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

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SISTEMAS DE INFORMAÇÃO E COMUNICAÇÕES

PRIMEIRO-TENENTE DIEGO DA SILVA CESPES

OS RISCOS E DIFICULDADES DA INTRODUÇÃO DA TECNOLOGIA DE COMPUTAÇÃO EM NUVEM NA MARINHA DO BRASIL.

Rio de Janeiro
2018

PRIMEIRO-TENENTE DIEGO DA SILVA CESPES

OS RISCOS E DIFICULDADES DA INTRODUÇÃO DA TECNOLOGIA DE COMPUTAÇÃO EM NUVEM NA MARINHA DO BRASIL.

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

Orientadora:
Capitão de Corveta (T) Kátia Cristina Altomare Silva

CIAW
Rio de Janeiro
2018

PRIMEIRO-TENENTE DIEGO DA SILVA CESPES

OS RISCOS E DIFICULDADES DA INTRODUÇÃO DA TECNOLOGIA DE COMPUTAÇÃO EM NUVEM NA MARINHA DO BRASIL.

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

Aprovada em 12 de junho de 2018.

Banca Examinadora:

CC (T) Kátia Cristina Altomare Silva (orientadora)

CMG (RM1-EN) Gian Karlo Huback M. de Almeida

Guilherme Colen, DSc - CIAW

CIAW
Rio de Janeiro
2018

Dedico esse trabalho À Deus, Aquele que muito me têm ajudado e abençoado nesta jornada, dando-me forças para que o foco na conclusão do presente curso nunca se perca e permitindo que o aprendizado adquirido influencie positivamente sempre minhas ações a partir de então.

AGRADECIMENTOS

À Deus, primeiramente, por proporcionar-me o dom da vida e abençoar-me com saúde e força para enfrentar os percalços deste caminho, permitindo que o objetivo final fosse alcançado.

À minha amada e estimada esposa, pela dedicação e por sempre se colocar ao meu lado, auxiliando cada detalhe e cada passo na jornada da vida. Agradeço por todos os momentos de incentivo e motivação, acreditando sempre no meu trabalho e na minha dedicação em prol da família.

Aos meus saudosos pais, que tanto se esforçaram ao longo de tantos anos para que eu pudesse absorver o máximo de conhecimento através dos estudos, me proporcionando toda a infraestrutura possível, apesar das dificuldades, para que todo esse caminho rumo à eterna aprendizagem fosse permitido.

Aos meus demais familiares, que sempre que possível e necessário, se colocam acessíveis e dispostos a ajudar de diversas maneiras e nos pequenos detalhes.

À Marinha do Brasil (MB), por proporcionar mais este momento de aprendizagem e aperfeiçoamento, provendo recursos para que este trabalho fosse realizado.

À prezada orientadora acadêmica, Capitão de Corveta (T) Kátia Cristina Altomare Silva, que apesar dos seus diversos afazeres e tarefas junto à Diretoria de Comunicação e Tecnologia da Informação da Marinha (DCTIM), sempre que necessário e requerida para auxílio, mostrou-se disponível para a mitigação de dúvidas e transmissão de conhecimento, além da permissão da utilização de sua excepcional dissertação de mestrado e de seu artigo, enriquecendo sobremaneira o referencial bibliográfico do presente estudo.

À Diretoria de Comunicação e Tecnologia da Informação da Marinha (DCTIM) pelo acesso irrestrito à realização dos levantamentos inerentes ao estudo, disponibilizando-se sempre de portas abertas para que o contato com a orientadora e a área técnica fosse possível.

Ao professor Helios Malebranche por todas as aulas e dicas para uma melhor realização e padronização desta monografia, auxiliando, de maneira certeira e eficaz, junto às regras da Associação Brasileira de Normas Técnicas (ABNT).

Aos demais professores da Pontifícia Universidade Católica do Rio de Janeiro (PUC-RIO), pela presteza na mitigação de dúvidas e questionamentos que envolviam, direta ou indiretamente, os assuntos afetos a este trabalho, contribuindo para a referênciação e o balizamento dos estudos da *cloud computing*.

Aos amigos e companheiros de turma que, durante esses nove meses, puderam intercambiar conhecimentos, demonstrando grande companheirismo e amizade.
À banca examinadora, pelo exame minucioso do trabalho, contribuindo com subsídios e sugestões de melhorias deste estudo.

“A maior recompensa para o trabalho do homem não é o que ele ganha com isso,
mas o que ele se torna com isso” John Ruskin

OS RISCOS E DIFICULDADES DA INTRODUÇÃO DA TECNOLOGIA DE COMPUTAÇÃO EM NUVEM NA MARINHA DO BRASIL.

Resumo

O mundo, como conhecemos, encontra-se em constante metamorfose, e como um dos principais produtos desta transformação, destaca-se a virtualização da computação, o que proporciona um aumento exponencial da utilização da computação em nuvem. Estar alheio a uma tão relevante mudança, não demonstra ser o melhor caminho a ser seguido, haja vista os benefícios proporcionados por tal tecnologia. Nesse contexto, a Marinha do Brasil (MB) possui a necessidade de acompanhar esse desenvolvimento, para que sua missão, como Força Armada de um país extremamente importante no cenário internacional, seja cumprida em sua completude. Por tanto, adotar planejamentos que visam proporcionar a melhoria dos serviços ao país, torna-se imperativo e, dessa maneira, valer-se de uma política de inserção da *cloud computing*, utilizando-se de seus recursos e benefícios na sua totalidade, demonstra um grande passo rumo ao futuro. Ou seja, utilizar-se dessa importante tecnologia nos seus diversos campos de atuação e das mais diversificadas maneiras possíveis, podem propor um nível de evolução sem precedentes à Força, empregando o uso de nuvens privadas, públicas, comunitárias e híbridas, de acordo com a necessidade imposta pela ocasião. Entretanto, utilizar-se de tais recursos, requer um mais elevado índice de prevenção e controle, objetivando a segurança e a proteção nesse novo âmbito de atuação da computação, criando barreiras frente a possíveis atuações nocivas, sejam de origem externa ou interna, e desse modo adotar políticas de segurança, através de Acordos de Nível de Serviço de Segurança *(Security Service Level Agreements – Sec-SLA)* confiáveis e capazes de abranger toda a demanda necessária da Força, para garantia da proteção das informações que afetam diretamente a Segurança Nacional. Este estudo propõe, portanto, as principais preocupações e modos de avaliar o caráter de aplicação dessa tecnologia, de maneira ampla e genérica, de acordo com os interesses da MB.

Palavras- chave: *Cloud Computing*, Nuvem, Segurança, Sec-SLA, Marinha do Brasil.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTAS DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ARQ	Arquitetura
CAPEC	*Common Attack Pattern Enumeration and Classication*
CEO	*Chief Executive Officer*
CONF	Conformidade
CIAW	Centro de Instrução Almirante Wandenkolk
CS&C	Escritório de Segurança Cibernética e Comunicações
CTIM	Centro de Tecnologia da Informação da Marinha
CVSS	*Common Vulnerability Scoring System*
DCTIM	Diretoria de Comunicação e Tecnologia da Informação da Marinha
FFAA	Forças Armadas
$FP_{nível}$	Faixa de Probabilidade(níveis)
$FR_{nível}$	Faixa de Risco(níveis)
$FS_{nível}$	Faixa de Severidade(níveis)
IaaS	*Infraestruture as a Service*
Internet	*Internacional Network*
MB	Marinha do Brasil
MPLS	*Multi-Protocol Label Switching*
NC	Nuvem Comunitária
NCL	Nuvem Comunitária Local
NCT	Nuvem Comunitária Terceirizada
NH	Nuvem Híbrida
NP	Nuvem Pública
NPr	Nuvem Privada

NPL	Nuvem Privada Local
NPT	Nuvem Privada Terceirizada
NVD	*Nacional Vulnerability Database*
PaaS	*Platform as a Service*
PRI	Privacidade
PUC-RIO	Pontifícia Universidade Católica do Rio de Janeiro
RECIM	Rede de Comunicações Internas da Marinha
SaaS	*Software as a Service*
Sec - SLA	*Security Service Level Agreement*
S_i	$Subcategorias_i$
SIC	Segurança da Informação e Comunicações
SLA	*Service Level Agreement*
SWA	*Software Assurance*
TI	Tecnologia da Informação
VM	*Virtual Machines*

SUMÁRIO

1. INTRODUÇÃO

No mundo em que vivemos, possuir acesso irrestrito a diversas e variadas aplicações através da internet, em qualquer lugar e a qualquer momento, é um desejo muito comum entre os usuários de equipamentos eletrônicos em geral, nas diversas plataformas como: *tablets*, celular, *notebooks* e etc.

A tecnologia de computação em nuvem permite que esse acesso e as possibilidades de utilização da internet seja amplificado, pois tal conceito engloba a utilização das plataformas, como se estas possuíssem todos os recursos disponíveis instalados em ambientes locais, tudo isso graças ao processo de virtualização.

A computação em nuvem, portanto, tem como principal característica, possuir unidades de processamento separadas e independentes, que através da conexão e gerenciamento entre redes, possui a capacidade de realizar o processamento das aplicações requeridas em diferentes estações ou servidores, apresentando todo o processo de maneira visível e transparente ao seu usuário final.

Como característica dessa tecnologia, podemos elencar também, a transferência da responsabilidade de gestão, gerência, manutenção, atualização e etc. das mãos dos usuários finais ou centro local de controle de dados, para que provedores terceirizados possam realizar essas tarefas como atividade fim. Com isso, empresas e usuários não possuem mais a necessidade de investir em equipamentos sofisticados que permitam essa gerência, já que, pagando uma mensalidade ao provedor de sua escolha, pode se utilizar dos recursos disponíveis em nuvem apenas possuindo acesso aos recursos oferecidos pelo provedor escolhido.

Podemos, desta forma, entender a adoção da tecnologia de computação em nuvem, como uma maneira de economizar recursos, pois com a redução dos investimentos em Tecnologia da Informação (TI), além de eximir a necessidade de monitorar e gerir uma grande quantidade de dados, não exige a necessidade de investimento da infraestrutura e de sua eventual modernização, já que estas funções ficam a cargo do provedor contratado.

Apesar disto, a mudança para uma nova tecnologia abre um leque de problemas a serem solucionados. Para que, tanto a implementação quanto a manutenção e segurança desses serviços sejam feitas de maneira satisfatória, existe a necessidade de se fazer uma profunda análise do provedor de serviços em nuvem, permitindo segurança por ocasião da utilização dos serviços, ainda mais quando um usuário potencial é uma Força Armada de um país.

Portanto, os parâmetros para escolha de um provedor ideal aos sistemas da Marinha do Brasil (MB), além de permitir verificação do índice de confiabilidade de um provedor, propicia a identificação de qual melhor se adequa às necessidade das demandas da organização.

Leva-se em conta nesse estudo, ainda, as peculiaridades da MB frente ao desenvolvimento tecnológico, apresenta-se como relevante questão, o ponto de conexão com provedores e a escolha destes, já que a proteção de informações de cunho estratégico-operacional e sensíveis à segurança nacional da nação constitui o objetivo final do uso desta tecnologia. Portanto, torna-se imperativo definir métodos de alocação, visando uma classificação e diversificação da aplicação da tecnologia propriamente dita para uma transição segura, sem proporcionar maiores problemas.

1.1 Apresentação do Problema

O tema escolhido expõe análises de riscos e estudos que possam identificar os impactos que uma nova tecnologia pode oferecer à segurança da informação digital.

Cotidianamente, como podemos presenciar, surgem novas invenções tecnológicas que modificam completamente a segurança da informação em vigor, quando nos referimos ao mundo digital, e tudo isso ocorre cada vez mais repentina e velozmente.

Como tema escolhido, a análise de riscos e segurança da computação em nuvem é de grande importância, uma vez que a tecnologia de informação como banco de dados na nuvem, por exemplo, aparece como uma alternativa extremamente eficiente e eficaz no papel que procura cumprir, dando celeridade aos processos, desburocratizando sistemas e criando ambientes não físicos para armazenamento de dados e gerenciamentos de bancos de dados. Essa tecnologia se apresenta como forte aliada à utilização de dados em larga escala por grandes organizações, já que possuem uma enorme massa de dados para processamento em pouco tempo e até mesmo, insuficiente espaço físico para geri-lo da melhor maneira possível.

Desta maneira, a evolução e simplicidade de acesso permitido pela nuvem é, de fato, extremamente bem-vinda e almejada por diversos perfis de usuários. Entretanto, não se pode considerar que todos os problemas são sanados com esta nova tecnologia, pelo contrário, novas tecnologias geram novos problemas que, na maioria das vezes, surgem maiores e mais complexos do que problemas anteriores.

Portanto, há que se ter em mente que, aliado a essas inúmeras vantagens e benefícios, surgem vulnerabilidades que podem influenciar diretamente a segurança digital dos usuários da nuvem. E os problemas não se esgotam somente na fase de utilização.

Umas das principais dificuldades, reside na instalação e adaptação de um novo cliente a este novo ambiente, onde a segurança já necessita de cuidados para que toda a implementação não seja comprometida.

Assim, este estudo torna-se direcionado a analisar e verificar os riscos que se apresentam diante da Marinha do Brasil frente a possível implantação desta tecnologia aos seus sistemas e o quão difícil e custoso seria aderir a uma implementação diversificada da tecnologia em questão, levando em consideração a totalidade do projeto e os parâmetros básicos e imprescindíveis de segurança.

1.2 Justificativa e Relevância

A computação em nuvem é uma realidade no mercado e encontra-se em vultuosa expansão, ganhando mercado e criando demandas jamais previstas pelos seus primeiros desenvolvedores. Devido às diversas possibilidades e segurança que esta tecnologia pode oferecer, micro, médias e grandes empresas juntam-se às multinacionais e investem cada vez mais, buscando migrar informações de seus negócios para a nuvem em diversos níveis, intentando potencializar vendas e aumentar os lucros, haja vista que a burocracia diminui e a produtividade aumenta.

Entretanto, a migração para esse sistema deve ser feita de maneira extremamente cuidadosa e planejada, onde a segurança seja primordial, havendo uma evolução sustentável e um sistema não vulnerável às cotidianas ameaças, diminuindo substancialmente os riscos de possíveis invasões ou ataques à rede compartilhada, já que tais incidentes podem colocar em risco toda a integridade digital da instituição.

Para a implantação dessa tecnologia na MB, é necessário conhecer a real necessidade de se adotar tal tecnologia para que não haja desperdício dos proventos da União, já que o país encontra-se passando por severas crises econômicas e, gastos desnecessários e impensados, somente aumentariam o déficit público.

Outro ponto a se atentar é a utilização de um SLA (*Service Level Agreement*), ou Acordo de Nível de Serviço, que nada mais é do que um contrato contendo todas especificações dos serviços oferecidos pelo provedor de prestação de serviço. Este contrato é firmado entre

este provedor e a empresa. Com este documento, pode-se prever os resultados que são esperados, em quanto tempo as atividades serão executadas, quem serão os responsáveis por cada setor de gerenciamento e a finalidade de cada um desses gerentes.

Essa falta de avaliação de todas as variáveis envolvidas no processo é o grande erro de muitas empresas que tentam utilizar-se dessa tecnologia e, com isso, acabam gerando gastos desnecessários, pois contratam um serviço mais caro e custoso que suficiente para atender suas necessidades. Tempo disponível para cada atividade, prazos, escalabilidade, plano de ação, praticas à segurança da TI, garantias e desempenho são algumas das variáveis que também são estudadas e avaliadas para contratação de um serviço de computação em nuvem junto ao provedor.

Outro erro fatal encontrado na implementação da *cloud computing* ocorre na gestão do sistema em si. É fato irrefutável que má gestão de segurança pode tornar toda a documentação e informação armazenada na nuvem vulnerável a ataques e assim comprometer toda integridade das informações acessadas gerando problemas administrativos e, no caso de tal tecnologia ser empregada à MB, informações de cunho estratégico-operacionais poderiam ser acessadas por indivíduos ou entidades não autorizados, devidamente, colocando em risco a Segurança Nacional.

Fato é, também, que o mundo da informática e ambientes virtuais passa por transformações diárias, propiciando, a cada instante, o surgimento de novos atores, perigos, riscos etc.

Algumas dessas evoluções são extremamente benéficas e bem vindas para a gestão de informação e quebra paradigmas por potencializarem a produtividade, permitindo ao usuário final uma acessibilidade antes nunca imaginada, além de novos parâmetros de segurança e um incrível poder de redução dos períodos gastos com tratos burocráticos e desnecessários, demonstrando, a cada dia, a capacidade de resolver problemas que muito pouco tempo atrás se manifestavam como insolúveis.

A tecnologia de computação em nuvem é uma extraordinária evolução, pois propicia o acesso à informação digital de qualquer lugar do planeta sem a necessidade de investimento em armazenamento físico, por parte da empresa contratante. Permitindo, desse modo, que qualquer usuário possa trocar informações e documentos, sem a preocupação de tempo, capacidade ou espaço de armazenamento. Tais benefícios fazem aguçar o interesse não só de corporações com fins lucrativos, já que a gestão de informações aplica-se ao mundo moderno em geral, e é de suma importância para a gerência de pessoal, seja em organizações de capital privado ou organizações do poder público.

Fazer-se valer da gerência de dados remota, acessando a informação desejada de qualquer lugar do mundo, a qualquer momento, necessitando apenas de acesso à internet, é sobremaneira atrativo e de valia incomensurável às Forças Armadas. Não somente pela singularidade da sua missão de proteção da pátria em todos os sentidos, inclusive ciberneticamente, mas pela facilidade administrativa como a gerência de contratos com empresas terceirizadas no país ou no exterior, além da gestão de seu pessoal, seja civil ou militar.

Inserindo-se essa tecnologia no ambiente de informação digital da MB, pode-se impulsionar a Força a elevados patamares de tecnologia no que se diz respeito a gestão e gerenciamento de banco de dados compatíveis com o sigilo da informação, provendo grande interconectividade entre as diversas Organizações Militares pertencentes a MB.

É importante, entretanto, salientar, que o puro uso desta tecnologia não se sustenta unicamente como inibidora de todos os problemas digitais da MB, mas pluraliza soluções e amplia os horizontes de expansão da Força rumo à interligação com o que existe de mais moderno em computação no mundo moderno, impulsionando o desenvolvimento cibernético das Forças Armadas do país.

1.3 Objetivos

Como objetivos traçados para a realização deste estudo, pode-se elencar objetivos distintos, sendo o Objetivo Geral como um foco de generalização de busca por meio da presente dissertação, e os Objetivos Específicos sendo aqueles que precisam ser alcançados para que o foco final do estudo seja alcançado, sendo relevante de alguma maneira pelo resultado alcançado.

1.3.1 Objetivo Geral

Introduzindo-se a tecnologia da Computação em Nuvem à MB, processos e atividades tornam-se mais ágeis e com menos burocracia, além de proporcionar uma facilidade de acesso às informações compartilhadas de maneira única em qualquer parte do planeta, facilitando conexões e trocas de informação entre diversos segmentos em diferentes cidades, estados ou países.

Adotar a computação em nuvem pode se tornar uma grande oportunidade para redução de investimentos e gastos em Tecnologia da Informação (TI) devido à sua flexibilidade.

Entretanto, introduzir uma tecnologia tão modificante e de efeitos com grande abrangência não é tarefa simples e, muito menos, possível de ser terminada em curto espaço de tempo. Há que se determinar todo o planejamento, desde a iniciação de intenções com o provedor à mais complexa atividade de gestão de segurança. Por isso, estudo, análise e previsões de problemas futuros são essenciais para uma transição rumo a uma nova tecnologia, independente de qual tecnologia seja aplicada.

Especificamente, o tratamento da adaptação da nuvem, pode-se fazer uma gradação dos níveis de segurança específicos para cada grau de complexidade de cada tarefa ou aplicação, levando-se em consideração todos os atributos relevantes ao gerenciamento de rede nos moldes tradicionais e como suas modificações irão impactar a resolução dos problemas da implementação da *cloud computing*.

Uma observação relevante após diversas análises levam à observância de certa preocupação com modelos que possam resolver e calcular a confiança dos provedores do serviço de computação em nuvem e assim, possa-se traçar paralelos entre os serviços prestados entre as diferentes empresas e qual o grau de confiabilidade pode-se alocar a cada uma delas, podendo analisar o perfil profissional de cada uma dessas empresas.

Pretende-se fazer um apanhado desses métodos e comentá-los avaliando a capacidade de previsão evidente dos métodos baseado nos parâmetros analisados.

Este estudo, portanto, tem por objetivo analisar os possíveis riscos à implementação da tecnologia em questão, permitindo que a MB possa, em um futuro próximo, desfrutar da *cloud computing*, tendo sempre em vista materiais e atividades que promovam esta segurança e possam, então, melhorar sua produtividade, executando da melhor maneira possível suas missões, garantindo que os seus objetivos sejam alcançados de maneira segura e eficiente.

1.3.2 Objetivos Específicos

Elencando-se determinadas diretrizes, pode-se alcançar o objetivo geral desse estudo, possibilitando um aplicação passo-a-passo da inicialização da introdução de uma maneira compatível desta tecnologia na MB, quebrando paradigmas de gestão e gerenciamento de dados.

As análises feitas serão de cunho específico e com foco na proteção dos ativos da informação contra invasões e acessos não autorizados, incluindo alterações indevidas que comprometem a integridade ou a total indisponibilidade do sistema como um todo por atuação de agente interno com intenções de prejudicar o tráfego de informações ou o acesso às mesmas.

Cada tipo ou modelo de nuvem será tratada separadamente devido as suas especificidades intrinsecamente desiguais, onde cada uma delas terá sua confiança medida de acordo com determinados aspectos como: arquitetura (ARQ), conformidade (CONF) e privacidade (PRI) relacionando à analises de literaturas utilizadas, considerando suas relações em categorias e suas subcategorias.

Será relacionado, também, os tipos de nuvem e como ocorrem sua implantação de serviço de acordo com cada categorização, elencando os agentes participantes das atividades de relevância para implantação, como por exemplo: Consumidor da Nuvem, Cliente da Nuvem, Provedor do serviço, Visibilidade e Controle. Além disso, definir os graus de relevância das medidas de segurança também possuem papel importante na análise deste estudo.

2. REFERENCIAL TEÓRICO

Dentre as diversas e relevantes bibliografias referenciadas para realização deste presente estudo, algumas foram de decisiva importância para a integração das ideias e encaixe do formato que se segue.

Dentre elas, pode-se destacar como principal basilar ao estudo que se propõe neste trabalho, a dissertação de Silva (2016) apresentada em [21] demonstra de maneira extremamente competente e com grande riqueza de detalhes o processo de consolidação da computação em nuvem no contexto da segurança da informação, como solução robusta e confiável. Analisando também as vulnerabilidades e riscos que a nova tecnologia carrega ao seu campo de atuação, correlacionando a capacidade de confiança dos provedores do serviço de *cloud computing*.

Em [8], Dan (2013) apresenta um artigo de extrema relevância ampliando os horizontes e apontando o riscos e vulnerabilidades em nuvens que prejudicam sua gestão e como pode-se prevenir ocorrências de relevante gravidade.

Já Badger (2012) exibe em [4], após um apanhado geral das generalidades envolvidas na implantação da nuvem como tecnologia, sugere soluções, recomendando a gerência desses ambientes.

Apresentando o código de prática para controles de segurança da informação em [1], explicitando as técnicas em questão que balizam a segurança em tecnologia da informação a nível nacional na atualidade, vale citar o uso da ABNT (2013).

Intentando exemplificar modelos de se fazer a verificação da confiabilidade dos serviços prestados no âmbito focal deste trabalho em [16], faz-se referência a Manuel (2013), onde registra-se a qualidade como orientação para a avalição da confiança do serviço provido.

Fazendo um apanhado geral e focalizando a segurança da informação como um todo, em [10], auxiliando em assuntos afetos à gestão estratégica de riscos aplicados à tecnologia da informação, temos a monografia de Freitas (2009), também aparece como subsídio a esta análise.

Temos, também, em [11] o trabalho de conclusão de curso de Gonçalves Júnior (2008), onde encontramos abordagens práticas para conscientização e implantação da mentalidade da segurança digital e de comunicações no mundo moderno.

Em [2, 20] elencam-se, ainda, as referências que foram utilizadas como apresentações nas aulas do Curso de Aperfeiçoamento Avançado para Oficias da Marinha do

Brasil (CAp-A) pela parceria PUC-Rio – CIAW, ministradas, respectivamente, pelo Professor Engenheiro de Computação e Mestre em Informática (PUC-Rio) Vitor Pinheiro de Almeida e pelo Professor Engenheiro de Computação Ph.D. em Ciências em Informática Anderson Oliveira da Silva.

Em [6], exibe-se, ainda, a relevante palestra ministrada pelo Capitão de Mar e Guerra da Marinha do Brasil, Carlos Rodrigo Cerveira, Superintendente de TI da DCTIM, apresentando a agenda desta Diretoria, demonstrando a real situação tecnológica da Marinha e como estão compartilhados e distribuídos seus sistemas de TI.

3. METODOLOGIA

Para a realização do estudo, levando em consideração a complexidade do tema, e como pode ser aplicado de forma efetiva e objetiva como referencial relevante para a implementação da tecnologia da computação em nuvem na MB, foram seguidas determinadas metodologias que se adequassem ao período disponível para os levantamentos e execução do trabalho.

Entregando, portanto, a metodologia mais indicada para a execução desta tarefa, segue a classificação da maneira como foi realizada a pesquisa em lide, para que o Objetivo Geral seja alcançado, deixando de modo claro como cada levantamento e informação foram obtidas e analisadas.

3.1 Classificação da Pesquisa

A presente dissertação possui classificação, analisando-se os fins e os meios.

3.1.1 Quanto aos fins

O referido estudo será alicerçado em análises explicativas e descritivas dos reais riscos à segurança de informação que assolam o planeta contemporaneamente, e como aplicar tais análises de maneira acessória à mentalidade de segurança de TI na MB.

Com a acelerada globalização prosseguindo em constante ascensão e a elevadas escalas nunca antes imaginadas, os perigos digitais se proliferam também a largos passos e criam um clima de apreensão constante aos usuários das redes de computadores em sua generalidade. Até porque, atualmente, a esmagadora maioria da população mundial se utiliza de recursos de informática e compartilha uma enorme massa de informações a todo momento nas redes e sub-redes espalhadas pelo planeta, criando vulnerabilidades sem precedentes.

Tal fato, expande horizontes para que os perigos e riscos aumentem de maneira exponencial, facilitando infiltrações indesejadas, proporcionando infestações de *virus*, *malwares*, *worms* e diversos outros programas maliciosos e nocivos que colocam em usuários em posição de temeridade e, por tal motivo, anseiam por ambientes mais seguros e livres de riscos às suas operações realizadas em rede.

O trabalho em lide busca explicitar analiticamente, descrevendo os estudos e pesquisas da área de segurança atrelada à tecnologia de *cloud computing*, que possam auxiliar o incremento da ideia de introdução desta tecnologia pela Marinha do Brasil, intentando subsidiar estudos de projetos futuros para a implementação efetiva.

Eleva-se, assim, a capacidade de compartilhamento de dados da Força, desburocratizando meios e aprimorando-a no sentido de prontidão cibernética, podendo ter elevado índice de segurança digital, ainda que se utilize de tecnologias sofisticadas e complexas.

3.1.2 Quanto aos meios

Como pode ser observado, vários trabalhos, pesquisas e estudos serão os fundamentos desta análise em questão. Cada conclusão, sugestão e avaliação será esmiuçada de maneira que surja, desta forma, uma relação que possa apontar caminhos e diretrizes das melhores ações e reações a serem seguidas para que o objetivo geral de possibilitar uma grande transformação no cenário atual da computação da MB, com a introdução de uma nova tecnologia que pode elevar os padrões de prontidão da Força a novos patamares.

Toda essa questão será tratada realizando-se uma profunda análise das excelentes Referências atreladas, teoricamente, possuindo um vetor bem determinado e um conjunto de diretrizes, intencionadas a subsidiar uma ideia de modernização dos atuais sistemas utilizados pela MB.

Desta maneira, a pesquisa bibliográfica será a fonte de subsídios para as conclusões e sugestões definidas, abrindo possibilidades de permitir reais propostas de melhorias e evoluções, com o intuito de aprimorar os sistemas da Força.

3.2 Limitações do Método

Após o balanço de todo o processo de análise executiva do trabalho, pode-se observar a complexidade do tema e como o assunto aponta para uma extensão inesgotável de informações, possibilidades e variáveis que exprimem a profundidade do assunto. E apesar de toda a análise ter sido realizada a miúde, torna-se praticamente impossível alcançar a totalidade de probabilidades de outros enfoques, metodologias e abordagens.

Torna-se dificultoso aplicar uma outra metodologia que não seja a utilizada. Até mesmo para uma revisão bibliográfica mais completa, haja vista os interesses do trabalho em questão. Entretanto, da melhor maneira possível, o método de avaliação e apreciação das excelentes bibliografias com conteúdos extremamente ricos e relevantes foi realizado.

Todos os objetivos esperados e desejáveis, ao fim deste estudo, são alcançados, tendo em mente o cabedal de conhecimento que torna-se enriquecido com a abordagem desse assunto, deixando evidente a necessidade de outros trabalhos futuros intencionados a complementar e expandir o conhecimento e, efetivamente, possibilitar o subsídio necessário à implantação concreta dos resultados obtidos, fruto de pesquisa e desenvolvimento, e possa-se expandir de maneira mais completa, focando em outras metodologias para que surja uma projeto sólido e real.

Desta maneira, espera-se que novas pesquisas e estudos penetrem a fundo na essência da execução prática do projeto, e que num futuro próximo, a MB possa usufruir da implementação da *cloud computing* nos seus sistemas.

3.3 Coleta e Tratamento de Dados

Conforme já demonstrado anteriormente, o presente estudo foca-se na análise bibliográfica das diversas referências indicadas, compilando uma gama de conhecimentos a despeito de segurança em computação em nuvem e procurando através do exame realizado, sugerir meios de iniciar um processo de incentivo à mentalidade de implantação dessa tecnologia nos sistemas informatizados da MB.

Dessa maneira, toda a coleta de dados se dará através das informações e análises contidas nas bibliografias utilizadas, visto que foram escolhidas de maneira extremamente criteriosa e possuem grande relevância de conhecimento comprovado e reconhecido.

Serão apresentados resultados de pesquisas e desenvolvimentos realizados por sondagens anteriores, moldando o perfil analítico deste trabalho e, desta maneira, poder gerar informações que possam subsidiar futuras pesquisas, disseminando e compilando os conhecimentos adquiridos através do exame das intenções de cada matéria de pesquisa referenciada

Com relação à compilação dos dados empregados, o consenso das explicitações e ideias serão amplamente aproveitados, fortalecendo conceitos e criando um vínculo conceptivo

de grandes especialistas e estudiosos da área em questão, para que as informações e análises possam servir de análises futuras.

4. A COMPUTAÇÃO EM NUVEM

No contexto mundial, vemos o avanço tecnológico avançar de maneira exponencial e realizar feitos inimagináveis e, até bem pouco tempo atrás, inalcançáveis para a raça humana. Inúmeras dessas vertentes tecnológicas vem se aprimorando e se tornando mais imprescindíveis com o passar do tempo, para aqueles que não pretendem ficar para trás diante da globalização que transforma o planeta.

Nesse cenário da *cloud computing*, ou em português, computação em nuvem, vem se destacando e demonstrando ser cada vez mais necessária, não só no âmbito pessoal mas, principalmente, para grandes organizações, sejam governamentais ou privadas.

O conceito de nuvem surgiu, mais exatamente, em 2006, quando o então Chief Executive Officer (CEO) da Google, Eric Schmidt, usou o termo pela primeira vez ao descrever um dos serviços oferecidos por sua empresa. A partir daí, outras grandes empresas como, por exemplo, a Amazon, começou a prestar o mesmo tipo de serviço, através do Elastic Compute Cloud.

O termo se popularizou e começou a ganhar destaque no meio das empresas que prestam serviço de TI e iniciou-se, então, uma série de definições para explicar o que de fato se apresentava como *cloud computing*.

Amrhein refere ao termo, em [3], como uma solução completa, na qual todos os recursos de computação são fornecidos rapidamente aos usuários, à medida de exigência da demanda, podendo controlar os recursos oferecidos, assegurando-se alta disponibilidade, segurança e qualidade, tendo como fator chave, a capacidade de serem reduzidas ou aumentadas gradualmente, de forma que os usuários tenham o acesso necessário, nem mais, nem menos.

A empresa de computação IBM define a *cloud computing* como uma categoria de soluções de computação na qual uma tecnologia e/ou serviço permite aos usuários acessar recursos de computação conforme sua necessidade, sejam os recursos físicos ou virtuais, dedicados ou compartilhados, independentemente de como eles são acessados, caracterizados por interfaces de autoatendimento que permitem aos clientes adquirir recursos quando e pelo tempo que for necessário.

Já Vaquero, em [24], refere-se ao conceito como um grande conjunto de recursos virtualizados, de fácil acesso que podem ser dinamicamente reconfigurados para ajustar a escala variável do sistema, permitindo a otimização dos recursos, estes que são explorados por um

modelo onde se paga pela quantidade de recursos utilizados, no qual as garantias são oferecidas por um provedor de infraestrutura por meio de um Service Level Agreement (SLA).

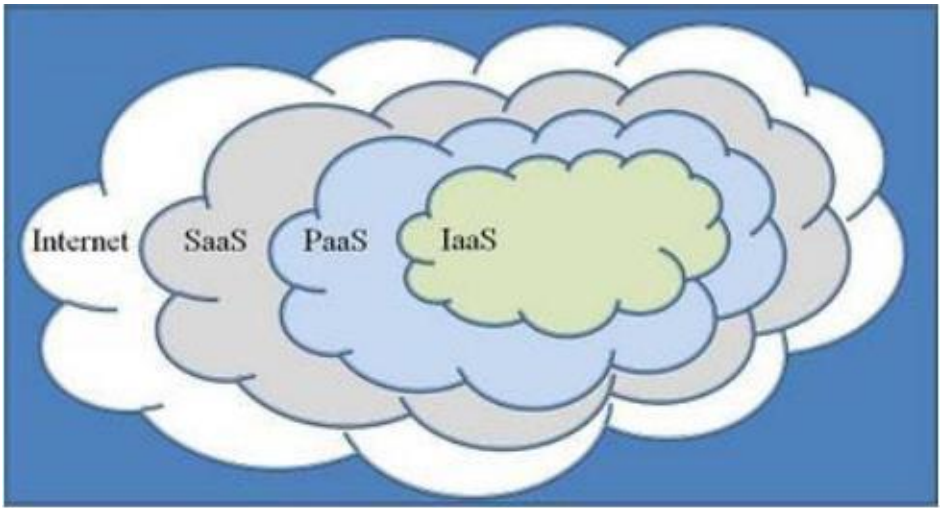
E, por fim, Taurion define, em [23], nuvem computacional como sendo um conjunto de recursos, como capacidade de processamento, armazenamento, conectividade, aplicações, plataformas e serviços disponibilizados na *Internet*, podendo ser vista como o estagio mais evolutivo do conceito de virtualização, a virtualização do próprio data center.

Todos os conceitos e definições são diferentes pontos de vista e explicam de maneira bem completa o que se define por nuvem no mundo computacional, cada um integrando valor e parte a um conceito abstrato e subjetivo, o qual podemos tentar resumir e explicar, sucintamente, como uma maneira de utilizar-se de memória, capacidade de armazenamento e processamento por computadores e servidores através da *Internet*, fazendo se valer dos princípios dos *clusters* e computação em grade.

4.1 Modelos de Serviço

A nuvem computacional é desmembrada, essencialmente, em três modelos de serviço, sendo estes alocados concentricamente como na Figura 4.1:

Figura 4.1 - Modelos de Serviço



Fonte: CLOUD Computing: Demystifying Cloud Terminology. <http://madgreek65.blogspot.com/2008/12/cloud-computing-demystifyng-cloud.html>

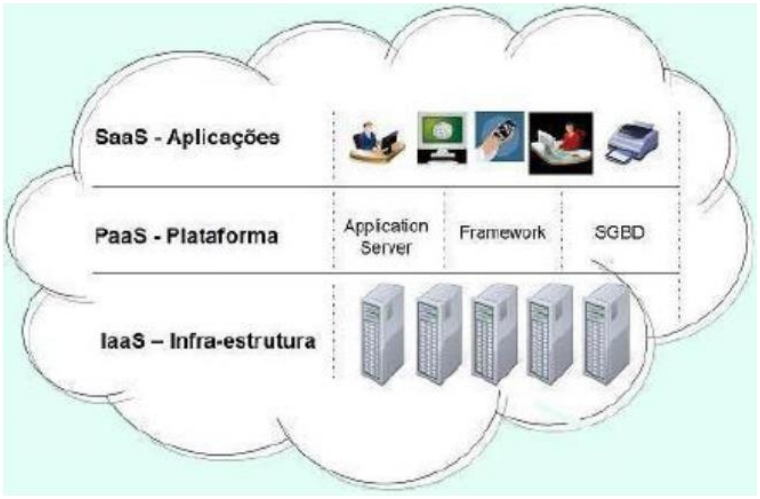
- Software como um Serviço (*SaaS – Software as a Service*);

- Plataforma como um Serviço (*PaaS – Platform as a Service*);

- Infraestrutura como um Serviço (*IaaS – Infraestructure as a Service*);

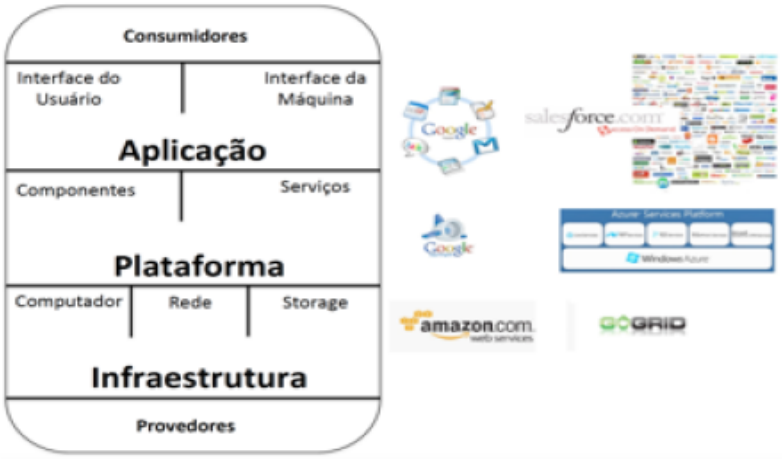
A divisão desses serviços e algumas soluções são exibidos na Figura 4.2 e 4.3.

Figura 4.2 - Soluções I



Fonte: GUERRA, G. Conceitos de Cloud Computing-Computação em Nuvem. <http://www.fromsoft.com.br/noticias/artcompnuvem.htmal>.

Figura 4.3 - Soluções II



Fonte: SILVA, K.C.A; Confiança na nuvem a partir da construção de Sec-SLA nos diversos modelos quanto à implantação e serviço.

4.1.1 *SaaS* – Software como Serviço

Diferentemente da forma tradicional de venda de licenças e cópias de softwares para utilização e instalação local, este modelo oferece softwares como aplicações, como por exemplo, processadores de texto através da rede, correio eletrônico e outros.

Este modelo surge num cenário onde as empresas buscam cada vez mais diminuir seus gastos, transferindo a responsabilidade de suporte, manutenção e atualização do produto final para o provedor do referido serviço.

Nos moldes de atuação deste modelo o cliente realiza o pagamento mensal ao provedor de uma taxa baseada na amplitude de atendimento, ou seja, baseia-se no número de usuários que efetivamente utilizam o produto. Este cliente, portanto, não fica responsável pela infraestrutura requerida pelo produto, além disto, este pode ser utilizado de qualquer lugar ou dispositivo, tipicamente através de um navegador web ou aplicativo específico. Alguns desses exemplos, como o Google app, são apresentados na figura 4.4.

Figura 4.4 - Exemplos SaaS

Fonte: CLOUD Computing: Demystifying Cloud Terminology. <http://madgreek65.blogspot.com/2008/12/cloud-computing-demystifyng-cloud.html>

4.1.2 *PaaS* – Plataforma como Serviço

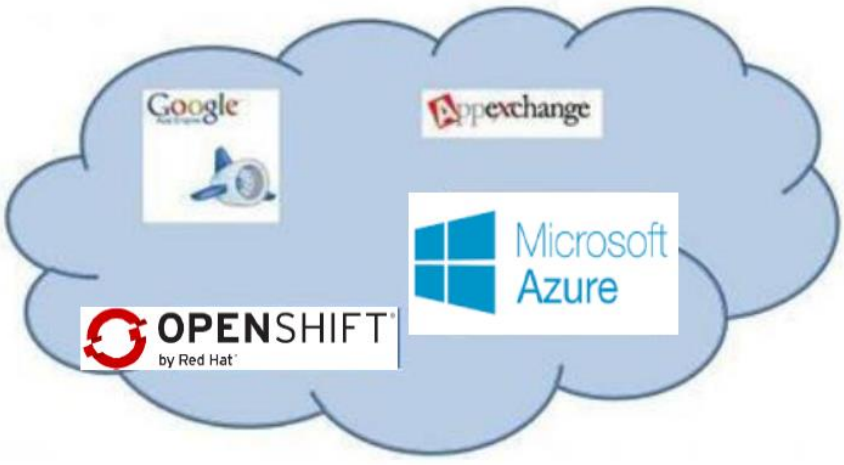
A plataforma como serviço surge de uma consequência natural do modelo SaaS, oferecendo a possibilidade de construção e operação das próprias aplicações, utilizando-se de ferramentas suportadas pelo provedor do serviço, não havendo a necessidade de despender tempo com instalações ou downloads de aplicações, pois todos os serviços se encontram disponíveis na nuvem, até mesmo ferramentas de desenvolvimento, teste, administração, hospedagem e gerenciamento.

Neste modelo de serviço, o cliente tem o controle apenas da aplicação paga, previamente, ao provedor de acordo com a utilização e, desta maneira, todo o controle da infraestrutura fica sob responsabilidade do provedor de serviço. Isso acaba facilitando o desenvolvimento de aplicações e programas que se destinam aos usuários do serviço de nuvem, provendo uma plataforma extremamente difundida e completa.

Entretanto, algumas pequenas limitações surgem com a utilização de tal modelo como, por exemplo, a obrigatoriedade de se executar o programa de aplicação na nuvem do provedor, e além disso, não são muitas as opções, atualmente, existentes no mercado de linguagens de desenvolvimento.

Alguns dos exemplos que encontramos no mercado, hoje em dia, são apresentados na Figura 4.5:

Figura 4.5 - Exemplos PaaS



Fonte: CLOUD Computing: Demystifying Cloud Terminology. <http://madgreek65.blogspot.com/2008/12/cloud-computing-demystifyng-cloud.html>

4.1.3 *IaaS* – Infraestrutura como Serviço

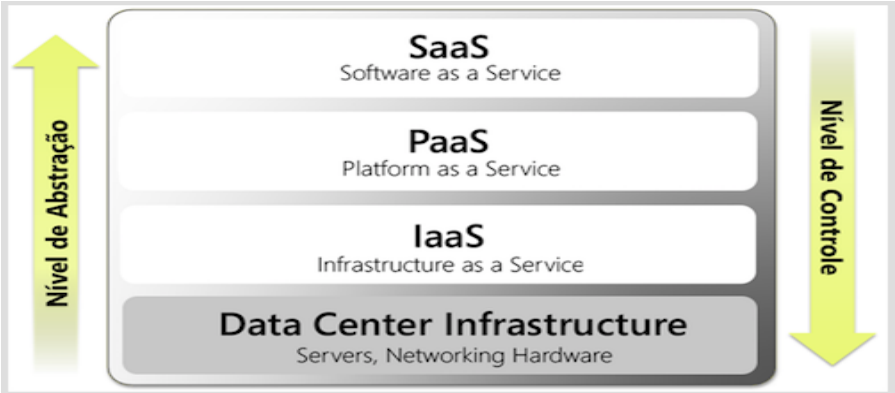
Este modelo de Infraestrutura como Serviço disponibiliza recursos, como processadores ou máquinas virtuais (*Virtual Machines* - *VM*), e dessa maneira, permite ao usuário realizar a escolha da maneira como os recursos disponíveis serão utilizados. Como exemplo destes, temos a Amazon, Google Cloud, Microsoft Azure e GoGrid. Alguns desses exemplos são demonstrados na Figura 4.6.

Figura 4.6 - Exemplos IaaS

Fonte: CLOUD Computing: Demystifying Cloud Terminology. <http://madgreek65.blogspot.com/2008/12/cloud-computing-demystifyng-cloud.html>

Levando-se em consideração os níveis de abstração e controle, Cambiucci em [5], apresenta na Figura 4.7, a seguinte esquematização.

Figura 4.7 - Relação (Modelos x Níveis)



Fonte: CAMBIUCCI, W. Computação em Nuvem: algumas perguntas sobre desafios em projetos. <https://blogs.msdn.microsoft.com/wcamb/2010/05/07/computao-em-nuvem-algumas-perguntas-sobre-desafios-em-projetos>

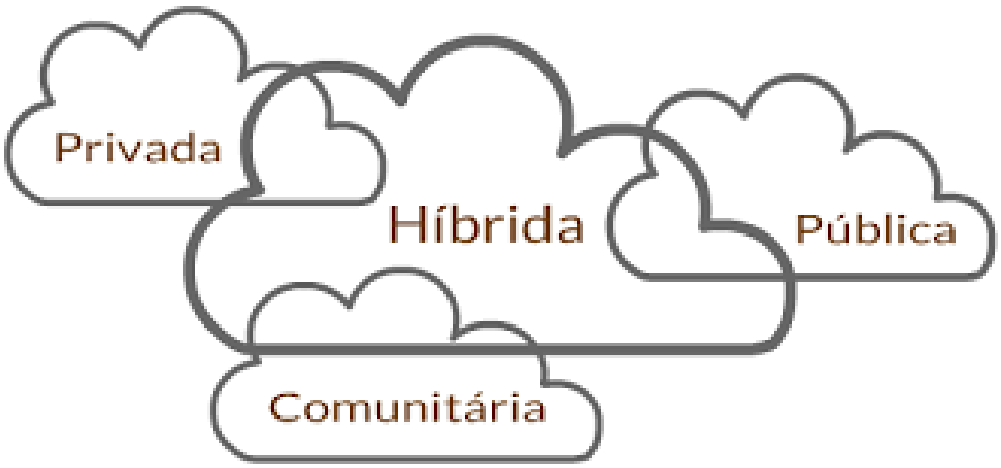
Ainda existem algumas outras classificações, como por exemplo, MaaS, BaaS, etc. Entretanto tais classificações são dedicadas a aglutinações e variações diversas ,especificada por cada prestador de serviço, das três cartesianas classificações dos modelos apresentados acima. Portanto, direcionando esse estudo ao que a bibliografia clássica se refere, cita-se apenas os modelos em questão.

4.2 Modelos de Implementação

Como modelo de implementação da tecnologia de *cloud computing*, temos quatro modelos que podem se aplicar separadamente ou em conjunto, proporcionando mais flexibilidade ao usuário final, criando enlaces de acordo com a necessidade final da organização contratante.

A nuvem computacional pode possuir quatro modelos de implementação, como apresentados na Figura 4.8:

Figura 4.8 - Modelos de Implementação



Fonte: ZORZI, L; BARDI, M.A.G. Reaproveitamento de dispositivos computacionais utilizando computação em nuvem com vistas à sustentabilidade na área de tecnologia da informação, 2017.

4.2.1 (NPr) Nuvem Privada

São nuvens que possuem características de estruturação que visam atender a apenas uma organização, independente se o gerenciamento é realizado de maneira interna ou remota.

Oferece a possibilidade de acesso as aplicações de qualquer lugar desejado, evitando o pagamento de taxa de licenciamento. Nuvem que possui políticas de segurança próprias, assim como políticas de gerenciamento e controle de acesso a cargo de sua própria gestão de TI.

Esse modelo proporciona, também, um ambiente extremamente favorável para soluções de segurança avançada, com disponibilidade ou tolerância a falhas a cargo da gerência de TI da própria empresa, adequando seu orçamento aos benefícios estruturais pretendidos.

Apesar desses benefícios, o investimento inicial para a instalação de uma infraestrutura desse porte ainda é elevado, já que trata-se de uma solução de cunho autônomo, requerendo todos os gastos com a montagem e implementação estrutural da referida nuvem.

4.2.2 (NC) Nuvem Comunitária

A utilização desta implementação, visa o atendimento de determinadas comunidades definidas e com interesses em comum, ou seja, pretendem possuir basicamente os mesmos requisitos de segurança, atendimento de serviços, políticas e regulamentações.

O gerenciamento tem a possibilidade de ser realizado em uma ou mais organizações presentes na comunidade, por um terceiro, através de dispositivos remotos ou, até mesmo, pode ser realizado de forma combinada para obtenção de melhores resultados.

A possibilidade de haver uma nuvem comunitária, diminui, de maneira significativa, os investimentos iniciais individuais das empresas participantes da comunidade, quando comparados aos investimentos necessários, caso cada uma delas buscasse a implementação de uma própria nuvem privada. Portanto, em certas situações, vale a pena investir nesse modelo de implementação.

4.2.3 (NP) Nuvem Pública

Esse modelo de nuvem disponibiliza seus serviços, aplicações e armazenamento através da *Internet* “como um serviço”, baseado no pagamento pelo cliente ao provedor de tarifas relativas a capacidade contratada ou, até mesmo, disponibilizado de maneira gratuita de forma experimental, como demonstração ao público.

Esses modelos são adequados para empresas que não possuem a intenção de investir em infraestrutura interna e nem pretendem realizar a contratação de profissionais que

possam administrar tal serviço. Isso se deve ao fato da arquitetura subjacente ser fixada e não permitir flexibilização, com respeito à personalizações em segurança e desempenho.

4.2.4 (NH) Nuvem Híbrida

O modelo de nuvem híbrida, combina dois ou mais dos modelos apresentados anteriormente (conforme apresentado na Figura 4.7), de maneira que a empresa ou corporação possa extrair benefícios de cada segmento de implementação conforme suas necessidades organizacionais.

Atualmente, a nuvem híbrida é utilizada na maioria das vezes em momentos de pico de utilização, ou seja, a empresa se utiliza da nuvem privada ou comunitária durante a maior parte do tempo, entretanto, em momentos de alto índice de utilização dos serviços, ocorre uma migração para utilização da nuvem pública, descongestionando a rede.

Vale ressaltar que todo esse mecanismo deve estar sempre atrelado e de acordo com as políticas e regras de emprego da organização que se utiliza dessa modalidade de implementação.

Dessa maneira permite-se que os serviços da *cloud computing* tenham o máximo de eficiência para seus usuários.

Considerando-se a NC como parte integrante da NPr, Farias em [9] às caracteriza apresentando seus riscos mais imediatos, como apresentado abaixo na Tabela 4.1.

Tabela 4.1 - Implantação x Riscos

Tipo de Implantação	Descrição	Provável Risco
 Nuvem Pública	Com a nuvem pública, os serviços são entregues aos clientes por meio de uma rede aberta para uso público.	Dificuldade para avaliar, implementar e gerenciar os controles de acesso.
 Nuvem Privada	A nuvem privada oferece mais segurança e controle porque os serviços são mantidos em uma rede privada protegida por firewall.	Os controles de acesso são mais fáceis de serem gerenciados e controlados.
 Nuvem Híbrida	Na nuvem híbrida temos uma composição dos modelos de nuvens públicas e privadas, oferecendo maior diversidade.	Os riscos relacionados a gestão do controle de acesso varia de acordo com o escopo de tecnologia aplicado.

Fonte: FARIAS, J. **"Cloud Computing": Computação em Nuvem, o novo desafio para Validação de Sistemas Computadorizados.** <http://www.farmaceuticas.com.br/cloud-computing-computacao-em-nuvem-o-novo-desafio-para-validacao-de-sistemas-computadorizados/>

5. SEGURANÇA NA NUVEM

Realizando a análise bibliográfica para elencar as Referências utilizadas, não foram encontrados trabalhos que, de maneira genérica, caracterizem os níveis de confiança na nuvem, nos diversos modelos existentes. Foram encontrados, somente, estudos sobre a operacionalização, negociação e definição de SLA, exibindo, apenas, simulações baseadas em *feedbacks* ou métricas de desempenho dos clientes e usuários para modelos específicos.

Um exemplo disso, encontramos na proposta de Silva em [21], onde ocorre a classificação dos serviços prestados em TI, dividindo-os em mensuráveis e não mensuráveis, com relação à medida de qualidade. Definem que serviços mensuráveis são aqueles onde são possíveis a realização das medições precisas de disponibilidade, capacidade, custo, tempo de provisionamento, latência e escalabilidade. Já os não mensuráveis são aqueles onde não é possível aferir métricas como modificabilidade, segurança e interoperabilidade. Entretanto os autores deixam claro que esse monitoramento de segurança visa o acompanhamento dos acordos de *Sec*-SLA, apenas para nuvens *SaaS*.

Como importante quesito a ser levado em consideração em qualquer situação de implementação tecnológica na área de TI, a preocupação com segurança torna-se particular no contexto computacional da nuvem. Segurança contra acesso não autorizado de ativos de informação, alterações indevidas ou, mesmo, indisponibilidade, além de ataques maliciosos remotos de monitoramento, necessitam de medidas preventivas e protetivas suficientes e compatíveis, que possam suprir as necessidades de um bem estruturado sistema de *cloud computing*. Nesse contexto, podemos inserir o conceito de confiança na nuvem.

5.1 Análise da Confiança na Nuvem

A questão apresentada neste tópico se refere ao motivo da falta de confiabilidade na *cloud computing* pelas organizações consumidoras, criando certo tipo de preconceito com relação a contratação dessa nova tecnologia.

Em conformidade com o exposto por Silva em [21], o valor que a informação possui e o público a que se destina é o motivo das preocupações, impedindo a adesão à nuvem computacional. Tal fato se dá, pois na nuvem, poderão ser encontradas informações ostensivas a todos e outras extremamente sigilosas.

Nesse contexto, encontra-se a MB, assim como outros órgãos públicos do Brasil, pois existe a necessidade de haver uma absoluta segurança de certos dados e informações que possuem caráter vital para a segurança nacional. Entretanto, nem toda a informação possui o mesmo valor e este valor de sigilo vai depender de quem poderá acessar, interna ou externamente à organização, e que possua a capacidade classifica-la.

Dentro da MB, assim como em qualquer organização de grande porte, podemos considerar três diferentes níveis de tomada de decisão: operacional, tático e estratégico. Acreditando que os dados pontuais do nível operacional serão agrupados, filtrados e analisados como informação do nível tático e que irão evoluir para o conhecimento e aporte à tomada de decisões no nível estratégico. Entretanto, a ênfase em processos horizontais com mais decisões sendo delegadas àqueles mais voltados ao nível operacional e tático eleva, portanto, comprometimento de todas as partes da organização, da mesma forma ocorrerá com sistemas confiados a nuvem computacional. De qualquer maneira, toda a cadeia de transformação por qual passa a informação é inquestionavelmente responsável por ela. Todos, assim, são responsáveis tanto pela informação como pelo uso da mesma. Ainda assim, a informação, como qualquer outro ativo da organização e da nuvem, deve ter um responsável, um proprietário, conforme expresso em [1] (NBR ISO/ IEC 27002:2013).

Desta maneira, torna-se imprescindível, a necessidade de haver políticas de controle de acesso e incidentes perfeitamente definidas e estabelecidas de maneira ampla e detalhada no *SLAs*, sendo levadas em consideração políticas de segurança e as operações de manutenção continua e de emergência que protejam a informação, sem deixá-la vulnerável.

Existe, também, a necessidade de verificação da disponibilidade do serviço e sua compatibilidade com as políticas de segurança. Como exemplo disso, podemos elencar os sistemas das Forças Armadas, que em suas intrínsecas características, possuem a necessidade de ter políticas que intentem para a proteção de dados sigilosos, garantindo a funcionalidade e discrição dos sistemas que se utilizam desses dados.

Num cenário de contratação de serviço de nuvem, após a análise de diversos aspectos, de que maneira pode-se chegar a absoluta certeza de não ocorrer vazamento de dados? De que maneira verificar se não ocorreu algum tipo de falha de segurança por parte do provedor? Como indicar um responsável pelo monitoramento? Como fazer a verificação das configurações e exigências do contratante por ocasião do estabelecimento do SLA?

Tem-se por intuito, apresentar nas próximas seções desse estudo, subsídios que tem por objetivo balizar sistemas de precauções, com o intuído de responder as questões

supracitadas de maneira que se defina de maneira ampla, como a Marinha do Brasil pode implementar em seus sistemas, de maneira eficaz e segura, a nuvem computacional.

5.1.1 Métricas de Arquitetura, Privacidade e Conformidade

Tendo em mente que os modelos de nuvem supracitados, relacionados à implementação e serviço, encontram-se previamente definidos pelas escolhas e definições selecionadas pelo contratante, verifica-se que os processos de confiança na nuvem são calculados quanto à arquitetura (ARQ), à privacidade (PRI) e à conformidade (CONF), em associação com a tabela 1, conforme descrito por Silva em [19].

Tabela 5.1 - Métricas

Métricas	Categoria	Subcategoria (Si)
Arquitetura (ARQ)	Segurança de Rede	S1 - Transferência de Dados
		S2 - Firewall
		S3 - Configurações
	Interface	S4 - API
		S5 - Interface Administrativa
		S6 - Interface do Usuário
		S7 - Autenticação
	Virtualização	S8 - Isolamento
		S9 - Vulnerabilidades do Hypervision
		S10 - Vazamento de Dados
		S11 - Identificação de VM
		S12 - Ataques Cross-VM
Privacidade (PRI)	Segurança dos Dados	S13 - Criptografia
		S14 - Redundância
		S15 - Eliminação de Dados
	Aspectos jurídicos	S16 - Localização dos Dados
		S17 - Pesquisas e conhecimento
		S18 - Controle de Riscos
Conformidade (CONF)	Serviços	S19 - SLA
		S20 - Falhas ou Desastres
		S21 - Auditoria

Fonte: SILVA, K.C.A; Confiança na nuvem a partir da construção de Sec-SLA nos diversos modelos quanto à implantação e serviço.

Considera-se, portanto, de acordo com Gonzalez et al. [12] que as medidas de segurança quanto à ARQ são subdivididas nas categorias de segurança de rede, interface e virtualização, estas que, por sua vez, estão relacionadas com subcategorias S_i de solução e mitigação das questões de segurança. Como, por exemplo, como uma dessas subcategorias temos a autenticação (S_6), que corresponde a uma medida de solução e mitigação da categoria interface.

5.1.2 Tipos de Nuvem Analisados - Implantação e Serviço

Podemos observar, quando analisamos o trabalho de Badger em [4], que o autor opta por considerar que um sistema de computação em nuvem poderá ser implementado em uma estrutura local das organizações clientes (privada ou comunitária), compartilhada de maneira efetiva remotamente (pública) ou, então, com alguns recursos locais e também compartilhados remotamente (híbridas).

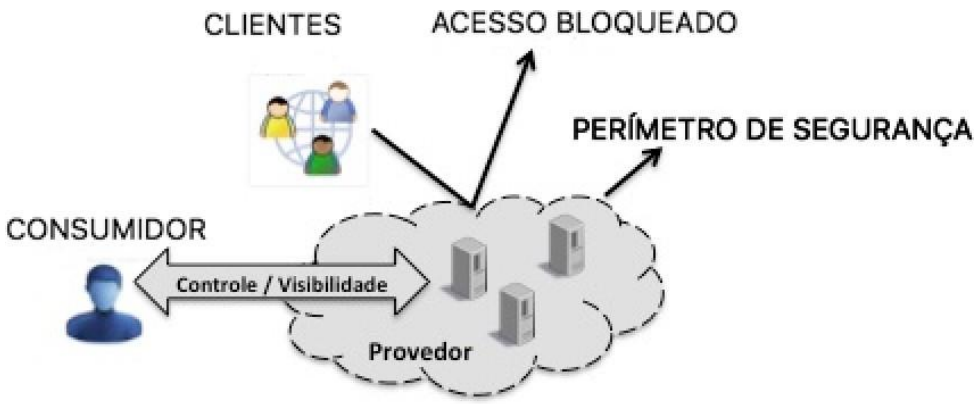
A partir do entendimento desse autor, pode-se, então, definir os seguintes modelos de nuvem computacional, quanto a sua implementação, da seguinte forma: Nuvem Privada Local (NPL), Nuvem Privada Terceirizada (NPT), Nuvem Comunitária Local (NCL), Nuvem Comunitária Terceirizada (NCT), Nuvem Pública (NP) e Nuvem Híbrida (NH).

Com relação aos serviços, segue-se o apresentado anteriormente neste estudo, na seção 4.1. Então teremos o *Software as a Service (SaaS)*, os ambientes de desenvolvimento especificados pela *Plataform as a Service (PaaS)*, ou recursos computacionais básicos como processamento e armazenamento caracterizados pela *Infrastructure as a Service (IaaS)*. Modelos estes escolhidos através de uma avaliação situacional com definições de responsabilidade de controle, bem como visibilidade dos recurso de computação. Define-se, portanto, um grupo de políticas de segurança física e programável como perímetro de segurança, de maneira a se obter níveis de proteção em uma conceitual fronteira a se contrapor às atividades maliciosas remotas. Grance et al. em [13] padroniza o perímetro de segurança da seguinte maneira, esquematizado na Figura 5.1:

- Consumidor da Nuvem: indivíduo ou organização, podendo ser este consumidor de uma nuvem que utiliza serviços de outras nuvens;
- Cliente: qualquer estação ou aplicação que acessa a nuvem por meio de uma conexão de rede, em busca de um serviço ou aplicação, oferecido pelo consumidor e hospedado na nuvem;
- Provedor da Nuvem: uma organização que oferece serviços em nuvem;

- Controle: capacidade de executar ações, com alta confiança, autorizar o que e quem poderá acessar os dados e sistemas do consumidor; e
- Visibilidade: capacidade de monitorar como os dados e sistemas do consumidor estão sendo acessados por outros, com alta confiança.

Figura 5.1 - Perímetro de Segurança



Fonte: SILVA, K.C.A; Confiança na nuvem a partir da construção de Sec-SLA nos diversos modelos quanto à implantação e serviço.

Entretanto, cada modelo de nuvem escolhido pelo cliente, o controle e visibilidade de seus dados e sistemas irão depender da localização, posse e capacidade de configuração de mecanismos de acesso e proteção de recursos utilizados pelo mesmo. Assim, nos tipos de nuvem definidos por Grance et al. [13], podemos associar a tabela de [21] – Tabela 5.2, com relação à obrigatoriedade das especificações de medidas de segurança a serem respeitadas pelos provedores, sendo elas: arquitetura, privacidade e conformidade na nuvem.

Tabela 5.2 - Especificações

Modelo \ Categoria	Segurança de Rede	Interface	Virtualização	Segurança dos Dados	Aspectos Jurídicos	Serviços
NPL						
NPT	✓	✓	✓	✓	✓	✓
NCL						
NCT	✓	✓	✓	✓	✓	✓
NP	✓	✓	✓	✓	✓	✓
SaaS	✓	✓	✓	✓	✓	✓
PaaS	✓		✓		✓	✓
IaaS	✓		✓		✓	✓

Fonte: SILVA, K.C.A; Confiança na nuvem a partir da construção de Sec-SLA nos diversos modelos quanto à implantação e serviço.

5.1.3 Grau das Métricas de Segurança

Nessa seção, apresenta-se a análise de Silva, em [21] a despeito do grau de importância de todos os itens de segurança quanto à arquitetura, à privacidade e à conformidade a comporem o Sec-SLA, utilizando como base, os padrões de ataque *Common Attack Pattern Enumeration and Classication (CAPEC)*, que foram elaboradas pela comunidade de segurança cibernética. Essa tabela é atualizada e disponibilizada pelo Departamento de Segurança Interna dos EUA como parte da *Software Assurance (SWA)*, iniciativa estratégica do Escritório de Segurança Cibernética e Comunicações (CS&C), desde 2007. Essa base, a *CAPEC*, enumera e classifica os principais domínios e mecanismos de ataques associados a 463 padrões de ataques, com medidas para mitigação e solução. Junta-se a isso o fato de a probabilidade e os impactos na confidencialidade, na integridade e na disponibilidade, sendo esses atributos avaliados como: muito baixo, médio, alto e muito alto.

Silva utiliza em [21] faixas de valores para itens de Sec-SLA presentes na base de vulnerabilidades *Nacional Vulnerability Database (NVD)* do *Common Vulnerability Scoring System (CVSS)*, proposta em [22] por Silva et al., onde é levado somente em consideração o impacto pela severidade da vulnerabilidade. Propõe, também, avaliar além do impacto na severidade, a probabilidade desses ataques, obtida pela *CAPEC* por um histórico de ocorrências, que juntos definirão o grau de risco a ser mitigado a partir das subcategorias S_i.

Em [19], foi onde obteve-se o Guia de Avaliação de Riscos como base, orientando a construção de uma matriz de risco baseada na probabilidade de ocorrência e no impacto das ameaças. Apesar dessa base de referência apresentar apenas três níveis (baixo, médio e alto), Silva, em [21], faz uma adaptação em uma matriz 4x4, representados na tabela 5.3.

Tabela 5.3 - Severidade/Probabilidade (níveis)

Severidade\ Probabilidade	Muito Alta	Alta	Média	Baixa
Muito Alta	100	75	50	25
Alta	75	56,25	37,5	18,75
Média	50	37,5	25	12,5
Baixa	25	18,75	12,5	6,25

Fonte: SILVA, K.C.A; Confiança na nuvem a partir da construção de Sec-SLA nos diversos modelos quanto à implantação e serviço.

As faixas de probabilidade estão denotadas por $FP_{nível}$, onde *nível* assume os respectivos parâmetros de probabilidade, onde $FP_{muito\ alta} = (0{:}75;\ 1{:}0]$; $FP_{alta} = (0{:}5;\ 0{:}75]$; $FP_{média} = (0{:}25;\ 0{:}5]$ e $FP_{baixa} = (0;\ 0{:}25]$. Foram definidos, analogamente, Faixas de Severidade denotadas por $FS_{muito\ alta} = (0{:}75;\ 1{:}0]$; $FS_{alta} = (0{:}5;\ 0{:}75]$; $FS_{média} = (0{:}25;\ 0{:}5]$ e $FS_{baixa} = (0;\ 0{:}25]$, e a partir daí, consegue-se obter o que foi definido como os diferentes níveis de Faixa de Risco ($FR_{nível}$). Para que isso ocorresse, foram multiplicados os valores extremos de cada um dos níveis das Faixas de Probabilidade por todos os valores extremos das Faixas de Severidade, portanto, temos: $FR_{muito\ alta} = (56{:}25;\ 100]$; $FR_{alta} = (25;\ 56{:}25]$;$FR_{média} = (6{:}25;\ 25]$ e $FR_{baixa} = (0;\ 6{:}25]$. Essas escalas de risco, portanto, serão associadas às medidas de mitigação e soluções (Si subcategorias) a serem levadas em consideração no cálculo da confiança. Nota-se, entretanto, que para auxiliar futuras explicações, atribui-se diferentes cores para cada uma das faixas de probabilidade, severidade e risco, sendo elas nas cores já adotadas acima: muito alta (vermelha), alta (laranja), média (verde) e baixa (azul).

5.1.4 Análise do Cálculo da Confiança na Nuvem

Para proposta de desenvolvimento de cálculo de confiança na nuvem em [21], Silva propõe um modelo que atribui a cada subcategoria Si um valor único de risco r(Si) a ser calculado a partir de valores únicos de severidade s(Si) e probabilidade p(Si), obtidos de acordo com as faixas de severidade e probabilidade calculadas. Utiliza-se, então, de métodos heurísticos para correlacionar as categorias e subcategorias apresentadas e seus valores de referência e níveis, podendo assim, criar um padrão para apoiar a resolução da questão fundamental de "Como apoiar os consumidores da nuvem na escolha do provedor que garanta uma maior confiança nos serviços a serem contratados?"

Ainda propõe estudos de caso para os diversos cenários, aplicando o modelo abstrato definido, permitindo o cálculo da confiança para modelos distintos de nuvem, com base nas medidas de prevenção a riscos elucidadas na base *CAPEC*, oferecidos pelos provedores em seus Catálogos de Serviço, diferindo, portanto da avaliação de desempenho provada [16, 17].

Analisa, portanto, em diferentes cenários individuais, as Nuvens Públicas *SaaS*, Nuvem Privada Terceirizada, Nuvens Públicas *Paas*, descrevendo os resultados.

Resultados estes, obtidos descrevendo o cálculo da confiança, notando que através da utilização de um valor único associado a cada subcategoria, proporcionando a possibilidade, portanto, de responder a fundamental questão “Como medir este grau de confiança?”.

Destacando como principal aspecto a ser observado, a partir das possibilidades de cenários, o fato de que para cada modelo de nuvem, avaliando implementação e serviço, associados às políticas de segurança do consumidor quanto à arquitetura, privacidade e conformidade, será necessário um padrão de Sec-SLA que se adapte a cada consumidor, implementando-os em uma ambiente real.

Dessa maneira, Silva analisa o ambiente real em [21], relacionando a Tabela 5.2 na seção 5.1.2, que define a responsabilidade de consumidores e provedores nos diversos modelos de nuvem quanto a implementação e serviço, notando as semelhanças que reduzem os possíveis ambientes a serem validados no cálculo de confiança, que são:

i. Os modelos de implantação de nuvens NPL e NCL serão de total responsabilidade do consumidor;

ii. Os demais modelos de implantação de nuvens NPT e NCT, NP e NH irão variar somente de acordo com o modelo quanto ao serviço escolhido:

    a. Os modelos *SaaS* serão de total responsabilidade do Provedor; e

    b. Os modelos *PaaS* e *IaaS*, terão responsabilidades distintas, onde as subcategorias *S1; S2; S3; S8; S9; S10; S11;S12; S16; S17; S18; S19; S20 e S21* serão de responsabilidade do provedor e as demais serão de total responsabilidade do consumidor.

Em [21] observa-se a análise do ambiente real para validação no Centro de Tecnologia da Informação da Marinha (CTIM), responsável por atuar como provedor interno a todas as Organizações Militares (OM) da MB. A partir do estudo neste ambiente, Silva (2016) reforça e embasa a utilização do modelo para o cálculo da confiança na nuvem, entretanto, alerta que garantir 100% de segurança em qualquer sistema de computação é uma tarefa muito difícil, até mesmo em sistemas privados e dedicados, necessitando, sempre, de definições de responsabilidades e *Sec-SLA* bem planejados e abordados, podendo-se, finalmente, promover a obtenção de modelos capazes de oferecer um maior nível de confiança aos consumidores em

ambientes de computação em nuvem. Nesse contexto, faz-se necessário analisar como a MB encontra-se com relação a tecnologia existente.

6. A TI NA MARINHA DO BRASIL

A globalização, transforma a sociedade diuturnamente e a deixa cada vez mais dependente das estruturas de TI e de uma mentalidade de informatização cada vez maior.

6.1 A Missão da MB

A Marinha do Brasil, assim como todas as instituições de grande porte, necessita se manter atualizada e, estar sempre atenta às nuances que essa constante globalização propicia no planeta como um todo, nos seus diversos aspectos.

Há portanto a ampla necessidade de manter as topologias cada vez mais adaptadas às metamorfoses da evolução técnico-cientifica, e a MB, como parte importante do Sistema de Defesa de uma das mais importantes nações no cenário geopolítico e militar no âmbito internacional, possui a necessidade de implementar, de forma ininterrupta, uma consciência situacional voltada à SIC, buscando sempre implementar tecnologias que possam propiciar uma melhor utilização de seu aspecto estrutural em prol da missão e visão de futuro da Força, complementado segundo [18]:

> "Preparar e empregar o Poder Naval, a fim de contribuir para a Defesa da Pátria; para a garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem; para o cumprimento das atribuições subsidiárias previstas em Lei; e para o apoio à Política Externa."

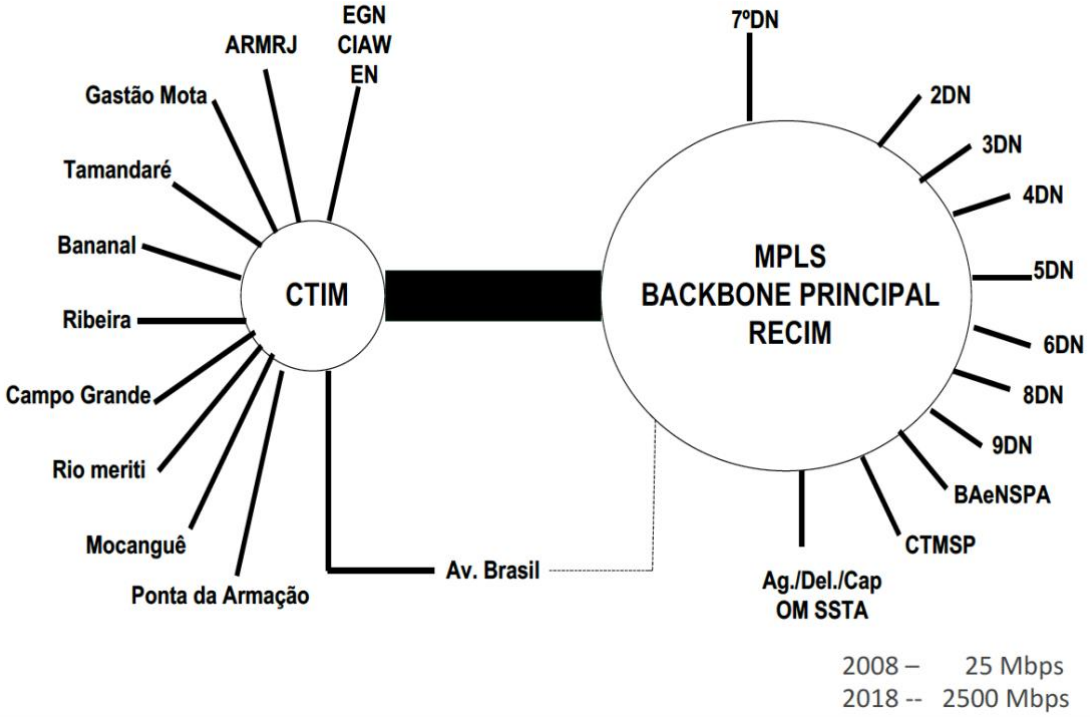
Toda essa evolução por qual o mundo passa, presentemente, acaba trazendo a pauta os desafios da SIC para a MB. Estruturar toda uma Força Armada e aparelhá-la ante aos riscos diversos e iminentes que se apresentam no cenário de TI atualmente não é missão fácil, e a MB apresenta planejamento estruturado para tais mudanças de perspectivas.

6.2 A Topologia da MB

Criada para prover comunicação entre os componentes internos da Força, a Rede de Comunicações Internas da Marinha (RECIM) apresenta uma topologia que integra dois

principais núcleos – o Centro de Tecnologia da Informação da Marinha (CTIM) e um Backbone (MPLS) principal – conforme exposto no esquema abaixo:

Figura 6.1 - Topologia da MB



Fonte: CERVEIRA, C.R. Agenda da Diretoria de Comunicações e Tecnologia da Informação da Marinha, 2018.

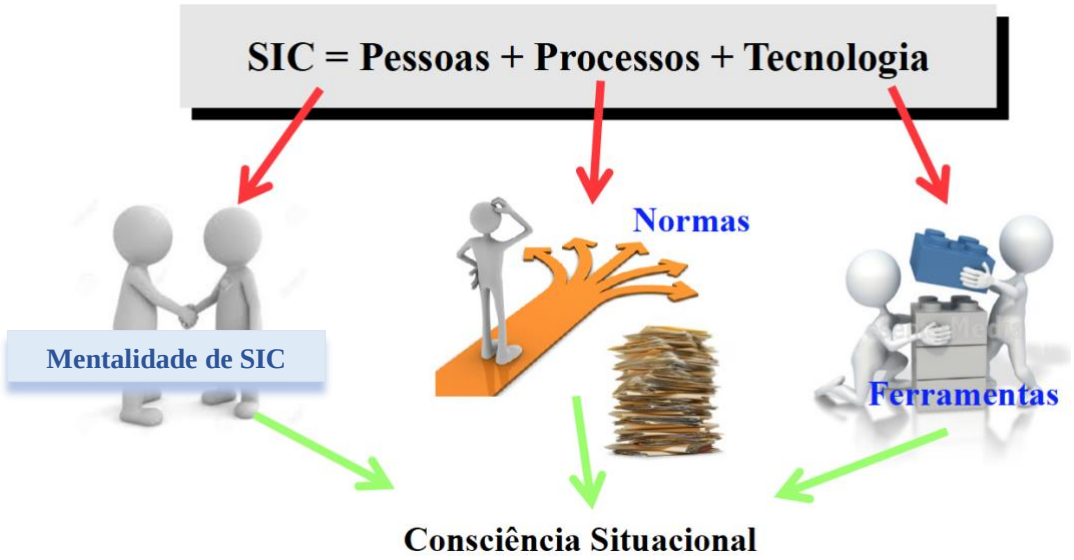
A comunicação é realizada através da conexão dos pontos em questão, pontos estes que são subestações com o objetivo de encaminhar e receber a tramitação dos dados junto aos pontos mais periféricos da rede. Podemos observar no gráfico, também, o aumento do tráfego na rede, que em dez anos (2008-2018) aumentou em cem vezes, demonstrando a necessidade cada vez maior de possuir uma estrutura suficientemente elástica e que possa prover a cobertura de toda a demanda.

Ainda segundo informações expostas em [6], a MB possui algo em torno de 40.000 estações de trabalho ativas, o que, além de demandar mão-de-obra qualificada, aumenta a necessidade de se possuir tecnologias cada vez mais modernas, capazes de proporcionar a gerência e armazenamento desses dados de maneira otimizada.

6.3 A Segurança da Informação e Comunicações na MB

Como parte da exposição, Cerveira (2018) em [6], ainda expõe a "equação" para balizamento das políticas de SIC que devem sempre ser observadas na MB de forma a evitar problemas e possa-se garantir um nível aceitável de segurança. Essa equação liga fatores como pessoas, processos e tecnologia, além de suas diversas variáveis, conforme mostrado abaixo na Figura 6.2.

Figura 6.2 - "Equação" SIC



Fonte: CERVEIRA, C.R. Agenda da Diretoria de Comunicações e Tecnologia da Informação da Marinha, 2018.

Nota-se que, como aspecto proeminente, que interfere de maneira diretamente proporcional ao resultado da "equação" de SIC, a tecnologia utilizada demonstra possuir elevado peso nessa igualdade.

Portanto, para que a MB possa garantir estar inserida no que há de melhor no mercado, ao que se refere à tecnologia de ponta e suas ferramentas, a computação em nuvem é uma implementação de extrema relevância e como apresentado nos capítulos anteriores, diversifica e pluraliza distintas operações e modos de utilização, gerando diversas vantagens.

6.4 Os Centros de Dados da MB

Apesar de existir na MB, em parte, a utilização de nuvens para transmissão de dados entre localidades muito distantes, dada a incapacidade da realização de enlaces de telecomunicações visuais e ao elevado custo dos enlaces satelitais, o serviço de *cloud computing* ainda não é utilizado de maneira ampla e abrangente pela Força, como proposto em sua completude pelos estudos apresentados anteriormente.

A MB, em busca de permitir uma padronização e consolidação da economia de recursos humanos e infraestrutura, aliado a um gerenciamento integrado, permitindo modularidade e escalabilidade, utiliza dos recursos de virtualização para armazenamento de dados. Para isso, possui dois bancos de dados privados que fazem o armazenamento utilizando-se de alguns princípios aplicados a nuvem computacional, o CD-MB (Centro de Dados da Marinha) - Figura 6.3 - e o CD-CTMSP (Centro de Dados do Centro de Tecnologia da Marinha em São Paulo), este último dedicado a dados referentes ao PROSUB (Programa de Desenvolvimento de Submarinos).

Figura 6.3 – Centro de Dados da Marinha

Fonte: CERVEIRA, C.R. Agenda da Diretoria de Comunicações e Tecnologia da Informação da Marinha, 2018.

Entretanto, a infraestrutura e manutenção de um banco de dados requerem uma dose significativa de investimento inicial, além recursos de conservação e aprimoramento, o que em

escala superiores, alavancam esses investimentos e custos de manutenção exponencialmente. Tal fato propicia uma maior atenção a utilização da nuvem computacional no seu plano descrito no presente estudo, demonstrando a capacidade de diversificação do serviço nos variados âmbitos de atuação, respeitado as peculiaridades referentes à cada cliente em potencial, neste caso, a Marinha do Brasil.

7. CONCLUSÃO

Este trabalho apresentou alguns proeminentes conceitos acerca da *cloud computing*, incluindo trabalhos, artigos e dissertações com conteúdos que especificamente ressaltam a importância da aderência à uma tecnologia que possibilita flexibilidade, escalabilidade, redundância, atuação sob demanda, acesso amplo, etc.

Para a MB migrar seu atual sistema para uma rede completamente aderida às capacidades que a nuvem computacional pode oferecer, em sentido amplo, ampliaria horizontes de alcance físico e virtual, oferecendo à Força capacidade de gerência de dados de maneira mais efetiva, sem os altos custos que uma aplicação estritamente privada (NPr) ocasionariam.

A partir dos estudos expostos e levando em conta a aplicação à MB com suas próprias peculiaridades e diferenças em relação a uma organização civil, sugere-se uma implementação desta tecnologia de maneira diversificada, atendendo às necessidades da Marinha em seus requisitos específicos e baseados em Sec-SLA bem estruturados e planejados, onde o modelo de NH pode ser aplicado, variando seus campos de atuação e modelos de implementação de acordo com as necessidades do cliente (MB).

As verificações e cálculos de confiança na nuvem para cada provedor particular e prestador de serviço apresentados em [21], a partir das variáveis apresentadas, podem basear, através de resultados heurísticos, a melhor configuração dentre os modelos existentes de aplicação, fundamentados em estudos de demanda e efetiva utilização, respeitando as necessidades de sigilo inerentes à uma Força Armada.

Dessa maneira, a MB poderia utilizar-se de todos os benefícios da tecnologia pertencente a provedores privados, de maneira sustentável e com custos adaptados às necessidade de demanda, sem despender-se de recursos de forma desnecessária, garantindo o atendimento das necessidades compatíveis com o momento, e caso seja necessário, modificar seus critérios de utilização.

Além disso, a MB ainda pode se fazer valer de uma NPr ou NC (em parceria com as demais Forças Armadas) de menor porte, para que informações e dados extremamente classificados com alto nível de sigilo sejam, desta forma, preservados.

7.1 Considerações Finais

Este estudo, portanto, através das diversas referências utilizadas, propõe um planejamento de utilização de serviços de nuvem computacional de maneira escalável,

analisando-se a demanda do cliente, Sec-SLA bem estruturados, além de estudos efetivos de cálculo da confiança necessária para correta e apropriada implementação da *cloud computing* à MB.

7.2 Sugestões para Futuros Trabalhos

O mundo se transforma muito rapidamente e esse processo tem se acelerado com o passar dos anos devido a extremos avanços tecnológicos. Uma ideia, principalmente no âmbito da TI, é desenvolvida e expandida em enormes velocidades e em pouco tempo se tornam realidade concreta, e não mais um mero planejamento ou estudo direcionado.

Deste modo, espera-se que o atual estudo seja utilizado como subsídio para outros trabalhos, num futuro próximo, que possam empregar metodologias desenvolvimentistas e práticas, podendo suprir de maneira completa a necessidade de inovar e implementar outras tecnologias inovadoras com intuito de desenvolver os sistemas computacionais não somente da MB, mas de todas as Forças Armadas (FFAA) do País.

Para tanto, sugere-se que novos e próximos trabalhos afetos ao tema utilizem-se das mais recentes informações e pesquisas no setor de segurança da informação em aplicações de nuvem e possam enriquecer com novos projetos e ideias.

Para qualquer organização da envergadura da MB, a inserção de tecnologias de última geração é uma necessidade constante. Portanto, esse fato requer uma vasta demanda de boas ideias e soluções de problemas já existentes, exigindo esforços no sentido de pesquisas voltadas à evolução tecnológica dos sistemas atuais.

REFERÊNCIAS

[1] ABNT, **Tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação.** Abnt – associação brasileira de normas técnicas, 2013. http:///http://www.abntcatalogo.com.br/norma.aspx?ID=306582.

[2] ALMEIDA, V.P. **Virtualização e Computação em Nuvem**, 2018. 183 slides**.** Material apresentado para disciplina de Virtualização e Computação em Nuvem para Curso de Aperfeiçoamento Avançado para Oficiais da parceria PUC-Rio – CIAW.

[3] AMRHEIN, D. **Computação em Nuvem para a Empresa: Capturando a Nuvem.** <http://www.ibm.com/developerworks/br/websphere/techjournal/0904_amrhein/0904_amrhein.html>. Acessado em: 25 de abril de 2018.

[4] BADGER, L. **Cloud computing synopsis and recommendations.** Nist special publication 800146,2012.http://cieseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.232.3178&rep=rep1&type=pdf. Acessado em: 04 de fevereiro de 2018.

[5] CAMBIUCCI, W. **Computação em Nuvem: algumas perguntas sobre desafios em projetos**. <https://blogs.msdn.microsoft.com/wcamb/2010/05/07/computao-em-nuvem-algumas-perguntas-sobre-desafios-em-projetos/> Acessado em: 04 de maio de 2018.

[6] CERVEIRA, C.R. **Agenda da Diretoria de Comunicações e Tecnologia da Informação da Marinha**, 2018. Material apresentado para disciplina de Virtualização e Computação em Nuvem para Curso de Aperfeiçoamento Avançado para Oficiais da parceria PUC-Rio – CIAW.

[7] CLOUD Computing: **Demystifying Cloud Terminology.** <http://madgreek65.blogspot.com/2008/12/cloud-computing-demystifyng-cloud.html>. Acessado em: 28 de abril de 2018.

[8] DAN, M. **Computação em nuvem: Vulnerabilidades na nuvem.** Technet magazine, 2013. http://www.cdn.ueg.br/source/trindade/conteudoN/3637/Computacao_em_nuvem_Vulnerabilidades_em_nuvem_TechNet_Magazine.pdf. Acessado em: 06 de fevereiro de 2018.

[9] FARIAS, J. **"Cloud Computing": Computação em Nuvem, o novo desafio para Validação de Sistemas Computadorizados.** <http://www.farmaceuticas.com.br/cloud-computing-computacao-em-nuvem-o-novo-desafio-para-validacao-de-sistemas-computadorizados/> Acessado em: 04 de maio de 2018.

[10] FREITAS, E. A. M. **Gestão de riscos aplicadas a segurança da informação: segurança estratégica da informação.** 2009. 72 f. Monografia (Pós-Graduação "Latu Sensu" em Gestão Estratégica e Qualidade) – Universidade Cândido Mendes.

[11] GONÇALVES JÚNIOR, A. **Metodologia de Gerenciamento de Risco em Sistemas de Tecnologia da Informação e Comunicação** – abordagem prática para conscientização e implantação nas organizações. 2008. 56 f. Trabalho de Conclusão do Curso de Especialização, Gerência e Segurança de Redes de Computadores – Universidade Federal do Rio Grande do Sul.

[12] GONZALEZ, N; MIERS, C; REDIGOLO F; CARVALHO T; SIMPLICIO M; NASLUND, M; POURZANDI, M. **A quantitative analysis of current security concerns and solutions for cloud computing**. IEEE 3rd International Conference on Cloud Computing Technology and Science, 2011.

[13] GRANCE, T; JANSEN, W. **Guidelines on security and privacy in public cloud computing**. Nist sp-800-144, 2011. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

[14] GUERRA, G. **Conceitos de Cloud Computing – Computação em Nuvem.** <http://www.fromsoft.com.br/noticias/artcompnuvem.htmal>. Acessado em: 26 de abril de 2018.

[15] IBM, D. **Computação em Nuvem: Comunidade e recursos técnicos para desenvolvedores e profissionais de TI.** <http://www.ibm.com/developerworks/br/cloud/xml/newto.html>. Acessado em: 26 de abril de 2018.

[16] MANUEL, D. P. **A trust model of cloud computing based on Quality of Service.** Annals of Operations Research, 2013.

[17] MANUEL, D.P; BARR, A. I. M; SELVI T. S. **A novel trust management system for cloud computing – IaaS providers,** 2011.

[18] MINISTÉRIO DA DEFESA. Marinha do Brasil. **Missão e Visão do Futuro da Marinha**. <http://www.marinha.mar.mil.br/content/missao-e-visao-de-futuro-da-marinha> – Intranet. Acessado em: 20 de abril de 2018.

[19] NIST. **Guide for conducting risk assessments**.2012.nist sp-800-30, rev.1, 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. Acessado em: 04 de fevereiro de 2018.

[20] SILVA, A.O. **Computação em Nuvem**, 2018. 69 slides. Material apresentado para disciplina de Fundamento da Segurança da Informação para o Curso de Aperfeiçoamento Avançado para Oficiais da parceria PUC-Rio – CIAW.

[21] SILVA, K.C.A; **Confiança na nuvem a partir da construção de Sec-SLA nos diversos modelos quanto à implantação e serviço.** Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense, 2016.

[22] SILVA, C.A; GEUS, P.L. **Arquitetura de monitoramento para security-sla em nuvem computacional do tipo SaaS**. Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2014.

[23] TAURION, C. **Computação em nuvem: transformando o mundo da tecnologia da informação.** Rio de Janeiro: Brasport, 2009.

[24] VAQUERO, L. **A break in the clouds towards a cloud definition.** <http://ccr.sigcomm.org/drupal/files/p50-v39n1l-vaqueroA.pdf>. Acessado em: 25 de abril de 2018.

[25] ZORZI, L; BARDI, M.A.G. **Reaproveitamento de dispositivos computacionais utilizando computação em nuvem com vistas à sustentabilidade na área de tecnologia da informação**, 2017.