INSTITUTO DE EDUCAÇÃO SUPERIOR DA PARAIBA
CURSO DE SISTEMAS DE INFORMAÇÃO
JEFFERSON RIBEIRO DA SILVA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:
Proposta de modelo de política de segurança de informações digitais nas organizações militares

Cabedelo
2018

JEFFERSON RIBEIRO DA SILVA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:
Proposta de modelo de política de segurança de informações digitais nas organizações militares

Monografia apresentada ao Curso de Sistemas de Informação da do Instituto de Educação Superior da Paraíba – Faculdades IESP. Como requisito básico para obtenção do título de Bacharel em Sistemas de Informação.

Prof. Orientador: Me. Hercílio Medeiros

Cabedelo/PB

2018

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca Padre Joaquim Colaço Dourado

S586p Silva, Jefferson Ribeiro da

Política de segurança da informação: proposta de modelo de política de segurança de informação digitais nas organizações militares / Jefferson Ribeiro da Silva. – Cabedelo, PB: [s.n], 2018.
50p.

Orientador: Prof. Me. Hercílio de Medeiros Sousa. Monografia (Graduação em Sistemas de Informação) – Instituto de Educação Superior da Paraíba - IESP.

1. Segurança da informação. 2. Sistema de informação. 3. Informação. 4. Ciência da informação. I. Título.

CDU 004.056

AGRADECIMENTOS

A Deus, minha força maior, que me dá ânimo força e coragem para vencer.

Aos professores, nos quais reconheço um esforço gigante com muita paciência e sabedoria. Foram eles que me deram recursos e ferramentas para evoluir um pouco mais todos os dias.

Agradeço em especial ao meu orientador Prof. Me. Hercílio de Medeiros Sousa, pelo suporte, palavras pertinentes e incentivos para que eu caminhasse sem esmorecer.

Com carinho e respeito, agradecer a Profa. Jeane Cavalcanti, que com paciência e muito carinho, trouxe críticas assertivas que ampliaram meu universo acadêmico.

É claro que não posso esquecer da minha família e amigos, porque foram eles que me incentivaram e inspiraram através de gestos e palavras a superar todas as dificuldades.

Um agradecimento especial para a minha Mãe, por todo amorincondicional, incentivo emoldurado na esperança de dias melhores e apoio traduzido em fé.

A todas as pessoas que de uma alguma forma me ajudaram a acreditar em mim eu quero deixar um agradecimento eterno, porque sem elas não teria sido possível.

Agradeço em especial a um grande amigo SuboficialÊnio, por todo apoio e incentivo e direcionamento profissional, necessários para minha caminhada até aqui.

A injustiça num lugar qualquer
é uma ameaça à justiça em todo o lugar.

Martin Luther King Jr.

RESUMO

Este trabalho tem por objetivo dialogar com os termos segurança, informação e sistemas de se informação, a partir do entendimento teórico dos autores da área de Sistemas da Informação - SI, em uma perspectiva multidisciplinar. Trata-se, portanto, de uma monografia, que para além de se dispor a discutir as terminologias pertinentes ao objeto, vem acentuar a necessidade de se discutir um efetivo modelo para a política de segurança de informações digitais nas organizações militares, uma vez que nos dias atuais, é um tema pertinente e necessário. A proposta desenhada neste trabalho não é uma solução de inviolabilidade, mas de cuidado a ser apontado na fragilidade dos sistemas de informação, que muitas vezes pode fazer surgir situações menos próprias, comprometendo as organizações. É uma pesquisa bibliográfica de abordagem qualitativa, por fornecer uma descrição complexa e uma interpretação do problema, somando contribuições em forma e discussão para outros trabalhos a serem desenvolvidos. Está concebido em três partes. Inicialmente, as duas partes iniciais apresentamo corpo teórico-metodológico da pesquisa e os objetivos propostos neste estudo, em seguida, vamos discutir os conceitos teóricos de Sistema de Informação e a Segurança no Sistema de Informação. Por último, vale reafirmar a necessidade de uma melhor gestão, de modo a garantir a segurança das informações no espaço digital e finalizando, apresentar considerações acerca da preocupação deum modelo adequado de política de segurança, voltado para a informações digitais nas organizações militares.

PALAVRAS-CHAVE: Informação. Sistemas de informação. Segurança da informação. Segurança informática.

ABSTRACT

This work aims to dialogue with the terms security, information and information systems, based on the theoretical understanding of the authors of the area of Information Systems - SI, in a multidisciplinary perspective. It is, therefore, a monograph that, in addition to discussing the terminologies pertinent to the subject, stresses the need to discuss an effective model for digital information security policy in military organizations, since is a relevant and necessary topic. The proposal drawn in this work is not a solution of inviolability, but of care to be pointed out in the fragility of information systems, which can often give rise to situations less proper, compromising organizations. It is a bibliographical research of qualitative approach, to provide a complex description and an interpretation of the problem, adding contributions in form and discussion to other works to be developed. It is designed in three parts. Initially, the two initial parts present the theoretical-methodological body of the research and the objectives proposed in this study, then we will discuss the theoretical concepts of System Information and Security in the Information System. Lastly, it is important to reaffirm the need for better management in order to guarantee the security of information in the digital space and, finally, to present considerations about an appropriate model of security policy, aimed at digital information in military organizations.

KEYWORDS: Information. Information systems. Information security. Computer security.

LISTA DE SIGLAS E ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

CITEx- Centro Integrado de Telemática do Exército

EB - Exército Brasileiro

IEC - InternationalElectrotechnicalCommission

ISA - International Federation of the NationalStandardizingAssociations

ISO - InternationalOrganization for Standardization

ISO - Organização Internacional de Padronização

ISMS - Information Security Management System

MD – Ministério da Defesa

NBR – Norma Brasileira

NORTI - Controle da Utilização dos Meios de Tecnologia da Informação no Exército

OM – Organizações

SI – Sistemas de Informação/Segurança de Informação

SIBCs - Sistemas de Informação Baseados em Computador

SIC - Segurança da Informação e das Comunicações

SISMC - Sistema Militar de Comando e Controle

TI – Tecnologia da Informação

TICs - Tecnologias de informação e comunicação

UNSCC - United Nations Standards CoordinatingCommittee

LISTA DE QUADROS E ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Um conceito muito importante para essas duas primeiras décadas do século XXI é o da segurança. Seja em qual âmbito for. Normalmente tentamos generalizar, segurança pode ser um vocábulo amplo, polissêmico e multiperspectivado, o que origina uma certa pluralidade.

Outro conceito muito caro é o da informação. Informação pode ser, grosso modo, algo que informa, que ajuda a elucidar. Mas também é diz respeito a uma gama muito maior de composições, podendo ser algo composto e construído.

Fato é que as sociedades atuais, estão pautadas na informação, tornando-se um fator importante em nosso dia-a-dia, uma vez que a todo instante estamos cercados por dados e informações diversas, que, a depender do bom uso, podemos enriquecer os nossos conhecimentos, sobretudo pelos motores de busca presentes no universo *online*, no qual buscamos subsídios, mas também interagimos, fornecendodados, que se por um lado são auxiliadores, por outro, constituem-se em armadilhas do mundo virtual.

Partindo dessas premissas, O´Brien (2004 p.6), vai afirmar que “[...] sistemas de informação é um conjuntoorganizado de pessoas, *hardware, software*, rede de comunicação e recursos dedados que coleta, transforma e dissemina informações em uma organização”. Portanto, nesta monografia, lançaremos mãos dos teóricos que embasam o conceito de Sistema de Informação, para discutir uma proposta de modelo, voltado para a política de segurança de informações digitais nas organizações militares, uma vez que nos dias atuais, é um tema pertinente e necessário. O que por si só, se justifica.Mais ainda, justifica-se não como uma solução de inviolabilidade, mas de cuidado a ser apontado na fragilidade dos sistemas de informação, que muitas vezes pode fazer surgir situações menos próprias, comprometendo as organizações.

Isto posto, é importante dizer que, pautado na literatura acadêmica, se procurou mostrar a necessidade do sigilo e da fidelidade dos operadores e dos sistemas por eles utilizados, garantindo uma gestão eficiente e consciente do seu papel.Para dialogar acerca da temática plural que é o sistema de informações e segurança em uma sociedade pautada na velocidade das tecnologias que compõem

a comunicação e, consequentemente, as informações. Assim,foram utilizadoso entendimentoteórico daquelesque procuram definir a informação. Para tal, foram essenciais os estudos deFalsarella*et al*(2003); Turban*et al* (2007); Cassarro(2010); Laudon eLaudon, (2010); Rezende e Abreu (2013); O'brieneMarakas, (2013), dentre outros. Para apontar a disposição das tecnologias inseridas no contexto das sociedades atuais, são consideráveis as contribuições de Burke (2003), Carr (2011) e Bauman (2012), além de muitos outros que à sua maneira concorreram para a construção de um texto acadêmico, centrado em uma proposta de trabalho, cuja contribuição maior, não será apontar as falhas, mas dinamizar o universo do sistema de segurança nos meios digitais.

Em busca de cumprir com os objetivos propostos a opção de pesquisa aqui que melhor corresponde é a investigação bibliográfica de abordagem qualitativa, porquedentre outras pretensões, tal formato abre-se para “[...].a reflexão do pesquisador, uma descrição complexa e uma interpretação do problema e a sua contribuição para a literatura ou um chamado à mudança” (CRESWELL, 2014, p. 50). Há de se observar a pesquisa qualitativa pode estudar significados, representar opiniões e perspectivas, ser mais abrangente e contextualizada, revelar conceitos existentes ou emergentes e usa múltiplas fontes (YIN, 2010).

Quanto a investigação bibliográfica, que por acontecer a partir da investigação dos registros disponíveis, decorrentes de pesquisas anteriores, nos quais os textos tornam-se fontes dos temas abordados e caberá ao pesquisador suscitar as suas respostas, baseando-se no arcabouço teórico constante nas suas fontes (SEVERINO, 2007). Portanto, feita a partir do levantamento das referências teóricas, sejam por meios por meios escritos e eletrônicos: artigos, livros, e-books, teses e dissertações, dentre outras fontes que servirão para fomentar tanto o arcabouço teórico, quanto a construção da perspectiva que quer evidenciar (GIL, 2002; SEVERINO, 2007).

Assim, diante do exposto, este trabalho foi concebido em duas partes. Inicialmente, apresentando os objetivos propostos neste estudo, sendo geral e específicos, em seguida, vamos discutir os conceitos teóricos de Sistema de Informação e Segurança no Sistema de Informação.Em segundo momento, vale reafirma a necessidade de uma melhor gestão, de modo a garantir a segurança das

informações no espaço digital e por fim, apresentar um modelo adequado de política de segurança, voltado para a informações digitais nas organizações militares.

1.1 OBJETIVO GERAL

Esclarecer a vulnerabilidade na segurança das informações contidas segundo a política de segurança da informação, apontando para a necessidade de uma gestão de informação baseada nos princípios daconfidencialidade, integridade e disponibilidade.

1.2 OBJETIVOS ESPECÍFICOS

- Apresentar de forma mais ampliada o conceito de informação;
- Reafirmar a necessidade de uma melhor gestão de segurança das informações digitais;
- Apontara norma ISO 270001 como a que corresponde em qualidade e excelência para o uso em um modelo de política de segurança de informações digitais nas organizações militares.

2 A SEGURANÇA NOS SISTEMAS DE INFORMAÇÃO

Ao abordar a segurança associando-a à tecnologia da informação, pretendemos seguir um caminho na qual estejam lado a lado, avaliando os possíveis riscos e sugerindo soluções para efetivas melhoras nessa área. Acerca dessa atenção para com a segurança da informação, pode ser dito, a sua validade, sobretudo, porque:

> Com o crescente aumento das tecnologias de informação e com a rápida disseminação dela, cresceram também os crimes relacionados à mesma, surgindo então, a necessidade de se manterem as informações empresariais e pessoais livres de riscos e perigos que possam danificá-la, para que haja uma informação confiável (OLIVEIRA; MOURA; ARAÚJO, 2012, p. 3).

Trazendo a questão acima disposta, para a dinâmica empresarial, na qual as novas tecnologias quebraram as barreiras geográficas e as corporações se tornaram transnacionalizadas, pode ser dito que a inserção da tecnologia, seus usos, e, dentro desse parâmetro a *internet* responde pela comunicação, agilidade, facilidade e rapidez, dentre outros aspectos imprescindíveis que facilitaram a forma de obtenção de informações, bem como o seu armazenamento.

Certo é que a segurança dessas informações precisa ser cuidada, o que para O´Brien (2004), essa mudança significativa nasempresas, que permitiu a expansão dos sistemas de informação e, consequentemente a necessidade de uma nova gerência dessas informações é uma tônica dos dias atuais.

Neste diapasão, toda organização, seja ela corporativa ou não, carece de gestão. A forma de gerenciar as informações, por sua vez, também necessitam serem organizadas e administradas, principalmente no que diz respeito a forma como são veiculadas. Assim, as características básicas, presentes na gestão da segurança da informação, devem possuir seus pressupostos baseados em confidencialidade, integridade e disponibilidade (OLIVEIRA; MOURA; ARAÚJO, 2012). Isto posto porque ao pensar em segurança de informações, remetemo-nos aos sistemas eletrônicos., por assim dizer:

> A Segurança da Informação se refere à proteção existente sobre asinformações de uma determinada empresa ou pessoa, isto é, aplicam-se tantoas informações corporativas quanto as pessoas. Entende-se por informaçãotodo e qualquer conteúdo ou dado que tenha valor para alguma organizaçãoou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao públicopara consulta ou aquisição (ARAUJO, 2008).

Diante do exposto, há a percepção de que o armazenamento da informação e ela própria, são questões que apresentam fragilidades, pois se em um passado não muito distante os arquivos informacionais se constituíam em espaços físicos, com a chega das tecnologias da informação, esse arquivo tornou-se amplo e praticamente impossível de quantificar. Isso porque:

> Com a chegada das tecnologias da informação e comunicação esse fator ficou bem mais complexo. Atualmente a maioria dos computadores conecta-se a internet e consequentemente a internet conecta-se a eles; além disto, sabemos que dados em formato digital são portáteis, fator este que fez com que estes ativos tornassem atrativos para ladrões. Mas isto não é tudo, pois existem inúmeras situações de insegurança que podem afetar os sistemas de informação tais como: incêndios; alagamentos; problemas elétricos; fraudes; uso inadequado dos sistemas; engenharia social, entre outros (OLIVEIRA; MOURA; ARAÚJO, 2012, p. 4).

A preocupação com as novas tecnologias e consequentemente com as novas regras do mercado mundial, traz também uma nova forma de ligar as pessoas, quer sejam por compromissos profissionais, quer sejam pessoais. O mais importante é que se saiba que os meios eletrônicos ainda carecem e muito de uma legislação que os assegurem de privacidade. Sem contar com a fragilidade dos muitos sistemas que ao colocarem os arquivos informacionais em formato digital, grosso modo, colocam toda a vida da organização, desde o seu sistema corporativo, a gestão, até mesmo a vida pessoal de cada colaborador.

Assim, facilmente expostos, é hora de pensar na “blindagem” desse sistema de informação, ou dos sistemas de informação, e tratar os dados de maneira ordenada e sistematizada, cuidando para que toda a “vida digital” da organização se mantenha íntegra e salva de problemas internos e ataques externos, uma vez que toda organização é passível de interesse de outros. O mundo da segurança é complexo e exige demandas que passam pelo valor das coisas, ou pelo valor que se

atribui as coisas. Com os sistemas de informação não é diferente. Quanto custam os projetos das empresas? Quanto custa a planta de uma casa? Portanto pensando nesse seguimento, mais adiante vamos abordar o em riscos gerais, passíveis de apropriação indevida e falhas técnicas, que igualmente os compromete. Dando seguimento a esta proposta, em seguida é colocado o entendimento do que é segurança para os sistemas de informação, que carecem de outras tantas discussões, tendo em vista que se trata de uma área de conhecimento vasta, relativamente recente e que se apresenta de modo dinâmico se reinventado todos os dias.

A segurança da informação vai se preocupar com a estrutura física que aorganização mantém, são os limites da materialidade dos seus sistemas de informação, nos quais se encontram as máquinas e os colaboradores que dimensionam os dados, transformando-os em informações preciosas para a organização. Mas a principal preocupação com a segurança, quando falamos de SI, é a preocupação com a sua intangibilidade, o que não pode ser visto, mas é palpável, no sentido de existência.

Para imprimir segurança nos SI, seja em qual organização for, é preciso antes de tudo, pensar que nenhum conceito, nenhuma ação é eficaz em sua totalidade as falhas serão sempre apontadas, mas os acertos devem prevalecer e a vigilância é inegavelmente constante (CARUSO, 1999; RAMOS et al., 2006) .

Também é importante ressaltar que investir em segurança exige um alto custo. Segundo Ramos et al. (2006), segurança é um estado onde se está livre de perigos e incertezas, mas partir para a criação de uma política de segurança é uma solução que a organização não deve perder de vista. De acordo com Caruso (1999), política de segurança é uma política elaborada,implantada e em contínuo processo de revisão, sendo válida para toda a organização.

2.1 ISO 27001 - A BALIZA DA QUALIDADE NA SEGURANÇA DOS SISTEMAS DE INFORMAÇÕES

Os caminhos percorridos para a obtenção do estado de segurança, seja percorrido em qual sentido for, vai obedecer aos parâmetros pensados para uma

ação a ser executada de acordo com o contexto do qual faz parte o sistema. Uma empresa grande precisa de mais segurança que uma pequena? Um hospital precisa que o sistema de informações guarde a vida pessoal dos seus pacientes em contexto hospitalar, assim, são os bancos, as fábricas, as lojas, as escolas, as organizações de modo geral, quer sejam privadas ou públicas, civis, religiosas e ou militares. Assim, o contexto para o qual a segurança foi pensada, também vai considerar a pertinência da segurança, sua ambiência e amplitude, além de obedecer aos padrões de qualidade.

Uma norma de qualidade é um padrão a ser seguido. Assim, o padrão ISO/IEC 27001 éum padrão consolidado, voltado para a gestão de segurança da informação e consequentemente dos sistemas de informação. O Information Security Management System – ISMS, foi publicado em outubro de 2005, pelo InternationalOrganization for Standardization e pelo InternationalElectrotechnicalCommission. Recebeu o nome de ISO/IEC 27001:2005 - Tecnologia da informação - técnicas de segurança - sistemas de gerência da segurança da informação, também apontado de forma comum como ISO 27001(MAEKAWA; CARVALHO; OLIVEIRA, 2013).

A sigla ISO, normalmente se remete ao conceito de padrão de qualidade, mas abrange uma gama muito maior do que isso. Na verdade, diz respeito às séries de normas ISO, que foram criadas pela Organização Internacional de Padronização - ISO, com o objetivo de melhorar a qualidade de produtos e serviços. A ISO, é uma das maiores organizações que desenvolve normas no mundo, e foi criada a partir dos entendimentos que uniram aInternational Federation of the NationalStandardizingAssociations - ISA e a United Nations Standards CoordinatingCommittee- UNSCC. Assim, a ISO começou a funcionar oficialmente no ano de 1947(MAEKAWA; CARVALHO; OLIVEIRA, 2013).

As normas ISO, certificam produtos e serviços em várias organizações no mundo todo. Essa normalização está baseada em um documento, que oferece um modelo padrão para a implantação do Sistema de Gestão da Qualidade. No Brasil, são compostas pela sigla NBR. Elas são criadas e gerenciadas pela Associação Brasileira de Normas Técnicas - ABNT.

A norma ISO/IEC 27001, foi elaborada para estabelecer um parâmetro, um modelo de implementação, operação, monitoramento, além de analisar criticamente,

manter e melhorar um Sistema de Gestão de Segurança da Informação – SGSI, sendo que esta deve ser uma decisão estratégica para uma organização. Sua especificação e implementação em uma organização resultam da influência das suas necessidades, além dos objetivos, que são as pertinências da segurança, bem como os processos empregados, além do tamanho e estrutura da organização, quer seja em dimensões físicas, quer sejam no mundo virtual.

A partir de 1995 foi publicado o Padrão Britânico (British Standard) BS 7799, padrão que originou a série ISO 27000. Anos depois, em 1999, o BS 7799 é alvo de uma revisão que vai gerar os padrões BS 7799-1, que atende as boas práticas para Gestão de Segurança da Informação, bem como o BS 7799-2, que é o Sistema de Gestão de Segurança da Informação e por fim, o BS 7799-3, no qual estão previstas as Orientações para Gestão de Risco.

A partir do ano 2000, o padrão BS 7799-1 passa a ser identificado como ISO 17799. De 2001 a 2004 a norma ISO 17799 sendo revisada vai resultar em uma nova versão ISO/IEC 17799:2005, publicada em junho de 2005, quando neste mesmo ano o BS 7799-2 foi adotado pela ISSO e recebeu a numeração 27000. A partir de então, tem início uma sérievoltada para a padronização de normas no âmbito da segurança da informação, lançado como norma ISO/IEC 27001. Em julho de 2007, o padrão 17799:2005 recebe nova numeração (ISO/IEC 27002:2005). No Quadro 1, adiante vê-se os padrões ligados ao SI a partir dos desdobramentos desse contexto que busca a qualidade para os sistemas de segurança da informação.

Quadro 1 - Padrões de Segurança da Informação ISO

Padrões	O que prevê
ISO 27000	Vocabulário de Gestão da Segurança da Informação (sem data de publicação).
ISO 27001	Esta norma foi publicada em Outubro de 2005 e substituiu a norma BS 7799 e revisada em 2013, para certificação de sistema de gestão de segurança da informação.
ISO 27002	Esta norma irá substituir em 2006/2007 o ISO 17799:2005 (Código de Boas Práticas).

ISO 27003	Esta norma abordará as diretrizes para Implementação de Sistemas de Gestão de Segurança da Informação, contendo recomendações para a definição e implementação de um sistema de gestão de segurança da informação. Publicada em 2006.
ISO 27004 -	Esta norma incidirá sobre as métricas e relatórios de um sistema de gestão de segurança da informação. Publicada em 2007.
ISO 27005	Esta norma será constituída por indicações para implementação, monitoramento e melhoria contínua do sistema de controles. O seu conteúdo deverá ser idêntico ao da norma BS 7799-3:2005 – "*Information Security Management Systems - Guidelines for Information Security Risk Management*", a publicar em finais de 2005. Publicada em 2008.
ISO 27006	Esta norma especifica requisitos e fornece orientações para os organismos que prestem serviços de auditoria e certificação de um sistema de gestão da segurança da informação.
ISO/IEC 27007	Diretrizes para auditoria em Sistemas de Gestão de Segurança da Informação
ISO/IEC TR 27008:	Diretrizes para auditores sobre controle de segurança da informação
ISO/IEC 27010	Gestão de segurança da informação para comunicação intersetorial e inter-organizacional
ISO/IEC 27011	Diretrizes para gestão de segurança da informação em organizações de telecomunicação com base na ISO/IEC 27002
ISO/IEC 27013	Diretrizes para a implementação integrada da ISO/IEC 27001 e ISO/IEC 20000-1

ISO/IEC 27014	Governança de segurança da informação
ISO/IEC TR 27015	Diretrizes para a gestão de segurança da informação em serviços financeiros
ISO/IEC TR 27016	Diretrizes para a gestão de segurança da informação – Empresas de economia
ISO/IEC 27007	Diretrizes para auditoria em Sistemas de Gestão de Segurança da Informação
ISO/IEC TR 27008	Diretrizes para auditores sobre controle de segurança da informação
ISO/IEC 27010	Gestão de segurança da informação para comunicação inter-setorial e inter-organizacional

Fonte:OSTEC (2016).

Longe de resolver por completo a situação da segurança na gestão das informações, mas os padrões orientam no sentido de que dentro deste formato as informações consigam se manter o mais distante possível dos riscos, ainda que novas ameaças surjam e intentem contra a vulnerabilidade. Assim, é muito importante que os componentes básicos de segurança sejam constantemente analisados e vigiados. Isto posto, vamos nos debruçar sobre a questão específica sobre a qual versa este trabalho, que é a segurança dos SI, nas organizações militares brasileiras, nas quais as informações envolvem a soberania nacional.

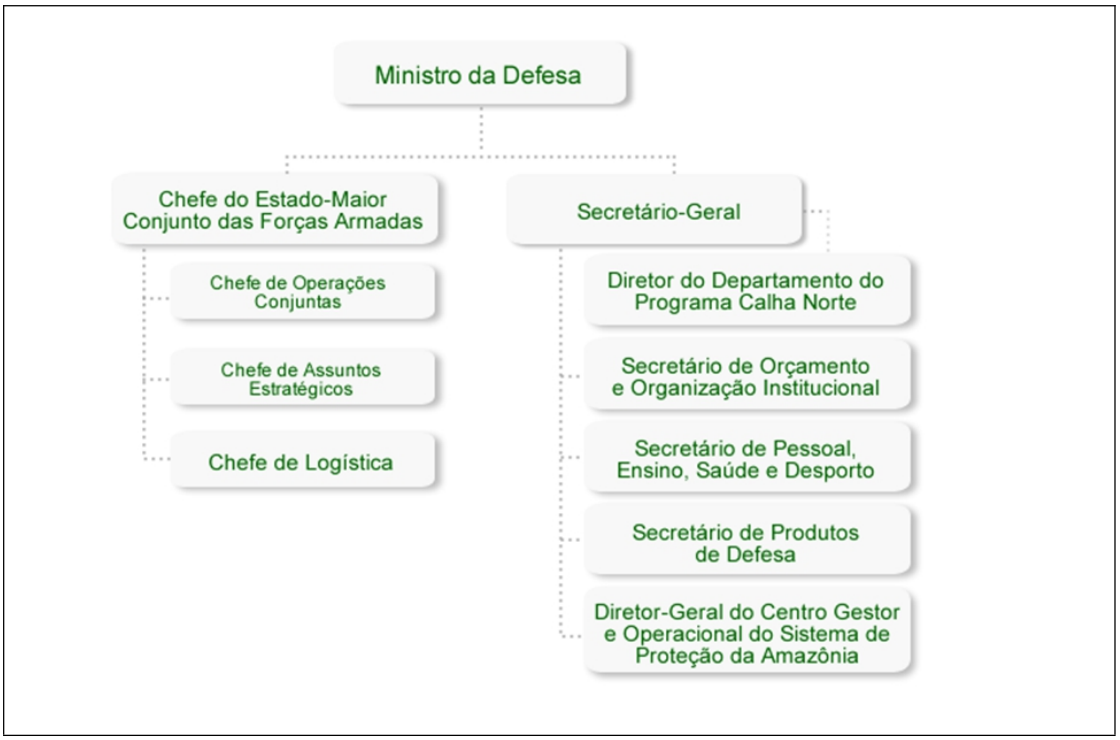
2.2 A SEGURANÇA DOS SISTEMAS DA INFORMAÇÃO DO SISTEMA MILITAR BRASILEIRO E O PADRÃO ISSO 27001

Ao nos debruçarmos sobre o tema e o envolvimento com a organização militar, é necessário dizer que a estrutura militar brasileira está sob o comando do Ministério da Defesa - MD, A página *online* do MD, assinala que se trata de um “arranjo institucional”criado em 1999, que marcou uma etapa importante no processo de integração das Forças Armadas: Marinha, Exército e Aeronáutica” (BRASIL, 2018, *online*).

Nesse modelo organizacional as três Forças que compõem a defesa do território brasileiro e a soberania nacional estão a serviço de uma única política, em um ambiente de coordenação e integração de meios e esforços. Abaixo, a Figura1 vai mostrar o organograma do MD, de modo que a compreensão do seu funcionamento seja melhor entendida, no que diz respeito à subordinação das Organizações Militares – OM, ao poder político civil.

.

Figura 1 - Organograma do Ministério da Defesa (Governo Brasileiro)



Fonte: BRASIL, 2018.

Assim, no contexto brasileiro atual, Marinha, Exército e Aeronáutica são comandos militares subordinados ao poder político civil. Além deles, outros cinco grandes segmentos estão contemplados na estrutura do Ministério da Defesa. A literatura acerca dos sistemas de segurança adotados pelo MD, no que diz respeito aos cuidados com os SI, é ainda incipiente e carece de muitos estudos na área, mas já se apresentam tímidos estudos do tema.

Sobre isso, a *Revista Rio Pesquisa* da FAPERJ, publicou em seu número VIII, no ano de 2014, um interessante artigo sobre a segurança dos sistemas de informação voltados para a questão militar, chamando a atenção para o fato de que:

> Passados apenas dois anos depois de o Brasil sediar a Copa do Mundo de futebol, o Rio receberá, em agosto de 2016, o maior evento esportivo do mundo: os Jogos Olímpicos. O assunto mobiliza setores de inteligência na área de segurança pública e de sistemas de informação do Brasil e de outros países, uma vez que milhares de cidadãos de todo o mundo estarão visitando a cidade para acompanhar a competição. As polícias e forças armadas de todo o País já vem se preparando desde os Jogos Mundiais Militares de 2011, que também ocorreram na capital fluminense, para evitarpossíveis ataques cibernéticos ou mesmo um inédito ataque terrorista no País. Desde então, grandes competições esportivas vêm acontecendo no Brasil desde 2012, com destaque para os Jogos Pan-americanos do Rio (2007) e aCopa do Mundo de Futebol de 2014. Nas Olimpíadas, os olhos do mundo estarão voltados para cá e tudo o que há de mais moderno nesta área estará à nossa disposição, através de ajuda que receberemos de polícias especializadas internacionais, como a Interpol", explica Luiz Alfredo Salomão, coordenador-geral, professor e pesquisador da Escola de PolíticasPúblicas e Gestão Governamental da Universidade Candido Mendes (EPPGG/Ucam).De acordo com o engenheiro, que entre os anos de 2009 e 2011 ocupou o cargo de secretário-executivo da antiga Secretaria de Assuntos Estratégicos (SAE), do governo federal, nenhum sistema de informação é completamente blindado contra ataques e violações. Corrobora essa afirmação o episódio envolvendo o administrador de vigilância computacional da CIA, a Agência Central de Inteligência dos Estados Unidos, e ex-funcionário da NSA, a Agência Nacional de Segurança daquele mesmo país, Edward Snowden, mostrou ao mundo que não existe nenhum sistema computacional 100% seguro (ZEPEDA, 2014, p. 48-50).

Com a publicação acima, pode ser visto que o fator humano é muito importante no uso dos sistemas de informações e que para tal utilizam *softwares*, mas que mesmo estes necessitam estar amparados na procedência e confiabilidade.

Assim, para além de não existir nenhum sistema computacional que garanta a sua eficiência em 100%, também no que diz respeito à gestão, tanto dos *softwares,* bem como as comunicações militares, os estudos que elaboram estratégias, o planejamento das operações etc., dependem de software. Aqui a preocupação é que os *softwares* são controlados por pessoas. Atentando também que para além desse controle, deve haver autonomia na gestão tecnológica, sem a qual a defesa do país e consequentemente a sua tecnologia passam a apresentar vulnerabilidades que comprometem a nação.

Neste pensamento, em 2015, o Governo Brasileiro no sentido de prover diretrizes estratégicas para aperfeiçoar a gestão da Segurança da Informaçãoe das Comunicações - SIC, no âmbito do Sistema Militar de Comando e Controle - SISMC, vai aprovar através da Portaria Normativa no. 2.327/MD, de 28 de outubro. No seu Capítulo II, ao falar de Conceitos e definições o Comando Militar assinala que:

> Atributos de Segurança da Informação e das Comunicações Os atributos clássicos de SIC, que também se aplicam ao SISMC[2], são os seguintes: a) confidencialidade: propriedade de negar a disponibilização ou revelação da informação a indivíduos, entidades ou processos não autorizados nem credenciados; b) integridade: propriedade de salvaguarda da exatidão e totalidade da informação, de forma a garantir que o conteúdo original da informação não seja modificado indevidamente por elemento humano ou qualquer outro processo; c) disponibilidade: propriedade de assegurar que a informação esteja acessível e utilizável sob demanda de uma entidade autorizada; d) autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade; e) não-repúdio (irretratabilidade): propriedade de assegurar que, num processo de envio e recebimento de informações, nenhum participante originador nem destinatário de informação possa, em um momento posterior, negar a respectiva atuação (BRASIL, 2015, p.15).

Ou seja, é necessário que os atributos estejam contemplados como garantias, pois pressupõem, como toda organização seja ela civil ou militar que as informações estejam amparadas nos princípios da confiabilidade e que haja ética na manipulação dos dados. Manipulação no sentido utilitário, uma vez que através dessa os dados que formam a informação são alterados ou mantidos para compor a informação necessária, plausível, acessível e à disposição, sem que para isso aconteça interrupções, alterações, interferências externas ou desvios dessas informações.

Tanto estudo apresentado pela Revista da FAPERJ (2014), quanto a Portaria Normativa do Governo Federal vem corroborar com o fato preocupante que é demonstrado pela empresa russa que atua no segmento de *softwares*de segurança para a *internet,* a Kaspersky Lab, que elaborou um estudo em 2016, afirmando que o Brasil é um dos países que mais atrai atraques cibernéticos na América Latina. Quando a análise se coloca em contexto mundial de ameaças dessa natureza, o país ocupa a nona posição, o que é deveras preocupante.

Nesse sentido, manter os sistemas atualizados de proteção contra ataques virtuais passou a ser um assunto de segurança nacional, se constituindo em uma importante estratégia para a sobrevivência das corporações. Atentando para essa realidade, o Exército Brasileiro, através do Centro de Desenvolvimento de Sistemas (CDS), resolveu empreender esforços e discutir a Segurança da Informação e Criptografia, no VI Seminário Nacional de Segurança da Informação, em 2017.

O evento contou com a presença de militares, acadêmicos e empresários do setor, na cidade de Brasília, capital do país.Tal reunião buscou discutir temas relevantes da defesa cibernética, segurança da informação e criptografia, contando com “salas temáticas para o debate de aspectos como sistemas criptográficos, segurança de sistemas operacionais, nuvens seguras e eletromagnetismo” (BRASIL, 2017, *online*).

Um estudo realizado em 2008, já chamou a atenção para o fato de que ao entrarem na reserva ou serem transferidos para as Organizações Militares nas mais diversas regiões do país, os militares não eram instruídos Com o título *Proposta de Norma de Segurança da Informação para o Gerenciamentodos Ativos e Direitos de Acesso dos Militares Transferidos do 3º Centrode Telemática de Área*, os pesquisadores Watanabe, Azevedo e Galegale, afirmam o seu cuidado com o assunto e lançam a proposta que tenciona dentre outras questões, chamar atenção para o fato de que “por ocasião dessas transferências, muitas vezes não são revisadas as questões depermissões de acessos à rede interna bem como aos sistemas de informação da OM (WATANABE; AZEVEDO; GALEGALE, 2008, p. 1).

Neste caso em particular, ainda que a Marinha e a Aeronáutica também possuam sistemas de informação e as suas práticas sejam semelhantes ao tratamento dado pelo Exército, uma vez que a Portaria Normativa 2.327/MD vai abranger as Forças Armadas de modo geral. Portanto, a título informacional, vamos

referenciar o Centro Integrado de Telemática do Exército - CITEx, responsável por operar os Sistemas de Informática e Comunicações de interesse do Sistema de Comando e Controle do Exército na área do Comando Militar do Sudeste – CMSE, que é o assunto do trabalho dos pesquisadores citados anteriormente. O EB possui divisões e subdivisões, uma delas é o 3º Centro de Telemática de Área que:

> [...] é uma OM do EB voltada para a tecnologia da informação, com várias atribuições, dentre as quais destacamos a instalação, operação, produção e manutenção (Hardware e Software) dos sistemas de informação que compõem o Sistema Estratégico na área do CMSE. Na área de segurança, o 3º CTA tem como atribuição o estabelecimento das medidas de segurança dos Subsistemas de Informática e de Comunicações, e ainda, deve fomentar a cultura de utilização das modernas Tecnologias de Informação em sua área de atuação. Atualmente, sua estrutura organizacional se divide em Chefia, Subchefia e quatro divisões: • Divisão Administrativa: responsável pelo patrimônio, pelas questões financeiras e materiais; • Divisão de Pessoal: trata dos assuntos relacionados com pessoas. Recursos Humanos (RH); • Divisão Técnica: voltada para o desenvolvimento de sistemas, treinamentos em informática, manutenção e suporte de sistemas; e, • Divisão de Operações: mantém os serviços de redes, comunicações, manutenção de equipamentos, suporte, operação de sistemas, servidores, telefonia, servidores, instalação de software, gerenciamento de usuários e senhas(WATANABE; AZEVEDO; GALEGALE, 2008, p. 4).

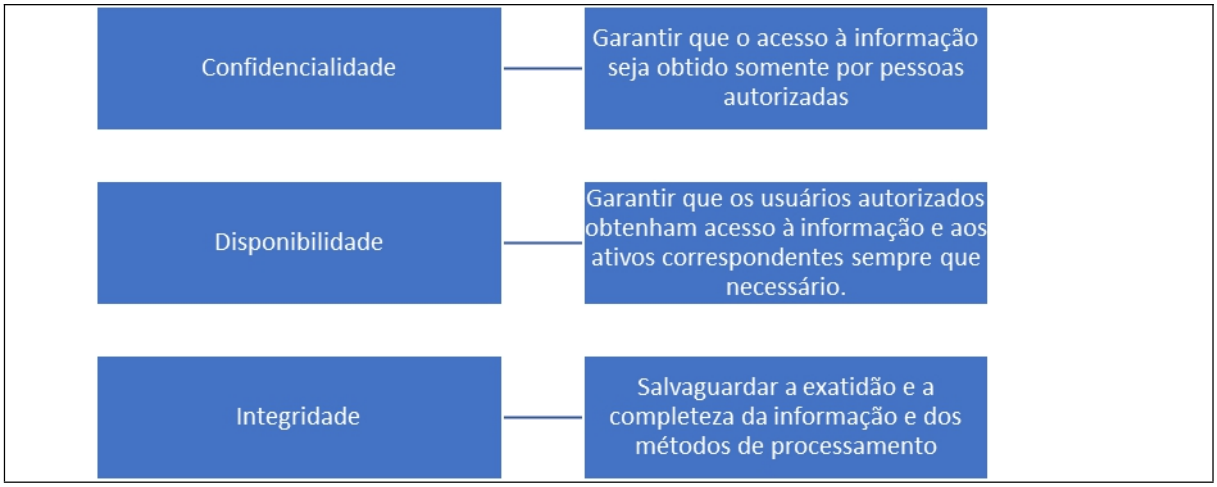
Como em praticamente todos os sistemas informáticos, o atendimento dos requisitos de segurança carece de uma senha de acesso individual que permite o acesso a rede interna. O acesso, por sua vez, condiciona privilégios de acordo com a função que o militar exerce, disponibilizando assim: serviços de impressão, áreas para backup e trocas de arquivos, acesso aos sistemas de informação internos, voltados para controles de patrimônio, de pessoal e de documentação, nos vários níveis de confidencialidade(WATANABE; AZEVEDO; GALEGALE, 2008).

Há ainda que se referir em relação a rede interna, que está integrada à Internet, de acordo com as Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército - NORTI. Sendo que o objetivo das NORTI é manter o controle sobre as informações dos dispositivos de TI de propriedade do EB, para inibir conteúdos que não estejam em conformidade com os critérios de licitude ou ainda, conteúdos que violemdireitos de terceiros, ou afete à moral, os bons costumes e assim, comprometa a disciplina.

A grande preocupação dos autores refere-se ao fato de que as NORTI, apesar de se constituírem como uma orientação para os militares e servidores civis quanto ao uso correto dos recursos de TI, não tratam dos procedimentos que devem ser feitos após o encerramento de atividades destes. O que no presente só demonstra que a importância da SI para a organização é essencial, além do cuidado a ser te quando este efetivo, civil e militar é transferido ou passa para a reforma, se constituindo uma aposentadoria, na qual os privilégios de quando estava na ativa, devem deixar de existir.

Tantos setores públicos, quanto privados devem proteger as suas infraestruturas no sentido de reduzir os riscos eminentes, mas como já dito, em se tratando de organização militar vai envolve um cuidado especial, por conter informações que dizem respeito à segurança nacional e por conseguinte à soberania da nação. ou reduz os riscos relevantes. Mas tal segurança deve ser feita de maneira dinâmica e constante, pois ficam expostas às ameaças cada dia mais sofisticadas e que possuem, por vezes um comércio. Ou seja, há um mercado voltado para as fraudes, espionagem, sabotagens e vandalismos. Em geral a figura do pirata informático, ou *hackers*; que se responsabiliza pelo ataque aos sistemas de Informação, grosso modo, nem sempre é uma pessoa, podendo ser um grupo ou muitos que agem em simultâneo e suas ações estão cada vez mais comuns, ambiciosas e sofisticadas. Na Figura 2 abaixo, podemos ver os requisitos básicos da Segurança da Informação.

Figura 2 - Requisitos básicos da SI



Fonte: WATANABE; AZEVEDO; GALEGALE, 2008.

Em relação a legislação, através da 9º *Pesquisa Nacional de Segurança da Informação* (2003), realizada pela empresa Módulo Security Solutions S.A., com uma participação significativa de cerca de:

> [...] 50% das 1000 maiores empresas do Brasil, nos diversos segmentos tais como governo, indústria e financeiro, mostra que 63,5% dos entrevistados utilizam a norma ISO 17799 para norteamento das ações de segurança de suas organizações, ficando 37% para as publicações do Governo Federal (decreto 4553 e outros), 30% as publicações do Banco Central (resolução 2554 e outras), 27% a Regulamentação da ICP-Brasil, 20% o COBIT e 20% as Publicações da CVM (Resolução 358 e outras). A norma NBR ISO/IEC 17799:2005 tem como objetivo o estabelecimento de diretrizes e princípios gerais para iniciação, implantação, manutenção e melhoria da gestão de SI em uma organização. Pode ainda servir como um guia prático para o desenvolvimento dos procedimentos de segurança, das práticas eficientes de gestão da segurança e para ajudar a criar a confiança nas atividades interorganizacionais. Esta norma, ainda pode ser considerada como um ponto de partida para que cada organização desenvolva suas diretrizes específicas, visto que nem todos os controles e diretrizes nela contidas podem ser aplicadas. Além disso, podem ser necessários controles adicionais(WATANABE; AZEVEDO; GALEGALE, 2008, p. 12).

Na pesquisa mencionada anteriormente, as legislações versam entre normas e regulamentações que vão nortear as organizações, para aqui demos destaque aquelas do Governo Federal, em particular, o portanto, o Decreto 4.553 vai tratar da salvaguarda de dados, informações, documentos e materiais sigilosos que pertencem a esfera da sociedade e do Estado, no âmbito da Administração Pública Federal. Para o Exército, foram aprovadas as IG 20-19 - Instruções Gerais de Segurança da Informação para o Exército Brasileiro, objetivando a orientação do planejamento, além da execução das ações relacionadas à SI, bem como as IG 20-19, que definem, de modo geral, as responsabilidades, orientações gerais, cujo objetivo é referenciar os princípios básicos para as documentações normativas de segurança.

Mais adiante, falando de vulnerabilidade, a qual qualquer sistema é passível, pode ser dito que é uma fraqueza encontrada em determinados recursos, processos e configurações, o que demonstra a ausência e/ou a ineficiência das medidas de proteção utilizadas para salvaguardar os ativos da organização. Mais adiante, no Quadro 2, podem ser vistos os fatores mais comuns de vulnerabilidade, atentando para o fato de que é a ação humana, direta ou indiretamente a maior preocupação.

Quadro 2 - Fatores de vulnerabilidade mais comuns

Falhas mais comuns apontadas	O que são?
Hardware	ausência de firewall e dispositivos de armazenamento ineficazes
Software	equipamentos não configurados corretamente, antivírus não atualizado.
Humanas	falta de treinamento, compartilhamento indevido de informações, funcionários mal intencionados
Naturais	podem se constituir em desastres naturais como inundações, terremotos.
Físicas	instalações inadequadas, fios elétricos e cabos de rede distribuídos de forma incorreta, ausência de extintores ou extintores inadequados

Fonte: WATANABE; AZEVEDO; GALEGALE, 2008.

Ainda sobre a questão da vulnerabilidade, e importante assinalar que esta não é assim uma conjugação singular, sendo melhor proposta como vulnerabilidades, uma vez que se apresenta em um contexto múltiplo e que depende de vários fatores. A 10ª Pesquisa Nacional de Segurança da Informação, realizada em 2006, pela Módulo Technology for GRC, que obviamente é uma empresa privada, portanto mantem em sua página *online*, soluções diversas e personalizadas para às questões de segurança, mas que não deixa de apresentar validade em relação aos dados apresentados em sua pesquisa.

Isto posto, os dados da pesquisa mostram que 1/3 das organizações não conseguem avaliar de maneira numérica as perdas ou ainda, identificar os responsáveis pelo problema da segurança. fato que aponta para a falta de planejamento formal na área. As dificuldades em elencar os responsáveis, bem como em planejar de maneira efetiva a segurança das organizações e nesse caso, as organizações de natureza militar, levam muitas vezes a apenas corrigirem as falhas, que em boa parte são causadas pela ação humana, ou seja, pelos colaboradores.Como falhas podem ser apontadas a presença de ação de *hackers*

(não colaboradores), vírus (por acesso inadequado e não-seguro), *spam* e fraudes de maneira geral.

O propósito de se apresentar um panorama geral para a segurança nos Sistemas de Informações, não é outro, senão apontar para mostrar a necessidade de que cada organização, seja civil ou militar, acrescente como uma questão essencial em sua gestão a necessidade de estabelecer uma política de segurança adaptada às suas realidades, nos mais diversos setores.

Assim como as teorias da administração, sejam da organização como um todo, seja na gestão de seu pessoal, se voltam para dinamizar a produção, também a política de segurança volta-se para a informática e o ambiente virtual, como uma premissa de garantia de bom funcionamento.

Ademais, toda e qualquer política que se volte para manter a integridade dos seus sistemas de informação será inválida se desconhecer o seu contingente operacional, aqui abrangendo desde a disposição dos seus equipamentos, técnicos que devem ser treinados devidamente, tanto na transformação de dados em informações, bem como no funcionamento devido desses sistemas, no quesito de operacionalidade.

A importância do bom uso de software adequado e que garanta o que se pretende na compilação e adequado uso das informações é uma questão pertinente. Lembrando que no que diz respeito à segurança militar, a criação do Ministério da Defesa juntou civis e militares, que não caminham opostamente, mas que possuem formações distintas, das quais a disciplina militar é entendida de maneira diferenciada daquela aplicada ao pessoal civil.

Antes de se estabelecer uma crítica mais veemente, não se quer com isso alertar que esta ou aquela sociedade, ou ainda, que há entre os militares uma disciplina que não acontece no modelo civil, mas sobretudo, que abarcam interesses que dizem respeito à Segurança Nacional, entendendo que esta não deve ser confundida com Defesa Nacional. O que pode ser dito:

> Segurança nacional e defesa nacional são conceitos diferentes? Na opinião de estudiosos ouvidos pelo Senado, como o professor GuntherRudzit, coordenador do Curso de Relações Internacionais da Fundação Armando Álvares Penteado (Faap), de São Paulo, defesa e segurança vão além das Forças Armadas e dos militares e são dois temas que precisam ser mais bem compreendidos pela sociedade no Brasil. Como explica o professor, há uma grande confusão na

> sociedade sobre o que é segurança e o que é defesa, surgida a partir da Constituição de 1988, que retirou o capítulo de Segurança Nacional e introduziu o de Defesa Nacional. Para ele, foi uma mudança compreensível, pelo que ocorreu durante o regime militar recém-encerrado no Brasil, mas gerou a dúvida: qual é o âmbito de atuação de defesa e o que é segurança? “Segurança é o todo de um país. O país pode ser ameaçado ou ter vulnerabilidades que podem levar a uma ameaça, como o apagão [nos anos 1990]. Sempre falo de uma política de segurança nacional como uma política maior, em que o governo que assume deve deixar claro quais são seus objetivos e quais são as ameaças e vulnerabilidades que percebe interna e externamente”, explica o professor, doutor em Segurança Nacional (BRASIL, 2012, online).

Evidentemente, o período nos qual os militares estiveram no poder no Brasil influenciou essa demanda que causa confusão aos desavisados. Assim, procuramos estabelecer o termo de que segurança e um estado e defesa é um ato. No mais o que se trata neste trabalho diz respeito à segurança, e a segurança de dados militares para ser mais específico.

Neste caso, é importante lembrar que ao estabelecer a fusão dos Ministérios das três Forças Armadas brasileiras, o governo do país, considerou que efetivos civis convivessem com regras miliares e vice-versa, no sentido de segurança esse processo vai atentar para o fato de que os dois segmentos compreendem segurança de maneira diferenciada. Assim, esclarecendo que segurança possui um conceito e defesa outro, podendo ser entendido como defesa, aquilo que faz parte das estratégias de segurança.

Nesse sentido, o uso da ISO 27001, como um padrão de qualidade e excelência para a segurança das informações voltadas ao ambiente militar, como a melhor alternativa a ser seguida. Uma vez que se trata de um procedimento de padrão internacional, extremamente rígido em seus princípios, que visa garantir a excelência e a qualidade. Por assim entender, faz-se necessário uma política de segurança dos sistemas de informação que se acautele, trazendo para o contexto daquilo que lhe compete defender, que é a soberania nacional, entendida como questão de defesa e segurança nacionais.

Ao adotar o padrão ISSO 27001, o Ministério da Defesa vai delegar um objetivo de excelência a ser atingido pelas Forças Armadas, nos seus três seguimento, ou seja, tanto na Marina, Exército e Aeronáutica, como forma de que cada uma, estabeleça normas internas, que por sua vez obedecerão à normativa

federal que consequentemente está assegurada nos padrões internacionais ISO 27001, como forma de que cada um, à sua maneira, crie padrões próprios para segurança das informações institucionais.

Também é importante salientar, que nenhum modelo de segurança é infalível, daí prescinde a importância de uma política dinâmica que se adapte às demais situações, previsíveis ou não, mas que garanta a preservação daquilo que é pertinente ao contexto das Forças Armadas, dentro do Ministério da Defesa. Em busca de melhor contexto e fornecer o entendimento necessário para a compreensão deste trabalho, em seguida trabalhamos os termos mais caros: informação, sistemas da informação e segurança dos sistemas de informação.

3 DEFININDO A INFORMAÇÃO E OS SISTEMAS DE INFORMAÇÃO

A produção do conhecimento científico e tecnológico, experienciada nas sociedades contemporâneas, trouxe-nos a denominação de ‘sociedade do conhecimento’ (CASTELLS,2002). Sob esse olhar, pode ser dito que esta sociedade se fundamenta no conhecimento da informação, o que torna imperativo o seu uso, que vai determinar as suas ações.

As organizações demandam preparo para lidar com os problemas internos e externos do contexto em que estão inseridas, para tanto buscam suporte no desenvolvimento de sistemas de informações, para assimilar de maneira efetiva e eficaz os dados informacionais que resultam em uma melhor solução desses problemas. Assim, fica entendido que “[...] a razão mais forte pelas quais as empresas constroem os sistemas, então, é para resolver problemas organizacionais e para reagir a uma mudança no ambiente” (LAUDON; LAUDON, 1999, p. 26).

Ao mencionar o termo informação dentro do âmbito das organizações é esperado que esse termo se ligue diretamente ao de Sistemas de Informação - SI que permitem desde a coleta até a disseminação da informação, sem descurar da segurança da sua armazenagem, nemda fonte de coleta dessas informações para fins muito específicos (TURBAN *et al*, 2007). Para Rainer Jr. eCegielski (2011), praticamente todos os ST possuem base computadorizada e servem de apoio organizacional para as empresas e corporações.

A associação entre os termos Informação e sistema estão sempre associados, pois para além das suas aproximações terminológicas e conceituais, a informação vai assumir as características sistema no qual ela está inserida, ou seja, é parte necessária a um sistema por ser ela - informação - a responsável pelo funcionamento organizado do mesmo (JANNUZZI; TÁLAMO, 2004). Em termos básicos, um sistema de informação em uma organização é compreendido como todos os registros e documentos gerados nas operações desenvolvidas por ela (CASSARRO, 2010), podendo ser manual ou informatizado. O reconhecimento da importância da informação nas organizações e o desenvolvimento significativo das tecnologias de informação e comunicação – TICs, favoreceram o surgimento de uma gama variada de sistemas de informação. Assim, considerando a afirmação de que "as organizações utilizam muitos tipos diferentes de sistemas de informação"

(TURBAN et al., 2007, p.5), é que se busca compreender conceitualmente esses sistemas e suas aplicações nas organizações a partir dos estudos apresentados na literatura.

Com base no entendimento de que as sociedades a partir do século XX fundamentam-se como sociedade de conhecimento, faz-se necessário que os conceitos de informação, sistemas de informação e segurança, tomem parte desse debate. O que a partir de então se discute.

3.1 O QUE É INFORMAÇÃO?

A partir de então, aqui se faz necessário relacionar algumas perspectivas sobre o termo“informação”, uma vez que possui muitos conceitos e estes variam de acordo com a aplicação. Assim, apresentando breves considerações sobre o fenômeno da informação, a sua relevância e os seus usos, são pertinentes, principalmente para que se tenha o panorama ampliado de um conceito que pode ser considerado polissêmico.

Entender o conceito de informação é importante, bem como considerar as novas formas de aquisição dessa informação, configuradas nas organizações corporativas e sociedade em geral, conferindo-lhe um caráter plural, não se constitui como uma tarefa fácil. Acerca desse pluralismo conceitual e os muitos conceitos para a o termo informação, pode ser dito que:

> Nos estudos e aplicações relacionados à informação é possível observar um amplo leque de conceitos sobre o tema, incluindo diversas categorizações em diferentes contextos. Este quadro conceitual resulta das características intrínsecas da informação, mas também do fato desta, enquanto fenômeno, estar presente como parte indissociável do processo de comunicação (JANUZZI; FALSARELLA, SUGAHARA, 2014, p. 96).

Diante do exposto, buscamos estabelecer não um conceitofechado, mas mostrar os múltiplos entendimentos dos teóricos acerca dos estudos da informação, de modo que possamos não consolidar uma resposta verdadeira, mas apresentar um leque delas, que em constante diálogo, isso essencialmente por que os variados

conceitos de informação dizem respeito à aplicabilidade, que por sua vez vai categorizá-la.

Entendendo que um breve histórico é necessário, portanto, vale apontar o que disse o historiador inglês, Peter Burke (2003), desde a Antiguidade, as sociedades coletam, armazenam, recuperam e suprimem informações. O que nos deixa vislumbrar que não é um fenômeno propriamente recente, uma vez que no Império Romano eram utilizadas como forma de controle sobre a população. O plágio, por exemplo, que é uma grande preocupação no meio acadêmico, já era uma crítica estabelecida entre os sofistas, liderados pelo filósofo grego Platão (427 a. C.). Porém, ainda segundo Burke (2003), somente a partir da Idade Moderna as informações passaram a ser acumuladas e organizadas.

Nas últimas décadas, o estudo acerca dos fenômenos da informação tem se intensificado, motivado principalmente pela inserção e utilização maciça das tecnologias e das informações nas atividades produtivas do homem, o que impulsionou um rápido desenvolvimento científico e tecnológico e despertou a atenção de estudiosos e pesquisadores de diversos campos do saber, com vistas a investigar as relações entre a sociedade, a informação e o conhecimento humano em toda sua complexidade.

A rotina do homem vem sendo alterada em uma construção cotidiana e, tais mudanças só mostram a situação de vulnerabilidade das relações sociais diante da velocidade com a qual as informações são elaboradas, repassadas e consumidas, o que trouxe grandes transformações na rotina do homem, e exigindo que esse reelaborasse as suas condutas. A partir de então, há uma nova ordem mundial, na qual a informação passa a desempenhar um importante papel, adquirindo estatuto de mercadoria, podendo ser mensurada e com valor monetário, ou seja, a informação pode ser produzida, acumulada, processada, veiculada e vendida. Assim:

> [...] a informação atua enquanto um regulador da vida social, permeando todos os espaços e atuando em todas as atividades humanas. [...] Informação é considerada a quinta necessidade do homem, precedida por ar, água, alimentação e abrigo. Inclui-se entre os recursos básicos da sociedade, juntamente com materiais, alimentos, energia, espaço vital e mão de obra. Mas, apesar de atuar intensamente na sociedade humana, pouco se sabe acerca da informação. Ora identificada como fenômeno, ora como processo, o fato é que a informação se apresenta como um conceito impossível de ser apreendido em toda sua totalidade, transcende qualquer

> tentativa de apreensão universal, resultando num emaranhado de abordagens que fraciona o conhecimento que podese obter acerca desse fenômeno (MESSIAS, 2005, p. 21).

Isto posto, o uso do termo – informação, a depender do contexto na qual se insere adquire importância conceitual pertinente a essa inserção. Para os estudiosos, teóricos e pesquisadores o termo assume o conceito que a sua ciência determina. Como por exemplo, para os historiadores, a informação é uma fonte histórica, podendo ser desde os registros físicos até os relatos orais. Nesse sentido, pode ser dito que as modificações sofridas no conceito de informação ao longo do decurso do tempo, acontecem (e acontecerão)como um processo evolutivo natural"[...] que se estabelece a partir das relações entre os sujeitos e suas práticas sociais, o que de certa forma, impõe novos olhares a antigos conceitos, promovendo a reconstrução dos mesmos"(MESSIAS, 2005, p. 21).

Em sua formação etimológica, deriva do latim*informare* ou *informatio*, que tem o sentido de dar forma, representar uma ideia, constitui uma noção de algo. Para Messias (2002; 2005), é uma tarefa impossível assinalar o período exato no qual o termo informação aparece pela primeira vez, podendo ser visto desde os períodos mais remotos, mas a sua popularização ganhou corpo nas últimas quatro décadas, enquanto que a preocupação com a sua conceituação será bem mais recente e alavancada pelo advento das novas tecnologias, incluindo a informatização dos mais diversos setores da sociedade.

A informação constitui a ordenação e a organização dos dados, de maneira que estes adquiram significado de forma a transmitir significado e compreensão dentro de um determinado contexto. Seria o conjunto ou consolidação dos dados de forma a fundamentar o conhecimento O dado não possui significado relevante e não conduz a nenhuma compreensão. Representa algo que não tem sentido a princípio. Portanto, não tem valor algum para embasar conclusões, muito menos respaldar decisões.

Vale salientar, apenas para que se conste o registro de que comumente a informação é confundida com 'dados'. Para Rezende (2015), os dados são os registros soltos, aleatórios, sem quaisquer análises, assim são a matéria prima da informação, ou seja, é a informação não tratada e por isso mesmo, não apresenta relevância.Osdados são fatos isolados, que podem servir ou não em determinado

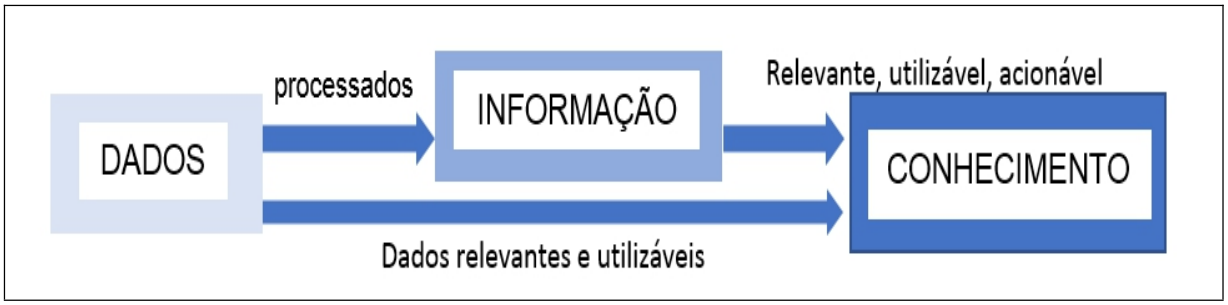
contexto, ser importante ou não para uma determinada situação. Isoladamente, a posse dos dados não assegura benefícios.

A compilação dos dados e a sua disposição de maneira ordenada, enquadrada em um contexto é o conjunto substancial da informação, a partir do qual pode ser vista a utilidade dos dados que gera conhecimento.Salientando que, “[...] o processo pelo qual estamos passando nos transforma na sociedade do conhecimento, na qual o principal recurso para os indivíduos e para a economia em geral é o conhecimento” (SOUSA; MELHADO, 2008, P. 130).

Diante da veloz transformação, pela qual a sociedade tem passado, é fundamental que as organizações, os gestores, as pessoas, as corporações, as associações, famílias, grupos sociais em geral, dentre tantos outros atores sociais, se abram para a inovação, para sair do lugar comum,de tudo o que significa estabelecido, costumeiro, conhecido e confortável, ou seja, a sociedade precisa estar preparada para transformações constantes (DRUCKER,1995). Portanto, nesse contexto, a função da empresapassa por dimensionar o conhecimento, formatando-o em ferramentas necessárias e disponíveis.

ParaTurban; MacLean; Wetherbe (2004), no universo dos sistemas da informação, o conhecimento adquire uma conceituação distinta daquilo que é entendido por informações, bem como, por dados. Conforme mostra a Figura 3, mais adiante.

Figura3 - Processamento de dados em informação e em conhecimento



Fonte: Turban; McLean; Wetherbe (2004), (adaptado).

Como visto no esquema representado na Figura 3, os dados representam uma coleção de fatos, parâmetros, estatísticas etc., que são processados compondo as informações que são os dados organizados ou processados, precisos e

fornecidos no momento oportuno. Já o conhecimento é a informação contextualizada, acentuando a sua relevância, utilidade e ação(Turban; McLean; Wetherbe, 2004).

A importância do conhecimento deriva da sua aplicabilidade, significa ter poder de dar uma solução para algo ou alguma situação, ou ainda, promover ações de divulgação. Nesse entendimento a informação não possui a mesma conotação. Nesse sentido, a informação, na sociedade atual, faz parte de um ambiente, no qual as novas tecnologias mudaram a forma de ser e estar de boa parte da população e a vigência da virtualidade nas relações sociais e de trabalho é uma realidade. Obter e repassar informações relaciona-se com o conceito de responsabilidade social, uma vez que o que se almeja é que seja disseminadade modo correto e seguro.

3.2 QUALIDADE DA INFORMAÇÃO

A discussão sobre qualidade da informação é uma atividade bastante árdua, complexa e de muita controvérsia (DE SORDI, 2009). Tanto quanto o conceito de informação, a qualidade da informação também suscita uma conceituação em contexto problemático. Vejamos, o que é valioso para uma empresa pode ser o descarte de outra, uma informação estritamente necessária para uma organização, pode simplesmente ser dispensável para outra, assim o conceito para alguns acaba sendo ambíguo, vago e subjetivo (PAIM; NEHMY e GUIMARÃES, 1996).

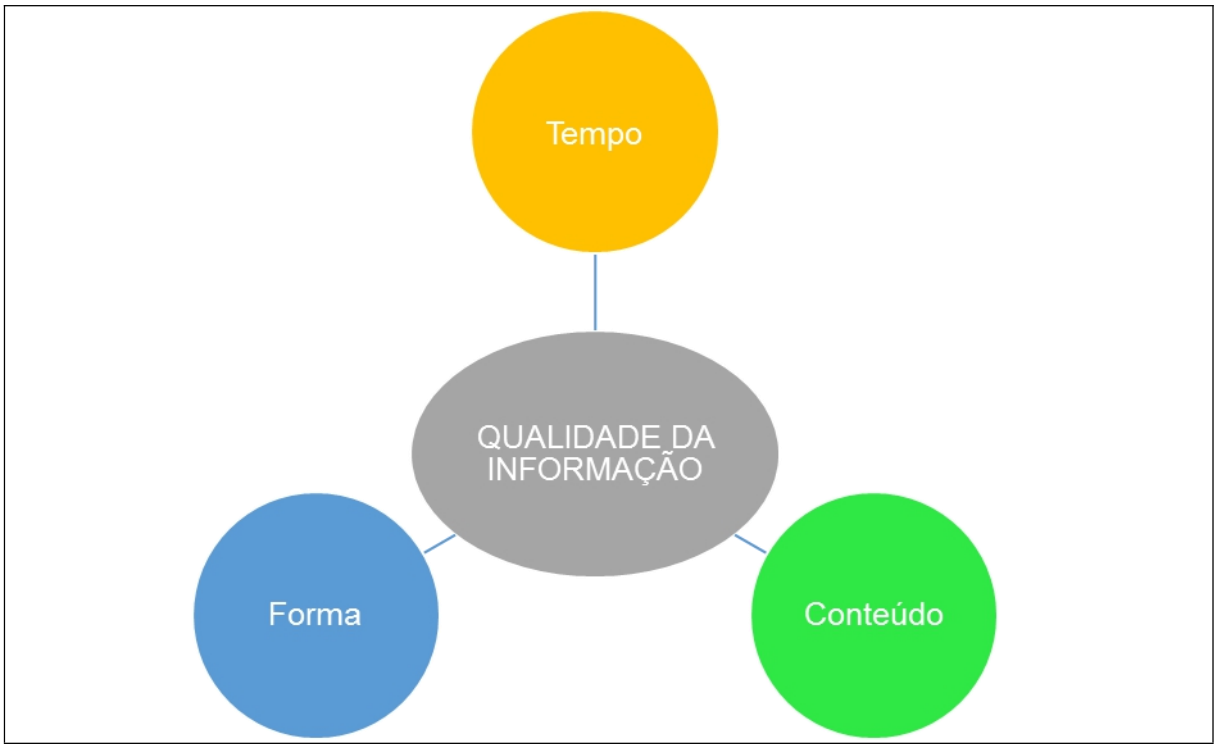
Todo conceito pressupões um estudo teórico, um ponto de vista, um olhar mais dedicado, portanto, a dificuldade em conceituar a qualidade da informação não deve servir como desestimulo, antes pelo contrário, deve constituir em estímulo, principalmente quando as organizações deve ser um estímulo ao estudo e compreensão em decorrência da importância crescente deste ativo, principalmente nas organizações, cujas estratégias estão baseadas em conhecimento (KLEINSORGE, 2014). A competição com o objetivo em manter a atenção do indivíduo, do cliente ou mesmo no eu diz respeito a dinâmica de estabelecer escolha, dando a devida importância a informação é uma tarefa a ser perseguida, vejamos:

> Competir pela atenção do indivíduo na sua escolha entre variadas fontes de informação e sua autopercepção de ganho de

> aprendizagem é um desafio adicional aos sistemas de informação os quais, invariavelmente, se voltam ao atendimento de demandas por informação apropriada, entendida como aquela apresentada no formato, conteúdo e tempo tido como ideal para um determinado grupo ou nível de usuários (KLEINSSORGE, 2015, p.15).
> .

Já O'Brien (2004), vai mensurar a qualidade da informação pelo que pode ser fornecido através dela, assim, informações antiquadas, inexatas ou difíceis de entender não possuem razão de existir, portanto, passíveis de descarte. Uma vez que nos dias atuais as organizações e consequentemente as pessoas desejam informações de alta qualidade, ou seja, produtos de informação com valores agregadores positivos, com características, atributos ou qualidades ajudem a torná-las valiosas. Para o autor a qualidade da informação pode ser avaliada a partir de três dimensões: Tempo, Conteúdo e Forma. Na Figura 4, podemos ver a disposição dada, segundo o entendimento do autor.

Figura4 - As dimensões que dão qualidade a informação

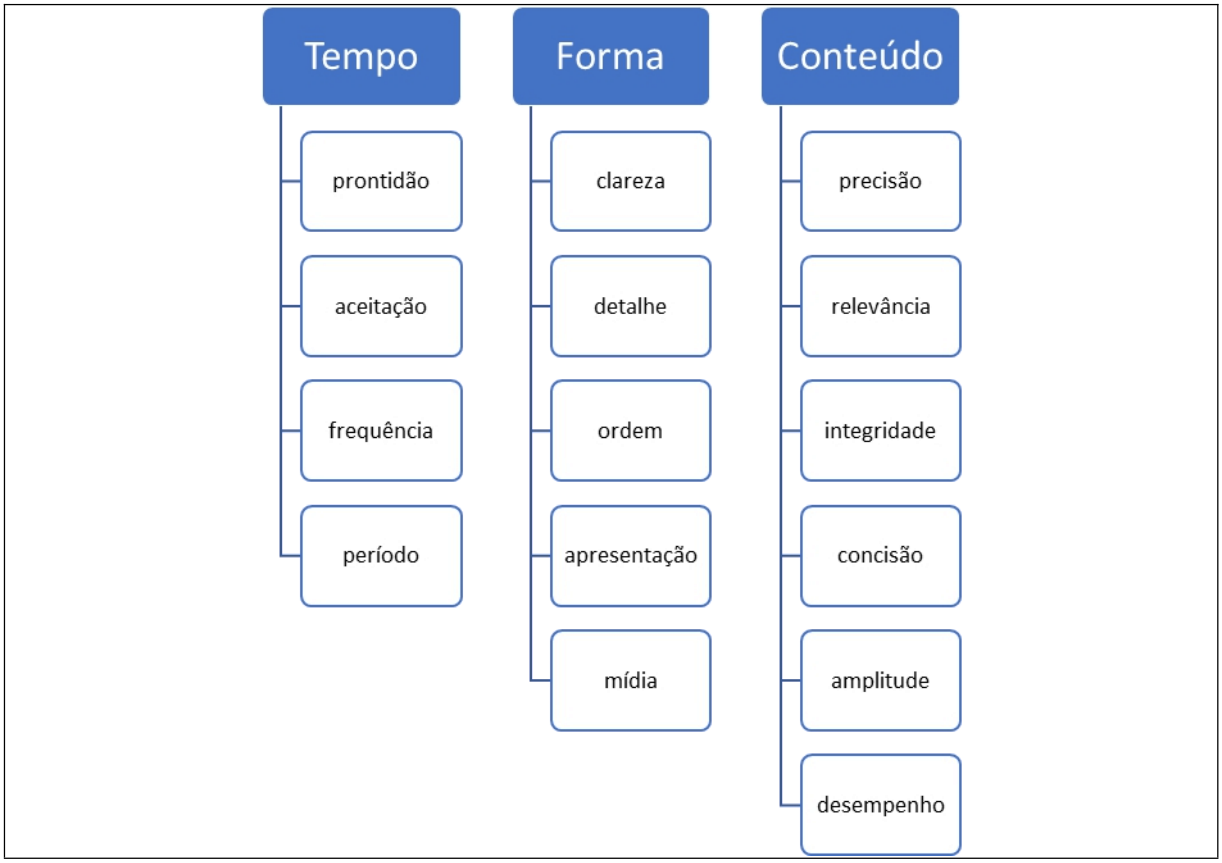


Fonte: O'Brien, 2004 (adaptado).

Cada dimensão possui seus atributos que tornam esta informação mais ou menos valiosa. Para De Sordi (2008), os gestores são desfiados cotidianamente no

sentido de fornecerem ao usuário/consumidor/cliente uma informação de qualidade, bem como dimensionar o conceito de qualidade, no sentido de distinguir, o que é uma informação de qualidade, principalmente pela velocidade com a qual as informações surgem, são criadas, processadas e colocadas à disposição. Mais adiante, na Figura 5, descrevemos os atributos de cada dimensão, ainda segundo o pensamento de O'Brien (2004).

Figura5 - Os atributos das dimensões das informações



Fonte: O'Brien, 2004 (adaptado).

Assim, a preciosidade da informação tem a ver com o contexto no qual a informação se insere e está dimensionada segundo os atributos que possui. Assim, na sua dimensão tempo, por exemplo, a informação de melhor qualidade é aquela que está disponível, atualizada, possua frequência etc. desta maneira, pode ser notada a preocupação de O'Brien (2004), em ordenar as dimensões e seus atributos, ao menos no sentido de auxiliar com um parâmetro, que forneça um padrão de valor.

Que fique claro, que outros atributos e mais detalhes vão qualificar a informação, incluindo a sua necessidade, a sua natureza e a quem vai servir, são

apenas alguns detalhes que podem ser utilizados na hora de atribuir um valor. Também que seja dito, que os parâmetros aqui utilizados, não se constituem em juízo de valor, mas apenas uma forma elaborada, com base nos escritos de James O'Brien (2004), de modo que fossem disponibilizados em formato mais didático, facilitando assim, a aquisição desse conteúdo, ainda que de modo sucinto.

3.3 SISTEMAS DE INFORMAÇÃO

Para atender as questões da competitividade do mercado e a demandatecnológica, as organizações contam com os seus sistemas de informação, que tem por objetivo, dentre outros, a resolução de problemas organizacionais internos frente às tendências de mercado.

Os sistemas de informação, a partir de uma definição técnica, podem ser entendidoscomo um conjunto de componentes que estando inter-relacionadoscoletam (ou recuperam), processam, armazenam e distribuem informações para a tomada de decisão e controle em uma organização (TAIT, 2000; GIL, 2002). Tal conjunto contém informações significativas para a organização ou em seu ambiente, aqui incluídas questões pessoais. A mesma autora, vai relatar que a crescente utilização dos sistemas informáticos e consequentemente dos computadores, transformoua visão das organizações, no que diz respeito aos seus sistemas de informação.

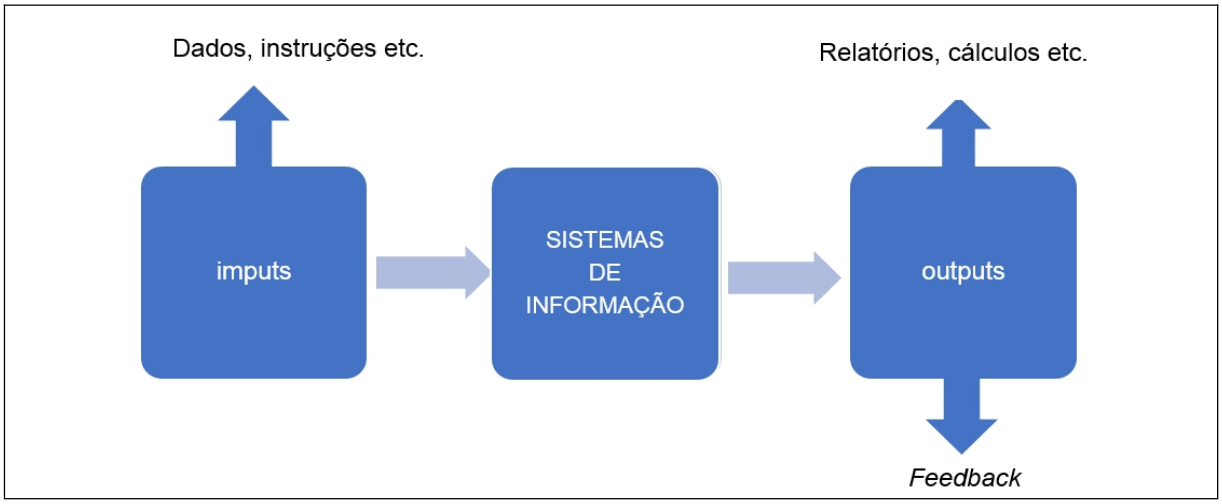
Para uma definição mais genérica de sistema de informação, vale citar o entendimento de Rezende e Abreu (2000), que apontam para o fato de que todo sistema, quer usem ou não a Tecnologia da Informação, desde que manipule e disponibilize a informação, pode ser considerado um sistema de informação. Isto posto, aponte-se que para uso neste trabalho, o termo "sistema de informação", refere-se ao computadorizado, uma vez que as informações e a segurança delineados nesse estudo são de natureza informática.

Assim, vamos utilizar o plural, porque se tratam de vários sistemas de informação, que em sua modalidade informática, podem ser classificados como: abertos e fechados. Portanto, "[...]os sistemas fechados não interagem como ambiente externo, enquanto que os sistemas abertos caracterizam-se pela interação

com oambiente externo, suas entidades e variáveis" (PADOVEZE, 1997, p.36), enquanto podem ser classificados de acordo com aforma de utilização, bem como o tipo de retorno que a organização busca. Podendo ser: operacional ou gerencial.

Para Stair (1998, p. 11), "[...] sistemas de informação é uma série de elementos ou componentes inter-relacionados que coletam (*imputs*), manipulam e armazenam (processo), disseminam (*outputs*) os dados e informações e fornecem um mecanismo de feedback".Na Figura 6, mais adiante, pode ser visto um esquema básico que dá corpo ao entendimento de um sistema de informação.

Figura6 -Esquema das informações e a sequênciados sistemas



Fonte: Stair (1998), Turban*et al*., (2007) (adaptado).

Já Gil (1999, p.14), define que "[...] os sistemas de informação compreendem um conjunto de recursos humanos, materiais, tecnológicos e financeiros agregados segundo uma sequência lógica para o processamento dos dados e a correspondente tradução em informações".

A dimensão humana dos sistemas de informações se dá a partir da interação das pessoas com os sistemas, haja vista a necessidade de alimentá-los com dados e também através da sua rotina na organização. Embora a presença da tecnologia se faça cada vez mais sentida no ambiente doméstico.Portanto, parte das necessidades das pessoas e dos ambientes organizacionais a urgência dos sistemas de informações. Entendendo que:

> Com o Sistema de Informação estruturado a apresentação das informações necessárias e também já propiciando uma visão das

> decisões, a empresa garante um grande diferencial em relação aos concorrentes, e os gestores podem tomar decisões mais rápidas e de fontes seguras. A exigência do mercado competitivo, dinâmico e principalmente globalizado motiva as empresas a operarem com um sistema de informação eficiente, garantindo níveis mais elevados de produtividade e eficácia(BAZZOTTI; GARCIA, 2006, p.10).

O que significa dizer, segundo Bazzotti e Garcia (2006), que na era da informação, o diferencial das empresas e dos profissionais está diretamenteligado à valorização da informação e do conhecimento, proporcionando soluções e satisfaçãono desenvolvimento das atividades. Sem querer se pretender reducionista, mas de forma mais genérica, a expressão ‘sistemas de Informação’ é a expressão utilizada para descrever um Sistema seja ele automatizado (que pode ser denominado como Sistema Informacional Computadorizado), seja manual, analógico ou através de apontamentos, que abrange pessoas, máquinas e/ou métodos organizados, que constituem informação para o usuário e/ou cliente.A partir de então, é necessário que se adquira consciência não só do valor da informação, bem como reconhecer que os sistemas de informação carecem de infraestrutura.

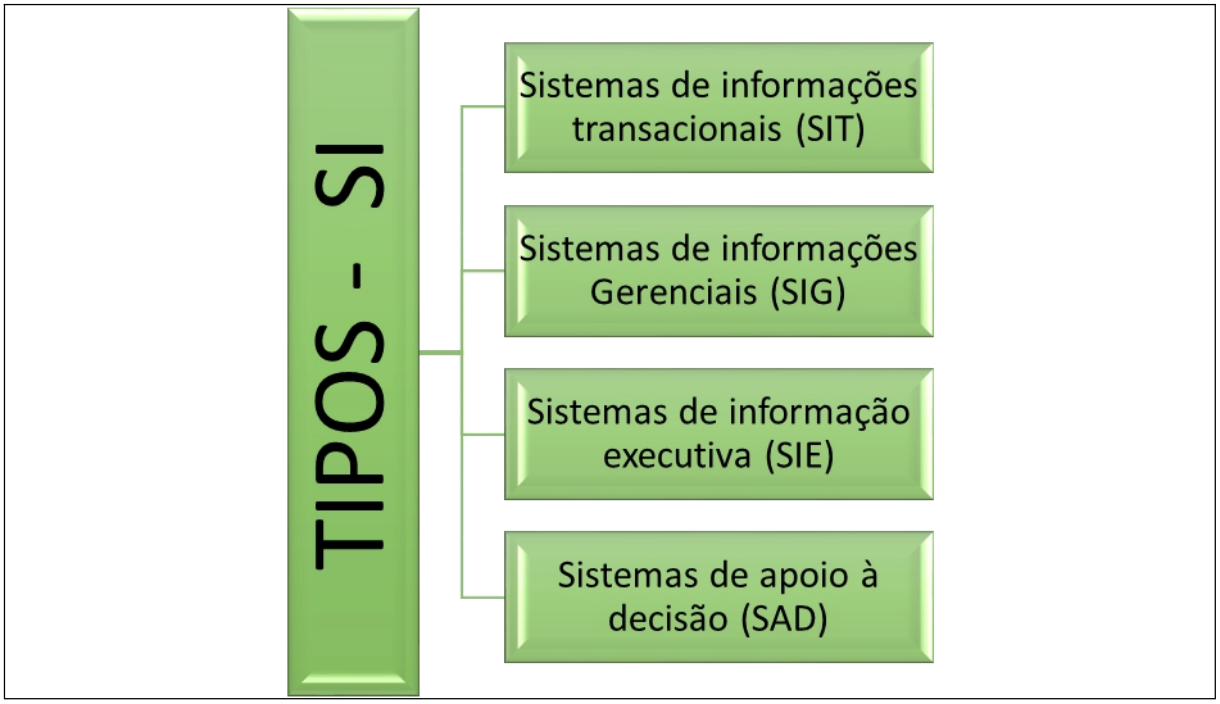
Segundo Turban*et al* (2007),, a infraestrutura de informação são as instalações que dão suporte para o seu funcionamento, ou seja, as instalações físicas, os serviços e o gerenciamento que tornam possível o funcionamento dos recursos computacionais em uma organização. Em geral, os componentes principais na infraestrutura são: *hardware*, *software*, redes e instalações de comunicação (incluindo internet), banco de dados e o pessoal técnico responsável pelo funcionamento dessa estrutura.Ainda de acordo com o pensamento dos autores o sistema de informação coleta, processa, armazena, analisa e dissemina informações voltado para um determinado contexto, porém como regra geral, inclui inputs (dados, instruções) e outputs (relatórios, cálculos). Para Laudon; Laudon (1999),Bazotti; Garcia (2006), os componentes que formamum sistema de informação é um conjunto de componentes que permitem coletar, recuperar, processar, armazenar e distribuir informações, com o objetivo de facilitar a vida da empresa/organização/instituição através do planejamento, coordenação, tomada de decisões, dentre outras coisas.

Em que pese a classificação dos sistemas de informação e, em se tratando de um contexto de segurança dos sistemas de informação, que é o objeto dessa proposta de trabalho, cabe dizer que de maneira simples, embora não haja intenção

em ser reducionista, mas sendo prático e o mais objetivo,podem ser classificados, segundo os seus princípios como: formais ou informais, enquanto que a sua tipologia pode ser identificada em 4 tipos distintos:sistemas de informação transacionais, sistemas de informaçõesgerenciais, sistemas de apoio a decisão e sistemas de informações executivas (O'BRIEN, 2004).

Os sistemas de informação, sobretudo, pela sua pluralidade e abrangência, o que novamente aparece aqui a importância do contexto. Para quê, para quem ou qual serviço/atividade ou questões afins, que porventura se faça. Objetivando clarificar de maneira didática, novamente vamos nos valer de O'Brien (2004), para através da Figura 7, dinamizar a apresentação, mostrando as tipologias apresentadas dos sistemas de informações.

Figura7 - Tipologia dos Sistemas de Informação



Fonte: O'Brien, 2004 (adaptada).

Diante do exposto e já reconhecendo o conceito, ainda que fluido, de sistemas de informação, tanto Araújo (1999), quanto O'Brien (2004), consolidam a afirmação de que o SI será o responsável por difundir as informações através da organização.Pela abrangência e dinamismo, deve ser flexível, fácil de usare lucrativo (ARAÚJO, 1999). Nesse diapasão e para dar sentido ao esquema no qual estão apresentados os SI mais presentes no nosso cotidiano, vale um pequeno quadro

explicativo, adiante, sinalizado como Quadro 3, no qual a primeira coluna aponta o tipo de sistema e a segunda descreve a sua função. Vejamos:

Quadro 3 - Tipos de Sistemas de Informação

TIPOLOGIA - SI	
Sistemas de informações transacionais (SIT)	São as informações rotineiras efetuadas, como por exemplo, emissão de notas fiscais,emissão de pedido, compra de mercadoria, etc. Essas informações normalmentealimentam um banco de dados para futuras consultas.
Sistemas de informações Gerenciais (SIG)	Geram informações que apoiam muitas das necessidades dos sistemasde tomada de decisão da administração. Os relatórios, telas e respostas produzidaspor esses sistemas fornecem informações para os gerentes para o adequadoatendimento de suas necessidades de informação. Esses produtos de informaçãopredefinidos satisfazem as necessidades de informação dos tomadores de decisãodos níveis operacionais e táticos, que encontram tipos de situações de decisão maisestruturados.
Sistemas de apoio à decisão (SAD)	Dizem respeito às decisões que devem ser tomadas em um ambiente complexo, queenvolve várias variáveis: localização de fornecedores, localização de clientes,impostos, política. Como exemplo, podem ser citados, a localização de uma novafábrica de automóveis ou onde deve ser montado um novo curso.
Sistemas de informação executiva (SIE)	Os sistemas de informação executiva possuem funções dos sistemas de apoioa decisão e dos sistemas de informações gerenciais. Geralmente essas informaçõessão disponibilizadas em um ambiente fácil e direto para que os executivos daempresa possam rapidamente obter uma informação.

Fonte: O'Brien (2004); Araújo (1999) (adaptado).

Longe de fornecer um conceito acabado, mas seguindo em busca de inovações, muito mais importante do que conceituar é perceber o que significa em termos de importância e a sua aplicabilidade nos mais diversos setores.Assim os sistemas de informação recebem atenção por constituírem uma parte essencial para o funcionamento da organização, seja de qual natureza for, não se concebe a sociedade sem a informação nos dias de hoje, praticamente não há. A partir de então, seguindo em busca dos mecanismos, da relevância e necessidade da segurança para os sistemas de informação das Forças Militares do país, fica disposto que o padrão ISO 27001, é de longe o que melhor responde aos preceitos de qualidade e excelência na Segurança dos Sistemas de Informação.

4 CONSIDERAÇÕES FINAIS

Todo trabalho científico, por melhor estruturado e por mais extensa pesquisa que seja feita, sempre será um olhar que vai envolver o pesquisador. No seu direcionamento profissional, da área à qual pertence e até a sua vida pessoal.Como efetivo da Marinha e aluno concluinte de Sistemas da Informação, apresentei nessa pesquisa aquilo que é preocupação, tanto no que diz respeito a instituição quando nos procedimentos em busca de melhor segurança dos sistemas de informação.

Ao traçar os objetivos deste trabalho, com projeto aprovado pelo orientador Ms. Hercílio Medeiros, procurei ser o mais fiel possível na apresentação dos objetivos, pois neles foram baseadas as informações que passei a adquirir para a construção do tema. Assim, trabalhar a segurança dos sistemas de informação em ambiente militar, em um trabalho de conclusão de curso – TCC, significa “começar do início”. Portanto, nessa caminhada alguns conceitos foram importantes: informação, sistemas de informação e segurança dos sistemas de informação.

Naquilo que é o entendimento desses conceitos que interligam-se, também se buscou o estudo dos padrões de qualidade para os sistemas de informação, bem como para a segurança destes. Por se tratar de uma proposta de qualidade e excelência, uma vez que a segurança dos sistemas de informação no contexto militar, vai também passar pelo entendimento daquilo que é mais caro a uma nação, a um país, a um povo, a soberania nacional.

Podemos perceber que já há uma preocupação do governo brasileiro, no sentido de buscar através das portarias e normativas, melhor controle do trato das informações e das tecnologias informáticas, ou seja, não só no sentido de armazenagem, como também no que abrange os aspectos comunicacionais com o mundo virtual.

Nesse entendimento e diante da preocupação do Estado Brasileiro, achamos por bem estabelecer uma análise dos parâmetros de qualidade ISO, delineando de forma detalhada a caminhada em busca de qualidade, empreendida por aqueles que estão envolvidos com a segurança de modo eficaz, efetivo e funcional.

Independentemente de qualquer normativa, a segurança dos sistemas de informação é uma premissa que diz respeito às garantias do cidadão, é uma questão

de privacidade. No entanto, quando isso passa para um contexto maior, que é a defesa nacional, que depende da segurança nacional, obviamente, vai adquirir um peso ainda maior, mesmo considerando que segurança não deve ser mensurável, pois, se trata de um conceito subjetivo que abrange multidisciplinaridade, ou seja, o que é segurança para uns, pode ser insegurança para outros, e vice-versa.

Ao sugerir o padrão de qualidade e excelência ISO 27001 para o tratamento da segurança dos sistemas de informação do Ministério da Defesa, procurou-se objetivamente compreender que de forma genérica as normativas federais vão ditar as regras de forma genérica, mas que cada Força Militar, possa atribuir um padrão próprio, segundo as normativas e portarias, procurando cada uma, à sua maneira, o melhor tratamento da questão.

Assim, procurando responder aos objetivos proposto, esperamos ter respondido de maneira efetiva, o nosso entendimento de segurança voltado para assegurar o melhor uso e operacionalidade das informações dessas instituições, no uso dos sistemas de informação.

REFERÊNCIAS

ARAÚJO, Nonata Silva. **Segurança da Informação** (TI). Disponível em:< http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/>. Acesso em 10 de set, de 2018.

BAZZOTI, Cristiani. GARCIA, Elias. A importância do sistema de informação gerencial na gestão Empresarial para tomada de decisões. **Revista UNIOESTE**, 2006.

BRASIL. MINISTÉRIO DA DEFESA. **Portaria Normativa 2.327/MD**, de 28 de outubro de 2015.

____. Exército Brasileiro. **Portaria nº 006-DCT**, de 05 de fevereiro de 2007. Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (NORTI). Departamento de Ciência e Tecnologia, 2007.

____. Exército Brasileiro. **Instruções Gerais de Segurança da Informação para o Exército Brasileiro** (IG 20-19). Portaria nº 483, de 20 de setembro de 2001. Exército Brasileiro, 2001.

____. **Decreto nº 4.553**, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Lex: Diário Oficial da União de 30 de dezembro de 2002, p. 6. Legislação Federal e marginalia.

____. Senado Federal. **A sociedade e as Forças Armadas**: debate sobre militares, defesa nacional e segurança pública no Brasil. Disponível em: https://www.senado.gov.br/NOTICIAS/JORNAL/EMDISCUSSAO/defesa-nacional/sociedade-armadas-debate-militares-defesa-nacional-seguranca.aspx. Acesso em: 28 de novembro de 2018.

CAMPOS, André L. N. **Sistema de Segurança da Informação**: Controlando os Riscos. Florianópolis: Visual Books, 2006.

CASTELLS, M. **A sociedade em rede**. A era da informação: economia, sociedade e cultura. 6. ed. São Paulo: Paz e Terra, 2002. v.1.

CARUSO, Carlos A.A; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**. 2ª Ed.rev.eampl. São Paulo: Editora SENAC, 1999.

CORNACHIONE Jr., Edgard B. **Informática aplicada às áreas de contabilidade**, administração e economia. 2. ed. São Paulo: Atlas, 1998.

CHIAVENATO, Idalberto. **Administração**: Teoria, Processo e Prática. 3. ed. São Paulo: Pearson Education do Brasil, 2000.

DAVENPORT, Thomas H; PRUSAK, Laurence. **Conhecimento empresarial**. Tradução de Lenke Peres. Rio de Janeiro: Campus; São Paulo: Publifolha, 1999.

DE SORDI, J. O. **Administração da Informação**: fundamentos e práticas para uma nova gestão do conhecimento, São Paulo: Saraiva, 2008.

JANNUZZI, Celeste Aída Sirotheau Corrêa; FALSARELLA, Orandi Mina; SUGAHARA Cibele Roberta. Sistema de informação: um entendimento conceitual para a sua aplicação nas organizações empresariais. In: **Perspectivas em Ciência da Informação**, v.19, n.4, p.94-117, out./dez. 2014. Disponível em: http://www.scielo.br/pdf/pci/v19n4/a07v19n4.pdf> Acesso em 29 de agosto de 2018.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**. 4. ed. LTC: Rio de Janeiro,1999.

____. **Sistemas de Informação Gerenciais**. São Paulo:Pearson Prentice Hall, 2010.

MESSIAS, Lucilene Cordeiro da Silva. **Informação**: um estudo exploratório do conceito em periódicos científicos brasileiros da área de Ciência da Informação. [Dissertação] Mestrado em Ciência da Informação. Universidade Estadual Paulista – UNESP. Marília, 2005. 197 f.

MÓDULO SECURITY SOLUTIONS S.A. **9ª Pesquisa Nacional de Segurança da Informação**. Rio de Janeiro, 2003. Disponível em: http://www.modulo.com.br/media/9a_pesquisa_nacional.pdf. . Acesso em 26 de novembro de 2018.

MÓDULO Technology for GRC. Governance Risk andCompliance. **10ª Pesquisa Nacional de Segurança da Informação**. 2006. Disponível em:

http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf. Acesso em 26 de novembro de 2018.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em ambientescooperativos**. São Paulo: Editora Futura, 2003.

O'BRIEN, JAMES A. **Sistemas de Informação e as Decisões Gerenciais na Era da Internet** – São Paulo: Saraiva, 2004.

____., MARAKAS, G. M. **Administração de Sistemas de Informação**.15ed. Porto Alegre: AMGH/McGraw-Hill/Bookman, 2013.

OLIVEIRA, Gabriella., MOURA, Rafaela K., ARAÚJO, Francisco de Assis. Gestão da segurança da informação: perspectivas baseadas na tecnologia da informação (T.I.). In: **Anais** do Encontro Regional dos Estudantes de Biblioteconomia, Documentação, Ciência e Gestão da Informação. Belo Horizonte. Jan. 2012. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/moci/article/viewFile/2111/1311. Acesso em 09 de setembro de 2018.

OSTEC. **Padronização e segurança**. 2016.Disponível em: <ostec.blog/padronizacao-seguranca/primeiros-passos-iso-27000> Acesso em 21 de outubro de 2018.

PADOVEZE, C. L. **Contabilidade Gerencial** – Um enfoque em sistema de informação contábil. 3. ed. São Paulo: Atlas, 1997.

SOUZA, Flávia R., MELHADO, Silvio B. A importância do sistema de informação para a gestão das empresas de projeto. **Revista Gestão & Tecnologia de Projetos**. Vol. 3, no. 1, maio de 2008, pp. 121-139.

STAIR, R. M.; REYNOLDS, G. W. **Princípios de Sistemas de Informação**. Anais...São Paulo: CENGAGE, Tradução da 9. ed. Americana, 2010.

TAIT, T. F. C. **Um Modelo de Arquitetura de Sistemas de Informação para oSetor Público**: estudo em empresas estatais prestadoras de serviços deinformática. Florianópolis: 2000. 227 f. Tese (Doutorado em Engenharia deProdução) - Centro Tecnológico, Universidades Federal de Santa Catarina.

TURBAN, E; MCLEAN, E; WETHERBE, J. **Tecnologia da informação para gestão**. Transformando os negócios da economia digital. 3°Edição. Porto Alegre. Editora

Bookman, 2004.

____.; RANIER JR., R. K.; POTTER, R.E. **Introdução a sistemas deInformação uma abordagem gerencial**. Tradução Daniel Vieira. Rio de Janeiro: Elsevier, 2007.

TURBAN, E.; RAINER JR., R.K.; POTTER, R.E. Administração de Tecnologia da Informação. **Teoria & Prática**. Rio de Janeiro: Campus, 2005.