídias), aborda a preocupação sobre vazamento de informações sigilosas e a importância de existir um controle das mídias removíveis e quando devem ser adotadas técnicas como criptografia para assegurar confidencialidade. No capítulo 9 (Segurança da Informação e Comunicações) a DGMM0540 enfatiza que estes dispositivos oferecem vulnerabilidades e ameaças, por isso devem ser evitados, apresentando alternativas para o compartilhamento e armazenamento de informações.

Na seção 9 da ISO27002 é abordado o controle de acesso, onde são definidas as políticas de acesso que devem ser elaboradas e documentadas. Em Perímetro de segurança no capítulo 9.4.1 é tratado a importância deste controle em um ambiente que possa conter informações sigilosas e como suas normas devem ser periodicamente revisadas.

Na subseção 9.1.2 (Acesso aos serviços de rede) são especificados os procedimentos para conceder o acesso aos serviços de rede. No capítulo 4 da DGMM0540 é informado que os acessos à serviços disponibilizados na Intranet são concedidos em função da necessidade do usuário no exercício de suas atividades, esse acesso é controlado por autenticação.

Na subseção 9.4.3 é especificado a importância de possuir um gerenciador de senhas para garantir a criação de credenciais de acesso fortes. Na DGMM0540, no capítulo 8.9, são definidos procedimentos que o usuário deverá seguir durante a criação de senhas.

Na seção 10 (Criptografia) da ISO27002 é retratado a importância de manter as informações sigilosas criptografadas e aborda o gerenciamento das chaves criptográficas. No capítulo 4.3.4 da DGMM0540 é informado que toda informação sigilosa deve ser protegida por algum mecanismo de criptografia.

Na seção 11 da ISO27002, é definido o controle de áreas seguras através de perímetros de segurança implementados por barreiras físicas que impedem o acesso indevido. Na DGMM0540, no capítulo 7.2.5, é especificada uma rede segregada fisicamente onde nenhuma informação poderá sair do perímetro.

A subseção 11.1.6, aborda a importância de possuir áreas de acesso aos fornecedores para evitar entradas não autorizadas. No capítulo 2.1.4 da DGMM0540 é informado que parceiros como fornecedores e órgãos privados, poderão trabalhar dentro ou fora das áreas da MB e por isso deve existir um bom gerenciamento de acesso e no capítulo 16.6, é especificado a seleção dos seus fornecedores.

Na seção 11.2.2 (Utilidades) aborda a importância de proteger equipamentos que exercem funções relacionadas à segurança da informação contra interrupções como falha elétrica. O capítulo 9.4.5 (Proteção da Alimentação Elétrica dos Equipamentos) da DGMM0540, informa que é desejável possuir fontes alternativas de energia nestes equipamentos, pois a sua falha pode impactar a disponibilidade.

Na seção 13 (segurança das comunicações) da ISO27002, o objetivo é garantir a segurança da informação na rede e nos serviços que lhe apoiam. No capítulo 9.6 da DGMM0540 (Segurança do Tráfego da Informação e Comunicações), é onde se encontram as medidas que visam impedir a obtenção não autorizada das informações que trafegam na rede.

Na seção 14 (Aquisição, desenvolvimento e manutenção de sistemas) da ISO27002, é abordada a importância na segurança em todos os ciclos de vida do sistema. Este tópico é tratado na DGMM0540 no capítulo 14 que especifica o conjunto de processos, fundamentos e requisitos para a aquisição de um sistema digital (SD).

Na seção 15 (Relacionamento na cadeia de suprimento) da ISO27002, o objetivo é controlar o acesso a ativos que entram em contato com os fornecedores. No capítulo 9.4.1 (Perímetro de Segurança) da DGMM0540, é especificado que a entrada de visitantes nos perímetros de segurança deve ser através de identificação e registro com data, hora e a razão da visita. Este acesso deverá ser limitado apenas para o propósito da visita.

O objetivo da seção 16 (Gestão de incidentes de segurança da informação) da ISO27002 é atribuir responsáveis pela segurança da informação para garantir respostas rápidas. No capítulo 2.3.2 (Suporte a serviços) da DGMM0540, a Central de Suporte aos Serviços e Ativos da RECIM (CSRECIM) é responsável por gerenciar os incidentes designando o grau de prioridade para que seja resolvido o problema e com isso, mantendo a disponibilidade.

A seção 17 (Aspectos da segurança da informação na gestão da continuidade do negócio) da ISO27002, visa a continuidade do negócio após a ocorrência de algum incidente

através de planejamento. No capítulo 2.3.2 da DGMM0540, são definidas métricas para a resolução do problema e no capítulo 10.4 (planos de contingência - PLCONT) são apresentados os pontos que devem estar presentes na elaboração do plano de contingência, que será acionado em caso de incidentes, para salvaguardar a continuidade operacional da rede.

Quadro 1 – Comparação entre índices das normas

NBR ISO/IEC 27002	DGMM0540	Descrição
Subseções 5.1 e 5.2	Introdução	Criação e atualização da norma
Subseção 6.1	Capítulo 8	Responsabilidades e atribuições
Subseção 6.2	Capítulo 12	Dispositivos móveis e trabalho remoto
Seção 7	Tópico 9.4	Segurança Física da Informação e Comunicações
Subseção 7.2	Capítulo 8	Durante a Contratação
Subseção 7.2	Tópico 8.4	Dos centros locais de tecnologia da informação
Seção 8	Tópico 1.2.3	Elemento Organizacional de Apoio – CLTI
Subseção 8.3	Capítulo 9	Segurança da Informação e Comunicações
Seção 9	Tópico 9.4.1	Controle de Acesso
Subseção 9.1.2	Capítulo 4	Serviços no Intranet
Subseção 9.4.3	Tópico 8.9	Usuário
Seção 10	Tópico 4.3.4	Divulgação da informação
Seção 11	Tópico 7.2.5	Segregação da rede
Subseção 11.1.6	Tópicos 2.1.4, 16.6	Gestão dos fornecedores
Subseção 11.2.2	Tópico 9.4.5	Proteção da Alimentação Elétrica dos Equipamentos
Seção 13	Tópico 9.6	Segurança do Tráfego da Informação e Comunicações
Subseção 14.2.6	Capítulo 14	Ambiente Seguro para o Desenvolvimento
Seção 15	Tópico 9.4.1	Perímetro de Segurança
Seção 16	Tópico 2.3.2	Suporte a serviços
Seção 17	Tópicos 2.3.2, 10.4	Gestão da continuidade do negócio

Fonte: elaborado pelo autor.

6. CONCLUSÃO

Através da análise comparativa da NBR ISO/IEC 27002 e a DGMM0540, podemos observar que a DGMM0540 atende a todos os controles apresentados na NBR ISO/IEC 27002, e, além disso, possui muitas outras formas de garantir os requisitos mínimos de segurança da informação que são necessários para que os objetivos da MB sejam atendidos.

Tal resultado já era esperado pois uma norma internacional de padrões de segurança da informação deve ser a mais genérica possível para que possa ser aplicada na maioria das organizações do mundo, enquanto uma norma especifica de uma organização deve ter também algumas particularidades da própria organização.

A norma NBR ISO/IEC 27002 é um guia para o desenvolvimento de diretrizes para uma organização fornecendo orientações, ou seja, nem tudo que é informado deverá ser necessariamente aplicado. Apesar de serem recomendações básicas, algumas organizações mais simples podem optar por não adotar todos os controles apresentados pois eles podem inviabilizar seus objetivos ou missão.

Cada instituição deverá se basear nesta norma internacional NBR ISO/IEC 27002, para a construção dos seus próprios procedimentos de segurança de forma que os objetivos da organização sejam cumpridos com um mínimo de interferência dos controles de segurança. Caso algum controle seja inviável de ser aplicado, o mesmo não deverá ser aplicado, ou seja, a segurança não deve atrapalhar os objetivos da empresa e sim auxiliá-la.

6.1 Considerações Finais

Apesar deste trabalho utilizar a última revisão da DGMM0540, que não alterou o capítulo sobre a segurança física, ela acrescentou um capítulo sobre dispositivos moveis na MB na sua última versão. Esse capítulo trata do controle de acesso destes dispositivos nas organizações militares (OM's) da MB e está associado a segurança física da informação e comunicação.

Neste novo capítulo é explicado que em OM's de ensino e de saúde, visitantes ainda podem portar dispositivos móveis, enquanto nas outras OM's de cunho mais operativo, não podem, devendo estas possuírem uma norma interna que irá implementar os controles de acesso desses dispositivos.

6.2 Sugestões para Futuros Trabalhos

Neste trabalho foram analisados os aspectos físicos da segurança da informação, sendo a parte lógica, como criptografia, também muito importante e necessitando então de uma comparação com as normas internacionais mais atualizadas.

A busca dos documentos usados na análise da SIC se limitou às informações que não são sigilosas, o que pode trazer algumas lacunas no estudo. Foram tratadas as informações gerais sobre a segurança para abranger o maior número de mecanismos de segurança disponíveis na MB, por isso, seria uma boa sugestão para trabalhos futuros a inclusão de informações sigilosas no estudo.

A implementação de meios para auxiliar a segurança física no acesso a áreas críticas é outro importante aspecto que não foi abordado neste trabalho. Essa medida é um complemento a segurança existente e deve ser utilizado a fim de proporcionar um acréscimo na proteção, como é o caso da tecnologia empregada nos sistemas de biométrica por via da íris, alarmes de presença em locais de pouco acesso, utilização de crachás inteligentes, dentre outros que não são citados na DGMM0540.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, **NBR ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.** Rio de Janeiro, p. 112. 2013.

ALMEIDA, M. do L. O. **Interpretação da norma NBR ISO/IEC 27001:2006.** Disponível em: https://docplayer.com.br/3276347-Interpretacao-da-norma-nbr-iso-iec-27001-2006.html. Acesso em: 22 de fev. 2020.

MARINHA DO BRASIL. **Site da Marinha do Brasil**. Brasília: Ministério da Defesa, 2020. Disponível em: https://www.marinha.mil.br/noticias/diretoria-de-comunicacoes-e-tecnologia-da-informacao-da-marinha-promove-curso-avancado-de Acesso em: 22 fev. 2020.

MARINHA DO BRASIL. **DGMM-0540: Normas de Tecnologia da Informação da Marinha**. 3. rev. Rio de Janeiro: Diretoria-Geral do Material da Marinha, 2019.

MARCONI, M. de A. LAKATOS, E. M., **FUNDAMENTOS DE METODOLOGIA CIENTÍFICA**. 5ª ed. São Paulo: Atlas, 2011

OSTEC. **ISO 27002: Boas práticas para gestão de segurança da informação**. Blog Ostec segurança digital de resultados, 2017. Disponível em: https://ostec.blog/padronizacao-seguranca/iso-27002-boas-praticas-gsi Acesso em: 22 fev. 2020.

SOUZA, T. A.; LAUTERT, R. M. **A Norma ABNT NBR ISO/IEC 27001:2006.** 106f. Trabalho de Conclusão de Curso – (Especialista em Redes de Computadores) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2006.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011.

WESTCON. **QUAL A DIFERENÇA ENTRE SEGURANÇA FÍSICA E SEGURANÇA LÓGICA?** Blog Brasil Westcon, 2017. Disponível em: https://blogbrasil.westcon.com/qual-a-diferenca-entre-seguranca-fisica-e-seguranca-logica Acesso em: 22 fev. 2020.

OLIVEIRA, F. B. **TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO processos, métodos e aplicações.** Rio de Janeiro: Fundação Getúlio Vargas, 2009.