Instituto Nacional de Metrologia, Qualidade e Tecnologia – INMETRO

Eduardo Augusto Maia Bezerra

PROPOSTA DE PROTOCOLO DE AVALIAÇÃO DE SOFTWARES EMPREGADOS EM UM MEIO NAVAL COM PROPULSÃO NUCLEAR

Duque de Caxias – RJ

2023

Eduardo Augusto Maia Bezerra

PROPOSTA DE PROTOCOLO DE AVALIAÇÃO DE SOFTWARES EMPREGADOS EM UM MEIO NAVAL COM PROPULSÃO NUCLEAR

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Metrologia e Qualidade do Instituto Nacional de Metrologia, Qualidade e Tecnologia como parte dos requisitos para a obtenção do título de Mestre em Metrologia e Qualidade.

Raphael Carlos Santos Machado
Orientador

Alan Oliveira de Sá
Coorientador

Duque de Caxias – RJ
2023

Eduardo Augusto Maia Bezerra

PROPOSAL FOR A PROTOCOL FOR THE EVALUATION OF SOFTWARE USED IN A NAVAL ENVIRONMENT WITH NUCLEAR PROPULSION

Master thesis submitted as partial fulfilment of the requirements for the Degree of Master of Metrology and Quality in the Postgraduate Program in Metrology and Quality of the National Institute of Metrology, Quality, and Technology.

Raphael Carlos Santos Machado
Advisor

Alan Oliveira de Sá
Coadvisor

Duque de Caxias - RJ
2023

B574p Bezerra, Eduardo Augusto Maia
Proposta de protocolo de avaliação de softwares empregados em um meio naval com propulsão nuclear / Eduardo Augusto Maia Bezerra. Duque de Caxias, RJ, 2023.
163 f. : il., color.

Dissertação (Mestrado) – Instituto Nacional de Metrologia, Qualidade e Tecnologia, Programa de Pós-Graduação em Metrologia e Qualidade, 2023.

Orientador: Raphael Carlos Santos Machado
Coorientador: Alan Oliveira de Sá

1. Meio naval com propulsão nuclear 2. Avaliação de software I. Machado, Raphael Carlos Santos II. Sá, Alan Oliveira de III. Instituto Nacional de Metrologia, Qualidade e Tecnologia IV. Título

CDD 005.14

BEZERRA, Eduardo Augusto Maia. **Proposta de protocolo de avaliação de softwares empregados em um meio naval com propulsão nuclear**. 2023. 163. Dissertação de Mestrado para qualificação ao mestrado em Metrologia e Qualidade – Instituto Nacional de Metrologia, Qualidade e Tecnologia, Duque de Caxias, RJ, 2023.

CESSÃO DE DIREITOS

NOME DO AUTOR: Eduardo Augusto Maia Bezerra.

TÍTULO DA MONOGRAFIA: Proposta de protocolo para avaliação de softwares em uma planta nuclear naval.

TIPO DE MONOGRAFIA: Dissertação de Mestrado em Metrologia e Qualidade / 2023.

_____

Eduardo Augusto Maia Bezerra

Eduardo Augusto Maia Bezerra

PROPOSTA DE PROTOCOLO DE AVALIAÇÃO DE SOFTWARES EMPREGADOS EM UM MEIO NAVAL COM PROPULSÃO NUCLEAR

A presente Dissertação, apresentada ao Programa de Pós-Graduação em Metrologia e Qualidade do Instituto Nacional de Metrologia, Qualidade e Tecnologia como parte dos requisitos para obtenção do título de Mestre em Metrologia e Qualidade, foi aprovada pela seguinte Banca Examinadora:

Doutor Raphael Carlos Santos Machado – Inmetro
Presidente da Banca Examinadora

Assinado por: **Alan Oliveira de Sá**
Num. de Identificação: TR-PT-9608M5M38
Data: 2023.04.25 15:16:23 +0100

Doutor Alan Oliveira de Sá – Universidade de Lisboa

Doutora Thaís Maria Pires dos Santos – Amazul

gov.br

Doutor Ricardo Kropf Santos Fermam – Inmetro

Doutora Diana Sasaki Nobrega – UERJ

Duque de Caxias, 31 de março de 2023.

Dedico esse trabalho aos meus pais, Manoel Bezerra de Medeiros Neto e Raimunda Fernandes Maia Bezerra, por todo amor, carinho, dedicação, atenção e educação que depositaram em mim.

AGRADECIMENTOS

Como sempre faço, agradeço primeiro ao pai por possibilitar a oportunidade trabalhar, rir, aprender e superar os desafios, e por colocar pessoas magnificas ao meu redor. E a Nossa Senhora, minha mãe, por cobrir-me com seu manto, protegendo-me de todo o mal.

Agradeço ao Seu Nel, meu pai, por mesmo nunca tendo sentado num banco escolar fez tudo para que tivesse acesso a um.

Minha esposa Virgínia e minha filha Manuela pelo carinho e amor incondicional, que nos manteve juntos nesses dois anos conturbados que encaramos

Agradeço ao meu orientador professor Dr. Raphael Machado pelo envolvimento que teve com essa pesquisa, pelos esclarecimentos, orientações e toda ajuda desprendida.

As colaborações do Cmte. Patrick Lara da AgNSNQ, da Cmte. Luciana Briggs e do Engº Medeiros do IpQM, e do Sr. Paulo Fernandes da Eletronuclear pelas horas com que se dedicaram na contribuição com a coleta de informações para esse trabalho.

Ao meu chefe, Cmte Kurt Rocha Branco, pelos conselhos e apoio que sempre precisei.

Aos colegas de trabalho Belezia, Amilton, Gregório, Gama e José Fernandes, pela ajuda, amizade e consideração.

RESUMO

A Marinha do Brasil como forte expressão militar no cenário mundial busca se manter equipada com os mais modernos meios marítimos, terrestres e aéreos, o que acarreta a constante modernização com a crescente implementação de equipamentos eletrônicos, digitais e informatizados. Dentre seus projetos de expansão e modernização, o mais inovador e moderno em andamento é o desenvolvimento de um submarino, convencionalmente armado, movido a energia nuclear, uma tecnologia singular, desenvolvida e prototipada em sua totalidade por brasileiros. Que faz grande uso de sistemas digitais na sua instrumentação e controle, que necessitam funcionar de forma correta segura, cuja comprovação dá pela demonstração do atendimento a uma série de requisitos e condições previamente especificadas em um processo de avaliação da conformidade. Visando atender a esta necessidade, este trabalho propõe um protocolo para avaliação de *softwares* empregados nos sistemas digitais de meios nucleares navais. Denominado ProAS-NN, acrônimo para Protocolo de Avaliação de *Softwares* no âmbito Nuclear Naval, utiliza a técnica de Validação e Verificação, o que acompanha o pensamento de diversos autores, e segue o que é praticado pelo setor nuclear de vários países e recomendado por órgãos reguladores ao redor do mundo, inclusive, em instalações fixas do Brasil, e segue normas para a avaliação de softwares aplicados na atividade nuclear emitidas pela IEEE e NRC, elaborado sob a forma de um guia, observa recomendações para a composição de sistemas de avaliação de software emitidas pelo ISO/IEC. Após seu desenvolvimento passou por um processo de validação, com a submissão a um painel de especialistas em avaliação de *software* no âmbito geral e nuclear, que expuseram suas opiniões, apontaram pontos fracos e necessidades de melhoria. Ainda passou por uma prova de conceito, ao avaliar um *software* de da Marinha do Brasil, utilizado para no auxílio a navegação, onde foi possível avaliar que a proposta de protocolo de avaliação pode ser utilizada para caracterizar um *software* de forma fidedigna, identificando possíveis ameaças à segurança, medidas de controle e proteções para mitigá-las e, sugerir oportunidades de melhorias.

Palavras-chave: avaliação de *softwares*; verificação e validação; planta nuclear naval; segurança da informação; qualidade de software.

ABSTRACT

The Brazilian Navy, as a strong military expression on the world stage, seeks to remain equipped with the most modern maritime, land and air means, which entails constant modernization with the increasing implementation of electronic, digital and computerized equipment. Among its expansion and modernization projects, the most innovative and modern in progress is the development of a submarine, conventionally armed, powered by nuclear energy, a unique technology, developed and prototyped entirely by Brazilians. That makes great use of digital systems in its instrumentation and control, which need to function correctly and safely, which is proven by demonstrating compliance with a series of requirements and conditions previously specified in a conformity assessment process. Aiming to meet this need, this work proposes a protocol for evaluation of software used in digital systems of naval nuclear means. Named ProAS-NN, an acronym for Software Assessment Protocol in the Nuclear Naval scope, it uses the Validation and Verification technique, which follows the thinking of several authors, and follows what is practiced by the nuclear sector in several countries and recommended by bodies regulators around the world, including in fixed installations in Brazil, and follows norms for the evaluation of software applied in nuclear activity issued by the IEEE and NRC, prepared in the form of a guide, observes recommendations for the composition of evaluation systems of software issued by ISO/IEC. After its development, it underwent a validation process, with submission to a panel of specialists in software evaluation in the general and nuclear scope, who expressed their opinions, pointed out weaknesses and needs for improvement. It also underwent a proof of concept, when evaluating a Brazilian Navy software, used to aid navigation, where it was possible to evaluate that the evaluation protocol proposal can be used to characterize a software in a reliable way, identifying possible threats security, control measures and protections to mitigate them, and suggest opportunities for improvement.

Keywords: software evaluation; verification and validation; naval nuclear plant; information security; software quality.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AFCEN	Sociedade Francesa de Regras de Projeto e Construção para Componentes de Ilhas Nucleares
AgNSNQ	Agência Naval de Segurança Nuclear e Qualidade
AIEA	Agência Internacional de Energia Nuclear
AMAZUL	Amazônia Azul Tecnologias de Defesa S.A
AMN	Associação Mercosul para Normalização
CISNE	Centro de Integração de Sensores e Navegação Eletrônica
CNEN	Comissão Nacional de Energia Nuclear
DIN	Instituto Alemão de Normas
ECDIS	Software para a Exibição de Informações de Cartas Eletrônicas
EdF	Electricité de France
ETN	Eletrobrás/Eletronuclear
GPS	Sistema de Posicionamento Global
I&C	Instrumentação e Controle
IEC	Comissão Eletrotécnica Internacional
IEEE	Instituto de Engenheiros Eletrotécnicos e Eletrônicos
IEN	Instituto de Engenharia Nuclear
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
IpQM	Instituto de Pesquisas da Marinha
ISO	Organização Internacional para Normalização
IVC	Índice de Validade de Conteúdo
IVCg	Índice de Validade de Conteúdo Global ou Geral
MB	Marinha do Brasil
MD	Ministério da Defesa
MSD	Média de Satisfação por Dimensão
MSE	Média de Satisfação por Ensaio
MSG	Média de Satisfação Geral

MSI	Média de Satisfação por Item
NUCLEP	Nuclebrás Equipamentos Pesados S.A
PNE	Planta Nuclear Embarcada
PNM	Programa Nuclear da Marinha
ProAS	Protocolo de Avaliação de Softwares
PROSUB	Programa de Desenvolvimento de Submarinos
RECIM	Rede de Comunicações da Marinha do Brasil
S-Br	Submarino Brasileiro
SD	Sistemas Digitais
SDL	Security Development Lifecycle
SGSI	Sistema de Gestão de Sistemas de Informação
SI	Sistemas de Informação
SisC2Geo	Sistema de Comando e Controle Georreferenciado
SN-Br	Submarino Nuclear Brasileiro
SO	Sistema Operacional
TF-SCS	Força-Tarefa de Reguladores em Software crítico de segurança
TI	Tecnologia da Informação
USNRC	Comissão Reguladora Nuclear Americana
V&V	Verificação e Validação
VIM	Vocabulário Internacional de Metrologia

SUMÁRIO

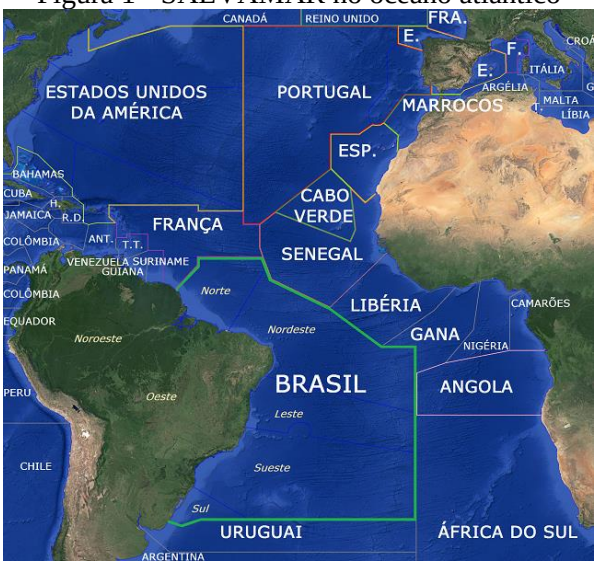
1. INTRODUÇÃO

O mar é um recurso de grande valor para países costeiros, por permitir projetá-los no panorama internacional por meio da navegação, que transporta fontes de energia, pessoas, insumos, alimentos e todo tipo de mercadorias (CARVALHO, 2018). O mar também é associado cada vez mais a uma perspectiva de modernidade e futuro, crítico ao desenvolvimento sustentável do planeta; fator ambiental por excelência; fronteira da ciência e tecnologia; e espaço de turismo, cultura, esporte e lazer (SILVA; SILVA, 2012).

Nessa região há um esplendor de vida nos oceanos, manguezais e recifes de corais, lar de diversas espécies de seres vivos, muitas importantes para o homem e outras que ele se quer conhecemos (ANDRADE et. al., 2018). Além disso, o transporte de quase todo comércio mundial e a exploração de petróleo e gás natural ocorre nos oceanos (SILVA, 2012). O que por si só torna essencial o desenvolvimento de ações à sua proteção.

Há também a responsabilidade que países litorâneos tem quanto as operações de busca, salvamento, atendimento a emergências e salvaguarda da vida humana no mar, conhecido com SALVAMAR, onde cada país é responsável por um setor delimitado, como apresenta a Figura 1 (MARINHA, 2022a).

Figura 1 - SALVAMAR no oceano atlântico



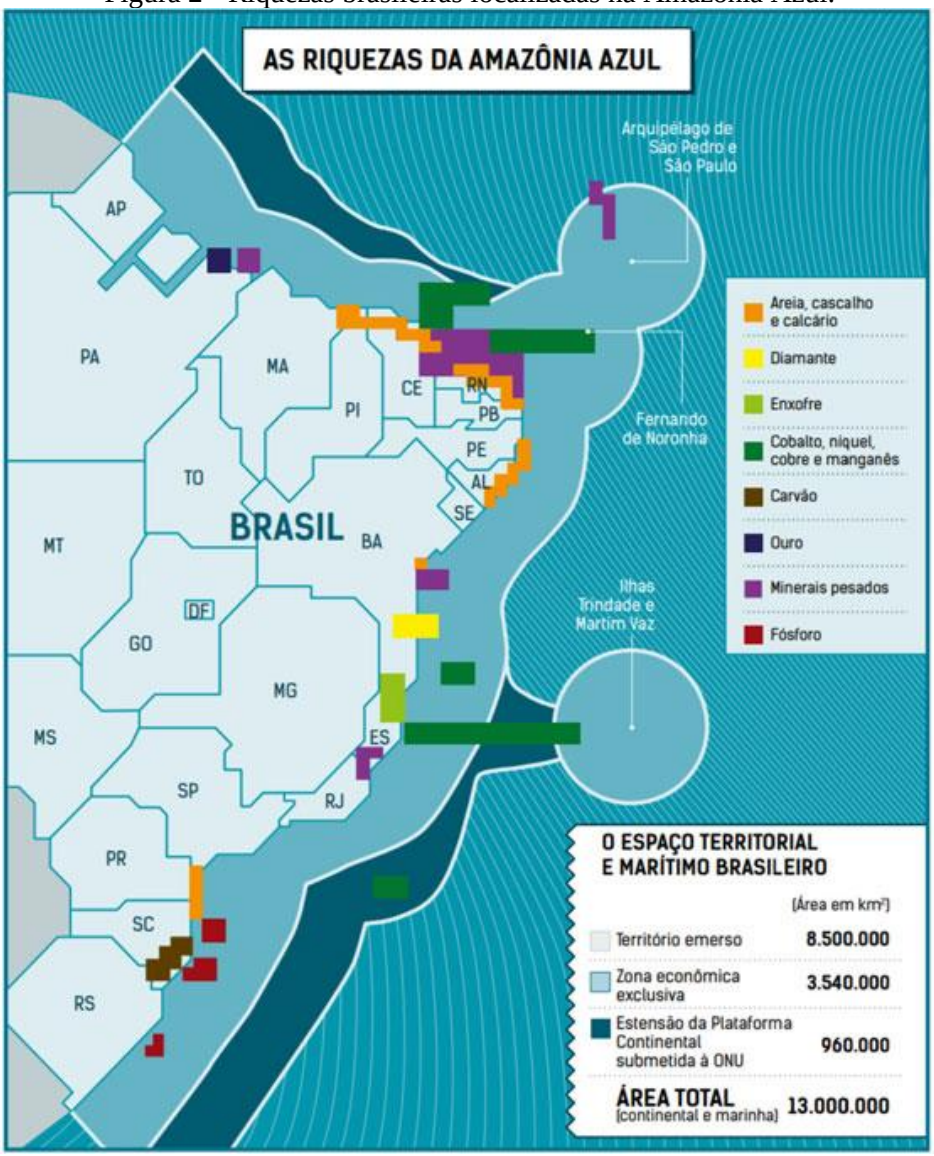
Fonte: SALVAMAR, 2015.

Para fazer-se presente no mar, o homem realiza o emprego de navios, sejam de superfície ou submarinos. Equipados com diversos sistemas digitais (SD) que processam, transmitem e armazenam dados e precisam funcionar de forma correta e segura (FILHO, 2011), pois esses dados, muitas vezes, são a única fonte de informação (SILVA et. al., 2007).

Devido ao enorme tamanho destas áreas marítimas, esses navios, precisam ter grande autonomia e velocidade, uma solução à esta necessidade é o emprego da propulsão nuclear. que utiliza SD nos diversos sistemas a bordo, inclusive no reator nuclear e seus sistemas auxiliares, na medição e avaliação de parâmetros de processos, no controle e atuação de equipamentos, na previsão e análise dos dados (RUDAKOV; DICKERSON, 1997). Que para Benko e Neto (1997) não podem ter suprimidos os processos de avaliação uma vez que a ocorrência de falhas nestes SD pode implicar em liberação e exposição de radiação ionizante ao homem e meio ambiente.

O Brasil com seus 7,5 mil quilômetros de costa (XAVIER, 2020) é soberano na exploração, conservação e gestão dos recursos vivos e não vivos em sua plataforma continental chamada de Amazônia Azul (UNITED NATIONS, 1982), ao explorar o turismo, pesca, transportes e reservas minerais (SILVA, 2012) como as ilustradas na Figura 2.

Figura 2 - Riquezas brasileiras localizadas na Amazônia Azul.



Fonte: Andrade et. al., 2018.

Para se fazer presente no mar, o Brasil investe na expansão do Poder Naval (BRASIL, 2020b). Atualmente, na busca de realizar essa tarefa, dentre outros projetos, está em andamento o Programa de Desenvolvimento de Submarinos Brasileiros (PROSUB) que dentre vários empreendimentos, inclui o desenvolvimento e a construção do Submarino Nuclear Brasileiro (SN-Br) (MARINHA, 2020a), uma aplicação militar da tecnologia nuclear

Entretanto, o Brasil é signatário da cooperação científica e técnica da atividade nuclear em prol do uso pacífico e seguro da tecnologia nuclear (AIEA, 1998) e, por este motivo, necessita cumprir princípios e requisitos de segurança nuclear e radiológica. Que implica que a responsabilidade pela segurança nuclear é papel do governo federal, que deve estabelecer os critérios legais relacionados à proteção das instalações nucleares. Deste fato emana a necessidade da adoção de política que regule o uso de energia nuclear e material radiológico.

Papel desempenhado pela Comissão Nacional de Energia Nuclear (CNEN) (CNEN, 2020), autarquia que licencia instalações nucleares no país, inclusive militares (CNEN, 2002), mas que não dispõe de experiência em meios navais.

Neste contexto e em sinergia com a CNEN, destaca-se o trabalho da Marinha do Brasil (MB) que, além de bicentenária na obtenção e operação desses meios, trabalha em seu programa nuclear há cerca de quarenta anos (MARINHA, 2020a). Tal fato motivou a criação da Lei nº 13.976 de 7 de janeiro de 2020 que combinada à Medida Provisória nº 1.049, de 14 de maio de 2021 atribuí à MB responsabilidade de licenciar e fiscalizar Plantas Nucleares Embarcadas (PNE) (BRASIL, 2020a, 2021a). Onde, segundo Sousa (2019) a Agência Naval de Segurança Nuclear e Qualidade (AgNSNQ), atual Secretaria Naval de Segurança Nuclear e Qualidade (SecNSNQ), (BRASIL, 2022) é a responsável por regular, licenciar e fiscalizar a segurança nuclear de produtos e sistemas navais de defesa (MARINHA, 2019e).

Para cumprir sua missão, a SecNSNQ necessita estabelecer procedimentos próprios para a avaliação da conformidade dos diversos serviços e produtos afetos a PNE do SN-Br (SOUSA, 2019). O que converge com Ahmed, Jung e Heo (2017) que afirmam que é importante ter ferramentas, métodos e processos disponíveis para avaliar *softwares* ao longo do seu desenvolvimento, abrangendo todo seu ciclo de vida. E assim garantir que foram analisados e testados até não serem mais encontrados erros, falhas e vulnerabilidades.

Benko e Neto (1997) confirmam que *softwares* empregados em instalações nucleares são uma categoria de produto que necessita de avaliação da conformidade. Pois diversos são os relatos de ocorrência de incidentes nestas, devido a falhas e vulnerabilidades de *softwares* ou ataques. PARK et. al. (2017) contam alguns, como o *worm* Slammer que aproveitou uma vulnerabilidade em *software* para realizar o ataque à instalação nuclear de DaviseBesse em 2003, que causou o mau funcionamento de sistemas de exibição de parâmetros de segurança. De modo semelhante, ocorreu o desligamento da planta nuclear de Browns Ferry em 2006. Jeong (2020) cita ainda o ataque a planta nuclear de Kudankulam na Índia pelo *malware* DTrack. E o mais emblemático ataque cibernético em a instalações nucleares, ocorrido em Natanz no Irã, provocado pela *malware* Stuxnet, que alterou o controle de centrifugas e provocou uma explosão que destruição um quinto dos equipamentos da unidade.

Como estabelece o método internacional para avaliação da segurança de computadores Common Criteria (2017), em que a avaliação da conformidade de *software* e produtos de Tecnologia da Informação (TI) ocorre por meio da análise e execução de testes que verificam

as medidas aplicadas e o atendimento de requisitos que possibilitam a confiança na segurança e funcionalidade.

1.1. MOTIVAÇÃO

A história apresenta a ocorrência de incidentes e acidentes devido falhas ou ataques a *softwares*. Como os apresentados a seguir.

A THERAC-25, uma máquina de radioterapia para tratamento de câncer que, por falha de *software*, provocou o óbito de pacientes por doses exageradas de radiação (LEVESON; TURNER, 1993). Estudos posteriores apontaram que o desenvolvimento do *software* não foi bem documentado, que não foi revisado e testado por uma parte independente. O acidente do gasoduto russo, maior explosão não nuclear registrada. Investigações indicaram que o acidente foi causado por um *malware* inserido no sistema de controle antes de seu comissionamento (CLARK; KNAKE, 2010).

No acidente que destruiu a nave *Mars Climate Orbiter*, estudos da Agência Espacial Americana (NASA) concluíram que um *software* realizava cálculos em unidades de medidas diferentes das informadas pelos sensores (STEPHENSON; CARTER, 1999). Semelhante ao que provocou a queda de dois aviões Boeing 737 MAX 8, que vitimaram 246 pessoas (MOREIRA, 2020).

Outro caso emblemático, ocorreu na usina de enriquecimento de urânio de Natanz, no Irã, que sofreu uma explosão proveniente de uma aceleração inesperada de centrífugas, controladas por um *software*, que mesmo desconectado de redes foi infectado por um *malware*, chamado STUXNET (ZETTER et. al., 2017). Segundo Baezner e Robin (2017), desenvolvido para atacar instalações nucleares iranianas e impedir seu uso. Radziwill (2018) informa que o STUXNET se propagou pelo mundo até chegar por mídia removível a um operador da usina, infectar seus dispositivos pessoais, de trabalho e da usina.

Estes acidentes, dentre vários outros, mostram o perigo que reside em *softwares* empregados em operações críticas de segurança. E demonstra a necessidade de implementar ferramentas de avaliação da conformidade de forma independente, para revelar falhas e vulnerabilidades (BENKO; NETO, 1997).

Segundo o Inmetro (2012) a avaliação da conformidade é um instrumento fundamental para a aceitação de produtos pela atestação da confiabilidade e segurança. Pereira (2005) cita que a avaliação da conformidade é uma maneira preventiva de evitá-los, que para Kotonya e

Sommerville (1998) permite a identificação de inconsistências, incoerências e inconformidades antes da versão final, o que para Neto (2005) traz economia de tempo e recursos.

Para Mednikarov et. al. (2020b) *softwares* que equipam sistemas navais são sujeitos a deficiências, e, por este motivo, sugerem a aplicação da avaliação da conformidade para sua descoberta e correção. No setor nuclear, por sua vez, a Agência Internacional de Energia Atômica (AIEA) e órgãos reguladores nacionais também propõem a avaliação de *softwares* críticos de instalações nucleares (NRC, 1995).

1.2. JUSTIFICATIVA

Segundo a AIEA (1999) grande é a importância e o uso da TI em instalações nucleares que, segundo a Eletronuclear (2022a), Jeong e Heo (2020) e Park et. al. (2017), vem de forma constante substituindo a Instrumentação e Controle (I&C) analógica. O que para Holmberg, Porthin e Tyrväinen (2016) representa dúvidas quanto à segurança, pois segundo Huang et. al. (2007) pode introduzir novos modos de falha, de acordo com Fukumoto et. al. (1997) a perda da capacidade de processamento de sinal pode levar a interrupção de funções de sistemas de proteção e controle ligados a materiais radioativos, cuja detecção pode ser difícil e demorada, e levar a uma condição insegura e causar um acidente radiológico. Isto, segundo a AIEA (1999; 2000), dificultou a introdução da TI no setor nuclear, e tornou necessária a criação de métodos e critérios específicos para avaliar e julgar sua segurança e integridade, com a atribuição da confiança adequada, e a evidência clara que erros foram detectados e tratados.

Assim como instalações terrestres, um meio naval com propulsão nuclear, pode trazer riscos, caso medidas preventivas como a avaliação da conformidade não sejam executadas (CAMPOS; CAMPO; ROCHA, 2014). O que torna fundamental que exista uma ferramenta especifica para identificar fragilidades e limitações, analisar desempenho e diagnosticar a necessidade de melhorias dos *softwares* empregados (SPERANDIO apud PEGORARO et. al., 2018). Baseado nisso, essa pesquisa apresenta uma proposta de protocolo de avaliação de *softwares* empregados em sistemas digitais de uma planta nuclear naval.

1.3. QUESTÃO DE PESQUISA

Algumas questões têm emergido das experiências e expectativas das atividades de avaliação e licenciamento dos diversos sistemas que irão compor o primeiro meio naval com propulsão nuclear brasileiro. Especificamente quanto aos *softwares*, a questão principal a ser respondida é:

Como avaliar *softwares* empregados em um meio naval com propulsão nuclear?

1.4. ESCOPO

Esse trabalho apresenta uma proposta de protocolo para avaliação de *softwares* empregados em meios navais com propulsão nuclear. Com ênfase na eliminação de falhas, vulnerabilidades e comportamentos maliciosos, essa avaliação considera aspectos construtivos, de projeto, de arquitetura física e lógica, funcionais, e o comportamento do *software*, com vistas ao funcionamento correto e em observação aos princípios da segurança da informação.

1.5. OBJETIVO

O objetivo geral desta dissertação é propor um método para avaliação dos *softwares* empregados na área nuclear de meios militares. Como objetivo específico propor um protocolo para avaliação de *softwares* empregados em sistemas digitais de meios navais com propulsão nuclear. Para denominá-la foi adotado o acrônimo ProAS-NN, para Protocolo de Avaliação de *Software*s empregados em um Meio Nuclear Naval, pertencente a MB.

1.6. ORGANIZAÇÃO DO TRABALHO

Esta dissertação encontra-se estruturada em sete capítulos, incluindo esta introdução:

- Capítulo 2 apresenta a fundamentação teórica sobre o tema, munindo o leitor com conceitos que permitam continuar a leitura do texto;

- Capítulo 3 apresenta o método de pesquisa realizado nesta dissertação. Cujos resultados são apresentados de forma sintetizada no capítulo 4;

- Capítulo 5 apresenta o protocolo de avaliação desenvolvido, explica e justifica sua composição e estrutura;

- Capítulo 6 demonstra o processo de validação realizado, por meio da opinião de especialistas, e a execução de protocolo proposto em um estudo de caso;

- Capítulo 7 descreve as considerações finais, apresentando as limitações do estudo e as sugestões para trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem como propósito apresentar ao leitor os principais conceitos relacionados ao tema desta dissertação, cuja familiarização é importante para a compreensão dos demais capítulos.

2.1. MEIOS NAVAIS

Objeto alvo da avaliação deste trabalho, meios navais, segundo a Marinha (2023) correspondem as embarcações nos seus mais variados tipos e modelos, desde *jet ski* e lanchas a navios em seus diversos tipos, como patrulha, de apoio, pesquisa e de combate, sejam de superfície ou submarinos.

2.2. SUBMARINOS

Classificado com um meio naval, o submarino é uma embarcação projetada e construída para navegar oculta no mar, o que representa vantagem no conflito militar, e poder de dissuasão contra elemento hostil. Para a Marinha (2021a) o diferencial de um submarino nuclear é a forma de geração de energia elétrica, em que motores a combustão interna são substituídos por turbinas que utilizam o vapor gerado pelo reator nuclear, o que torna a embarcação independente de ar atmosférico, sendo capaz de permanecer submerso por longos períodos, além da capacidade de se deslocar a velocidades mais altas e profundidades maiores, tal tecnologia é mantida em segredo por quem a constrói, o que faz com que cada país tenha de desenvolver a sua, como mostra o Quadro 1.

Quadro 1 - Países que detém tecnologia em propulsão nuclear

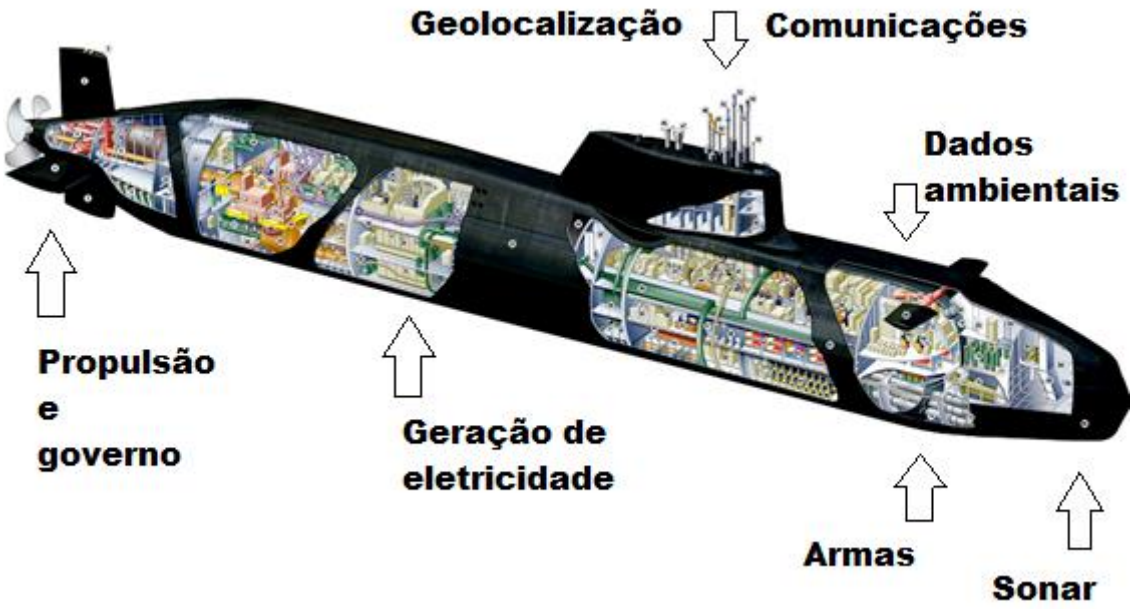
Países que dominam a tecnologia de construção de submarinos nucleares		
Posição	**1ª Embarcação**	**Data de lançamento**
1º	USS Nautilus	21 de janeiro de 1954
2º	K-3 Leninsky Komsomol	9 de agosto de 1957
3º	HMS Dreadnought (S101)	21 de outubro de 1960
4º	Redoutable (S 611)	29 de março de 1967
5º	Changzheng 1 (401)	1970
6º	INS Arihant	26 de julho de 2009
7º	SN Álvaro Alberto (SN-10)	Em construção

Fonte: Wikipedia, 2021.

Um submarino é uma máquina complexa de ser operada, pois navega em um ambiente sem referenciais e “às cegas”. O que torna necessário o embarque de diversos sistemas para apoio a operação, como os sistemas controladores de processo: controle de potência do reator;

controle de pressão; controle de nível e fluxo de resfriamento do reator; controle de pressão; controle de nível de condensador e controle de despejo de vapor, controlador de potência, controle de pressão do condensador, e controle de nível do condensador (BUSQUIM; SILVA, 2021). A Figura 3 demonstra alguns sistemas de um submarino movido a energia nuclear.

Figura 3 - Demonstração de sistemas de um submarino nuclear



Fonte: Adaptado de Marinha, 2018.

Que com o avanço da tecnologia, cada vez menos são empregados sistemas analógicos, devido sua obsolescência e necessidades e manutenção, e mais utilizados sistemas digitais por causa de sua maior disponibilidade, velocidade e capacidade de processamento e transmissão de informações.

2.3. SISTEMAS DIGITAIS

Sistema Digital (SD) é a definição da associação de componentes eletrônicos, integrados em circuitos, placas ou painéis, chamados de *hardware*, com uma unidade lógica, chamada de *software*, responsável por realizar comandos e controles com o emprego e utilização sinais elétricos para medir, receber, processar, controlar e transmitir dados (KERSCHBAUMER, 2020). Para Kastensmidt (2021) SD utilizam equipamentos de *hardware*, como processadores, circuitos integrados e placas lógicas para tratar e armazenar informações e dados por meio de algoritmos lógicos, *softwares*.

2.4. SOFTWARE

Software pode ser traduzido como o suporte lógico para a execução de tarefas em ambiente físico ou virtual. É composto por uma sequência de instruções a serem seguidas e/ou executadas, na manipulação, redirecionamento ou modificação de dados ou informações (FERNANDES, 2002). Pode ser executado em computadores ou qualquer dispositivo microcontrolado, como telefones celulares, painéis de veículos, equipamento com eletrônica embarcada, calculadoras etc. (TOCCI, 2003). Executam desde funções simples que requerem pouco poder computacional, como controles de semáforo de trânsito, a complexas como navegação de naves espaciais não tripuladas (LEE, 2002).

Sobre o contexto da avaliação, a norma NM ISO/IEC 9126-1:2008 (ANM, 2008a) informa que o *software* não deve ser abordado sozinho, pois faz parte de um sistema maior, ao ser integrado a um *hardware* e interagir com usuários por meio de interfaces. A MB (2019a) conceitua *softwares* como todos os sistemas que, utilizam recursos de TI para tramitar, gerar, desenvolver, processar ou arquivar informações. Envolvem sistemas administrativos e operacionais; podendo ser produtos comerciais ou modificados e desenvolvidos sob encomenda, de forma autógena ou terceirizada. Sommerville (2003) complementa ao dizer que o software não deve ser compreendido apenas como a sua programação, como normalmente é feito por um usuário, mas como toda a documentação e dados de configuração que permitem sua correta operação e avaliação.

2.5. AVALIAÇÃO DE SOFTWARES

A avaliação de *software* é o procedimento de identificação da consistência, precisão e contextualização de requisitos, com objetivo de garantir a conformidade, prevenir e eliminar erros, falhas e defeitos, com foco simultâneo no produto e em seu desenvolvimento, por meio da análise da documentação e da realização de testes (BARTIÉ, 2002).

Não deve ser encarada apenas como uma etapa do processo produtivo, mas como uma atividade que envolve o acompanhamento ao longo do ciclo de vida (NRC, 2015). Para Rocha e Campos (1993) e Pressman e Maxim (2021) a avaliação de *software* deve conter o conjunto de ações para verificar o atendimento às necessidades explicitas dos usuários, com confiabilidade e segurança, considerando seu uso pretendido.

Cortes e Chiossi (2001) informam que para *software*s empregados em funções críticas, como controle de veículos e sistemas de geração e distribuição de eletricidade de países inteiros, devem ter uma avaliação mais específica e criteriosa. Já Eom et. al. (2013) trazem que na área

nuclear, órgãos reguladores realizam a avaliação de *softwares* para sua aceitação e licenciamento por Verificação e Validação de (V&V). Segundo Matsuyama (2004) executado continuamente durante todas as fases do desenvolvimento.

2.6. VERIFICAÇÃO E VALIDAÇÃO

A V&V apesar de parecer um processo só, são processos diferentes e com objetivos diferentes (AIEA, 1999). Conforme Pressman (2006) a verificação se refere às atividades que garantem que o *software* implementa corretamente uma função específica, enquanto a validação tem a finalidade de assegurar que o *software* corresponde a requisitos especificados. Wazlawick (2013) complementa que a verificação analisa se o *software* está sendo construído de acordo com o que foi especificado, e a validação que necessidades e expectativas do cliente são atendidas.

Sommerville (2007) informa que a validação demonstra o atendimento às expectativas do usuário. E a verificação evidencia se os produtos de cada fase de desenvolvimento atendem aos requisitos ou condições impostas pela fase anterior e se o sistema ou componente final está em conformidade com requisitos especificados.

2.7. VALIDAÇÃO DO MÉTODO DE AVALIAÇÃO

Segundo Pegoraro et. al. (2018) a validação do conteúdo de um instrumento que avalia a qualidade de um *software* deve ocorrer por um estudo metodológico, realizado em três fases: adaptação do instrumento, validação de conteúdo e testes. Como fizeram Benedetti et. al. (2021) após desenvolverem um *software* que avalia o desempenho de praticantes de Pilates, validado com o apoio de profissionais com conhecimento e experiência no assunto, que receberam o sistema, o utilizaram, e responderam a um questionário quanto a experiência de utilizá-lo. Os autores submeteram as respostas a análise estatística, que possibilitou verificar e confirmar a normalidade pelo teste de Shapiro-Wilk, analisar reprodutibilidade inter-avaliador e intra-avaliador pelo Coeficiente de Correlação Intraclasse (ICC), o teste t-pareado, a ANOVA *oneway*, o percentual de concordância (C) e a medida de concordância Kappa de Cohen (BENEDETTI et. al., 2021).

Lopes (2001) fez semelhante ao realizar a validação de *software* aplicados no ensino de enfermagem, junto a especialistas, que o utilizaram e em seguida preencheram formulários para avaliá-lo, as respostas e tratamento estatístico permitiu realizar o cálculo das variáveis. Assim como Pegoraro et. al. (2018) na validação do *software* que avalia e classifica os riscos no atendimento clínico de pacientes, Oliveira e Freitas (2015) com um *software* de gerenciamento

de documentos para a atividade de enfermagem. E Costa et. al. (2011) e Oliveira et. al. (2021) com *softwares* para avaliação esportiva.

Neto (2012) desenvolveu um método para avaliação da qualidade de *software*. Utilizou questionários direcionado a especialistas, que os preencheram após o uso, com questões relacionadas às características avaliadas e que permitiam identificar o grau de adequação do sistema ao proposto, além de uma visão geral de quão preciso ele se apresenta. E em seguida realizou um teste piloto, com objetivo de validar seu processo de avaliação em um *software* cedido por uma empresa de desenvolvimento.

3. MÉTODO DE PESQUISA

Várias são as razões que demandam a execução de uma pesquisa, como reunir informações para responder a um problema, ou a adequada organização e correlação para sua solução (GIL, 2017). Neste capítulo são apresentadas as atividades realizadas no desenvolvimento da pesquisa, dividida em três fases, a saber:

a) Revisão bibliográfica;
b) Pesquisa documental;
c) Pesquisa de campo.

3.1. REVISÃO BIBLIOGRÁFICA

Foi realizada a revisão bibliográfica da literatura, utilizando livros, revistas, jornais, teses, dissertações e anais de eventos científicos conforme explica Gil (2017). Onde se identificou:

a) Como deve ser realizada a avaliação de *softwares*;
b) A importância e necessidade de realizar avaliação de *softwares* de instalações nucleares;
c) Procedimentos para a avaliação de *softwares*.

3.1.1. Delineamento

As bases de buscas consultadas para a pesquisa foram o Google Acadêmico, SCOPUS e o catálogo de teses e dissertações da CAPES. O Quadro 2 apresenta os termos utilizados na pesquisa, em português e inglês, e a justificativa para a seleção dele. Com o objetivo de obter como retorno artigos que tratem da avaliação de softwares utilizados em instalações nucleares, militares e civis, por meio do processo de verificação e validação.

Quadro 2 – Termos de pesquisa

Termo	Português	Inglês	Justificativa do termo
T1	VALIDAÇÃO E VERIFICAÇÃO	VERIFICATION AND VALIDATION (V&V)	Foi selecionado por ser o método de avaliação de *softwares* realizado por órgãos reguladores internacionais seguidores da AIEA (1999).
T2	SOFTWARES	SOFTWARES	Objeto que se pretende avaliar.
T3	INSTRUMENTAÇÃO E CONTROLE	INTRUMENTATION AND CONTROL (I&C)	Aplicação do objeto que se deseja avaliar.
T4	PLANTA NUCLEAR	NUCLEAR POWER PLANT (NPP)	Refina e restringi a pesquisa a uma população menor
T5	MARINHA	NAVY	Restringi a pesquisa a uma população muito específica.
T6=T1 + T2+T3 +T4+T 5	(VERIFICAÇÃO E VALIDAÇÃO) + (SOFTWARES) + (INTRUMENTAÇÃO E CONTROLE) +	(VERIFICATION AND VALIDATION) + (SOFTWARES) + (INTRUMENTATION AND CONTROL) +	A *string* foi formada pela combinação de todos os termos, com o objetivo de ser o mais específica possível. E ter como resultado da busca o que

	(PLANTA NUCLEAR) + (MARINHA)	(NUCLEAR POWER PLANT) + (NAVY)	é praticado na V&V de *softwares* aplicados em instalações nucleares militares navais.
T7=T1 + T2+T3 +T4	(VERIFICAÇÃO E VALIDAÇÃO) + (SOFTWARES) + (INTRUMENTAÇÃO E CONTROLE) + (PLANTA NUCLEAR)	(VERIFICATION AND VALIDATION) + (SOFTWARES) + (INTRUMENTATION AND CONTROL) + (NUCLEAR POWER PLANT)	A *string* foi formada pela combinação de quase todos os termos com exceção do que faz referência a força militar naval. Na busca por caracterizar o processo de V&V de *softwares* classificados como nucleares de maneira geral.
T8=T1 + T2+T4	(VERIFICAÇÃO E VALIDAÇÃO) + (SOFTWARES) + (PLANTA NUCLEAR)	(VERIFICATION AND VALIDATION) + (SOFTWARES) + (NUCLEAR POWER PLANT)	A *string* foi montada para abranger da forma mais ampla o processo de V&V de *softwares* de instalações nucleares.

Fonte: o autor.

3.1.2. Período de busca

A pesquisa ocorreu entre os meses de julho e outubro de 2022, artigos, teses e dissertações que se encaixaram nos critérios especificados foram selecionados.

3.1.3. Critério de seleção utilizado

Foi dada preferência para textos em inglês e português, e publicados de preferência a partir do ano 2000, com o objetivo de encontrar as informações mais atuais, a pesquisa também utilizou janelas temporais mais estreitas, a partir de 2015, 2010 e 2005, contudo, o retorno da pesquisa ficou bastante limitado. A seleção dos textos ocorreu pela da leitura dos títulos e resumos, e de acordo com o julgamento sobre a utilidade do material encontrado.

3.1.4. Resultados

Por meio de busca pelas *strings* compostas pelos termos T6, T7 e T8, foram identificados 426 artigos pela ferramenta de busca. Ao dar preferência pela *string* correspondentes ao termo T6, o mecanismo de busca não retornou artigos encontrados. Ao utilizar a *string* T7, aplicado o filtro da língua portuguesa e inglesa e com datas a partir de 2000, foram identificados 58 artigos, nos quais o mecanismo de pesquisa encontrou no texto os termos pesquisados. Com a leitura dos títulos, a seleção se restringiu para 31 artigos, que com a leitura do resumo foi identificado que nem todos não eram adequados ao proposto. Sendo selecionados 18 artigos para leitura completa. Cujos informações extraídas são apresentadas e debatidas no próximo capítulo.

3.2. PESQUISA DOCUMENTAL

A pesquisa documental utiliza como fonte de dados documentos elaborados para finalidades diversas tais como: regimentos, procedimentos, autorizações, normas e comunicações, fontes primárias, pois não passaram por tratamento analítico (GIL, 2017).

3.2.1. Delineamento

Na pesquisa documental buscou-se fontes cujo conhecimento técnico e reputação sejam de domino público, no âmbito nacional e internacional, no campo regulatório, da tecnologia da informação e nuclear. Foram consultadas as seguintes fontes:

a) Agência Internacional de Energia Atômica (AIEA);
b) Associação Brasileira de Normas Técnicas (ABNT);
c) Associação Mercosul de Normalização (AMN);
d) Comissão Eletrotécnica Internacional (IEC);
e) Comissão Nacional Reguladora dos Estados Unidos (NRC);
f) Comissão Nuclear de Energia Atômica (CNEN);
g) Instituto de Engenheiros eletrônicos e Eletricistas (IEEE);
h) Organização Internacional de Normalização (ISO);
i) Microsoft Corporation

3.2.2. Período de busca

A pesquisa ocorreu entre os meses de julho e setembro de 2022.

3.2.3. Critério de seleção utilizado

O levantamento documental buscou por normas e documentos utilizados para definir requisitos e estabelecer sistemas de avaliação de *softwares*, de preferência, utilizados em instalações nucleares.

3.2.4. Resultados

Nesta etapa foram identificadas normas que balizam a medição de atributos de *softwares*, pela avaliação; sistemas de gestão da segurança da informação; e requisitos para verificação e validação de *software* em instalações nucleares. Como as ISO/IEC das séries 9126, 14598, 25000 e 27000; IEEE 1012, 7.4.3.2, 603 e 352; AIEA 384 e NS.G.1-1; e NUREG-CR4640, CR-6316 e 08000. Apresentadas e discutidas no próximo capítulo.

3.3. PESQUISA DE CAMPO

Na pesquisa de campo é realizada a observação e a investigação direta do que se está estudando, por meio da coleta de dados pelo próprio pesquisador onde ocorre o fato estudado (GIL, 2017). Seu desenvolvimento tem a característica exploratória, pois busca desenvolver hipóteses, aumentar a familiaridade do pesquisador com o determinado ambiente, fato ou

fenômeno e clarificar conceitos. Possibilita descrever o objeto de interesse, devido a análises conceituais e práticas (MARCONI e LAKATOS, 2003).

3.3.1. Delineamento

Buscou-se por fontes de dados que atuassem na área nuclear, complementadas com dados cujas fontes não atuam na área nuclear, para formar o conhecimento. Na pesquisa de campo foram coletados métodos de avalição praticados por instituições e organismos para serem utilizados de modelos na composição do objeto desta pesquisa. Buscou-se as seguintes fontes:

a) Amazônia Azul Tecnologias de Defesa S.A. (Amazul);
b) Eletrobrás Eletronuclear (ETN);
c) Instituto Brasileiro da Qualidade Nuclear (IBQN);
d) Instituto de Engenharia Nuclear (IEN);
e) Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO);
f) Marinha do Brasil (MB);
g) Nuclebrás Equipamentos Pesados S.A. (NUCLEP).

3.3.2. Período de busca

A pesquisa de campo ocorreu entre os meses de agosto e novembro de 2022.

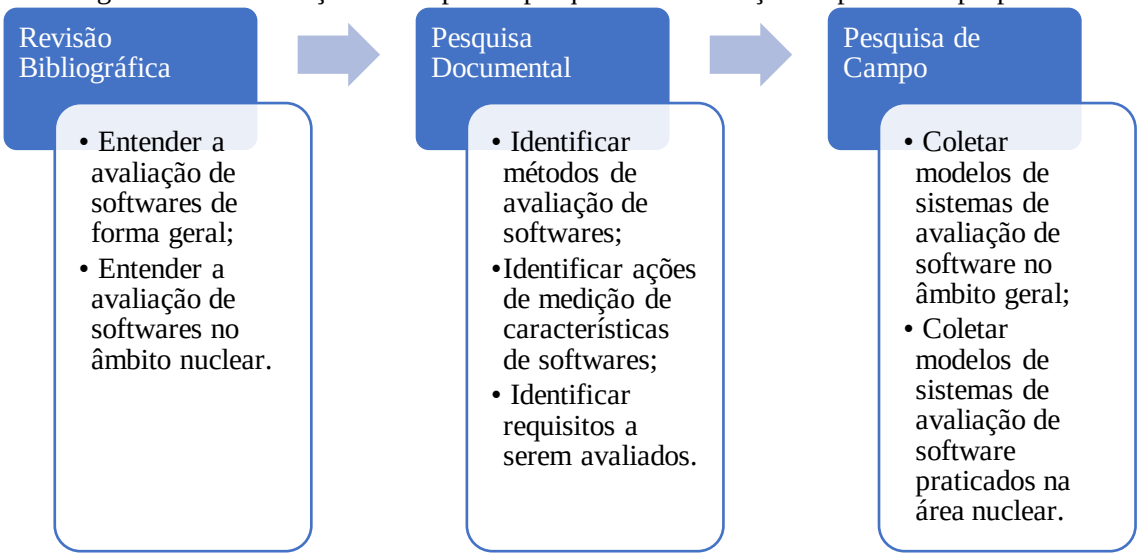
3.3.3. Resultados

Foram coletados os métodos de avaliação de *software* da MB e Inmetro com o auxílio de integrantes de tais instituições, devidamente autorizado para a exploração na pesquisa, na área nuclear foram coletados os métodos de avaliação praticados pela Amazul e Eletronuclear, por meio de visitas as instalações de tais empresas, com a demonstração e explicação de sua utilização.

Os métodos de avaliação coletados não estão disponíveis para consulta pública na internet ou qualquer outra base de dados, esta parte da pesquisa foi caracterizada como pesquisa de campo, porque foi necessário o contato pessoal do autor com membros das instituições e empresas, através de visitas e reuniões, para que fosse possível coletar ou compreender tais métodos, que são apresentados e explorados no próximo capítulo.

Com a realização das três etapas de pesquisa foi possível elaborar a proposta de protocolo sugerida, objetivo principal dessa dissertação, a Figura 4 demonstra a contribuição de cada etapa para o trabalho final.

Figura 4 – Contribuição das etapas da pesquisa na elaboração do protocolo proposto.



Fonte: o autor.

4. RESULTADOS DA PESQUISA

Este capítulo apresenta de forma resumida os resultados obtidos ao realizar as atividades de pesquisa previstas no capítulo anterior, pela revisão bibliográfica, pesquisa documental e de campo, são apresentadas as opiniões e contribuições acerca da avaliação de *softwares* dos autores pesquisados, as recomendações e instruções contidas nas normas estudadas, e a estrutura e conteúdo dos modelos de avaliação de *software* coletados.

4.1. REVISÃO BIBLIOGRÁFICA

Segundo Neto (2005) mundialmente são estabelecidas formas para avaliar *software*, em que o procedimento é essencial para caracterizar o que há por trás da interface. A AIEA (1999) apresenta que em diversos países esses procedimentos são elaborados com base no processo de V&V, como demonstrado no Quadro 3. O que dá credibilidade e sustenta a hipótese de utilizá-lo para a elaboração do procedimento para a avaliação de *softwares* empregados em meios navais com propulsão nuclear no Brasil.

Quadro 3 - Países que realizam o V&V de *software* em instalações nucleares

País	Prática de V&V
Canadá	Realizada pelas revisões de requisitos, pela avaliação da documentação de projeto e do código-fonte; análise de riscos, testes estáticos de caixa branca e caixa preta, e simulações dinâmicas (AIEA, 1999)
Coréia do Sul	Investe constantemente na atualização do processo de avaliação, apoiado pela academia (PARK, SUH, PARK, 2016). Realiza a revisões de requisitos, de forma independente ao longo do ciclo de vida do software (JEONG, 2020). Pela avaliação dos documentos gerados ao longo do ciclo de vida do *software*, complementados por testes dinâmicos (AIEA, 1999)
França	Realizada pela análise documental e realização de testes de requisitos funcionais, por equipe independente (AIEA, 1999).
Hungria	Desenvolvida pelo avanço nuclear do país, dá ênfase na realização de testes nas fases de desenvolvimento do *software* (AIEA, 1999)
Alemanha	Realizado pela revisão documental e por meio de testes que buscam evidenciar o atendimento a requisitos de segurança e assim atribuir confiabilidade ao *software* (AIEA, 1999).
Rússia	Desenvolvido com a experiência nacional apoiada em atividades industriais e acadêmicas, em engenharia de *software* e construção de projetos nucleares. Executada pela avaliação passo a passo, teste de caixa branca e preta, testes de aceitação de fábrica e no local (AIEA, 1999).
Reino Unido	Faz parte do SGQ dos órgãos e empresas que trabalham com instalações e projetos nucleares, aborda a revisão de toda a documentação, código-fonte, inspeção física e verificação do atendimento a requisitos por meio da realização de testes estáticos e dinâmicos, por equipe independente (AIEA, 1999) (FUKUMOTO et. al., 1997).
Suécia	Ocorre com foco na realização de testes funcionais e de segurança. É realizada da comparação com sistemas já utilizados e consolidados

	(AIEA, 1999)
EUA	A avaliação de requisitos de projeto, funcional, controle e de segurança, ao longo do desenvolvimento do *software* (AIEA, 1999).
Japão	Executa o processo de V&V por equipe independente, abrange etapas do projeto, fabricação e testes, previamente planejado. As ações e informações são documentadas, para permitir futuras auditorias (FUKUMOTO et. al., 1997)

Fonte: o autor.

Os processos praticados nestes países trazem informações relevantes sobre a avaliação de *softwares*, praticada por meio da V&V, como praticado no Canadá pela *Atomic Energy of Canada Limited* (AECL) e *Canadian Nuclear Safety Commission* (CNSC), na França pela *Eletricidade de França* (EdF) e no Japão pela Comissão de Energia Atômica Japonesa (AEC), que realizam a revisões de requisitos, por meio da avaliação da documentação de projeto e do código-fonte, análise de riscos, testes estáticos de caixa branca e preta, e simulações dinâmicas que abrangem etapas do projeto, fabricação e testes previamente planejado por equipes de avaliação independentes. As ações e informações são documentadas, para permitir futuras auditorias do mesmo modo que órgãos reguladores da Suécia, Rússia, Alemanha, e evidenciar o atendimento a requisitos de segurança e, assim, atribuir confiabilidade ao software (AIEA, 1999). (AIEA, 1999) (FUKUMOTO et. al., 1997) (PARK, SUH, PARK, 2016) (JEONG, 2020). Aspectos e características que devem ser exploradas para a composição do protocolo de avaliação objetivo deste trabalho.

De acordo com Song (2020), embora os *softwares* utilizados em instalações nucleares sejam semelhantes aos das demais industriais, possuem especificações que os difere quanto a arquitetura e função, para atender a requisitos de segurança nuclear, que necessitam de métodos específicos para a avaliação de segurança, realizados ao longo do ciclo de vida. Que vem sendo estudados há tempos, como feito por Charles Fox, da Marinha Americana, na década de 70 (FOX, 1977). E são alinhadas com a avaliação de softwares empregados em instalações nucleares fixas.

Autores demonstram que a melhor forma de realizar a avaliação em *softwares* empregados em instalações nucleares ocorre pelo processo de V&V, como apresentado no Quadro 4 que resume as contribuições relevantes de cada autor para a avaliação de *softwares* com base na V&V.

Quadro 4 - Contribuições de autores para a V&V de *softwares* na área nuclear

Autor	Contribuição
Fox, 1977	A avaliação de *softwares* empregados em meios navais com propulsão nuclear é de fundamental importância para seu licenciamento. E não pode se restringir a análise do produto pronto, deve ocorrer ao longo do ciclo de vida do *software*. Pela análise da documentação e realização de testes funcionais e estressores.
Eom et. al. (2013)	A avaliação de *software* empregados em instalações nucleares ocorre por meio da V&V, e deve envolver todo o processo de desenvolvimento e demais atividades relacionadas ao ciclo de vida do *software,* com o objetivo de garantir sua confiabilidade e segurança.
Huang et. al. (2017)	A avaliação de *software*s de instalações nucleares deve ocorrer pela V&V, por meio de ferramentas de análises estáticas e dinâmicas. Seguindo as recomendações das normas IEEE 7-4.3.2 e 1012, a árvore de análise de falhas e análise de riscos no processo de V&V.
Jeong e Heo (2020)	*Softwares* críticos em atividades nucleares necessitam passar por rígido processo de avaliação de segurança exercido ao longo do seu ciclo de vida, por meio do processo de V&V, pois cerca de 70% das falhas e vulnerabilidades existentes no produto pronto, surgiram no início do seu processo de desenvolvimento.
Walace e Fujii (1989)	V&V é uma técnica que contribui com a segurança de *softwares* aplicados em instalações nucleares, pela análise de seu processo de desenvolvimento e da realização de teste, ao longo do seu ciclo de vida.
Wei-Tek, Vishnuvajjala e Zhang (1999)	A avaliação de *softwares* empregados em instalações nucleares deve ser realizada por meio da técnica de V&V ao longo do seu ciclo de vida, para evidenciar o atendimento a metas e objetivos, identificar problemas, erros e falhas, que possam impedir o atingimento das expectativas dos usuários.
Rudakov e Dickerson (1997)	A avalição de *software*s em instalações nucleares deve ocorrer pelo processo de V&V, considerado o aspecto mais importante em seu desenvolvimento, pois evita que falhas não detectadas nas fases iniciais se tornem progressivamente mais caras, complexas e difíceis para corrigir nas fases posteriores. Deve ser realizada seguindo o que recomendam normas como a IEC 60880 e IEEE 1012, no que diz respeito aos seus processos de V&V.
Instituto Pengfei Gu de Tec. Nuclear (2016)	V&V deve ser utilizada na avaliação de softwares de instalações nucleares, para garantir que por meio de testes e revisões requisitos afetos a funcionalidade e segurança sejam implementados corretamente.
Andres e Cibys (2000)	A avaliação do *software* empregado na atividade nuclear deve focar em critérios relativos à utilização e funcionamento, e deve demonstrar sua segurança e desempenho adequado.
Cheon et. al. (2004)	V&V é uma ferramenta muito interessante para a avaliação de *softwares* nucleares de I&C de instalações nucleares, pela busca por erros, vulnerabilidades ou falhas. É realizado de acordo com o ciclo de vida do *software*, e inclui a verificação, revisão e inspeção de requisitos de forma rastreável, pela análise documental e realização de testes.

Cheon et. al. (2005)	A V&V deve ocorrer em conjunto com o ciclo de vida do *software*. Com a verificação entre as fases de especificação de requisitos de *software*, especificação do projeto do *software*, escrita do código, integração e testes. Pela revisão, inspeção e análise de requisitos; e realização de testes, com a análise da segurança e um gerenciamento de configuração de *software*
Bahill e Henderson (2004)	A avaliação de *softwares* nucleares deve ocorrer por meio da V&V executada em conjunto, para que ocorra tanto a aprovação na verificação de requisitos, quanto a validação integrada de contexto e o software possa ser licenciado.
Fukumoto et. al. (1997)	A avaliação de *software* em instalações nucleares baseado no processo de V&V, desenvolvido com base em normas e diretrizes japonesas e internacionais, como as IEEE 7.4.3.2 e 1012. Realiza testes estáticos e dinâmicos que devem ser reprodutíveis e auditáveis, por isto devem ser bem documentados, executado por equipe independente de projeto e fabricação, e abranger todas as etapas do projeto e fabricação do sistema, realizado seguindo um plano de avaliação.
Park, Suh e Park (2017)	Sugere um método de implementação de segurança cibernética para *software*s aplicados em sistema de segurança de instalações nucleares, implementado em seu ciclo de vida, com a análise de riscos pela modelagem de ameaças, composta pela identificação de ativos, riscos, ameaças e vulnerabilidades, combinada com a execução de testes de penetração. Recomenda a utilização de normas da NRC, IEC e IEEE na construção de métodos de V&V, em que o processo de avaliação deve envolver *software*s novos e proprietários, pelo processo de V&V, devidamente documentado para possibilitar a realização de auditorias. Apresenta fases do processo de verificação e como deve ser realizada, além de testes executados no processo de validação.
Rankin e Jiang (2011)	A V&V ajuda a determinar se a qualidade ou o desempenho do *software* corresponde as informações documentadas, conforme declarado, pretendido ou exigido, por meio de evidências objetivas de que todos os requisitos funcionais, de desempenho e de interface foram atendidos
Jung et. al. (2016)	Propõe um processo avaliação específica para *softwares* proprietários utilizados em instalações nucleares, por meio de V&V, recomenda que o processo de avaliação de *software* faça parte de um PGQ, de forma a envolver a confiabilidade, PGQ de fornecedores, processos de V&V, processos de gerenciamento de configuração, revisões de projeto, relatórios de teste, rastreabilidade de requisitos, relatório e rastreamento de *bugs* e erros. Em que a verificação é realizada. Em cada etapa do ciclo de vida de desenvolvimento de *software*, para confirmar se o produto de cada fase satisfaz sua especificação de requisitos, pela realização de testes, análise documental, demonstrações de segurança, históricos de uso, define e especifica fases de verificação que devem ser realizadas em *softwares* proprietários.
Ahmed, Jung e Heo (2017)	Aborda a importância da avaliação de *software*s críticos de segurança em instalações nucleares, mediante vulnerabilidades e ataques cibernéticos, por meio da V&V ao longo do ciclo de vida do *software*,

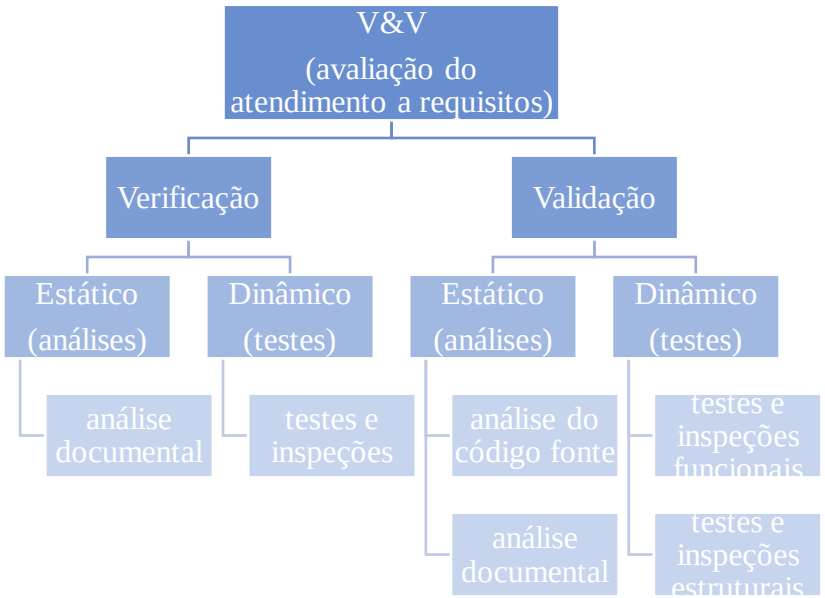
	recomenda o uso das normas IEEE 1012, 7.4.3.3 e 603. Faz uma reflexão da importância da modelagem de ameaças, com a identificação de ativos, análise do fluxo de informação, e criação do diagrama arquitetural do SD. Divide o ciclo de vida em fases e as especifica.
Koo et. al. (2005)	Sugere uma técnica eficaz para a análise de requisitos de *software* por V&V que usa a inspeção de *software*, rastreabilidade de requisitos e especificação formal com decomposição estrutural; define as funções e a composição da equipe de avaliação; apresenta fases do processo de verificação e como devem ser realizadas, e testes executados no processo de validação, bem como os documento utilizados.

Fonte: o autor.

Que de forma sintetizada significa que o processo de avaliação por meio da V&V deve ser realizado ao longo do ciclo de vida do *software* empregado em instalações nucleares, de forma documentada, por equipe independente, o que é de suma importância na garantia da confiabilidade do seu funcionamento correto e seguro, essencial no atendimento às necessidades explícitas dos usuários.

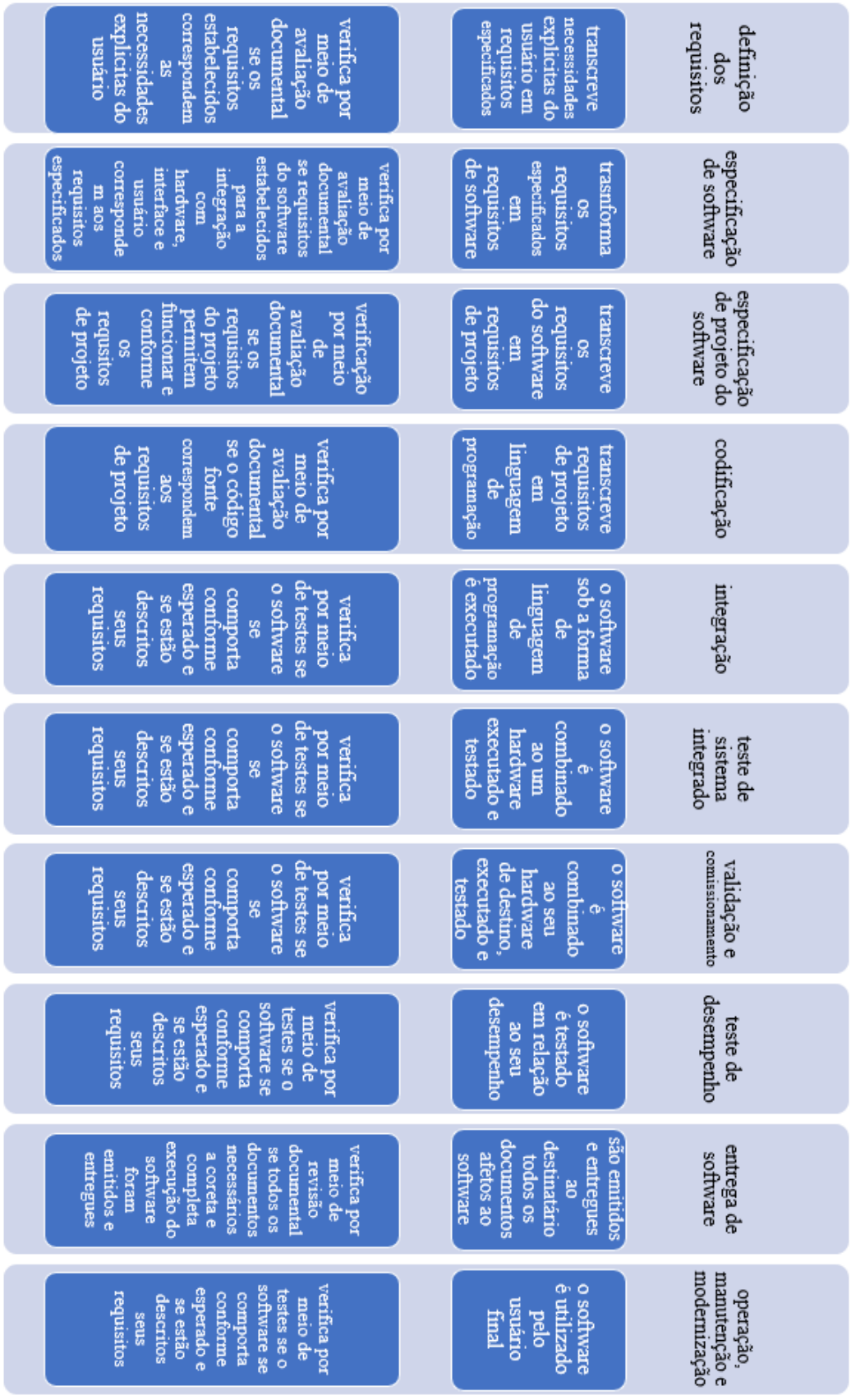
Segundo Bahill e Henderson (2004) e Wei-Tek, Vishnuvajjala e Zhang (1999), a V&V, é realizada pela análise de documentos, manuais diagramas, relatórios e do código-fonte, juntamente com a realização de testes e inspeções físicas, o que coaduna com o prescrito pela AIEA (1999) que chama esses processos de avaliação estática e dinâmica, respectivamente, como mostra a Figura 5.

Figura 5 - Representação do processo de avaliação por V&V



Fonte: o autor.

Figura 6 - Fases do processo de verificação



Fonte: o autor

Walace e Fujii (1989) e Davidson et. al. (2006) apresentam como deve ser dividido o processo de desenvolvimento de *software* em fases, e o que deve ser analisado em cada fase, complementando o que é previsto pelas normas IEEE 1012 (2016), AIEA TR-324 (1999) e NUREG-CR4640 (NRC, 1987), este processo é exposto de forma simplificada na Figura 6, o Quadro 5 representa as fases do processo de verificação abordadas por cada órgão e autor.

Quadro 5 - Organização das fases de verificação

Autores / Fase de verificação	AIEA	ETN	NRC	IEEE	Walace e Fujii (1989)	Davidson et. al. (2006)	Matsuyama (2004)	Park et. al. (2017)	Jung et. al. (2016)	Jeong (2020)	Song et. al, 2012.	Ahmed, Jung, Heo, (2017)	Fukumoto et. al., (1997)
Especificação dos requisitos do sistema	X	X	X	X	X	X	X	X		X	X		X
Especificação do sistema	X	X		X	X	X		X	X	X	X		X
Especificação do projeto do software	X	X	X	X	X		X	X		X	X		X
Codificação do software	X	X	X		X	X	X	X	X	X	X	X	X
Integração do sistema	X	X	X	X	X	X	X	X		X	X	X	X
Testes do sistema integrado	X	X	X	X		X	X	X	X	X	X	X	X
Testes de validação e comissionamento	X	X	X	X				X		X	X	X	X
Desempenho do software	X	X		X									X
Teste de aceitação de fábrica	X	X	X							X	X		X
Teste de aceitação local	X	X								X	X		X
Entrega do sistema	X	X		X			X						X
Operação, manutenção e modificação	X	X	X	X		X	X			X	X		X

Fonte: o autor

Essas informações permitem definir como deve ser realizado o processo de verificação de forma ordenada, utilizando as análises estáticas e dinâmicas.

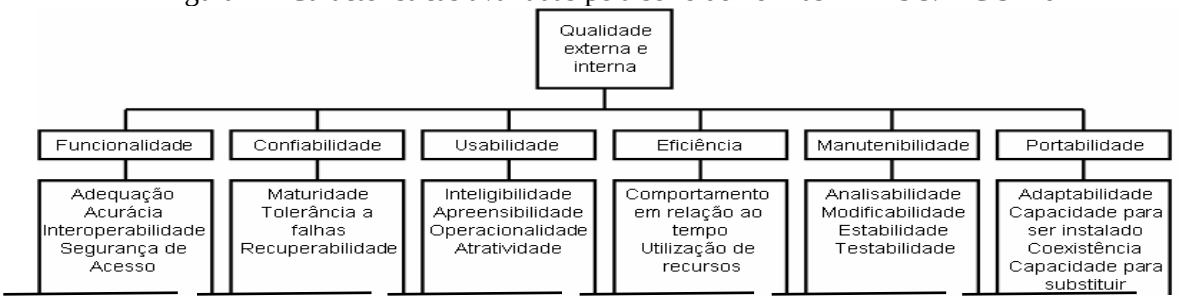
A Revisão Bibliográfica contribuiu para o desenvolvimento do protocolo de avaliação de *softwares*, objetivo deste texto, com o entendimento de como é realizada a avaliação de softwares, principalmente no âmbito nuclear, ao redor do mundo, pela técnica de V&V.

4.2. PESQUISA DOCUMENTAL

A segunda parte da pesquisa, é a pesquisa documental em que se buscou por normas que orientam a avaliação de *softwares*, quanto à qualidade e segurança, de forma geral e específica na atividade nuclear. Dentre as quais, há as séries de normas, NM ISO/IEC 9126, NM ISO/IEC 14598 e ABNT ISO/IEC 25000, de avaliação de *software* no âmbito geral, que

definem modelos de avaliação quanto à qualidade, com o objetivo de identificar erros e inconsistências, pela avaliação de características internas (medidas estáticas do produto intermediário), externas (medição do *software* quando utilizado) e de utilização (de acordo com o atendimento as necessidades do usuário) (ANM, 2008a) (ANM, 2008b) (ABNT, 2014). E a série ABNT ISO/IEC 27000 que trata de processos de avaliação da segurança da informação. Tais normas são aplicadas na avaliação de *softwares* no âmbito geral, pelo estabelecimento de características a serem avaliadas, que podem ser aplicadas na avaliação de *softwares* empregados na atividade nuclear, pois conforme CHUA e DYSON (2004) estas séries de normas constituem um importante conjunto de regras, que objetivam padronizar a avaliação da qualidade de *software*. A Figura 7 apresenta as características de qualidade de *software* avaliadas pela norma NM ISO/IEC 9126:2008.

Figura 7 – Características avaliadas pela série de normas NM ISO/IEC 9126



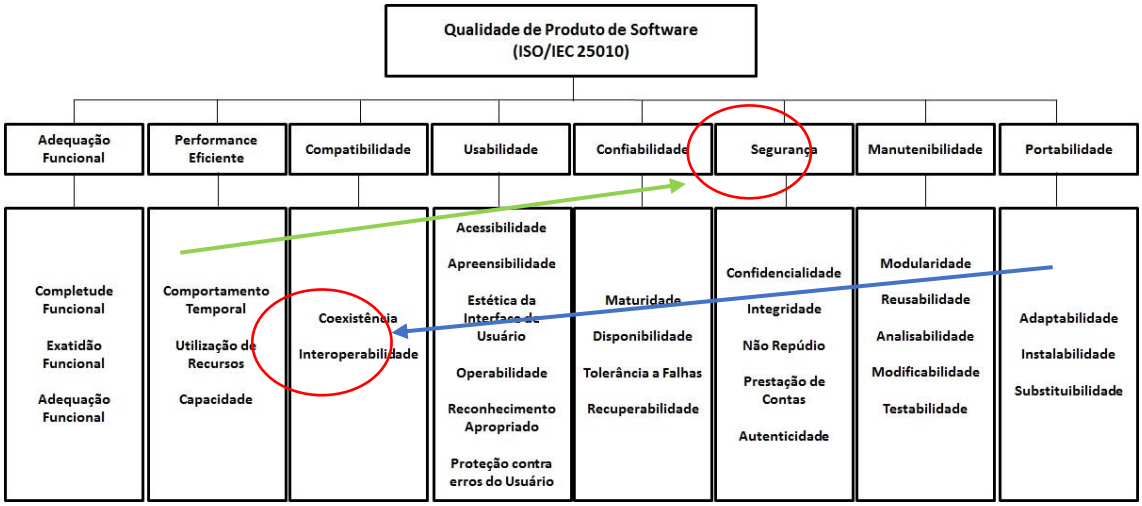
Fonte: adaptado NM ISO/IEC 9126-1:2008.

As normas da série ABNT NBR ISO/IEC 25000 (ABNT, 2008) avaliam as mesmas características, organizadas de uma forma pouco diferente, como apresentado na

Figura 8 que destaca que a SEGURANÇA, tratada na série 9126 como subcaracterística, passa a ser característica e as subcaracterísticas COEXISTÊNCIA e INTEROPERABILIDADE da PORTABILIDADE, passam a compor a característica COMPATIBILIDADE.

Esta série de normas compõe o Modelo de Referência para Medição da Qualidade de Produto de Software (MR-MQPS), que define os procedimentos de identificação, medição, registros e a evidência objetiva das características avaliadas. Assim como a determinação e registro de maneiras para melhorar ou corrigir discrepâncias ou inconsistências afetas a estas características, O que é semelhante a norma ABNT NBR ISO/IEC 15939 na identificação de atividades e tarefas de medição de projeto e estruturas de medição.

Figura 8 - Características a serem avaliadas segundo a série ISO/IEC 25000



Fonte: adaptado ABNT NBR ISO/IEC 25000, 2008.

Outra série de normas ISO/IEC utilizada para a avaliação de *softwares* é a ABNT NBR ISO/IEC 27000 criada para Sistemas de Gestão de Segurança da Informação (SGSI) (ABNT, 2013a), que busca a confiança que os riscos à segurança são adequadamente gerenciados. E que define as características que podem ser resgatadas e aplicadas na composição do procedimento de avaliação de *softwares* objeto desta pesquisa, em seu processo de validação.

Semelhante ao que fazem a ISO e a IEC, a IEEE também publica normas sobre a avaliação de *software* utilizados em funções de críticas de instalações nucleares. O Quadro 6 traz as principais contribuições dessas normas.

Quadro 6 – Contribuições das normas IEEE para V&V de *software* na área nuclear

Normas	Contribuições
IEEE 1012 (2016)	Fornece orientações sobre a V&V ao longo do ciclo de vida do *software* empregado em instalações nucleares, para a identificação e tratamento de potenciais falhas, erros e vulnerabilidades. Faz uso de análises, avaliações, revisões, inspeções e testes, para identificar a presença de anomalias e medição de desempenho do *software*. Possibilita confirmar a conformidade com requisitos, funcionamento de acordo com o uso pretendido e o atendimento as necessidades do usuário.
IEEE 7.4.3.2 (2010)	Especificam requisitos a serem avaliados em *softwares* empregados em instalações nucleares.
IEEE 603 (2009) e 352 (1987)	Trazem recomendações sobre a identificação e gerenciamento de riscos, e a prevenção de problemas potenciais, pela avaliação do seu impacto e determinação de quais foram tratados para garantir o atingimento de metas. Recomenda a utilização da análise de árvore de falhas, FMEA ou modelagem do sistema. Se concentra nos mecanismos de falha em vez de verificar sua operação correta, e estabelece o nível de risco com base no dano associado e na probabilidade da ocorrência. O que permite a correção antecipada, mais fácil e a custo menor.

Fonte: o autor.

As normas IEEE estudadas, por si só já constituem um procedimento de avaliação de *softwares* empregados em instalações nucleares por meio da V&V, o que permite o resgate de vários fragmentos destas normas para a organização do procedimento de avaliação de *softwares* empregados em meios navais com propulsão nuclear.

Para a Agência Internacional de Energia Atômica (AIEA), organização para a cooperação científica e técnica do uso pacífico da tecnologia nuclear, a avaliação deve fazer parte do processo de desenvolvimento do *software*, por meio da análise da documentação e realização de testes, com o objetivo de identificá-los, para a correção de falhas e erros, que podem afetar seu funcionamento e prejudicar seu desempenho. Além de, garantir que requisitos funcionais e de segurança sejam atendidos (AIEA, 2000).

A AIEA (1999) recomenda a utilização do método de V&V para a avaliação de *softwares* empregados em instalações nucleares, que deve ser planejada de acordo com o tipo de *software*, classificados, conforme Quadro 7.

Quadro 7 – Tipo de *software* segundo a AIEA

Tipo software	definição	Verificação	Validação
Software novo	Desenvolvido especificamente para a aplicação, possui toda documentação necessária para a avaliação disponível. Por ainda não ter sido avaliado ou usado, não possui registros e histórico de uso e testes.	Ocorre junto ao desenvolvimento entre suas fases, possibilita a correção de falhas antes do início da próxima fase, sua principal fonte de informação é a documentação.	Baseada nos requisitos do sistema, envolve simulações estáticas e dinâmicas que representam operação normal. Cada função oferecida deve ser confirmada por meio de testes.
Software acessível existente	Já foi empregado, possui documentação, código-fonte e experiência operacional disponíveis à avaliação. Encontradas anomalias serão registradas e não resolvidas.	O acesso a documentação de desenvolvimento e de aplicações anteriores, possibilita verificar se funcionalidades e desempenho são condizentes. A revisão da documentação ocorre da mesma forma que no novo *software*.	Envolve a mesma validação do *software* novo, na medida em que a documentação permita, para conferir se seu desenvolvido ocorreu de acordo com boas práticas. Analisa o histórico de uso.
Software proprietário existente	É um produto comercial que atende à necessidade, mas em que o código-fonte e a	A pouca documentação disponível, serve para revisar os	Como normalmente não se pode fazer uso de documentos de desenvolvimento e do

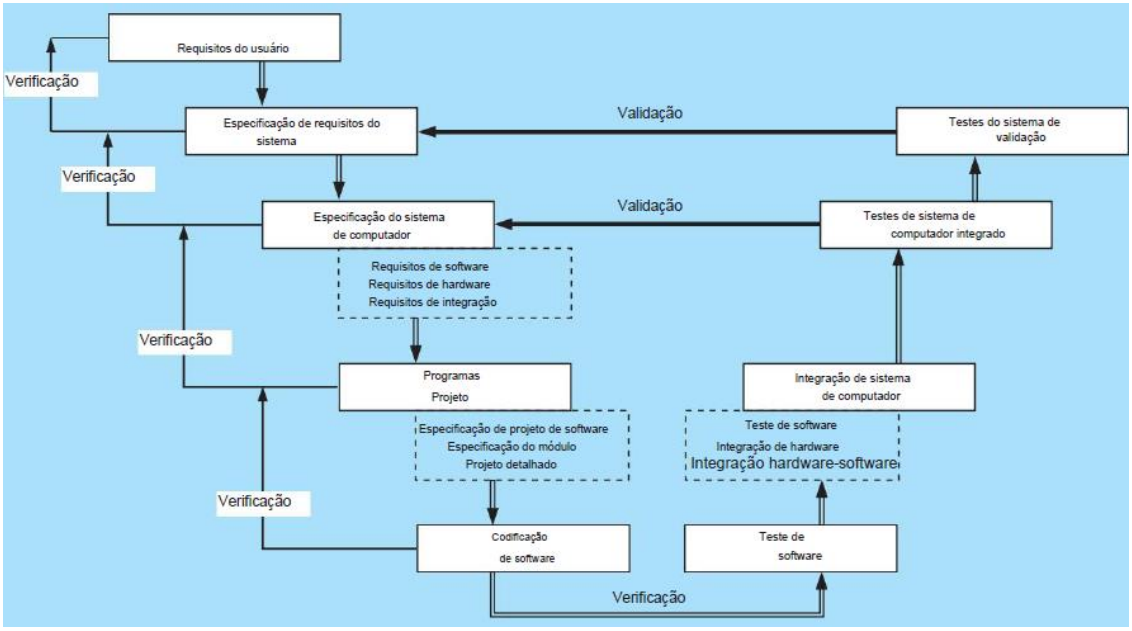
	documentação são pouco disponíveis. Sua avaliação se baseia na experiência de uso e nos testes. Necessita da cooperação do desenvolvedor ou fornecedor para a avaliação.	requisitos, de forma semelhantes a *softwares* novos, mas com testes adicionais. Os registros de uso e testes são usados para demonstrar a adequação ao propósito.	código fonte, o histórico operacional referente a um período adequado deve ser avaliado. Combinado a realização de inspeções físicas e testes.
Software configurável	É o que pode ser configurado de acordo com a demanda, sua avaliação é dividida, uma etapa para o *software* básico e outra para a versão modificada.	A parte configurável deve ser verificada como um *software* novo. O *software* básico pode ser tratado como *software* existente, a verificação de acordo com a documentação.	Segue as abordagens descritas para *softwares* acessíveis ou proprietários existentes. Os aspectos configurados do software devem ser validados como *software* novo.

Fonte: o autor.

Assim sendo, o processo de V&V deve ser realizado de acordo como o tipo de *software*, em que cada tipo possui peculiaridades que permitem a realização da avaliação de uma maneira distinta o que se adequa ao previsto na estruturação do processo de avaliação apresentado pela ISO/IEC, em que deve se caracterizar o *software* e seu ambiente para planejar o processo de avaliação.

A Figura 9 ilustra como a AIEA realiza a V&V. O processo de verificação entre as fases do desenvolvimento já foi apresentado neste texto. A validação ocorre nas fases finais do processo de desenvolvimento, com o *software* já próximo de seu estágio final. E é realizado pela análise do atendimento aos requisitos iniciais que motivaram a sua produção, juntamente com requisitos estabelecidos pelo processo de avaliação.

Figura 9 - ciclo de vida do *software*

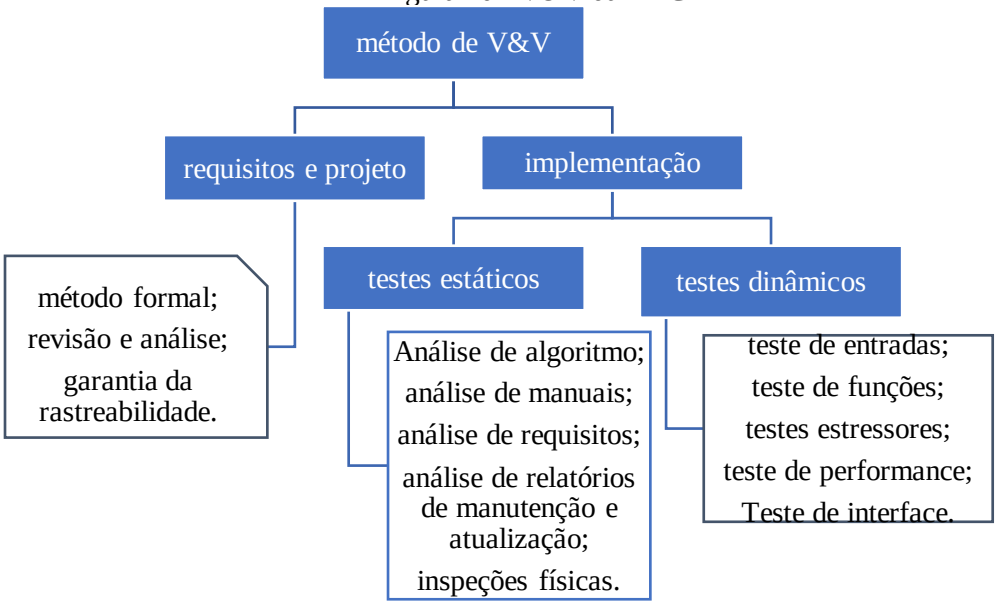


Fonte: AIEA, 1999.

A Comissão Reguladora Nuclear dos EUA (NRC) faz uso do processo de V&V no desenvolvimento e aplicação de *software* em instalações nucleares, ao compilar recomendações e boas práticas de engenharia na aplicação de requisitos para garantir o uso seguro de *software* pela norma NUREG-CR4640 para o processo de V&V (NRC, 1987).

A NRC estabelece ainda a necessidade de implantação de um Programa de Garantia de Qualidade (PGQ) na execução da V&V, que deve ocorrer de forma incorporada ao projeto e desenvolvimento do *software* inclui revisões, auditorias e testes, como demonstrado na Figura 10.

Figura 10 - V&V da NRC



Fonte: adaptado de NRC, 1995.

Esse PGQ consiste em atividades planejadas e sistemáticas para avaliar as características necessárias, pela aplicação de procedimentos, técnicas e ferramentas ao longo do ciclo de vida do *software* para garantir que esteja em conformidade ao atender requisitos pré especificados, no processo de desenvolvimento. E tenham um desempenho satisfatório. A verificação garante que o desenvolvimento de *software* progrida ao longo do ciclo de vida de maneira rastreável, planejada e ordenada, verifica se as saídas de cada fase representam as entradas. A validação é mais ampla, realizada por meio de dois critérios fundamentais, primeiro que o *software* executa de forma adequada e correta todas as funções pretendidas e, segundo que não execute qualquer função que por si só ou em combinação com outras funções possam degradar o desempenho do sistema. Para prevenir problemas e remover defeitos à medida que são encontrados e antes de se tornarem mais complicados, além de contribuir com a usabilidade e manutenibilidade do *software.*

A NUREG 08000 (NRC, 2016) cita que as informações a serem revisadas no processo de V&V podem estar contidas nos seguintes documentos:

- Plano de Gerenciamento de Software;
- Plano de Desenvolvimento de Software;
- Plano de Garantia de Qualidade de Software;
- Plano de Integração de Software;
- Plano de Instalação de Software;
- Plano de Manutenção de Software;
- Plano de Treinamento de Software;
- Plano de Operações de Software;
- Plano de Segurança de Software;
- Plano de Verificação e Validação de Software;
- Plano de gerenciamento de configuração de software;
- Plano de Teste de Software;
- Relatórios de testes.
- Relatórios de gerenciamento de configuração;
- Documentos de projeto.
- Tabelas de configuração de instalação;
- Manuais de operação, manutenção e treinamento.

A NRC por meio da NUREG-CR-6316 (1995) define as fases do processo de verificação, enquanto a NUREG-CR4640 (NRC, 1987) estabelece atributos que devem ser validados.

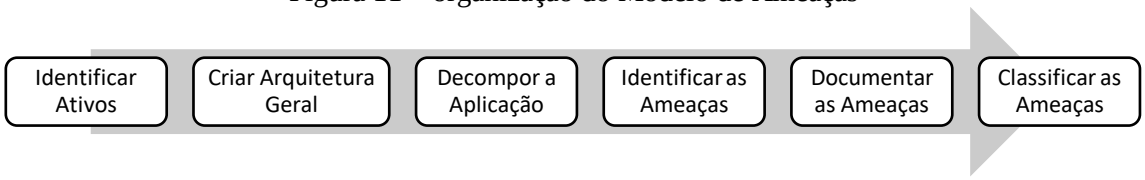
Microsoft Corporation também realiza a avaliação de segurança de seus produtos, dentre as atividades realizadas no *Security Development Lifecycle* (SDL), método voltado a segurança

e privacidade das informações, que abrange todas as fases do desenvolvimento do software, em busca sistemas mais seguros e com menos custos, está contida a modelagem de ameaças.

Um método de análise de riscos que busca pela demonstração de segurança e qualidade, para a identificação, categorização e classificação de ameaças com o levantamento antecipado de erros, falhas e vulnerabilidades, que possibilita a adoção de contramedidas efetiva para sua correção (SILVA, 2018).

A Figura 11 demonstra o passo a passo da realização do modelo de ameaças. Pela visão arquitetural de alto nível do sistema, com a lista de ameaças e riscos identificados, organizadas de acordo com a gravidade, não percebidos durante o desenvolvimento, o que faz que medidas de proteção e controle sejam priorizadas (DONDA, 2012).

Figura 11 – organização do Modelo de Ameaças



Fonte: o autor.

As ameaças são identificadas pela técnica STRIDE que por meio da investigação de riscos às propriedades do software, apresentada no Quadro 8, possibilita a formulação do modelo de ameaças (JEGEIB, 2021) (SILVA, 2018). Que contém a lista de riscos associados.

Quadro 8 – Identificação de riscos pela técnica STRIDE

Ameaça	Propriedade	Definição
Spoofing	Autenticação	Personifica algo ou outra pessoa que não é para o acesso ilegal, burlando a segurança (INFOMACH, 2020).
Tampering	Integridade	Modifica dados ou códigos propositalmente e com má intenção (SILVA, 2018).
Repudiation	Não repudio	Alega não ter realizado uma ação, sem que haja maneiras de provar o contrário.
Information disclosure	Confidencialidade	Expor informações não autorizadas.
Denial of servise	Disponibilidade	Negar, degradar ou torna um sistema inacessível, pela exploração exagerada e não autorizada de seus recursos, de forma a não atender demanda legitima (ALVES, 2021).
Elevation of Privilege	Autorização	Obter recursos sem a autorização adequada, e a escalada de privilégio (RODRIGO, 2020).

Fonte: adaptado de Donda, 2012.

De acordo com a Microsoft Corporation (2003), os riscos são classificados de acordo com a pontuação estabelecida pelo método DREAD apresentada no Quadro 9, com os respectivos parâmetros para atribuir a pontuação, de acordo com suas características, e estabelece a ordem de prioridade para as ações de tratamento. Os riscos são ranqueados de acordo com a pontuação obtida pela análise dos seus efeitos e na facilidade em sua execução,

que é dividido em níveis, correspondente a pontuação demonstrada no Quadro 9 (MICROSOFT, 2003).

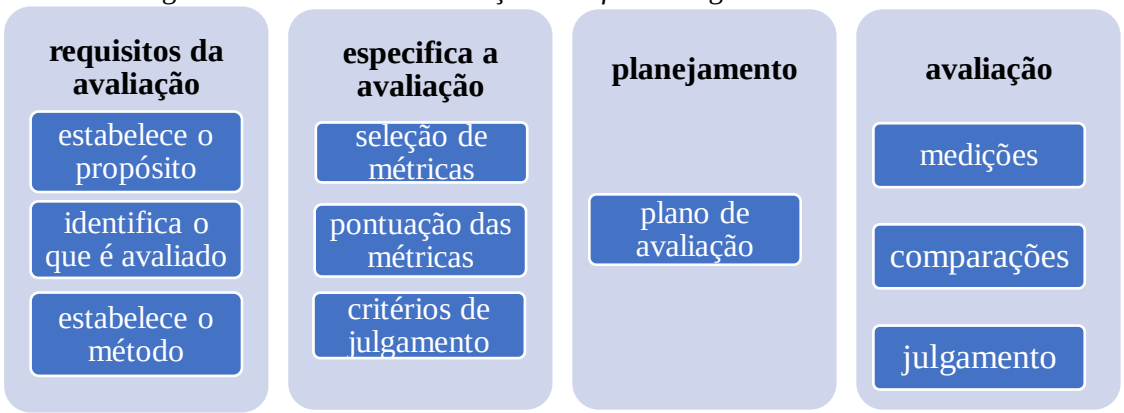
Quadro 9 - Técnica DREAD de classificação da ameaça

Classe Valor atribuído	Muito baixo (0)	Baixo (1)	Médio (2)	Alto (3)
Damage (Danos)	Atividade sem danos	Vazamento trivial de informações acerca dos ativos e/ou usuários	Vazamento de informação sensível dos ativos e/ou usuários, ou perda de informação	Permite que o atacante controle um ativo ou se torne seu administrador
Reproducibility (Reprodução)	Os mecanismos de proteção repelem os ataques	Um ataque realizado é difícil ou impossível de reproduzir	O ataque apenas pode ser reproduzido em um tempo e condição particular	O ataque pode ser reproduzido a qualquer momento
Exploitability (Exploração)	Mesmo que haja probabilidades de exploração, requer diversos recursos, menos disponíveis ao atacante.	O ataque requer uma pessoa com profundo conhecimento técnico ou com conhecimento interno do sistema.	Uma pessoa tecnicamente hábil, pode realizar o ataque e depois, repetir os passos de exploração	Uma pessoa com pouco conhecimento técnico pode realizar o ataque em tempo seguindo um guia
Affected Things (Coisas afetadas)	O ataque não afeta coisa alguma	Um pequeno número coisas são afetadas	Um grupo de coisas são afetadas	Todos as coisas são afetadas
Affected Users (Usuários afetados)	Não traz riscos ou danos diretos aos usuários do sistema	Traz baixo riscos ou danos diretos aos usuários	Traz risco consideráveis e danos diretos aos usuários	Traz alto risco e danos diretos aos usuários do sistema
Discoverability (Acobertamento)	Uma solução alternativa é aplicada e corrige a vulnerabilidade	O ataque é visível ou facilmente perceptível	O ataque é difícil de ser entendido. É muito difícil compreender os danos de sua exploração.	O ataque pode ser percebido apenas por alguns usuários e com muito esforço.

Fonte: o autor.

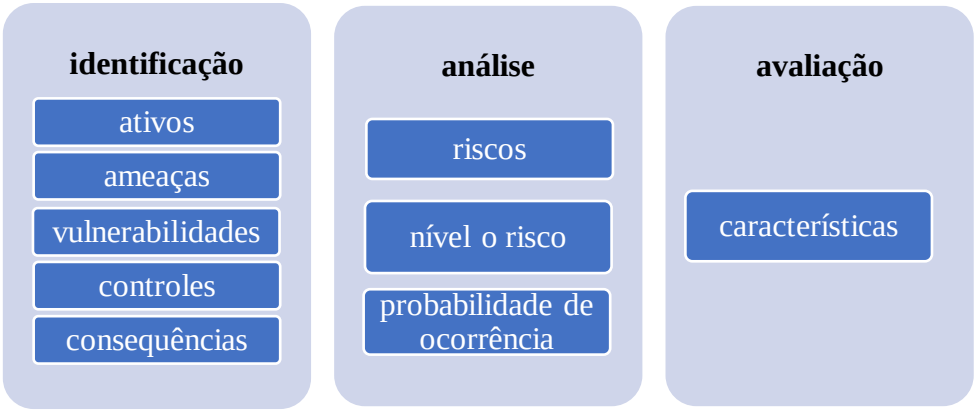
Quanto a estrutura do processo de avaliação, a norma ABNT ISO/IEC 14598 (ABNT, 2018) apresenta a estrutura do processo de avaliação, dividido em quatro fases principais, como ilustra a Figura 12, que permite identificar o que está sendo avaliado, especificar o que se pretende avaliar, planejar e realizar a avaliação. A série de normas ABNT NBR ISO/IEC 27003 e 27005 (ABNT, 2019) sugerem outra divisão do processo de avaliação, composta por três momentos, como representa a Figura 13 em que se identifica o objeto a ser avaliado, seguida pela análise dos riscos aos quais o *software* pode ser exposto e a realização da avaliação.

Figura 12 - Processo de avaliação de *software* segundo a ABNT ISO/IEC 14598



Fonte: adaptado de ISO/IEC 14598, 2018.

Figura 13 – Processo de avaliação da ABNT NBR ISO/IEC 27005



Fonte: o autor.

As estruturas destes dois processos de avaliação podem ser combinadas, de forma a compor um processo de avaliação mais completo, iniciado pela identificação sumária do SD que tem o software avaliado, seu ambiente, contexto e escopo, e, o que permite especificar e planejar o processo de avaliação, iniciado pela análise de riscos; avaliação das características presentes no software, por meio de medições de evidencias objetivas e comparações com padrões estabelecidos, o que fornece informações para ratificar ou refutar a adequação do software em relação ao uso pretendido, ambiente físico e lógico e aos riscos que está exposto. Ao fim da avaliação ocorre a emissão do relatório com as informações identificadas em todo o processo e possíveis sugestões de melhorias e correções.

A Pesquisa Documental contribuiu para o desenvolvimento do protocolo de avaliação de *softwares*, objetivo deste texto, com a identificação de como deve ser estruturado um método de avaliação de *softwares* no âmbito nuclear, quais as características que devem ser avaliadas e como devem ser realizadas as ações para sua medição, quais as fases de verificação que devem ocorrer, como os tipos de *software* devem ser classificados e quais as diferenças no processo de avaliação de acordo com o tipo de *software*.

4.3. PESQUISA DE CAMPO

A pesquisa de campo buscou identificar como instituições e organizações realizam a avaliação de *softwares* de uso geral e específico na aplicação nuclear. Por meio da coleta de protocolos praticados, aqui expostos, destacadas partes relevantes a serem utilizadas na composição de um protocolo objetivo deste trabalho. O Quadro 10 apresenta, de forma resumida, informações importantes de cada método que podem ser aproveitados, de formal integral ou modificada, nesta tarefa.

Quadro 10- Métodos de avaliação de *software* coletados

Instituição	Contribuição
INMETRO	O processo de avaliação de SD praticado utiliza um conjunto de requisitos que devem ser avaliados, por meio de ensaios realizados em três níveis, para demonstrar conformidade e confiança. Nível Conceitual verifica a consistência, clareza e completude da especificação em relação aos riscos, sua adequação às soluções tecnológicas e a adoção dos princípios básicos de segurança. Pela análise documental e inspeção do ambiente e ativo. Nível Operacional verifica se o *software* se comporta de forma consistente quando executado no ambiente em que foi projetado para operar. É executada por meio de testes Funcionais (operação real) aplicado para ratificar o atendimento aos requisitos especificados na documentação, onde chaves, teclas e combinações devem ser empregadas, menus e demais elementos gráficos devem ser ativados e avaliados. E testes de Segurança, que averiguam o comportamento de funções relacionadas à segurança, exploração de vulnerabilidades, penetração e sobrecarga. Nível Estrutural verifica a consistente implementação do sistema, inclui aspectos de projeto, *hardware*, *firmware* e *software*; e verifica se seu comportamento é consistente com as especificações, com base na documentação de engenharia, especificações de requisitos, códigos de *software*, planos e relatórios de testes (INMETRO, 2020).
Marinha do Brasil	Traz o método de execução de avaliação na força, pela análise heurística, das especificações técnica, e da execução de testes funcionais, para verificar os requisitos, tecnologias, infraestrutura, hospedagem, conectividade e segurança (MARINHA, 2019b), e a conformidade com os padrões de arquitetura; com o devido impacto sobre a infraestrutura de redes; aspectos de segurança e se atende ao projeto (MARINHA, 2019a).
Amazul	O método de avaliação de *softwares* praticado faz parte do seu PGQ e observa as recomendações da série de normas ABNT ISO/IEC 25000. Onde um órgão independente, mas sob sua responsabilidade, com comprovada qualificação, experiência e proficiência necessárias, busca demonstrar por meio de evidências a adequada funcionalidade, o cumprimento de requisitos estabelecidos, e que os testes estabelecidos foram realizados adequadamente. São verificados detalhamentos de requisitos funcionais, de qualidade e segurança. Cabendo a Amazul verificar a documentação da avaliação e ratificá-la (AMAZUL, 2022).

Eletronuclear	O processo de avaliação tem ênfase na qualidade e segurança, pelo processo de V&V ao longo do ciclo de vida (ETN, 2022b). São observados aspectos semelhantes as características avaliadas pelas normas NM ISO/IEC 9126 (ANM, 2008), NM ISO/IEC 14598 (ANM, 2008), observando aspectos de qualidade do sistema e de segurança, controle e proteção da unidade. As atividades são realizadas por um grupo independente de funcionário da empresa, composto por engenheiros e analistas de sistema designados, com apoio de usuários especialistas na aplicação (ETN, 2022b), em buscam de desvios e erros, por procedimentos e instruções de trabalho, inserido no PGQ da empresa (ETN, 2022a).

Fonte: o autor.

A modelagem de ameaças sugerida Microsoft (2018) é ilustrada na Figura 11.

O Quadro 11 sintetiza as características de *software* que os métodos coletados realizam e que as normas estudadas sugerem. O que possibilita estabelecer as características que devem ser avaliadas no processo de validação.

Quadro 11 - Comparação ente os métodos e normas estudados (atributos)

Aspectos / fontes	Amazul	ETN	INMETRO	ISO 9126 /14598	ISO 27000	NRC	MR-MQPS ISO 25000	MB	AIEA	Eom et. al. (2017)	Guerra et. al. (2006)	Martins et. al (2010)	Gomes (2008)	Neto (2012)	Park et. al. (2013)	Laplace e Brun (1998)	Andres e Cybis (2000)	Jeonh (2020)	Sampaio et. al. (2015)
Acurácia	X			X															
Acessibilidade					X		X					X					X	X	
Adaptabilidade	X	X		X			X												
Adequação funcional	X	X		X			X		X										
Ambiente operacional	X		X		X							X						X	
Analisabilidade	X	X		X			X			X					X				
Apreensibilidade	X			X			X					X					X		
Atratividade	X			X															
Auntenticidade			X				X		X										
Coexistência	X	X		X			X	X											
Completude funcional		X	X			X	X			X				X					
Comportamento dos recursos	X	X	X	X			X	X											
Comportamento do tempo	X	X	X	X			X	X											
Confidencialidade		X		X	X		X	X	X										

Contestabilidade			X		X			X	X										
Controle de acesso	X	X	X	X			X	X	X									X	
Corretude funcional		X	X			X				X				X					
Criptografia			X		X			X											
Disponibilidade		X	X				X	X	X	X					X				X
Estabilidade	X			X															
Eficiência			X			X													
Exatidão							X			X		X		X			X		
Flexibilidade						X													
Geração números aleatórios			X																
Instalação	X			X					X										
Integridade		X		X	X	X	X	X											
Inteligibilidade	X	X		X								X					X		
Interfaces	X	X	X				X					X	X	X		X	X		
Interoperabilidade	X	X		X	X	X	X						X	X		X			
Instalação	X			X			X												
Maturidade	X			X			X			X					X				X
Manutebilidade	X	X		X	X	X												X	
Modificabilidade	X			X			X			X					X				
Modularidade		X	X				X			X					X				
Operacionalidade	X	X		X			X	X	X			X					X		
Controle de acesso		X	X		X			X											
Proteção de erros					X		X												
Recuperabilidade	X			X						X					X				X
Registro de Eventos			X		X					X					X				
Redundância		X																	
Responsabilização			X	X	X														
Reusabilidade						X	X			X					X				
Segurança física	X	X	X		X			X	X		X	X							
Serviços e funcionalidade			X						X	X				X					
Substituição	X			X			X												
Temporalidade			X																
Testabilidade	X			X		X	X			X					X				
Tolerância a falhas	X			X			X			X					X				X

Fonte: o autor.

Com base nos conhecimentos e opiniões oriundas dos artigos estudados, é possível inferir que a avaliação de *softwares* utilizados em atividades nucleares deve ocorrer pelo processo de V&V, o que está alinhado com o praticado por órgãos reguladores e instalações nucleares de diversos países, inclusive no Brasil. Que seguindo um processo estruturado e organizado de avaliação de *softwares*, elaborado com base em normas nacionais e internacionais, realiza as análises estática e dinâmica, por meio da revisão documental e da execução de testes de uso e estressores. Que permitem realizar as tarefas de verificação do atendimento a requisitos entre as fases do ciclo de vida do *software*, conforme preconizam normas internacionais e é realizado por órgãos que executam a atividade nuclear. Bem como a validação de requisitos funcionais e de segurança, extraídos de normas e procedimentos de avaliação gerais e específicos da atividade nuclear. O que garante que o *software* empregado em meios navais com propulsão nuclear funcione corretamente, seja seguro e atenda às necessidades explícitas do usuário. O conjunto destas informações e procedimentos serviu de base para a organização do Protocolo de Avaliação de *Software*s aplicado no âmbito Nuclear Naval (ProAS-NN), objetivo deste trabalho e tema do próximo capítulo.

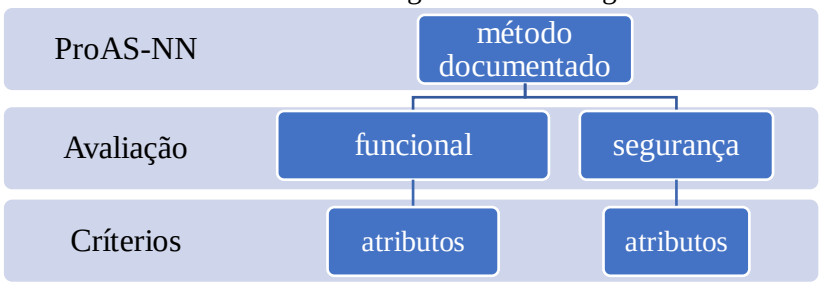
A pesquisa de campo contribuiu de sobremaneira com o desenvolvimento do protocolo de avaliação, objetivo desta pesquisa, por trazer modelos de métodos de avaliação de software no âmbito e geral e nuclear, o que possibilitou a escrita do texto do protocolo de avaliação de forma organizada e condizente com o que é praticado.

5. APRESENTAÇÃO DO PROTOCOLO DE AVALIAÇÃO DE SOFTWARE NUCLEAR NAVAL - PROAS-NN

Este capítulo apresenta o protocolo de avaliação de *softwares* a ser aplicado em meios navais com propulsão nuclear, objetivo deste estudo, elaborado de acordo com os métodos coletados, normas e preceitos apresentados no capítulo anterior.

A visão geral deste protocolo de avaliação é composta pela avaliação funcional do *software*, com a demonstração que ele executa o que foi projetado para executar; e da avaliação técnica de segurança, que visa verificar o atendimento a uma série de requisitos que garantem seu funcionamento seguro, com a evidência objetiva da demonstração do atendimento a critérios estabelecido, conforme demonstra a Figura 14, o que representa os conceitos trazidos por Andres e Cibys (2000), Rocha (1992) e a AIEA (1999).

Figura 14 – Visão geral do ProAS-NN



Fonte: o autor.

O ProAS-NN está contido no apêndice A deste trabalho.

Seguindo o que recomendam as normas ISO/IEC 27003 (ABNT, 2019) e 27005 (ABNT, 2020), o ProAS-NN possui as seguintes seções:

- Introdução;
- Objetivo;
- Campo de aplicação;
- Documentos;
- Definições;
- Responsabilidade;
- Avaliação (método, fases de verificação, atributos de validação e ensaio);
- Relatório.

As seis primeiras seções trazem informações relevantes para a compreensão e realização da avaliação de *softwares*, empregados em meios navais com propulsão nuclear, com o estabelecimento de objetivos, aplicações, conceitos e responsabilidades, que possibilitam a realização da avaliação, que por sua vez é dividida em três subseções:

- Identificação;
- Análise de riscos;
- Verificação e Validação.

A última seção do protocolo de avalição, compreende a confecção do seu relatório.

5.1. INTRODUÇÃO

A primeira seção do ProAS-NN apresenta o processo de avaliação propriamente dito, suas peculiaridades e funcionamento. Também apresenta o fluxograma geral do protocolo, com o método de execução completo e detalhado passo a passo, de acordo com o tipo do software avaliado.

Esta seção foi adotada no ProAS-NN para introduzir e apresentar resumidamente ao leitor o procedimento de avaliação, segue recomendações da série de normas ISO/IEC 9126 (ANM, 2008) e 14598 (ANM, 2008). Seção semelhante foi identificada nos processos de avaliação do Inmetro (2020) e da Amazul (2022).

5.2. OBJETIVO

A segunda seção do ProAS-NN apresenta aos usuários, seja requerente, avaliador, desenvolvedor ou licenciador, seu objetivo, como um guia para a avaliação de *softwares* e, o objetivo de sua aplicação, como avaliação, para a demonstração da confiabilidade de *softwares* empregados em meios navais com propulsão nuclear.

Esta seção foi adotada para demonstrar o objetivo da aplicação do ProAS-NN, compor a justificativa para sua aplicação e inseri-la no processo de licenciamento do sistema que o *software* faz parte. Segue recomendações da série de normas ISO/IEC 9126 (ANM, 2008) e 14598 (ANM, 2008), em seus processos de avaliação, o Inmetro (2020) e a Amazul (2022) adotam uma seção semelhante.

5.3. CAMPO DE APLICAÇÃO

A terceira seção do ProAS-NN define os *softwares* que podem ser submetidos ao processo de avaliação, sejam comerciais ou desenvolvidos sob encomenda. Esta seção faz parte do ProAS-NN, pois, assim como ocorre nos processos de avaliação do Inmetro (2020) e Amazul (2022), possibilita aos usuários utilizá-lo de forma específica na avaliação dos *softwares* para os quais o ProAS-NN foi elaborado.

5.4. DOCUMENTOS

A quarta seção do ProAS-NN elenca os documentos que são produzidos durante o processo de avaliação, e que servem de evidências objetivas de sua execução.

5.5. DEFINIÇÕES

A quinta seção do ProAS-NN apresenta as definições dos termos utilizados, foi adotada para padronizar a terminologia utilizada e, por consequência, evitar que ocorram interpretações errôneas e equívocos pelos usuários. De maneira análoga, os processos de avaliação do Inmetro (2020), MB (2019d) Amazul (2022) e ETN (2022a) e (2022b) dedicam uma seção ao mesmo tema. Em sua composição, foram utilizadas referências trazidas da ABNT (2021) e (2017a), ANM (2008) e AIEA (1999) e (2000).

5.6. RESPONSABILIDADES

Na sexta seção do ProAS-NN são definidas as responsabilidades e papéis dos atores envolvidos no processo de avaliação, tanto por quem avalia como por quem é avaliado.

É previsto que a equipe de avaliação possua independência organizacional de qualquer estrutura ou pessoa envolvida com os processos de desenvolvimento e aquisição de *softwares* e sistemas, como sugere a IEEE (2016), o que segundo o Instituto Pengfei Gu (2016) garante a realização da V&V de forma justa, objetiva e sem interferências, e traz resultados mais reais e evidências de rastreabilidade, também é previsto que a equipe seja composta por pessoal técnico de TI e conte com a participação de profissional especializado na área objeto do *software* avaliado, como aponta Neto (2005) e realiza a ETN (2022a).

Esta seção foi adotada no ProAS-NN para definir as responsabilidades dos agentes envolvidos e garantir que eles tenham clareza de seus papéis, o Inmetro (2020), ETN (2022a), Amazul (2022) e a MB (2019d) também definem as responsabilidades dos envolvidos em seus processos de avaliação.

5.7. MÉTODO DE AVALIAÇÃO

O ProAS-NN busca demonstrar a existência de propriedades de segurança e funcionais, que satisfaçam as necessidades explícitas do usuário, pela análise do atendimento a requisitos especificados e pela avaliação do seu comportamento em operação, por meio de testes (ANM, 2008).

Antes da realização do processo de avaliação é necessária sua formalização entre os participantes, pelo estabelecimento de um acordo ou contrato, que prevê entre outras coisas, que se observe a confidencialidade e imparcialidade no processo, como recomenda a norma ABNT NBR ISO/IEC 9001 (ABNT, 2015).

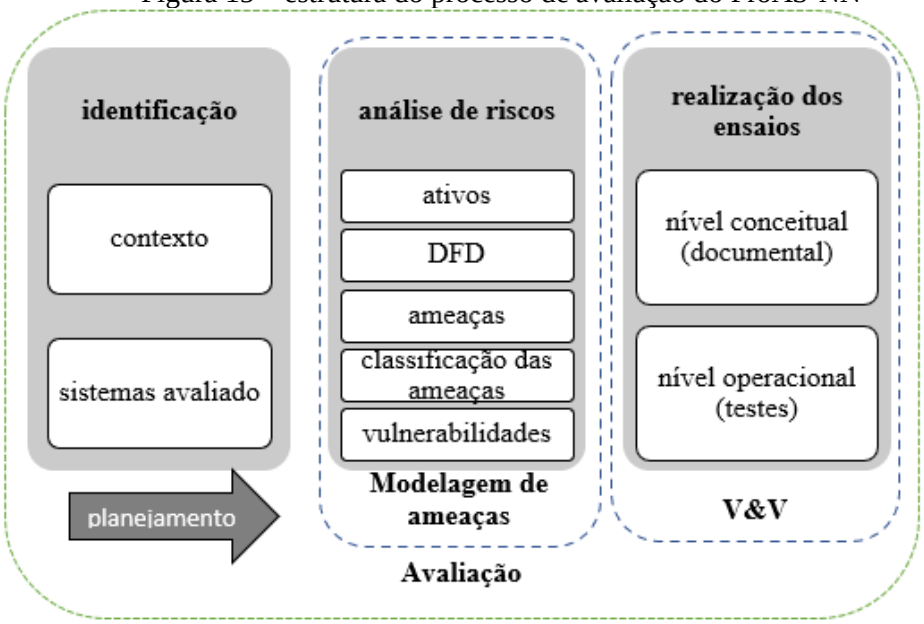
Estabelecido a formalidade do processo de avaliação, segue-se a etapa de preparação para a avaliação, onde cabe:

- ao avaliado montar o dossiê com a documentação do *software*, providenciar uma unidade do *software* para a avaliação e, se for o caso de utilização de *hardware* específico, este também precisa ser disponibilizado ao avaliador;

- ao órgão avaliador nomear formalmente, por meio de ordem de serviço, portaria de designação ou outro documento, os profissionais selecionados dentro dos disponíveis em seu grupo de avaliadores qualificados, para compor a equipe de avaliação; preparar o ambiente físico para a avaliação condizente com o *software* que está sendo avaliado; e as ferramentas físicas e lógicas necessárias para avaliação, conforme informa a NRC (1995).

Para a montagem do método de avaliação do ProAS-NN foi utilizada uma estrutura combinada entre as recomendações de organização do processo de avaliação presentas nas normas ABNT ISO/IEC 14598, 27003 e 27005 (ABNT, 2019) (ABNT, 2020) já apresentadas neste texto pelas Figura 12 e Figura 13, que possibilitou ao ProAS-NN ter um processo de avaliação organizado, célere e prático, sem deixar lacunas e questões importantes passarem despercebidas, que possibilite ser documentado, repetido e auditado. Desta forma, o processo de a avaliação do ProAS-NN ficou organizado em três subseções, onde é realizada a identificação inicial do *software* que possibilita o planejamento da avalição, é utilizado o método de modelagem de ameaças para a análise de riscos e, aplicado o processo de V&V, como demonstra a Figura 15, e é explicado na sequência.

Figura 15 – estrutura do processo de avaliação do ProAS-NN



Fonte: o autor.

5.7.1. Identificação e Planejamento

Na primeira subseção da avaliação, o ProAS-NN realiza a identificação do contexto em que o *software* está inserido, caracteriza a organização usuária do sistema, o ambiente e o sistema em que opera, como descrito por Song et. al. (2012). Por meio da leitura de sua documentação, como descrevem as normas ISO/IEC da série 27000 (ABNT 2019).

O que possibilita identificar o tipo do *software*, dentre os estabelecidos pelo ProAS-NN, que segue a classificação estabelecida pela AIEA (2000), o que permite planejar a execução da avaliação, pois cada tipo de *software* permita a verificação de um conjunto de fases diferentes, conforme citam Andres e Cibys (2000). Também são identificados e estabelecidos os atributos do *software* que passarão pela validação, dentre os previstos no método, pois seguindo o contido nas normas ISO/IEC 27001 e 15288 (ABNT, 2009) (ISO, 2002) a depender do *software* avaliado, nem todas os atributos estarão presentes.

Com o planejamento a equipe de avaliação terá, como sugerem Fukomoto et. al. (1997) e a NRC (1995), um plano que aponta o momento e forma de coleta de dados; a realização de testes, o agendamento de reuniões, entrevistas e visitas; e a organização cronológica dos documentos necessários para a avaliação e os que são gerados durante o processo. O ProAS-NN traz, em seu anexo A um modelo para o planejamento da avaliação, que também é utilizado para a confecção do seu relatório, em complemento ao modelo contido em seu anexo C.

5.7.2. Análise de Risco

Na segunda subseção da avaliação, o ProAS-NN realiza a análise das consequências e probabilidades de ocorrência de riscos, com a identificação e atribuição de valor aos ativos, identificação de ameaças, falhas, vulnerabilidades e medidas de controle, sua relação e efeitos caso se concretizem, organizados em prioridades, como específica Song et. al. (2012) e Huang et. al. (2005) e é recomendado pelas normas ABNT NBR ISO/IEC 27001 (ABNT, 2013a) e IEEE 1012 (IEEE, 2016).

Caso a documentação do *software* não contemple uma análise de riscos, o ProAS-NN, traz, em seu anexo B, o procedimento para a realização da análise de riscos. Dentre as diversas técnicas existentes, foi selecionada a modelagem de ameaças, como recomendam Rudakov e Dickerson (1997) e Ahmed, Jung e Heo (2017). Composta pela visão arquitetural de alto nível do sistema e da lista de riscos à segurança organizada e classificada conforme sua gravidade (DONDA, 2012). Com as vantagens de detectar problemas e falhas que os métodos tradicionais ignoram; identificar novas formas de ataque; ampliar a visão em relação às ameaças, indo além dos ataques padrão (MAUÉS, 2016) e (BRAGA, 2007).

A modelagem das ameaças, como representa a Figura 16, inicia pela identificação dos ativos que formam o sistema avaliado, conforme informa Goulart (2002). Em seguida são mapeados os pontos de interação desses ativos, identificado o fluxo de dados do sistema e as tecnologias utilizadas, com o objetivo de compor o diagrama arquitetural do sistema de acordo com o previsto por Silva (2018) e na norma ABNT NBR ISO/IEC 27001 (ABNT, 2013a).

Figura 16 – Método para criação do Modelo de Ameaças

Fonte: O Autor.

O que permite identificar os riscos que o *software* é exposto, sob a forma de ameaças, considerado fundamental pela norma ABNT/ISO 27005 (ABNT, 2019). O ProAS-NN utiliza a técnica STRIDE (MICROSOFT, 2003), recomendada por Guan et. al. (2011) e Zhang et. al. (2022).

As ameaças são classificadas, conforme sugere a ABNT (2019), quanto a criticidade, utilizando o método DREAD (MICROSOFT, 2003) sugerido por Guan et. al. (2011) Zhang et. al. (2022) e Song et. al. (2012).

Também é feita a identificação das vulnerabilidades que podem ser exploradas para comprometer ativos, como recomendam as normas da série ISO 27000 (ABNT, 2019).

Utilizando a árvore de análise de falha recomendado por Huang et. al. (2017), Sakurada (2001) e Song et. al. (2012), o que possibilita estabelecer a relação causa-efeito de eventos, identificar as causas raízes e obter maior conhecimento do funcionamento do sistema e assim identificar e caracterizar os mecanismos de falhas.

O modelo de ameaças apresentado ainda traz exemplos de ameaças e vulnerabilidades para utilização pelo avaliador, baseado em listas das normas das séries ISO/IEC 9126 e 27000 (ANM, 2008) (ABNT, 2017b).

5.7.3. Validação e Verificação (Realização de Ensaios)

Na terceira subseção da avaliação, o ProAS-NN realiza os ensaios de avaliação, foi adotado o processo de verificação e validação, alinhado com o que é praticado no setor nuclear conforme a ETN (2022) e a AIEA (2000), e por diversos países como o Canadá, Suécia, Reino Unido, Hungria, Rússia, Japão e Coréia do Sul (AIEA, 1999). Que possibilita a melhoria de *softwares* pela identificação de seus defeitos e problemas e da verificação do atendimento aos requisitos e expectativas de usuários, pela análise da documentação, código fonte, testes e simulações, de forma barata e segura, conforme apontam Davidson et. al. (2006) e Bourque e Fairley (2004).

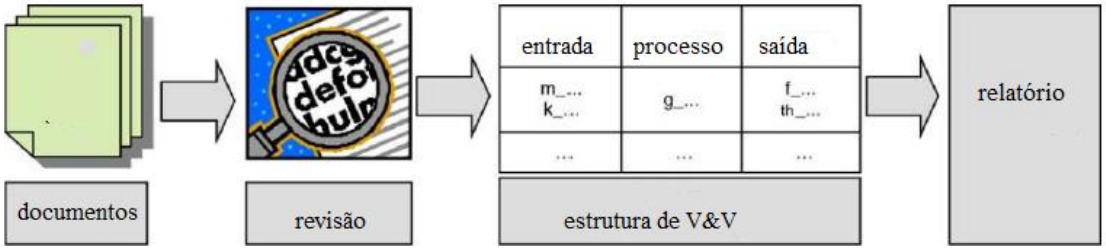
O método de V&V adotado no ProAS-NN é executado durante todo seu ciclo de vida do *software* empregado em meios navais com propulsão nuclear, para garantir a sua confiabilidade e segurança, como apresentam Eom et. al. (2013) e o Instituto Pengfu Gu (2016) e, alinhado com o praticado pela *Electricité de France* (EdF), a Sociedade Francesa de Regras de Projeto e a Construção para Componentes de Ilhas Nucleares (AFCEN) e o Instituto Alemão de Normas (DIN) (AIEA, 1999).

O ProAS-NN executa a V&V por meio dos ensaios de avaliação conceitual pela análise da documentação e operacional pela realização de testes sistemáticos, semelhante ao realizado pelo Inmetro (2020) em seu processo de avaliação. Os ensaios são análogos a avaliação estática e dinâmica descritas pela AIEA (1999), e medições internas e externas com descrito pela ISO/IEC (ANM, 2008a, 2008b) (ABNT, 2014).

O processo de verificação adotado no ProAS-NN é realizado em função do tipo de *software*, seguindo o que define a AIEA (1999, 2000) e a IEEE 1012 (IEEE, 2016), também são estabelecidas as tarefas que devem ser realizadas e os requisitos que devem ser verificados durante cada fase do processo de verificação, conforme descrito pela AIEA (1999). A Figura 17 representa o processo de verificação nas fases do ciclo de vida, em que os documentos

pertencentes a cada fases são verificados na entrada das fases, durante seu processo e na saída das fases, para a composição do relatório de avaliação.

Figura 17 - representação do processo de verificação, por fase.



Fonte: Koo et. al., 2005.

Para o ProAS-NN foi adotada na integralidade a divisão das fases do ciclo de vida recomendada pela AIEA (2000), e por consequência o estabelecimento das fases do processo de verificação, que são seguidas pela ETN (2022a), semelhante ao adotado pela IEEE (2016), que aborda de forma mais ampla a divisão adotada por Davidson et. al. (2006), Wallace e Fujii (1989) e Matsuyama (2004). A Figura 18 apresenta estas fases de verificação de acordo com o tipo de *software*, utilizadas para a verificação por meio do ProAS-NN.

Figura 18 – Fases do processo de verificação de acordo com o tipo de *software*

Fonte: o autor.

Em relação a validação, o ProAS-NN avalia 17 características do *software*, chamadas de atributos, que devem ser validados para garantir que o *software* seja considerado em conformidade e atenda necessidades do usuário de forma segura, como abordado por Eom et. al. (2013). Esses atributos foram selecionados seguindo o preconizado pela norma NM ISO/IEC 9126-1:2008 (ANM, 2008) que descreve que os critérios de avaliação de *software*, sua utilização, funções e usuários. Os atributos selecionados para compor o processo de validação são listados no Quadro 12, juntamente as normas que os referenciam e órgãos que os praticam.

Quadro 12 – Atributos, normas que os recomendam e praticantes

Atributo a ser validado	Norma de referência	Praticantes
Ambiente operacional e cenário de aplicação	ISO 9126 (ABNT, 2008), ISO/IEC 27003 (ABNT, 2019)	Inmetro (2020), Amazul (2022) e órgão reguladores nuclear do Canadá e Coréia do Sul (AIEA, 1999)

Arquitetura de ***hardware*** e segurança física		Inmetro (2020), Amazul (2022), ETN (ETN, 2022a), MB (2020), órgão reguladores nuclear do Canadá, Reino Unido e Coréia do Sul (AIEA, 1999)
Interface de comunicação e interoperabilidade	NUREG-CR4640 (NRC, 1984), ISO/IEC 9126, 14598 e 25000 (ABNT, 2008a, 2014, 2008b)	Inmetro (2020), ETN (2022a) e Amazul (2022)
Serviços e funcionalidades	NUREG-CR4640 (NRC, 1984), ISO/IEC 9126, 14598 e 25000 (ABNT, 2008a, 2014, 2008b)	Inmetro (2020), MB (2020), reguladores da Alemanha, Canadá, Reino Unido e Coréia do Sul (AIEA, 1999)
Usabilidade	ISO/IEC 9126, 14598 e 25000 (ABNT, 2008a, 2014, 2008b)	MB (2020), órgão reguladores nuclear do Canadá e Coréia do Sul (AIEA, 1999)
Mecanismos de autenticação do usuário	ISO/IEC 27003 (ABNT, 2019)	Inmetro (2020), órgão reguladores nuclear do Reino Unido (AIEA, 1999)
Controle de acesso	ISO/IEC 27000 (ABNT, 2014)	Inmetro (2020), MB (2020) e ETN (2022a), órgãos reguladores do Reino Unido (AIEA, 1999).
Criptografia e módulos criptográficos	ISO/IEC 27000 (ABNT, 2014)	MB (2020), Inmetro (2020) e órgãos reguladores do Reino Unido (AIEA, 1999)
Geração de números aleatórios	ISO/IEC 9126 (ABNT, 2008a)	Inmetro (2020)
Disponibilidade e eficiência	ISO/IEC 27000 (ABNT, 2019) e NUREG-CR4640 (NRC, 1984)	Inmetro (2020)
Confiança e desempenho	ISO/IEC 9126, 14598 e 25000 (ABNT, 2008a, 2014, 2008b)	Amazul (2022), ETN (ETN, 2022a), MB (2020) e Inmetro (2020)
Registro de eventos	ISO/IEC 9126 (ABNT, 2019) e ISO/IEC 27000 (ABNT, 2014)	Inmetro (2020)
Temporalidade	ISO/ABNT (2019)	Inmetro e ETN (ETN, 2022a)
Manutenibilidade	NUREG-CR4640 (NRC, 1984) e ISO/IEC 9126, 14598 e 25000 (ABNT, 2008a, 2014, 2008b)	Órgãos reguladores do Canadá, Coréia do Sul (AIEA, 1999) e China (PENGFEI GU, 2016). Amazul (2022) e ETN (2022a)
Segregação de redes	AIEA 384 (AIEA, 2000)	ETN (ETN, 2022a)
Redundância	AIEA 384 (AIEA, 2000)	ETN (ETN, 2022a)
Simplicidade	AIEA 384 (AIEA, 2000)	ETN (ETN, 2022a)

Fonte: o autor

Estes atributos foram selecionados para compor o processo de validação do ProAS-NN, com base nas normas e métodos de avaliação citados, bem como na recomendação de autores estudados.

a) Ambiente operacional e cenário de aplicação - visa, segundo o Inmetro (2020), caracterizar e verificar se o *software* está adequado para ser utilizado perante as peculiaridades e condições ambientais a ele submetidas, selecionado como trazem Martins et. al. (2010) por permitir identificar se o ambiente pode trazer riscos a utilização do *software*;
b) Análise da arquitetura de *hardware* e segurança física – visa demonstrar aspectos de segurança física pertencentes ao *hardware* que carrega o *software*, adotado com o objetivo de identificar se o *software* possui ferramentas para se blindar contra possíveis ameaça presentes no ambiente em que se pretende utilizá-lo (GUERRA et. al. 2006);
c) Interface de comunicação e interoperabilidade – tem como objetivo analisar a segurança e funcionalidade das interfaces e o comportamento do *software* em cooperação com outros. É recomendado por Gomes (2008) e Neto (2012) e foi incorporado ao ProAS-NN por permitir identificar se as interfaces do *software* são seguras contra possíveis ameaça oriundas de sua utilização e se permitem-se ser utilizadas de forma condizentes com o ambiente em que se pretende utilizá-lo, o que é de suma importância para a correta operação do *software*, por ser fonte da maioria das falhas segundo Laplace e Brun (1998);
d) Serviços e funcionalidades - avalia se o *software* executa o que foi projetado para executar, e se sua utilização é natural e fluída, bem como a existência de funções ocultas, adotado por ser considerado a essência da avaliação de *software* por normas da NRC (1984), ISO/IEC (2008a, 2008b, 2014). Segundo Neto (2005) e Eom et. al. (2013) é de suma importância para a avaliação, principalmente em instalações nucleares;
e) Usabilidade – visa descrever a facilidade par entender, utilizar e operar o *software*, com o objetivo de representar o quão fácil e agradável sua utilização é para o usuário, adotado pois segundo Andres e Cibys (2000) e Martins (2004 apud PEREIRA, 2016) é a principal característica que deve ser avaliada em um *software*. Sua avaliação é recomendada pela ISO nas séries de normas ISO/IEC 9126, 14598 e 25000 (ANM, 2008a, 2008b) (ABNT, 2014);
f) Mecanismos de autenticação do usuário – tem o objetivo de caracterizar os mecanismos utilizados para autenticar usuários, passou a fazer parte do ProAS-NN por ser considerado pela ISO/IEC (2019) imprescindível no processo de avaliação e, conforme Cruz, Duarte e Goldschmidt (2017) possibilita que apenas usuários que façam jus acesse a aplicação, um requisito básico e ao mesmo tempo essencial da segurança;
g) Controle de acesso – visa a caracterização da política de controle de acesso, tipos de agentes e separação de deveres, adotado no ProAS-NN por permitir identificar se há a correta separação dos privilégios de utilização do *software* de acordo com o usuário, para que um usuário de uma camada mais inferior não acesse o que é de interesse apenas de usuários de camadas superiores. A ISO trata a característica como essencial na avaliação (ABNT, 2019);

h) Módulos criptográficos – tem o objetivo de caracterizar o uso de algoritmos criptográficos na segurança do armazenamento e transmissão de dados, adotado devido a sua importância na avaliação da segurança, conforme citam Sopran et. al. (2017);
i) Geração de números aleatórios – tem o objetivo de avaliar a geração de números aleatórios e pseudoaleatórios utilizados pelo *software*, passou a fazer parte do ProAS-NN de acordo com recomendações de sua importância pela ISO/IEC (ANM, 2008a);
j) Disponibilidade e eficiência - visa avaliar aspectos de disponibilidade e eficiência em função do uso, adotado pelo ProAS-NN por ser considerado importante por Wei-Tek, Vishnuvajjala e Zhang (1999) por avaliar a capacidade de atendimento a demandas crescentes de usuários, sem perdas, considerando o comportamento em relação ao uso de recursos e tempo;
k) Confiabilidade e desempenho - avalia o comportamento do *software* quanto a sua maturidade, tolerância e recuperabilidade na ocorrência de falhas, foi adotado por ser considerado fundamental na avaliação de *softwares* pela ISO/IEC (1999) e segundo Sampaio et. al. (2015) e Eom et. al. (2013) é essencial na avaliação de *softwares* em instalações nucleares;
l) Registro de eventos – visa permitir que futuras auditorias sejam realizadas no *software*, e revele a ocorrência de fraudes, ou a fonte de erros e falhas, faz parte do ProAS-NN pois segundo Park et. al. (2013) é importante na avaliação de *software*s em instalações nucleares;
m) Temporalidade - avalia os aspectos de marcação de tempo utilizados na operação do *software*, sua avaliação é recomendada pela ISO/ABNT (2019) e Eom et. al. (2013).
n) Manutenibilidade - avalia características e aspectos que influenciam os recursos para modificar o *software* de forma autorizada, como modificabilidade, analisabilidade, testabilidade e adaptabilidade, passou a fazer parte do ProAS-NN pois segundo Reis, Costa e Vale (2015) é fundamental para determinar se as informações de um *software* são seguras e adequadas, confirmado por Marçal e Bueren (2007) e Eom et. al. (2013). Sua avaliação é recomendada pelas normas NRC (1984) e ISO/IEC 9126, 14598 e 25000 (ANM, 2008a, 2008b) (ABNT, 2014);
o) Segregação de redes – visa avaliar se o *software* se comporta adequadamente quando isolado de qualquer rede ou dispositivo externo ao sistema que faz parte. A AIEA (2000) e a ETN (2022a) consideram imprescindíveis que haja sua validação em *softwares* críticos a segurança de instalações nucleares;
p) Simplicidade – visa demonstrar que o *software* foi construído com a maior simplicidade possível, evitando funções complexas e rebuscadas. A AIEA (2000) e a ETN (2022a) consideram como característica fundamental a ser avaliada em *softwares* aplicados em atividades nucleares;
q) Redundância – seu objetivo é avaliar se há pelo menos duplicidades em aspectos como backup e canais de comunicação, para evitar que, a falha de um componente pode ocasionar perda simultânea de múltiplas funções (HUANG et. al., 2007). Sem afetar de forma negativa a consistência da simplicidade, é outra das características que a ETN (2022a) baseada no que faz a AIEA (2000) considera importante ser avaliada.

5.8. RELATÓRIO

Toda a execução do ProAS-NN, os resultados obtidos e observações realizadas são documentadas, seguindo o que recomenda as ABNT NBR ISO/IEC 27001, 27003 e 14598 (2013a, 2020, 2009), e como fazem a NRC (1995), MB (2020), Inmetro (2020), ETN (2022) e Amazul (2022).

O ProAS-NN possui em seu anexo C, um modelo de relatório de avaliação, para facilitar e agilizar sua confecção, pois segundo Fukumoto et. al. (1997) a confecção do relatório de avaliação consome muito da mão de obra da equipe de avaliação, podendo chegar a 2/3 de seu tempo, este modelo permite ao avaliador apresentar todas as informações levantadas desde o processo de planejamento da avaliação, juntamente com aspectos positivos do software identificados e os resultados dos testes realizados, além de ser uma evidência objetiva que comprove sua execução.

6. VALIDAÇÃO DO MÉTODO PROPOSTO

Este capítulo aborda a validação do ProAS-NN, com o objetivo de demonstrar sua adequação ao objetivo proposto, e garantir que é exato, preciso e reprodutível o suficiente para ser aplicado na avaliação de *softwares* empregados em meios navais com propulsão nuclear, seguindo o que recomenda a norma ABNT NBR ISO/IEC 27001 (ABNT, 2013a).

Para Sperling, Coser e Cardoso (2018), Melo (2018) e Lopes (2001) o desenvolvimento de um novo método, envolve um processo de avaliação que estime sua eficiência. Para Benedetti et. al. (2021) e Currell e Jeukendrup apud Oliveira (2021) a validação permite perceber se o método mede realmente o que pretende medir, e se apresenta similaridade com a realidade.

O método de validação do ProAS-NN é composto por dois estágios, a avaliação por especialistas e a prova de conceito por meio de um estudo de caso, como propõe Coluci, Alexandre e Milani apud Sperling, Coser e Cardoso (2018), em três etapas:

1º os especialistas avaliam o ProAS-NN utilizando questionários;

2º os especialistas sugerem melhorias, que são implementadas de acordo com a significância;

3º é realizada a avaliação prática de um software utilizando o ProAS-NN.

6.1. VALIDAÇÃO POR ESPECIALISTAS

Apoiaram nesta fase, seis profissionais com conhecimento e experiência, pois conforme Andres e Cybis (2000) a validação é mais fiel se houver participação de usuários alvos, estes receberam convites à participação voluntária.

6.1.1. Processo de avaliação por especialistas

Foi considerado especialista o profissional com conhecimento e experiência na avaliação de *software*. A seleção dos especialistas, se baseou em uma escala de pontuação, atribuída a critérios, conforme apresentado na Tabela 1, vinculados à experiência prática e acadêmica na avaliação de *softwares*, foi considero especialista o profissional que apresentou a marca mínima de 12 pontos.

Tabela 1 - Parâmetro para seleção de especialistas

CRITÉRIO	PONTOS
Ter curso técnico na área de Tecnologia da Informação	1
Ter curso superior na área de Tecnologia da Informação	3
Ter pós-graduação lato sensu na área de Tecnologia da Informação	1
Ser mestre na área de Tecnologia da Informação	2
Ser doutor na área de Tecnologia da Informação	3

Ter pós-graduação em Avaliação, Qualidade ou Segurança da Informação	5
Ter pós-graduação na área de Qualidade	2
Ter publicado trabalho afeto Avaliação, Qualidade ou Segurança da Informação	2
Ter publicado trabalho na área de Qualidade	1
Participar de grupo/projeto de pesquisa afeto a Avaliação/Segurança de Software	2
Participar de grupo/projeto de pesquisa afeto a Qualidade	1
Ter realizado Avaliação de Software	4
Trabalhar com Avaliação, Qualidade de Software ou Segurança da Informação	4

Fonte: o autor.

Participaram do processo de validação especialistas do Inmetro, Marinha do Brasil e Eletronuclear, foram realizadas tratativas com profissionais ligados a outras instituições, mas não se obteve sucesso. Todos os especialistas que participaram do processo de validação, tem formação acadêmica em engenharia ou sistemas de informação e trabalham com a avaliação de softwares. A Tabela 2 apresenta a pontuação representativa aos especialistas e a entidade a que está vinculado.

Tabela 2 - Identificação da pontuação dos especialistas

Especialista	Entidade Vinculada	Pontuação
A	Inmetro	21
B	Marinha do Brasil	22
C	Marinha do Brasil	21
D	Inmetro	22
E	Eletronuclear	17
F	Eletronuclear	16

Fonte: o autor.

Os avaliadores realizaram a leitura do ProAS-NN, para compreender o funcionamento do método de avaliação e seus critérios, e utilizaram os questionários montados para o processo de validação, respondendo as questões específicas para a avaliação de conteúdo de cada item do ProAS-NN, organizados em 3 blocos, a saber:

- BLOCO I: visa identificar o perfil do respondente, com informações sobre sua escolaridade, formação técnica e experiência, presente no Apêndice B;

- BLOCO II: avalia as fases da verificação; os atributos da validação; e os ensaios de avaliação, com perguntas diretas e respostas objetivas, em uma escala de 1 a 5, onde 5 significa ótimo, 4 bom, 3 regular, 2 deficitária e 1 é ruim, de acordo com a percepção do grau de satisfação do avaliador em relação a importância da análise do item; a clareza, facilidade de entendimento e aplicabilidade do modelo proposto; e a capacidade e completude da avaliação do item. Os questionários seguem descritos nos Apêndices C, D e E deste texto;

- BLOCO III: composto por perguntas abertas para que o avaliador possa expressar comentários e sugestões. É apresentado no Apêndice E deste trabalho.

Para a análise dos dados, foi realizada a verificação da confiabilidade dos questionários pelo coeficiente "α de Cronbach", descrito por Maroco, Garcia-Marques (2006). Quanto a verificação da normalidade dos dados, foi realizado o teste de Shapiro-Wilk demonstrado por Benedetti et. al. (2021) e Corrar (1993). Também foi calculado o Índice de Fidedignidade ou Concordância Inter avaliadores (IVC), para as análises das fases de verificação, atributos e ensaios, para avaliar a extensão em que os especialistas são confiáveis nas avaliações dos itens conforme apontam Waltz, Strickland e Lenz apud Sperling, Coser e Cardoso (2018). Assim como a concordância entre os avaliadores por meio do Coeficiente de Correlação de Pearson e do teste t-pareado, seguindo o recomendado por Benedetti et. al. (2021). A análise dos resultados dos questionários foi baseada nas Média de Satisfação por Item para as Fase de Verificação, Atributo e Ensaio (MSF, MAS e MSE). Foi feita a análise dos Quartis para identificação dos itens mais críticos, como proposto por Oliveira et. al. (2021).

6.1.2. Análise dos questionários

Os avaliadores responderam os questionários sob o ponto de vista de um provável usuário, o que conforme descrevem French e Thomas apud Costa et. al. (2011) e Oslin et. al. apud Costa et. al. (2011) remete a uma avaliação mais fidedigna ao propósito da validação. As respostas dos questionários do Bloco III, foram consolidadas em planilhas eletrônicas para realizar o tratamento, foram utilizados os *softwares* Microsoft Excel e JAMOVI, um software de modelagem estatística, livre e aberto (CREMONA, 2021).

Pelo Excel foi calculado o valor do alfa de *Cronbach*, identificando um valor de $\alpha = 0,8899$ para a avaliação das fases de verificação, $\alpha = 0,8938$ para a avaliação dos atributos, e $\alpha = 0,7866$ para a análise dos ensaios. Pelos valores obtidos, chegou ao resultado qualitativo que a confiabilidade do questionário está assegurada e quantitativamente está entre muito boa e aceitável, o que significa, segundo Freitas e Rodrigues apud Freitas e Campos (2012), que os questionários podem ser utilizados para a avaliação do ProAS-NN.

Foi verificado se as respostas aos questionários representaram uma distribuição normal pelo testes de Shapiro Wilk, por meio do Excel e JAMOVI, cujos resultados estão demonstrado na Tabela 3 para os atributos validados, na Tabela 4 para as fases de verificação e na Tabela 5 para os ensaios de avaliação.

Tabela 3 - testes de Shapiro Wilk para os atributos

Normality Test (Shapiro-Wilk)

			W	p
A	-	B	0.819	< .001
A	-	C	0.770	< .001
A	-	D	0.701	< .001
A	-	E	0.758	< .001
A	-	F	0.819	< .001
B	-	C	0.863	< .001
B	-	D	0.863	< .001
B	-	E	0.872	< .001
B	-	F	0.879	< .001
C	-	D	0.761	< .001
C	-	E	0.662	< .001
C	-	F	0.745	< .001
D	-	E	0.732	< .001
D	-	F	0.794	< .001
E	-	F	0.643	< .001

Fonte: o autor

Tabela 4 - testes de Shapiro Wilk para fases de verificação

Normality Test (Shapiro-Wilk)

			W	p
A	-	B	0.869	< .001
A	-	C	0.749	< .001
A	-	D	0.796	< .001
A	-	E	0.771	< .001
A	-	F	0.714	< .001
B	-	C	0.891	0.003
B	-	D	0.854	< .001
B	-	E	0.807	< .001
B	-	F	0.825	< .001
C	-	D	0.736	< .001
C	-	E	0.807	< .001
C	-	F	0.794	< .001
D	-	E	0.752	< .001
D	-	F	0.767	< .001
E	-	F	0.637	< .001

Fonte: o autor.

Tabela 5 - teste de Shapiro Wilk para os ensaios

Normality Test (Shapiro-Wilk)

			W	p
A	-	B	0.699	< .001
A	-	C	0.863	0.053
A	-	D	0.774	0.005
A	-	E	0.753	0.003
A	-	F	0.818	0.015
B	-	C	0.807	0.011
B	-	D	0.699	< .001
B	-	E	0.327	< .001
B	-	F	0.809	0.012
C	-	D	0.784	0.006
C	-	E	0.818	0.015
C	-	F	0.802	0.010
D	-	E	0.753	0.003
D	-	F	0.818	0.015
E	-	F	0.828	0.020

Fonte: o autor.

Pelo teste de Shapiro Wilk pelo Jamovi se identificou que a distribuição das respostas aos questionários corresponde a uma distribuição normal, com nível de significância de 5%, para a análise das fases de verificação, atributos validados e ensaios de avaliação, pelos cálculos do Excel chegou-se ao resultado: "Não temos evidências para rejeitar a hipótese nula, e os dados são, pelo menos aproximadamente, provenientes de uma distribuição Normal", ou seja, que a distribuição representa uma normal.

Na comparação entre avaliadores foram realizados o teste-t e o cálculo do coeficiente p de *Pearson*, para avaliar o nível de concordância ou reprodutibilidade entre avaliadores, agrupados dois a dois como forma de avaliar a confiabilidade quando estes realizam a mesma avaliação, a Tabela 6 apresenta os valores obtidos nas comparações entre especialistas na avaliação das fases, a Tabela 7 para os atributos e a Tabela 8 traz os valores para os ensaios, a

Tabela **9** expõe os valores de p de Pearson para as três análises.

Tabela 6 – Teste t pareado para fases

Paired Samples T-Test

			statistic	df	p
A	B	Student's t	4.596	32.0	< .001
	C	Student's t	0.000	32.0	1.000
	D	Student's t	−0.702	32.0	0.488
	E	Student's t	−0.571	32.0	0.572
	F	Student's t	−0.780	32.0	0.441
B	C	Student's t	−4.690	32.0	< .001
	D	Student's t	−5.523	32.0	< .001
	E	Student's t	−6.614	32.0	< .001
	F	Student's t	−6.294	32.0	< .001
C	D	Student's t	−1.000	32.0	0.325
	E	Student's t	−0.683	32.0	0.500
	F	Student's t	−0.849	32.0	0.402
D	E	Student's t	0.297	32.0	0.768
	F	Student's t	0.000	32.0	1.000
E		Student's t	−0.373	32.0	0.712

Fonte: o autor.

Tabela 7 - Teste t pareado para atributos

Paired Samples T-Test

			statistic	df	p
A	B	Student's t	3.590	50.0	< .001
	C	Student's t	−0.599	50.0	0.552
	D	Student's t	−1.062	50.0	0.293
	E	Student's t	−0.299	50.0	0.766
	F	Student's t	0.629	50.0	0.532
B	C	Student's t	−5.680	50.0	< .001
	D	Student's t	−6.040	50.0	< .001
	E	Student's t	−5.567	50.0	< .001
	F	Student's t	−3.789	50.0	< .001
C	D	Student's t	−0.468	50.0	0.642
	E	Student's t	0.574	50.0	0.569
	F	Student's t	1.936	50.0	0.059
D	E	Student's t	1.000	50.0	0.322
	F	Student's t	1.940	50.0	0.058
E		Student's t	1.768	50.0	0.083

Fonte: o autor.

Tabela 8 - Teste t pareado para ensaios

Paired Samples T-Test

			statistic	df	p
A	B	Student's t	−0.561	11.0	0.586
	C	Student's t	−1.173	11.0	0.266
	D	Student's t	0.000	11.0	1.000
	E	Student's t	−1.000	11.0	0.339
	F	Student's t	−0.804	11.0	0.438
B	C	Student's t	−1.149	11.0	0.275
	D	Student's t	0.561	11.0	0.586
	E	Student's t	−1.000	11.0	0.339
	F	Student's t	−0.432	11.0	0.674
C	D	Student's t	1.773	11.0	0.104
	E	Student's t	0.804	11.0	0.438
	F	Student's t	0.692	11.0	0.504
D	E	Student's t	−1.000	11.0	0.339
	F	Student's t	−0.804	11.0	0.438
E		Student's t	0.000	11.0	1.000

Fonte: o autor

Tabela 9 - Valores de p de Pearson

avaliadores	p (fase verificação) %	p (atributo validado) %	p (ensaio) %
A e B	90	84	22
A e C	96	71	79
A e D	99	45	34
A e E	86	73	31
A e F	77	54	58
B e C	93	87	77
B e D	88	85	46
B e E	67	73	14
B e F	80	97	90
C e D	70	69	94
C e E	92	47	85
C e F	99	38	56
D e E	75	63	58
D e F	86	63	97
E e F	48	23	90

Fonte: o autor.

Com os resultados dos testes t e do coeficiente de Pearson é possível inferir que a as notas atribuídas pela maioria dos avaliadores apresenta uma forte correlação. E existe uma correlação mais fraca entre as opiniões do avaliador B com os demais, o que foi causado pelas notas por ele atribuídas terem sido mais baixas que a dos demais.

Em relação aos valores das notas fornecidas pelos avaliadores, em resposta aos questionários, a Tabela 10 apresenta a média das notas dos avaliadores em relação as fases de verificação, atributos validados e ensaios, com seus respectivos valores de desvio padrão. Foi visto pelos valores do desvio padrão, uma variação pequena nos valores atribuídos aos itens por cada avaliador, o que representa homogeneidade em suas respostas. Na comparação entre as médias das respostas dos avaliadores se observou valores altos e equivalentes, em torno de 4,5. o que demonstra uniformidade e homogeneidade entre suas opiniões, o que é positivo para o método de validação, pois demonstra que os avaliadores compreenderam o protocolo e seu processo de validação.

Tabela 10 - Média por avaliador

	Avaliador	A	B	C	D	E	F
fase de verificação	Nota	4,636	3,606	4,636	4,757	4,727	4,757
	Desvio Padrão.	0,846	0,982	0,642	0,494	0,445	0,494
atributo de validação	Nota	4,588	3,882	4,666	4,705	4,627	4,509
	Desvio Padrão	0,932	0,899	0,511	0,496	0,483	0,724
ensaio	Nota	4,416	4,5	4,75	4,416	4,583	4,583
	Desvio Padrão	0,759	0,5	0,433	0,493	0,493	0,493

Fonte: o autor.

Foi realizado o cálculo do Índice de Validade do Conteúdo (IVC), com o objetivo de validar a estrutura utilizada nos questionários para a validação do ProAS-NN, os valores obtidos são apresentados na Tabela 11, considerados válidos os com valor mínimo de 80% de concordância, o valor para o IVC geral, que corresponde à média dos IVC dos itens, calculado para a análise das fases de verificação foi de 0,85, para os atributos foi de 0,87 e para os ensaios foi de 0,97. Foi possível validar o método de validação do ProAS-NN, pois os valore obtidos para os itens individuais ficaram acima de 0,8, o que garante a validade do conteúdo, dessa forma, considera-se que os questionários obtiveram a aprovação e ratifica a forma com que foi realizada a validação do constructo, e que houve fidedignidade e concordância entre os avaliadores, determinando como confiáveis as análises dos avaliadores.

Tabela 11 - Resultados de IVC/fase de verificação

		IVC
Fases de verificação	Especificação de requisito do sistema	0,83
	Especificação de Software	0,89
	Especificação de projeto de Software	0,83
	Codificação de Software	0,89
	Integração de Sistema	0,83
	Teste do sistema integrado	0,89
	Teste de validação e comissionamento	0,83
	Teste de desempenho	0,83
	Teste de aceitação de fábrica	0,83
	Teste de aceitação no local	0,89
	Entrega do sistema	0,83
	Operação, manutenção e modificação	0,83
Atributos	Ambiente operacional e cenários de aplicação	0,94
	Arquitetura de *hardware* e segurança física	0,88
	Interfaces de comunicação e interoperabilidade	0,88
	Serviços e Funcionalidades	0,94
	Usabilidade	0,94
	Mecanismos de autenticação de usuário	0,88
	Controle de acesso	0,83
	Criptografia e módulos criptográficos	0,83
	Geração de números aleatórios	0,83
	Confiabilidade e desempenho	0,94
	Registro de Eventos	0,88
	Disponibilidade e eficiência	0,83
	Temporalidade	0,83
	Manutenibilidade	0,78
	Segregação de redes	0,88
	Redundância	0,83
	Simplicidade	0,88
Ensaios	Nível Conceitual	0,97
	Nível Operacional	0,97

Fonte: o autor.

Em relação a opinião dos avaliadores quanto a composição do ProAS-NN a Tabela 12 apresenta as médias das notas atribuídas pelos avaliadores quanto a satisfação para as fases de verificação, MSF, em valor bruto e percentual.

Tabela 12 - Valores das MSF.

FASE DE VERIFICAÇÃO	MSF	
Especificação de requisito do sistema	4,278	86%
Especificação de Software	4,556	91%
Especificação de projeto de Software	4,389	83%
Codificação de Software	4,5	90%
Integração de Sistema	4,722	94%
Teste do sistema integrado	4,556	91%
Teste de validação e comissionamento	4,333	87%
Teste de desempenho	4,278	86%
Teste de aceitação de fábrica	4,667	93%
Teste de aceitação no local	4,611	92%
Entrega do sistema	4,611	92%
Operação, manutenção e modificação	4,667	93%

Fonte: o autor.

A Tabela 13 apresenta as médias das notas atribuídas pelos avaliadores quanto a satisfação dos atributos a serem validados, MSA, em valor bruto e percentual.

Tabela 13 - Valores das MSA.

ATRIBUTO	MSA	
Ambiente operacional e cenários de aplicação	4,778	96%
Arquitetura de ***hardware*** e segurança física	4,5	90%
Interfaces de comunicação e interoperabilidade	4,611	92%
Serviços e Funcionalidades	4,778	96%
Usabilidade	4,333	87%
Mecanismos de autenticação de usuário	4,5	90%
Controle de acesso	4,333	87%
Criptografia e módulos criptográficos	4,222	84%
Geração de números aleatórios	4,556	91%
Disponibilidade e eficiência	4,778	96%
Confiabilidade e desempenho	4,5	90%
Registro de Eventos	4,333	87%
Temporalidade	4,389	88%
Manutenibilidade	4,111	82%
Segregação de redes	4,611	92%
Simplicidade	4,5	90%
Redundância	4,611	92%

Fonte: o autor.

E a Tabela 14 apresenta as médias das notas atribuídas pelos avaliadores quanto a satisfação em relação aos Ensaio (MSE). Em valor bruto e percentual.

Tabela 14 - Valores das MSE

ENSAIOS	MSE	
Nível Conceitual	4,5	90%
Nível Operacional	4,583	92%

Fonte: o autor.

Os cálculos da MSF, MAS e MSE permitiram visualizar a opinião dos avaliadores em relação a cada item avaliado. Para as fases de verificação os avaliadores consideraram positiva a análise e atribuíram notas com valores em torno de 90%, o que se repetiu na avaliação dos atributos a serem validados e atribuíram notas com valores superiores a 90%, para os ensaios de avaliação notas com valores superiores a 95%.

Pela MSF se verifica unanimidade dos avaliadores quanto a importância da análise das fases de verificação propostas, que há clareza e completude na forma com que o protocolo trata as fases da verificação, pois a maioria obteve valor máximo, indicando que o método de avaliação consegue envolver o que se pretende avaliar.

Pela MSA, se verifica a importância da análise dos atributos propostos para validação, indicando que o ProAS-NN, que sua análise está bem dimensionada em relação ao que se propõe a realizar, indicando que o método de avaliação consegue envolver o que pretende avaliar, possui clareza e completude com que o protocolo trata a validação, dentro do V&V.

Pela MSE, se verifica a opinião positiva dos avaliadores quanto a forma com que se avaliar os itens verifica a unanimidade dos avaliadores quanto a correta solicitação dos documentos para a avaliação de software, que os níveis de avaliação possibilitam realizar as verificações de forma adequada, quanto a clareza, completude e praticidade dos ensaios, que a aplicação dos ensaios está bem dimensionada, ao que se propõe a realizar. Isto permite interpretar que, de maneira geral, há satisfação entre os avaliadores quanto a forma com que o ProAS-NN realiza a avaliação dos *softwares* empregados em meios navais com propulsão nuclear.

Foi feita a divisão das médias de satisfação dos itens em Quartis, para identificar quais possuem valores de avaliação mais baixos na análise das fases de verificação e atributos de validação, como proposto por Freitas et. al. apud Oliveira et. al. (2021), os itens pior avaliados foram as fases de:

- Teste de validação e comissionamento;
- Teste de desempenho.

Os atributos pior avaliados foram:

- Manutenibilidade;
- Criptografia e módulos criptográficos;
- Usabilidade;

- Controle de acesso.

Sobre as os itens pior avaliados, para a fase de verificação que compreende os Teste de validação e comissionamento, a causa de suas notas terem sido mais baixas ocorreu pela confusão causada pelo uso dos termos “sistema” onde deveria haver “*software*” e ao citar que as “funcionalidades devem satisfazer as necessidades do usuário”, quando deveria conter “as funções do *software* possam ser exercidas e expressem a resposta esperada”. Quanto a fase de verificação dos Teste de desempenho, o fator que levou aos avaliadores atribuírem notas mais baixas, foi a ausência da descrição da realização desses testes, parte do processo de avaliação que transcende o objetivo da dissertação.

Sobre os atributos pior avaliados, para a Manutenibilidade, é um atributo que avalia quatro características do *software*, e tem sua descrição no ProAS-NN mais sintetizada, não ficando claro para o avaliador a totalidade de sua execução e abordagem.

Para a validação da criptografia, os avaliadores acharam que a realização dos testes de abuso pode não ser suficientes para garantir sua conformidade, não sendo claro para eles que a validação do uso da criptografia se dá pela definição e implementação de algoritmos criptográficos já consolidados na indústria e comunidade científica.

Para a usabilidade as notas mais baixas atribuídas pelos avaliadores se deve ao fato do texto do ProAS-NN não estar escrito de forma clara, deixando algumas lacunas na sua interpretação.

Para o atributo que valida o controle de acesso os avaliadores atribuíram notas mais baixas por julgarem que o método adotado no ProAS-NN não previu a realização de testes de abuso.

De forma geral, os resultados demonstram que o instrumento, foi considerado muito adequado pelos avaliadores. Na análise de reprodutibilidade intra e inter avaliadores, os resultados foram classificados como excelente e na análise de constructo, o instrumento demonstrou sua capacidade em avaliar as dimensões propostas por seus ensaios.

Constatou-se que, do ponto de vista funcional, o ProAS-NN é uma ferramenta que atende ao que se propõe a fazer, e é possível sua correta aplicação e execução, indicando que as funcionalidades do sistema atendem ao estipulado em seus requisitos, e que na íntegra, permite avaliar *softwares* embarcados em uma planta nuclear naval.

6.1.3. Contribuições dos especialistas

Os avaliadores puderam realizar mais contribuições no processo de validação, por meio de sugestões, abaixo relacionadas:

- ampliar a definição de verificação e validação, seção 5 do ProAS-NN, pois para dois avaliadores não estava bem delimitada a atuação de cada uma;
- esclarecer na prática quem é que requer a execução do ProAS-NN e quem a executa, componente da seção 8 do ProAS-NN;
- correção de redundâncias textuais na seção 8;
- o uso do termo "*software* embarcado" causou confusão em três avaliadores, que sugeriram altera-lo para "*software* empregado";
- foi sugerida a melhora do texto do ProAS-NN relativo a validação da usabilidade;
- dois avaliadores emitiram nota baixa para a fase de verificação da especificação dos requisitos do sistema, item 10.1 do ProAS-NN, por não considerar claro o método de avaliação, e sugeriram melhoria na descrição do método;
- um avaliador não entendeu bem a verificação da fase de verificação dos testes de validação e comissionamento, item 10.7 do ProAS-NN, por não considerar claro o método de avaliação, e sugeriram melhoria na descrição do método;
- três avaliadores não entenderam a verificação da fase de verificação de entrega do sistema, item 10.11 do ProAS-NN, por não considerar claro o método de avaliação, e sugeriram melhoria na descrição do método;
- foi sugerido a realização de testes de uso para os atributos: mecanismos de autenticação e controle de acesso;
- foi sugerido a realização de testes de abuso para os atributos registro de eventos e controle de acesso;
- um avaliador não entendeu o objetivo de validar o atributo redundância, e sugeriu que este seja melhorado.

6.2. VALIDAÇÃO POR ESTUDO DE CASO

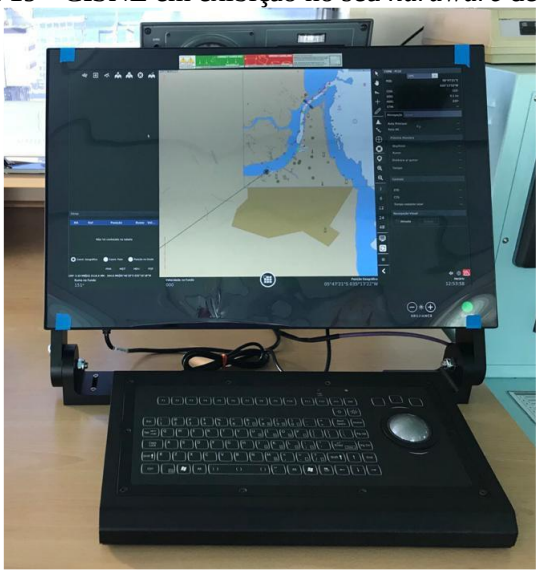
De posse da ferramenta para validação de *softwares* já validada por especialistas, é possível a sua aplicação, em um estudo de caso, visando medir o grau de adequação do mesmo a seu objetivo.

Para Neto (2005) a simulação baseada em cenários realísticos possibilita a identificação de não-conformidades tanto no sistema avaliado como no sistema de avaliação, bem como a identificação de oportunidades de melhoria, conforme Jung et. al. (2016) a utilização prática de uma ferramenta de avaliação permite avaliar sua aplicabilidade.

Desta forma, o ProAS-NN foi aplicado na avaliação do Centro de Integração de Sensores e Navegação Eletrônica (CISNE), exibido na Figura 19, cujo relatório de avaliação segue no Apêndice F deste texto. O CISNE é um software desenvolvido pela MB, para

integração de vários sensores do navio; como GPS, bussola eletrônica, medidor de profundidade; cujas informações são apresentadas sobre uma carta náutica eletrônica e interativa, comercialmente denominado de ECDIS, que foi utilizado, devido a sua maturidade, está instalado em treze navios da MB, efetivamente em uso, possui documentação consistente e vasta, e há uma unidade física funcional nas dependências do IPqM, o que possibilitou a realização de atividades práticas de inspeções e testes de uso, não sendo possível a realização de testes de abusos e estressores por questões que transcendem a atividade de pesquisa desenvolvida.

Figura 19 - CISNE em exibição no seu *hardware* dedicado



Fonte: Carneiro e Junior, 2018.

6.3. CONSTATAÇÕES DO ESTUDO DE CASO

Na aplicação do ProAS-NN no CISNE não foram observadas dificuldades pela equipe de avaliação, composta pelo autor deste texto com a colaboração do grupo de engenheiros e analistas que desenvolveu e presta suporte ao CISNE. O processo de verificação se mostrou organizado, possibilitou a análise de forma fluida e de acordo com a cronologia da documentação, foi possível entender de forma clara o processo de desenvolvimento do software, e evidenciar a busca do atendimento aos requisitos.

A composição da equipe de avaliação envolvendo os profissionais que desenvolveram o produto avaliado, quebra a importante regra da independência da equipe de avaliação de qualquer envolvimento ou desenvolvimento do *software* avaliado, contudo, o ProAS-NN como fruto de uma atividade acadêmica, foi sendo construído à medida que a pesquisa avançava, e do mesmo modo ocorreu sua aplicação, ao passo que as técnicas e métodos foram sendo refinados e incorporados ao ProAS-NN, eram aplicadas ao CISNE, como forma de verificar sua

adequação e de tornar o processo de avaliação mais célere, com a redução do tempo necessário para treinar uma terceira parte para avaliação, para que está a execute.

No processo de validação, devido ao autor conhecer bem o ProAS-NN, à medida que ele lia a documentação já conseguia enxergar a abordagem dos atributos e extrair as informações para caracterizá-los, o que tornou o processo rápido e possibilitou a evidência do atendimento aos requisitos.

A técnica de modelagem das ameaças foi de grande valia para a aplicação do ProAS-NN no CISNE, pois trouxe objetividade na validação dos atributos que foram identificados como possíveis fontes de riscos, e abordar os aspectos e características que eliminam tais riscos.

Também foi verificado que para uma maior efetividade da aplicação do ProAS-NN a equipe de avaliação deve ter domínio do conhecimento e experiência em TI, o que possibilita entender bem os processos, ferramentas e técnicas utilizadas para desenvolver o software.

Outro fato importante de ser registrado, foi a participação do desenvolvedor no processo de avaliação, que deve ocorrer sem interferências, apenas prestando esclarecimentos e fornecendo informações e documentos complementares, o que possibilitou sanar dúvida geradas durante o processo, complementar documentação que não havia sido entregue no início do processo e ajudar o avaliador ao apontar evidências do atendimento aos requisitos na documentação e demonstrar funções e ferramentas de segurança implementadas na unidade física estudada.

Assim, a aplicação do ProAS-NN foi útil e confirmou que ele é capaz de identificar com consistência, precisão e contextualização os requisitos que compõe o ciclo de vida de um *software*, pela da revisão documental e teste de requisitos.

E que seu processo de validação, permite apontar a necessidade de correção de incoerências e inconformidades no processo de desenvolvimento, e minimizar o tempo gasto na detecção dessas incoerências e inconformidades devido à eficiência na sua descoberta.

7. CONSIDERAÇÕES FINAIS

Neste capítulo são descritas as conclusões obtidas neste estudo, bem como limitações identificadas e as sugestões para trabalhos futuros.

7.1. CONCLUSÃO

A imensidão de riquezas e fluxo do comércio exterior faz com que os países necessitem proteger seus interesses no mar, pela constante presença do homem, necessita de equipamentos proporcionais ao tamanho da missão, cumprida por meio de uma força naval moderna e eficiente, que permite controlar essas áreas e negar o uso desautorizado do mar.

O Brasil, com o objetivo de fortalecer seu poder naval vêm desenvolvendo o projeto do submarino com propulsão nuclear, um equipamento que será dotado de diversos sistemas assistidos por *softwares*, que mediante a possibilidade da ocorrência de falhas e ataques, necessita demonstrar de forma objetiva, que possuem confiabilidade e estão isentos de falhas e vulnerabilidades, sendo adequados ao uso.

O que é papel da Marinha e gerou a necessidade da existência de uma sistemática para a avaliação da conformidade do *software*, o que vai além da realização de testes com o produto pronto, devendo ser uma preocupação com seu processo de desenvolvimento e operação.

Para suprir essa necessidade foi desenvolvido o ProAS-NN, acrônimo para Protocolo de Avaliação de *Softwares* no âmbito Nuclear Naval, que utiliza a técnica de Validação e Verificação, que acompanha o pensamento de diversos autores que estudam a avaliação de *softwares* aplicados em atividades nucleares. Segue o que é praticado pelo setor de desenvolvimento nuclear e recomendado por órgãos reguladores de vários países ao redor do mundo, como Alemanha, Canadá, EUA, Suécia, Japão, Rússia, China, Coreia do Sul e, inclusive, no Brasil. Observa normas para a avaliação de softwares aplicados na atividade nuclear emitidas pela IEEE e NRC.

Foi elaborado sob a forma de um guia, observa recomendações para a composição de sistemas de avaliação de software emitidas pelo ISO/IEC, de forma lógica e organizada, que possibilita sua devida documentação e reprodutibilidade.

Esse protocolo passou por um processo de validação que demonstrou sua qualidade, com a avaliação por especialistas por meio de questionários, que puderam avaliar as fases de verificação e atributos para validação previstos no ProAS-NN, bem como os ensaios para a realização das análises, expondo a importância, clareza e objetividade de cada item, além de

sugerirem melhorias textuais e estruturais no protocolo de avaliação. E com a aplicação prática, por meio do estudo de caso, que possibilitou perceber que o protocolo se mostra confiável e coerente com os objetivos que pretende atingir, de forma a permitir uma avaliação de forma mais fidedigna, ágil e serena das características de *softwares* aplicados em um meio naval com propulsão nuclear e possibilita a identificação de falhas, vulnerabilidades e necessidades de melhoria. O que o consolidou como instrumento para a análise do processo de verificação e de validação.

Os resultados obtidos permitem inferir que o ProAS-NN está pronto para ser utilizado na avaliação de *softwares* utilizados na instrumentação e controle dos diversos sistema presentes em meios navais com propulsão nuclear.

7.2. LIMITAÇÕES DO ESTUDO E TRABALHOS FUTUROS

A partir das limitações e vislumbrando o desenvolvimento e melhoria do protocolo são sugeridos os seguintes trabalhos futuros:

a) Analisar a capacidade de utilizar o ProAS-NN em sistemas não nucleares, como foi o sistema abordado no estudo de caso;

b) Aplicação do ProAS-NN em outros *softwares*;

c) Aplicação do ProAS-NN por pessoa que o desconhece;

d) Aperfeiçoar o ProAS-NN e amplificá-lo em outros *softwares*;

e) Criação de um sistema inteligente para a execução do ProAS-NN, em que o requerente possa solicitar a avaliação, troque informações e documentos, acompanhe o andamento e os resultados parciais e, auxilie o avaliador;

f) Divulgação para órgãos e instituições como forma de disseminação do conhecimento.

8. REFERÊNCIAS BIBLIOGRÁFICAS

____: **Common Criteria for Information Technology Security Evaluation**. April 2017

____: Novas ameaças expõe riscos de ataques a sistemas de comunicação de navios. Site SideChannel, 2018. Disponível em: https://www.sidechannel.blog/novas-ameacas-expoe-riscos-de-ataques-a-sistemas-de-comunicacao-de-navios/index.html. Acesso em: 18 jan. 2022.

_____: **Conheça o "Modelo de Ameaça" STRIDE.** Site Infomach. 2020. Disponível em: <https://www.infomach.com.br/conheca-o-modelo-de-ameaca-stride/>. Acesso em: 08 Jan. 2022.

_____: **Microsoft Security Development Lifecycle.** Microsoft Corporation, 2018. Disponível em: https://www.microsoft.com/en-us/securityengineering/sdl. Acesso em: 24 Set. 2022.

_____: **Vocabulário Internacional de Metrologia –** Conceitos Fundamentais e gerais e termos associados. (VIM 2021). Duque de Caxias: INMETRO 2021.

ADEE, S.; The Hunt For The Kill Switch, **IEEE Spectrum**, vol. 45, nº 5, pp. 34-39, maio de 2008, DOI: 10.1109/MSPEC.2008.4505310.

AHMED, I.; JUNG, J.; HEO, G. Design verification enhancement of field programmable gate array-based safety-critical I&C system of nuclear power plant. **Nuclear Engineering and Design,** 317, 232–241. DOI: 10.1016/j.nucengdes.2017.03.06. Acesso em: 31 Jan. 2023

AIEA, **Software for Computer Based Systems Important to Safety in Nuclear Power Plants** - IAEA Safety Guide NS G.1-1., Agência Internacional de Energia Atômica, Vienna, 2000.

AIEA, **Verification and Validation of software related to Nuclear Power Plant instrumentation and control**, Technical Reports 384, Agência Internacional de Energia Atômica, Vienna, 1999.

AIEA. History. **Site da Agência Internacional de Energia Atômica**, 1998. Disponível em: https://www.iaea.org/about/overview/history. Acesso em: 15 Out. 2022.

ALBERNAZ, C. M. R.; FREITAS, A. L. P.; Um modelo para avaliação da qualidade de serviços de suporte de Tecnologia da Informação. **Anais do XXX ENEGEP**. 2010

ALVES, L. **STRIDE – Modelagem de ameaças.** Site Hacking Brasil Organization. 2021. Disponível em: https://hackingbrasil.org/?p=320. Acesso em: 08 Jan. 2022.

AMAZUL, **Avaliação da Conformidade de Softwares**. Rev. 1. Procedimento Operacional. Amazônia Azul Tecnologias de Defesa S.A, 2022, Rio de Janeiro.

ANDRADE, I. O.; SILVA, M. M. F. F.; HILLEBRAND, G. R. L.; FRANCO, L. G. A. **Submarino nuclear brasileiro: defesa nacional e externalidades tecnológicas.** Texto para Discussão, 2018. DOI: http://hdl.handle.net/10419/211378.

ANDRES, D.; CYBIS, WR. **Um estudo teórico sobre as técnicas de avaliação de software educacional**. 2000. Disponível em: http://sedici.unlp.edu.ar/handle/10915/23499. Acesso em: 19 nov. 2021.

ASOCIACIÓN MERCOSUR DE NORMALIZACIÓN. **NM ISO/IEC 14598-1:2008: Tecnologia de informação: Avaliação de produto de software** - Parte 1: Visão geral 2008a.

ASOCIACIÓN MERCOSUR DE NORMALIZACIÓN. **NM ISO/IEC 14598-2:2008: Tecnologia de informação: Avaliação de produto de software -** Parte 2: Planejamento e Gestão, 2008b.

ASOCIACIÓN MERCOSUR DE NORMALIZACIÓN. **NM ISO/IEC 14598-3:2008: Tecnologia de informação: Avaliação de produto de software -** Parte 3: Processo para desenvolvedores, 2008c.

ASOCIACIÓN MERCOSUR DE NORMALIZACIÓN. **NM ISO/IEC 9126-1:2008: Engenharia de software: qualidade de produto. Parte** 1: modelo de qualidade. São Paulo-SP, Brasil, 2008a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 14598-6:2004: engenharia de software: avaliação de produto.** Parte 6: documentos de módulos de avaliação. Rio de Janeiro; 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 14598-5:2001: Tecnologia de Informação** – Avaliação de produtos de software. Parte 5: Processo para avaliadores. Rio de Janeiro, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 17000:2021 - Avaliação da conformidade** - Vocabulário e princípios gerais. Rio de Janeiro. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 17025:2017 - Requisitos gerais para a competência de laboratórios de ensaio e calibração.** Rio de Janeiro. 2017a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 25020:2009 - Engenharia de software — Requisitos e avaliação da qualidade de produto de software (SQuaRE) — Guia e modelo de referência para medição** Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 25030:2008 - Engenharia de software — Requisitos e avaliação da qualidade de produto de software (SQuaRE) — Requisitos de qualidade.** Rio de Janeiro, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.** Rio de Janeiro. 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.** Rio de Janeiro. 2013b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27003:2020 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações.** Rio de Janeiro. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27004:2017 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação.** Rio de Janeiro. 2017b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2019 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.** Rio de Janeiro. 2019.

AURÉLIO, M.; **Radar**. Site Brasil Escola, 2013. Disponível em: https://brasilescola.uol.com.br/fisica/radar.htm#:~:text=O%20princ%C3%ADpio%20de%20funcionamento%20do,atrav%C3%A9s%20das%20ondas%20de%20r%C3%A1dio.&text=O%20radar%20%C3%A9%20constitu%C3%ADdo%20de,curto%20per%C3%ADodo%20e%20feixe%20curto. Acesso em: 29 jan. 2022.

BACELLAR, R. S.; **A importância da segurança cibernética para a Marinha do Brasil**. 2018. Monografia do curso de Aperfeiçoamento Avançado, CIAW - Marinha do Brasil, Rio de Janeiro-RJ. Disponível em: https://www.repositorio.mar.mil.br%2Fbitstream%2Fripcmb%2F844782%2F1%2FCApA-GE-08-1T%2520Ricardo%2520dos%2520Santos%2520BACELLAR-TCC.pdf&clen=76501818. Acesso em: 19 jan. 2022.

BAEZNER, M.; ROBIN, P. **Stuxnet**. Editora: Zurich, 2017.

BAHILL, A. T.; HENDERSON, S. J. Requirements Development, Verification, and Validation Exhibited in Famous Failures, **Systems Engineering** nº 8(1), pg. 1–14. 2004. DOI: 10.1002 / sys.20017.

BARROS, M. **Como o transporte marítimo está enfrentando as ameaças à Segurança Cibernética**. Rio de Janeiro, 2021. Disponível em: https://www.defesaemfoco.com.br/como-o-transporte-maritimo-esta-enfrentando-as-ameacas-a-seguranca-cibernetica/. Acesso em: 18 jan. 2022.

BARTIÉ, A.; **Garantia da Qualidade de Software**: adquirindo maturidade organizacional. Rio de Janeiro: Gulf Professional Publishing. 2002.

BENEDETTI, G.; CANDOTTI, C. T.; GONTIJO, K. N. S.; BAMPI, G. M.; LOSS, J. F.; **Vista do Desenvolvimento e validação de um método de avaliação do nível de prática no método Pilates por meio de exercícios do próprio método**. 2021. Disponível em: https://portalatlanticaeditora.com.br/index.php/fisioterapiabrasil/article/view/10/115. Acesso em: 20 set. 2021.

BENEDETTI, T. R. Validade e clareza dos conceitos e terminologias do Guia de Atividade Física para a População Brasileira. **Revista Brasileira de Atividade Física & Saúde**, v. 26, p. 1-11, 2021.

BENKO, P. L., NETO, J. M. O.: **Análise de confiabilidade e segurança de sistemas digitais aplicados em proteção de reatores nucleares.** São Paulo, 1997.

BOURQUE, P.; FAIRLEY, R. E. **Guide to the Software Engineering Body of Knowledge**, (Ed.). SWEBOK, 2004.

BRAGA, A. M. Visão geral das boas práticas para construção de softwares seguros. **Revista Técnica IPEP**, São Paulo, SP, v. 7, n. 2, p. 65-78, 2007.

BRASIL Decreto Nº 11.283, de 13 de dezembro de 2022: **Altera o Decreto nº 5.417, de 13 de abril de 2005, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Comando da Marinha, do Ministério da Defesa, e remaneja e transforma cargos em comissão e funções de confiança**, Brasília - DF 2022.

BRASIL, Medida Provisória Nº 1.049, de 14 de maio de 2021. **Cria a Autoridade Nacional de Segurança Nuclear**, Brasília, DF, 2021a.

BRASIL. Lei Nº 13.976, de 7 de janeiro de 2020. **Dispor sobre competência do Comando da Marinha para promover o licenciamento e a fiscalização dos meios navais e suas plantas nucleares embarcadas para propulsão e do transporte de seu combustível nuclear**, Brasília - DF 2020a.

CAMPOS, F.; CAMPOS, G. H. B.; ROCHA, A. R.; **Dez etapas para o desenvolvimento de software educacional do tipo hipermídia.** Rio de Janeiro: Coppe UFRJ 2014.

CAMPOS, G. H. B. **Construção e validação de ficha de avaliação de produtos educacionais para microcomputadores**. Dissertação de Mestrado – Faculdade de Educação, Universidade Federal do Rio de Janeiro. pg. 110, 1989.

CAMPOS, G. H. B.; **Metodologia para avaliação da qualidade de software educacional.** Diretrizes para desenvolvedores e usuários**.** Rio de Janeiro: Coppe UFRJ 1994.

CARNEIRO, M. M.; JUNIOR, J. G. C. **CISNE**: Centro de Integração de Sensores e Navegação Eletrônica. Marinha do Brasil. 2018.

CARVALHO, A. B. **Economia do mar**: conceito, valor e importância para o Brasil. 2018.

CHEON, G. Y.; PARK, K. H.; CHA, J. S.; LEE, K. C. Kwon the Software V&V Tasks for a Safety-Critical Software Based Protection System in Nuclear Power Plants. **IEEE International Conference on Industrial Technology**. 2005, DOI:10.1109/icit.2005.1600654

CHEON, S. W.; KWON, K. C.; YOUN, C.; HAN, H. C.; KIM, D. H. Development of a Software Configuration Management System for Software Life Cycle Management, **Proceedings of the NPIC&HMIT 2005**, Columbus, Ohio, Sept. 19-22, 2005. Disponível em: https://koreascience.kr/article/JAKO200428317682795.kr&sa=U. Acesso em: 21 Dez. 2022.

CHOON, S. W.; LEE, J. S.; KWON, K. C.; KIM, D. H.; KIM, H. The software verification and validation process for a PLC-based engineered safety features-component control system in nuclear power plants. **30th Annual Conference of IEEE Industrial Electronics Society**, 2004. IECON 2004. DOI:10.1109/iecon.2004.1433422

CHUA, B.B.; DYSON, L. E. Applying the ISO 9126 model to the evaluation of an e-learning system. In: **Proc. of ASCILITE**. 2004. p. 184-190.

CNEN, Quem Somos**. Site da Comissão Nacional de Energia Nuclear**, 2020. Disponível em: http://antigo.cnen.gov.br/quem-somos. Acesso em: 9 Mai. 2022.

CNEN. Norma CNEN NE 1.04 LICENCIAMENTO DE INSTALAÇÕES NUCLEARES. **Site da Comissão Nacional de Energia Nuclear**, 2002. Disponível em: http://appasp.cnen.gov.br/seguranca/normas/pdf/Nrm104.pdf. Acesso em: 11 outubro

CORRAR, L. J. **O modelo econômico da empresa em condições de incerteza aplicação do método de simulação de Monte Carlo**. Cad. estud. (8) Abr. 1993. DOI: https://doi.org/10.1590/S1413-92511993000100004.

CORTES, M.; CHIOSSI, T. **Modelos de Qualidade de Software**. Campinas, SP, Editora da Unicamp, Instituto de Computação, 2001.

COSTA, I. T.; GARGANTA, J.; GRECO, P. J.; MESQUITA, I.; MAIA, J.; **Sistema de avaliação táctica no Futebol (FUT-SAT):** Desenvolvimento e validação preliminar Motricidade, vol. 7, núm. 1, 2011, pp. 69-84 Desafio Singular - Unipessoal, Lda Vila Real,

Portugal. Disponível em: https://www.redalyc.org/pdf/2730/273019759008.pdf. Acesso em: 13 out. 2021.

CREMONA P.; **JAMOVI**. Site Prof. Cremona. 2021. Disponível em: https://www.profcremona.com/materiais/software/jamovi. Acesso em: 26 out. 2021.

CRUZ, M. A. S.; DUARTE, J. C.; GOLDSCHMIDT, R. R. Dinâmica da digitação aplicada a autenticação periódica de usuários em ambientes virtuais de aprendizagem. **Revista Brasileira de Informática na Educação**, v. 25, n. 02, p. 36, 2017.

DAVIDSON, R.; MATHIS, A.; MATHIS, D. SPAKOVSKY, A. P. **Software Independent Verification & Validation (SIV&V) Simplified**. Naval Postgraduate School, California, 2006.

DONDA, D. **STRIDE** – Modelo de ameaças Microsoft. Site Daniel Donda, 2012. Disponível em: https://danieldonda.com/stride-modelo-de-ameacas-microsoft/. Acesso em: 08 Jan. 2022.

DOS SANTOS, C. W. **Processo de V&V Aplicado ao Desenvolvimento de Software do NTIC**. Trabalho de Conclusão de Curso (Graduação) – Universidade Federal do Pampa, 2015.

EOM, H.; PARK, G.; JANG, S.; SON, H. S.; KANG, H. G. V&V-based remaining fault estimation model for safety–critical software of a nuclear power plant. **Annals of Nuclear Energy**, 51, 38–49. 2013. DOI: 10.1016/j.anucene.2012.06.030.

ETN, **Comissionamento e Controle de Softwares**. Procedimento da Qualidade. Eletrobrás - Eletronuclear, 2022b, Angra dos Reis.

ETN, **Projeto para Softwares Essenciais**. Procedimento Operacional. Eletrobrás - Eletronuclear, 2022a, Angra dos Reis.

FERNANDES, J. **O que é um Programa (Software)?**, 2002. Disponível em: https://www.cic.unb.br/~jhcf/MyBooks/iess/Software/oqueehsoftware.html. Acesso em: 1º jul. 2021.

FILHO, J. R. M. O projeto do submarino nuclear brasileiro. **Contexto Internacional**, v. 33, n. 2, p. 277-314, 2011. Disponível em: https://www.scielo.br/j/cint/a/DnWMLkPj5h9nC7QphZ8PzZH/?format=pdf&lang=pt. Acesso em 25 jun. 2021.

FOX, C. E. **Life Cycle Support of Computer Software Aboard Fast Attack Nuclear Submarines**. Defense Systems Management College. Department of Defense. 1977. Disponível em: https://apps.dtic.mil/sti/citations/ADA042881. Acesso em: 20 Dez 2022.

FREITAS, A. L. P.; RODRIGUES, S. G; **A avaliação da confiabilidade de questionários:** uma análise utilizando o coeficiente alfa de Cronbach. Anais do XII SIMPEP. 2005

FUKUMOTO, A.; HAYASHI, T.; NISHIKAWA, H.; SAKAMOTO, H., TOMIZAWA, T.; YOKOMURA, T. A verification and validation method and its application to digital safety systems in ABWR nuclear power plants. **Nuclear Engineering and Design**, 183(1-2), pgs 117–132.1997. DOI:10.1016/s0029-5493(98)00186-1. Acesso em: 31 Jan. 2023.

GIL, A. C. **Como elaborar projetos de pesquisa**. 5. São Paulo: Atlas, 2017.

GOMES, A. S. Referencial teórico construtivista para avaliação de software educativo. **Revista Brasileira de Informática na Educação**, v. 16, n. 02, 2008.

GOUDOSSIS, A.; KATSIKAS, S. K.; Towards a secure automatic identification system (AIS). **Jornaul of Marine Science and Technology**, nº 24, pp 410-429. https://doi.org/10.1007/s00773-018-0561-3, 2019.

GOULART, A. M. C. O conceito de ativos na contabilidade: um fundamento a ser explorado. **Revista Contabilidade & Finanças**, v. 13, n. 28, p. 56–65, abr. 2002.

GU, P.; WANG, S.; CHEN, W.; YU, S. A study about safety I&C system software V&V in nuclear power plant. **24th International Conference on Nuclear Engineering** ICONE24 June 26-30, 2016, Charlotte, North Carolina.

GUAN, H.; CHEN, W. R.; LI, H.; WANG, J. Stride–based risk assessment for web application. **Applied Mechanics and Materials**. Trans Tech Publications Ltd, p. 1323-1328, 2011.

GUERRA, E.; TRAVASSOS, G. H.; SANTOS, G. MAFRA, S.; BARRETO, A.; ROCHA, A. R. Melhoria de Processos no Desenvolvimento de Software e Hardware–O Caso Maxtrack. In: **Anais do V Simpósio Brasileiro de Qualidade de Software**. SBC, 2006. p. 326-333. DOI: https://doi.org/10.5753/sbqs.2006.15619

HOLMBEG, J.; PORTHIN, M.; TYRHÄINEN, T.; **Reliability Analysis of Digital I&C in Nuclear Power Plants.** 2016. Disponível em: https://www.researchgate.net/publication/315684357_Reliability_Analysis_of_Digital_IC_in_Nuclear_Power_Plants/link/58db51f492851ce5e96a8a6f/download. Acesso em 12 out. 2021

HUANG, H. W.; SHIH, C.; YIH, S.; CHEN, M. H.; LIN, J. M. Model extension and improvement for simulator-based software safety analysis. **Nuclear Engineering and Design,** 237(9), pgs. 955–971. 2007. DOI:10.1016/j.nucengdes.2006.10.018. Acesso em: 31 Jan. 2023.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 1012:2016 - Standard for System, Software, and Hardware Verification and Validation**, New York - EUA, 2016.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 1233:1998 - Guia IEEE para Desenvolvimento de Sistema:** Especificações de requisitos, New York - EUA, 1998.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**. IEEE 352:2016 - IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Systems and Other Nuclear Facilities**, New York - EUA, 2016.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 603:2018 - IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations**, New York - EUA, 2018.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**. IEEE 7-4.3.2:2010 - IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations**, New York - EUA, 2010.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 828:2005 - Standard for Software Configuration Management Plans**, New York - EUA, 2005.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA, **Serviço de avaliação de Produto Cibernético do LAINF**. 2020a.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA. **Avaliação da Conformidade**. 6ª ed. Duque de Caxias – RJ: [s.n.], 2012. 56 p.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA; **DOQ-CGCRE-008 – Orientação sobre Validação de Métodos Analíticos**. Duque de Caxias - RJ, 2020b.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIAINMETRO. **Vocabulário Internacional de Metrologia**. Conceitos fundamentais e gerais e termos associados (VIM 2012). Instituto Nacional de Metrologia, Qualidade e Tecnologia Duque de Caxias - RJ, 2012.

INSTITUTO PENGFEI GU DE TECNOLOGIA NUCLEAR E NOVA ENERGIA. Um estudo sobre segurança I&C sistema software V&V. **Anais da 24ª Conferência Internacional de Engenharia Nuclear**. Carolina do Norte, 2016.

INTERNATIONAL ORGANIZATION OF PADRONIZATION. **ISO/IEC 25000 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE.** Suíça, 2014.

INTERNATIONAL ORGANIZATION OF PADRONIZATION. **ISO/IEC 25010 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models**. Suíça, 2011a.

INTERNATIONAL ORGANIZATION OF PADRONIZATION. **ISO/IEC 25040:2011 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE**. Suíça, 2011b.

INTERNATIONAL ORGANIZATION OF PADRONIZATION. **ISO/IEC 25041:2012 - Systems and software engineering** — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation guide for developers, acquirers and independent evaluators. Suíça, 2012.

JEGEIB. **Ameaças -** Microsoft Threat Modeling Tool**.** Site Microsoft. Disponível em: https://docs.microsoft.com/pt-br/azure/security/develop/threat-modeling-tool-threats. Acesso em: 08 Jan. 2022.

JEONG, J.; HEO, G. Cyber Security Evaluation for Nuclear I&C Systems Corresponding to V-Model. **Korean Nuclear Society Spring Meeting** (KNS). 2020.

JUNG, S.; KIM, E. S.; YOO, J.; KIM, J. Y.; CHOI, J. G. An evaluation and acceptance of COTS software for FPGA-based controllers in NPPS. **Annals of Nuclear Energy**, 94, 338–349. 2016. doi:10.1016/j.anucene.2016.03.026. Acesso em: 31 Jan. 2023

JUNIOR, G. B. V.; **Coeficiente Kappa**. 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=http%3A%2F%2Fwww.cpaqv.org%2Festatistica%2Fkappa.pdf&clen=723533&chunk=true. Acesso em: 26 out. 2021.

JUNIOR, W. C. L.; MORAES, C. C.; DE ALBUQUERQUE, C. E. P.; MACHADO, R. C. S.; SÁ, A. O.; **A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems**. *Sensores* 2021, *21* (9), 3195; https://doi.org/10.3390/s21093195

KANG, H.G.; EOM, H.-S.; SON, H. S. **Software failure probability quantification for system risk assessment**. Sch. Res. Exch. 1999. Acesso em: 20 Dez. 2022.

KASTENSMIDT, F. G. L. **Introdução a Sistemas Digitais**. Nota de Aulas Sistemas Digitais. UFGS, 2021E.

KERSCHBAUMER, R. **Sistemas Digitais**. Instituto Federal de Educação, Ciência e Tecnologia Catarinense, 2020.

KHAN, M. U. A.; ZULKERNINE, M.; **"Activity and Artifact Views of a Secure Software Development Process"**. International Conference on Computational Science and Engineering. 2009, pp. 339 - 404.

KOO, S. R.; SEONG, P. H.; YOO, J.; CHA, S. D.; YOO, Y. J. An effective technique for the software requirements analysis of NPP safety-critical systems, based on software inspection, requirements traceability, and formal specification. **Reliability Engineering & System Safety**, 89(3), pgs. 248–260. 2005. DOI: 10.1016/j.ress.2004.08.024. Acesso em: 31 Jan. 2023

KOTONYA, G.; SOMMERVILLE, I. **Requirements Engineering**: Processes and Techniques. Editora Wiley, fl 294, 1998.

LEE, E. A. Embedded Software. **To appear in Advances in Computers**, Vol. 56, Academic Press, London, 2002. Disponível em: https://ptolemy.berkeley.edu/publications/papers/02/embsoft/embsoftwre.pdf. Acesso em: 24 ago. 2021.

LEVESON, N. G.; TURNER, C. S. An investigation of the Therac-25 accidents. IEEE **Journal of Biomedical and Health Informatics**, 1993.

LIN, M.; HOU, D.; LIU, P.; YANG, Z.; YANG, Y. Main control system verification and validation of NPP digital I&C system based on engineering simulator. **Nuclear Engineering and Design**, 240(7), pgs. 1887–1896. 2010. DOI :10.1016/j.nucengdes.2010.03.011. Acesso em: 31 Jan. 2023.

LOPES, M. V. O.: **Validação de software educativo para auxílio ao ensino de sinais vitais.** Tese de Doutorado em Enfermagem. Universidade Federal do Ceará**.** Fortaleza - CE. 2001. Disponível em: http://repositorio.ufc.br/bitstream/riufc/54911/1/2001_tese_mvolopes.pdf. Acesso em 24 jun. 2021.

MARÇAL, E. K.; BUREN, I. M. Auditoria da qualidade de um software de contabilidade. **Revista Gestão & Regionalidade**, v. 23, n. 66, 2007. DOI: https://doi.org/10.13037/gr.vol23n66.68.

MARCONI, D. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MARINHA DO BRASIL **Agência Naval de Segurança Nuclear e Qualidade.** Acervo Arquivístico da Marinha do Brasil, 2019e. Disponível em: http://www.arquivodamarinha.dphdm.mar.mil.br/index.php/agencia-naval-de-seguranca-nuclear-e-qualidade-2. Acesso em: 09 maio. 2022.

MARINHA DO BRASIL **Submarino nuclear.** Site da Marinha do Brasil, 2021a. Disponível em:<https://www.marinha.mil.br/ctmsp/submarino-nuclear. Acesso em: 29 jun. 2021.

MARINHA DO BRASIL. **104 Anos da Força de Submarinos**. Site da Marinha do Brasil, 2018a. Disponível em: https://www.marinha.mil.br/content/104-anos-da-forca-de-submarinos. Acesso em: 25 jun. 2021.

MARINHA DO BRASIL. **AIS -** Automatic Identification System**.** Site da Marinha do Brasil, 2014. Disponível em: https://www.marinha.mil.br/cismar/?q=ai>. Acesso em: 06 set. 2021.

MARINHA DO BRASIL. **Cartilha de segurança da informação digital**. Diretoria de Comunicações e Tecnologia da Informação da Marinha, 2016b. Disponível em: https://www.marinha.mil.br/ceimna/sites/www.marinha.mil.br.ceimna/files/upload/DCTIM-Cartilha_SID_v2.pdf. Acesso em: 08 Mar. 2022.

MARINHA DO BRASIL. **Centro de Integração de Sensores e Navegação Eletrônica** (CISNE). Site da Marinha do Brasil, 2021e. Disponível em: https://www.marinha.mil.br/ipqm/node/44. Acesso em: 24 ago. 2021.

MARINHA DO BRASIL. **Conhecendo o Navio**. Site da Marinha do Brasil, 2022. Disponível em: Disponível em: https://www.marinha.mil.br/tradicoes-navais/conhecendo-o-navio. Acesso em: 18 dez. 2022.

MARINHA DO BRASIL. **CTMSP: Programa Nuclear da Marinha.** Site da Marinha do Brasil, 2019b. Disponível em: https://www.marinha.mil.br/ctmsp/programa-nuclear-da-marinha. Acesso em: 29 jun. 2021.

MARINHA DO BRASIL. **DCTIM lança campanha de segurança da Informação Digital.** Centro de Comunicação Social da Marinha, 2016a. Disponível em: https://www.marinha.mil.br/node/2449. Acesso em: 9 mar. 2022.

MARINHA DO BRASIL. **Gerenciamento do Registro de Eventos computacionais relevantes.** Diretoria de Comunicações e Tecnologia da Informação da Marinha. 2021c.

MARINHA DO BRASIL. **História Naval**. Site da Marinha do Brasil, 2017. Disponível em: https://www.marinha.mil.br/content/historia-naval. Acesso em: 24 jun. 2021.

MARINHA DO BRASIL. **Manual de instalação e configuração do Centro de integração de sensores e navegação eletrônica** (CISNE). Instituto de Pesquisas da Marinha, 2021f.

MARINHA DO BRASIL. **Marinha apresenta projeto-piloto do Sistema de Gerenciamento da Amazônia Azul para o Ministro da Segurança Pública**. Centro de Comunicação Social da Marinha, 2018b. Disponível em: https://www.marinha.mil.br/noticias/marinha-apresenta-projeto-piloto-do-sistema-de-gerenciamento-da-amazonia-azul-para-o. Acesso em: 6 Mar. 2022.

MARINHA DO BRASIL. **Meios Navais.** Site da Marinha do Brasil, 2023. Disponível em: <https://www.marinha.mil.br/meios-navais. Acesso em: 14 fev. 2023.

MARINHA DO BRASIL. **Navio Oceanográfico "Antares" completa três mil dias de mar.** Site da Marinha do Brasil, 08 Abr. 2019. Disponível em: https://www.marinha.mil.br/noticias/navio-oceanografico-antares-completa-tres-mil-dias-de-mar. Acesso em: 01 fev. 2022.

MARINHA DO BRASIL. **Navio-Patrulha Oceânico "Araguari" e Navio-Patrulha "Macau" realizam operações com Centro Integrado de Sensores e Navegação Eletrônica**. 2020b. Disponível em: https://www.marinha.mil.br/noticias/navio-patrulha-oceanico-araguari-e-navio-patrulha-macau-realizam-operacoes-com-centro. Acesso em: 6 Mar. 2022.

MARINHA DO BRASIL. **Norma para o Uso de Redes Sem Fio na MB** Diretoria de Comunicações e Tecnologia da Informação da Marinha. 2021d.

MARINHA DO BRASIL. **Norma sobre Conformidade, Homologação e Hospedagem de Sistemas Digitais (SD) na MB**. Diretoria de Comunicações e Tecnologia da Informação da Marinha. 2019d.

MARINHA DO BRASIL. **Normas de Tecnologia da Informação na Marinha.** Diretoria-Geral do Material na Marinha, 2019a.

MARINHA DO BRASIL. **Plano de Gestão de Incidentes Cibernéticos**. Diretoria de Comunicações e Tecnologia da Informação da Marinha. 2021b.

MARINHA DO BRASIL. **Programa de Construção de Submarinos**, 2020a. Disponível em: https://www.marinha.mil.br/programas-estrategicos/prosub. Acesso em 22 jun. 2021.

MARINHA DO BRASIL. **Salvamar Brasil,** 2022a. Disponível em: https://www.marinha.mil.br/salvamarbrasil/. Acesso em: 17 nov. 2022.

MARINHA DO BRASIL. **TI e Sustentabilidade**. Diretoria de Comunicações e Tecnologia da Informação da Marinha. 2015.

MARINHA DO BRASIL. **Utilização de certificados digitais emitidos pela Autoridade Certificadora de Defesa (AC Defesa) no âmbito da Marinha do Brasil (MB).** Diretoria de Comunicações e Tecnologia da Informação da Marinha. 2019c.

MAROCO, J.; GARCIA-MARQUES, T. **Qual a fiabilidade do alfa de Cronbach? Questões antigas e soluções modernas?** 2006. DOI: https://doi.org/10.14417/lp.763.

MARTINS, L. E. G.; JUNIOR, R. S.; OLIVERIA, H. P.; PEIXOTO, C. S. A. TERASE: Template para Especificação de Requisitos de Ambiente em Sistemas Embarcados. In: **WER**. 2010.

MARTINS, M. de L. O. **O papel da usabilidade no ensino a distância mediado por computador. Dissertação de Mestrado.** Centro Federal de Educação tecnológica de Minas Gerais. Minas Gerais, 2004.

MATSUYAMA, F.; NAKANE, R. T.; ESPÍRITO-SANTO, R.; GEDRAITE, R.; FEREIRA, J. C. P. **Implantação de uma metodologia de projeto de instrumentação para uma aplicação em centrais nucleares a água pressurizada**. 2004. Disponível em: https://www.ipen.br/biblioteca/cd/inac/1997/ENAN/E04_292.PDF. Acesso em: 22 Dez. 2022.

MAUÉS, M. B. **Modelagem de ameaças antiforenses aplicada ao processo forense digital**. 2016. xxiii, 113 f., il. Dissertação (Mestrado em Engenharia Elétrica) — Universidade de Brasília, Brasília, 2016.

MEDNIKAROV, B.; TSONEV, Y.; LAZAROV, A.; Analysis of Cybersecurity Issues in the Maritime Industry. **Information & Security**, vol. 47, no. 1 (2020): 27-43 https://doi.org/10.11610/isij.4702. 2020b.

MELO, E. P. A. **A Importância da Validação de Métodos Analíticos.** Site da Revista Analytica. 2018. Disponível em: https://revistaanalytica.com.br/a-importancia-da-validacao-de-metodos-analiticos/#:~:text=O%20objetivo%20da%20valida%C3%A7%C3%A3o%20consiste,se%20espera%20identificar%20ou%20quantificar. Acesso em: 20 set. 2021.

MICROSOFT CORPORATION. **Microsoft Threat Modeling Tool overview - Azure**. 2020. Disponível em: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool . Acesso em: 18 jan. 2022.

MOREIRA, L. S.: **Gerenciamento de segurança operacional: um estudo envolvendo os acidentes com as aeronaves Boeing 737-800 MAX**. Universidade do Sul de Santa Catarina. Palhoça - RS 2020. Disponível em: https://www.riuni.unisul.br/bitstream/handle/12345/10438/TCC%20vers%c3%a3o%20RIUNI.pdf?sequence=1&isAllowed=y. Acesso em: 24 jun. 2021.

MUCCIN, E.; **Combatendo Ameaças à Segurança Cibernética Marítima**. Jun. 2015. Maritime Reporter & Engineering News. Disponível em: http://pt.marinelink.com/news/combatendo-amea%C3%A7as-seguran%C3%A7a-cibern%C3%A9tica-mar%C3%ADtima-261517. Acesso em: 19 jan. 2022.

NETO, J. M. M. **Um processo para avaliação de produtos de software através de análise por especialista.** UFPE, Recife, 2005.

NETO, M. M. F.; FREITAS, A. L. P. Melhoria da qualidade de software como um serviço (SAAS): uma contribuição sob o ponto de vista dos funcionários. **Anais do XXXII Encontro Nacional de Engenharia de Produção**. Bento Gonçalves, Brasil. 2012.

NETO, M. M. F.; **QualySaaS:** uma metodologia para avaliação da qualidade de software como serviço. Campo dos Goytacazes-RJ. Dissertação de Mestrado. UENF, 2012.

NRC. NUREG 0800 - **Guidance on software reviews for digital computer-based instrumentation and control systems.** U.S. Nuclear Regulatory Commission. 2005.

NRC. NUREG/CR-6316 **Guidelines for the Verification and Validation of Expert System Software and Conventional Software**, U.S. Nuclear Regulatory Commission 1995.

NRC. NUREG-CR4640 - **Handbook of Software Quality Assurance Techniques Applicable the Nuclear Industry**, U.S. Nuclear Regulatory Commission. 1987.

NRC. **Software Reliability and Safety in Nuclear Protection Reactor** - Lawrence Livermore National Laboratory, U.S. Nuclear Regulatory Commission 1993. Disponível em: https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6101/index.html. Acesso em: 25 jun. 2021.

NUNES, L. A. R.; **Guerra Cibernética**: está a MB preparada para enfrentá-la? Tese do Curso de Política e Estratégia Marítimas, EGN - Marinha do Brasil, Rio de Janeiro-RJ, 2010.

OLIVEIRA, J. G.; GRAÇA, A.; SEBRA, A.; GARGANTA, J.; **Validação de um sistema de avaliação da assimetria funcional dos membros inferiores em Futebol (SAFALL-FOOT).** Portugal, 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Frpcd.fade.up.pt%2F_arquivo%2Fartigos_soltos%2F2012-3%2F04.pdf&clen=189739& chunk=true. Acesso em: 12 out. 2021.

PADILHA, L., **NPaOc Araguari e o NPa Macau realizam operações com o Centro Integrado de Sensores e Navegação Eletrônica**. Site Defesa Aereanaval, 2020. Disponível em: https://www.defesaaereanaval.com.br/naval/npaoc-araguari-e-o-npa-macau-realizam-operacoes-com-o-centro-integrado-de-sensores-e-navegacao-eletronica. Acesso em: 24 ago. 2021.

PARK, J.; SUH, Y.; PARK, C. Implementation of cyber security for safety systems of nuclear facilities. **Progress in Nuclear Energy**, 88, pgs. 88-94. 2016. DOI: 10.1016/j.pnucene.2015.12.009. Acesso em: 31 Jan. 2023

PEGORARO, L. G. O.; GVOZD, R.; HADDAD, M. C. F. L.; VANNUCHI, M. T. O.; SILVA, L. G. C.; ROSSANEIS, M. A.; Validação de instrumento para avaliar software de classificação de risco de pacientes. **Revista Brasileira de Enfermagem**. 2018; 71(3):975-82. DOI: 10.1590/0034-7167-2017-0053.

PEREIRA, W. S.; FILHO, R. J. C.; SILVA, W. R. A.; SILVA, R. S. T.; DANTAS, V. F.; AGUIAR, Y. P. C.; **Validação de uma abordagem combinada para avaliação de software educativo**: avanços e desafios. Revista Tecnologias na Educação. Ano 8. Número/Vol. 16. Edição Temática. Anais do Congresso Regional sobre Tecnologias da Educação. 2016.

PRESSMAN, R. **Engenharia de software**. McGraw-Hill, 2006.

PRESSMAN, R. S.; MAXIM, B. R. **Engenharia de software**. McGraw Hill, Brasil, 2021.

RADZIWILL, N. M. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. **Quality Management Journal**, 25 (2), 109-110. 2018.

RANKIN, D. J.; JIANG, J. A Hardware-in-the-Loop Simulation Platform for the Verification and Validation of Safety Control Systems. **IEEE Transactions on Nuclear Science**, 58(2), pgs. 468–478. 2011. doi:10.1109/tns.2010.2103325. Acesso em: 31 Jan. 2023.

REIS, J. N.; VALE, G.; COSTA, H. Manutenibilidade de tecnologias para programação de linhas de produtos de software: Um estudo comparativo. **Anais do XIV Simpósio Brasileiro de Qualidade de Software**. SBC, 2015. p. 64-78.

ROCHA, A. R.; CAMPOS, G. H. B.; Avaliação da qualidade de software educacional. **Aberto**, 12:32–44. 1993.

RODRIGO, P.; **Modelo de ameaça STRIDE**: exemplo e visão geral. Site Estudyando**,** 2020. Disponível em: https://pt.estudyando.com/modelo-de-ameaca-stride-exemplo-e-visao-geral/#. Acesso em: 08 Jan. 2022.

RODRIGUES, F. D.; ZUFFO, M. K.; BELLOC, M. C. O.; FERRAZ, F. **Sistema de Realidade Virtual para Simulador de Passadiço**. XI SBGames. Brasília – DF, Brazil, November 2nd - 4th, Escola Politécnica, Universidade de São Paulo, Brasil, 2012.

RUDAKOV, S.; DICKERSON, C. E. Harmonization of IEEE 1012 and IEC 60880 standards regarding verification and validation of nuclear power plant safety systems software using model-based methodology. **Progress in Nuclear Energy**, 99, 86–95. 1997. DOI:10.1016/j.pnucene.2017.04.003

SÁ, A. O., MACHADO, R. C. S., ALMEIDA, N. N., O encontro da guerra cibernética com as guerras eletrônica e cinética no âmbito do poder marítimo**.** DOI 10.21544/1809-3191.v25n1.p89-128. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 25, n. 1, p. 89-128. janeiro/abril. 2019.

SAKURADA, E. Y. **As técnicas de Análise dos Modos de Falhas e seus Efeitos e Análise da Arvore de Falhas no desenvolvimento e na avaliação de produtos**. Dissertação de Mestrado. UFSC, 2011.

SAMPAIO, F. M. B.; GROSSI, L. G.; NETO, A. L. M.; LOUREIRO, A. A. F.; OLIVEIRA, L. B. Uma avaliação de toolkits para criptografia baseada em emparelhamento bilinear**.** 2015. **Anais do XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2015. p. 330-333. DOI: https://doi.org/10.5753/sbseg.2015.20108

SAUL, J. **Cyber threats prompt return of radio for ship navigation**. Revista Reuters, 2017. Disponível em: https://www.reuters.com/article/us-shipping-gps-cyber-idUSKBN1AN0HT. Acesso em: 18 jan. 2022.

SILVA W. P., SANTIAGO V., VIJAYKUMAR N. L., MATTIELLO-FRANCISCO F.: **SPAC:** Ferramenta para Processamento e Análise de Dados Científicos no Processo de Validação de Software em Aplicações Espaciais**.** Instituto Nacional de Pesquisas Espaciais (INPE) - São José dos Campos, SP – Brasil 2007.

SILVA, M. E. S.; SILVA, C. B. Variabilidade Climática–processos físicos e dinâmicos nos oceanos e atmosfera. **Revista do Departamento de Geografia**, p. 372-406, 2012. Disponível em https://comum.rcaap.pt/bitstream/10400.26/1364/1/NeD108_TiagoPittaeCunha.pdf. Acesso em: 17 Jan. 2023.

SILVA, M. M. F. F. **Submarino nuclear de ataque:** Nova Dimensão Estratégica para a Defesa Nacional. Monografia (Especialização) – Departamento de Estudos da Escola Superior de Guerra, Rio de Janeiro, 2012.

SILVA, V. A. O.; **Uma Metodologia para Modelagem de Ameaças em Ambientes Baseados na Internet das Coisas.** Monografia de Graduação. UFPE, Recife-PE, 2018.

SOMMERVILLE, I. **Engenharia de Software**. Editora Pearson Addison, 2007.

SOMMERVILLE, I. **Engenharia de Software**. Editora Pearson Addison, 2003.

SOPRAN, R.; MELO, D. R.; ZEFERINO, Z. A.; BEZERRA, E. A. Análise Comparativa do Custo e do Desempenho de um Algoritmo de Criptografia para Sistemas Embarcados Explorando o Particionamento Hardware/Software. **Anais do Computer on the Beach**, p. 259-268, 2017. DOI: https://doi.org/10.14210/cotb.v0n0.p259-268.

SOUSA, A. A. G. de. **Sistemas de Gestão da Qualidade ISO 9001 nas Forças Armadas: proposta de um organismo certificador para a Marinha do Brasil**. 2019. Dissertação Mestrado Profissional em Metrologia e Qualidade - Instituto Nacional de Metrologia, Qualidade e Tecnologia, Duque de Caxias – RJ, 2019. 208f.

SPERLING, S. G.; COSER, J.; CARDOSO, S. M. M.; Processo de validação de instrumento de pesquisa: um relato de experiência. **XVII Seminário Internacional de Educação no MERCOSUL**, 2018.

STEPHENSON, M.; CARTER, J. Teste de voo inicial dos computadores de controle de voo de suporte de produção no NASA Dryden Flight Research Center. **Conferência e Anexo sobre Orientação, Navegação e Controle** 1999. Disponível em: https:// https://arc.aiaa.org/doi/abs/10.2514/6.1999-4203. Acesso em: 24 ago. 2021.

SVILICIC, B.; BRČIĆ, D.; ŽUŠKIN, S.; KALEBIĆ, D.; **Raising Awareness on Cyber Security of ECDIS**. the International Journal on Marine Navigation and Safety of Sea Transportation. Volume 13 Number 1 March 2019 DOI: 10.12716/1001.13.01.24, 2019c.

SVILICIC, B.; KAMAHARA, J.; CELIC, J.; BOLMSTEN, J.; **Assessing ship cyber risks**: a framework and case study of ECDIS security. WMU J. Marit. Aff. 18, 509-520. https://doi.org/10.3390/jmse7100364. 2019b.

SVILICIC, B.; KAMAHARA, J.; ROOKS, M.; YANO, Y.; **Maritime cyber risk management**: An experimental ship assessment. The Journal of Navigation, Volume 72, 5ª Edição, Set. 2019, pg 1108-1120. 2019a

SVILICIC, B.; RUDAN, I.; FRANCIŸ, V.; MOHOVIC, D.; Towards a Cyber Secure Shipboard Radar. **The Journal of Navegation**, pg 1 - 12. The Royal Institute of Navigation. DOI 1017/S0373463319000808. 2019d.

TOCCI, R. J. **Sistemas Digitais**. Princípios e aplicações. 8ª ed. São Paulo. Prentice Hall, 2003.

UNITED NATIONS. **UNITED NATIONS CONVENTION ON THE LAW OF THE SEA**. 10 Dez. 1982. Disponível em: https://www.un.org/depts/los/convention-agreements/texts/unclos/cosingnox.htm. Acesso em: 12 jul. 2021.

VICENZI, A. M. **Orientação a Objeto:** Definição, Implementação e Análise de Recursos de Teste e Validação. São Carlos-SP, USP, 2004. Disponível em: https://www.teses.usp.br/teses/disponiveis/55/55134/tde-17082004-122037/publico/tese.pdf. Acesso em: 30 jun. 2021.

WALLACE, D. R.; FUJII, R. U. Software Verification and Validation: An overview. **IEEE Software**, nº 6 (3), pg. 10–17. 1989. DOI: 10.1109/52.28119.

WAZLAWICK, R. S. **Engenharia de Software**: Conceitos e Práticas. Elsevier, 2013.

WEI-TEK T.; VISHNUVAJJALA, R.; ZHANG, D. Verificação e validação de sistemas baseados em conhecimento. **Transações IEEE sobre Conhecimento e Engenharia de Dados**. 1999. DOI: 10.1109 /69.755629

XAVIER, B. **Qual é o comprimento da costa do Brasil?** Notas de Aula, UFRJ, 2020.

ZHANG, L.; TAAL, A.; CUSHING, R.; DE LAAT, C.; GROSSO, P. A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. **International Journal of Information Security**, v. 21, n. 3, p. 509-525, 2022.

APÊNDICE A

Protocolo de Avaliação de Software - Nuclear Naval

ProAS-NN

SUMÁRIO

1. INTRODUÇÃO

É inegável o desejo de se ter segurança em tudo o que se usa, em alguns casos, a segurança é algo que vai além do desejo ou de uma necessidade e se torna uma obrigação, principalmente quando se lida com riscos a vidas humanas, pela manipulação de um produto intangível como *softwares*.

Que estão sujeitos a diversas possibilidades de falhas e vulnerabilidades, e cujas consequências podem ser muito perigosas, como é o caso do *software* empregado na atividade nuclear, cujo mau funcionamento, pode ser muito mais danoso à pessoas e ao meio ambiente que a maioria dos *softwares*, devido a possibilidade da ocorrência de um acidente radiológico.

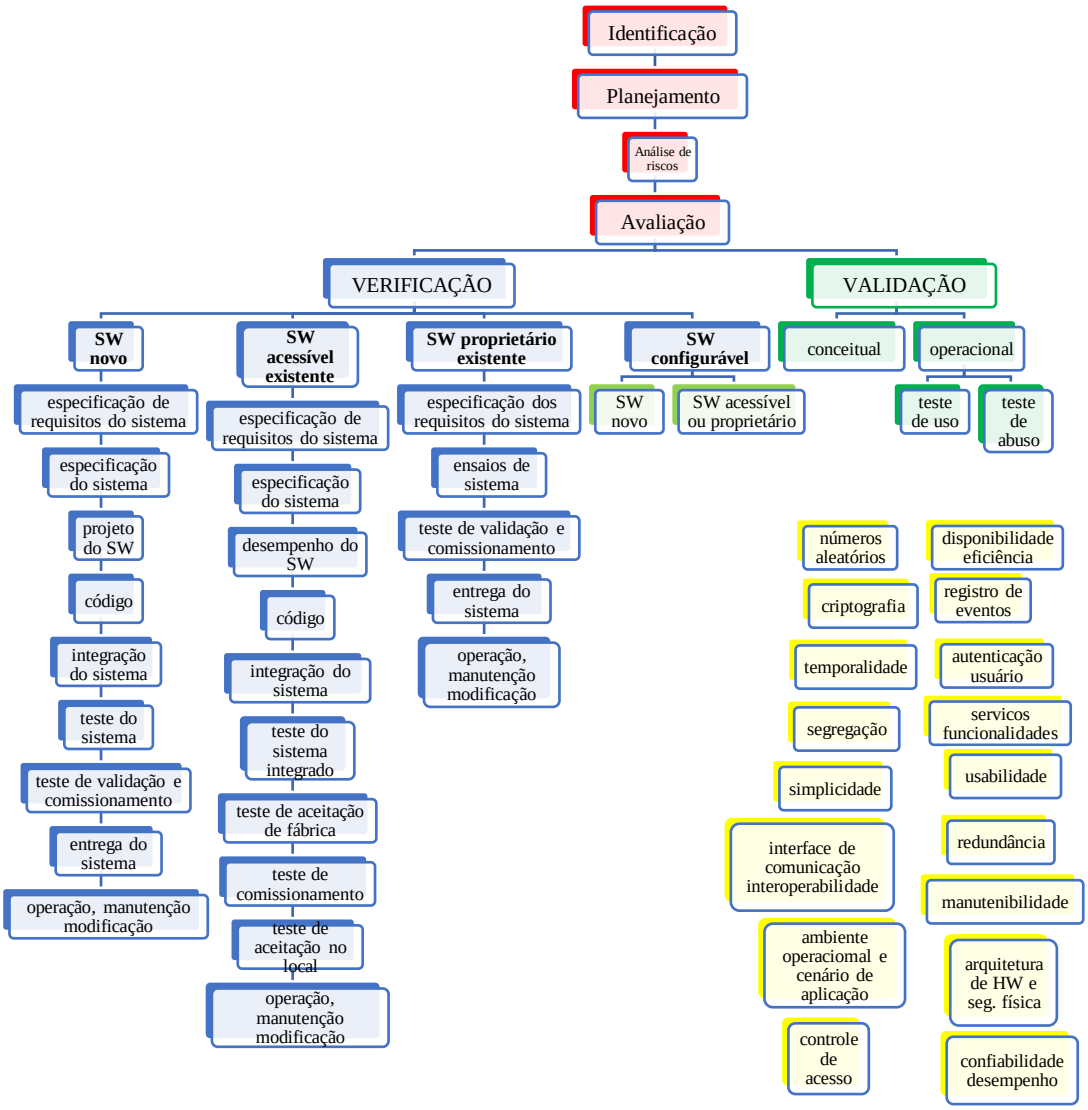
Além de que, cada *software*, em cada sistema e aplicação, possui uma configuração e um comportamento único, depende de fatores internos, externos e de uso. Por isso, é necessário a criação de um método de análise flexível e abrangente, que possibilite a garantia da segurança de tais produtos.

Para tanto, foi elaborado este documento, que serve de guia para a avaliação de *softwares* empregados em meios navais com propulsão nuclear, denominado de Protocolo de Avaliação de Softwares no âmbito Nuclear Naval (ProAS-NN), que estabelece o propósito, o público-alvo, o passo a passo da avaliação, os aspectos e ensaios para a demonstração da adequação e conformidade a requisitos de segurança e cujo funcionamento atenda às necessidades explicitas do usuário.

Este documento está organizado de forma a atingir todos os campos possíveis de avaliação de um *software* empregado em meios navais com propulsão nuclear, por meio dos processos de verificação e validação, com base em normas nacionais e internacionais, práticas e métodos de órgãos e instituições que realizam a avaliação de instalações críticas de segurança nuclear. E visa garantir confiabilidade ao demonstrar a segurança no uso de *software* e que este executa de forma consistente e correta as funções que foi planejado, pelo atendimento a

requisitos funcionais, de qualidade e segurança. A Figura 20 representa graficamente a realização do ProAS-NN, da maneira mais completa, onde o processo de verificação é divido em função o tipo de *software*, em que cada tipo permite a verificação de um conjunto específico de fases, em seu ciclo de vida.

Figura 20- Fluxograma do protocolo de avaliação



Fonte: o autor.

2. OBJETIVO

O objetivo do ProAS-NN é fornecer aos usuários, seja o requerente, avaliador, desenvolvedor ou licenciador, uma sistemática para as atividades de avaliação da conformidade de *softwares* empregado em meios navais com propulsão nuclear. Pela descrição de como realizar a verificação do atendimento aos requisitos nas diversas fases do ciclo de vida do software e da validação dos diversos requisitos presente, sob a forma de atributos.

Com vistas em preservar a inviolabilidade, disponibilidade, integridade e autenticidade, garantir trilhas para futuras auditorias, o correto funcionamento e atendimento as necessidades explicitas dos usuários, o que inclui seu *hardware*, *firmware* e *software*.

Tendo como resultado o aumento da sua confiabilidade pela eliminação de falhas, vulnerabilidades e comportamentos indesejáveis, importante à segurança nuclear aplicados em meios navais. E o atendimento das necessidades do usuário, pela execução das funções especificadas para o sistema.

3. CAMPO DE APLICAÇÃO

Este procedimento deve ser aplicado em *softwares* empregados nos diversos sistemas digitais utilizados para medir, monitorar, consolidar, tratar, transmitir, receber e apresentar dados, parâmetros e informações em meios navais com propulsão nuclear, como sistemas de propulsão, armas, apoio a vida, governo, comunicação, navegação, geração de eletricidade, monitoramento e controle do reator, entre outros.

Podem ser submetidos ao ProAS-NN *softwares* novos, cuja produção é própria ou contratada e *softwares* já prontos de produção própria, contatada ou um produto comercial, mesmo que já tenha uso consagrado e tenham passado por processo de avaliação, desde que o fabricante ou seu representante concorde e colabore com a avaliação, fornecendo subsídios necessários para a realização das análises.

A avaliação pode ser aplicada a quatro tipos de *software*:

- *Software* novo;
- *Software* acessível;
- *Software* proprietário;
- *Software* configurável.

Para que seja realizada a avaliação, o *software* deve possuir documentação e especificações que o caracterize de forma clara, completa e consistente, incluindo todos os seus aspectos conceituais, de projeto, implementação, operação e manutenção.

4. DOCUMENTOS COMPLEMENTARES

Os documentos listados são gerados durante o processo de avaliação, e devem sofrer o devido controle e registro, para os dois primeiros, podem ser utilizados modelos de documentos já praticados pelo avaliador e/ou avaliado, para os demais, o ProAS-NN traz os modelos específicos a serem utilizados.

- Contrato entre requerente e avaliador, que formalize a avaliação;
- Termo de responsabilidade da equipe de avaliação;
- Modelo de Plano de Avaliação (Anexo A);
- Guia para análise de Riscos (Anexo B);
- Modelo de Relatório de Avaliação (Anexo C).

5. DEFINIÇÕES

Os termos utilizados ao longo do texto do ProAS-NN são apresentados na sequência, com objetivo de dirimir eventuais dúvidas e excluir possibilidades de interpretações e equívocos pelos usuários.

Atributos – Diversas características, aspectos ou propriedades que caracterizam os requisitos de um *software*, que pode ser distinguida quantitativa ou qualitativamente;

Demonstração da Conformidade – Processo de verificação de atendimento a um conjunto de requisitos, por meio da realização de ensaios;

Requerente – organização militar, empresa, instituição ou entidade que requer a execução da avaliação do ProAS-NN em algum *software* empregado em meio naval com propulsão nuclear, seja esta usuária, desenvolvedora ou fornecedora do *software*, ente intermediário ou de coordenação;

Requisitos - definição documentada de uma propriedade ou comportamento que um produto ou serviço particular deve atender;

Segurança Cibernética – Proteção à adequada operação de sistemas e redes, e às informações por ele processadas, visando à proteção dos aspectos de integridade, confidencialidade, disponibilidade e autenticidade de dados e serviços;

Segurança nuclear – situação que representa a obtenção de condições operacionais, prevenção e controle de acidentes e mitigação apropriada das consequências de acidente, resultando em proteção de indivíduos ocupacionalmente expostos, do público em geral e do meio ambiente contra os riscos da radiação ionizante;

Sistema digital – combinação de dispositivos projetados para manipular informação lógica, composto pelo *software* integrado a um *hardware*;

***Hardware* -** parte física do computador, componentes eletrônicos, peças e equipamentos que fazem o computador ou dispositivo que precisam de algum tipo de processamento computacional funcionar;

Software – componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador ou sistema digital;

***Softwares* essenciais** – são os sistemas importantes à segurança, que necessitam de atenção especial. Como:

a) Relacionados com processos vinculados à Segurança Nuclear;
b) Que mitigam o mau funcionamento dos sistemas vinculados à Segurança Nuclear;
c) Que atuam nas falhas dos referidos acima.

***Software* novo -** é o que foi escrito especificamente para a aplicação, e toda documentação necessária para a avaliação é gerada. Demanda mais das atividades de teste na avaliação, pois não passou por algum processo de avaliação ou operação.
***Software* acessível -** é o que já foi empregado em sistema similar, possui toda documentação, código-fonte e experiência operacional disponíveis à avaliação, o que dá confiança do funcionamento correto e permite análises adicionais.
***Software* proprietário -** é um produto comercial que atende à necessidade do sistema, mas cujo código-fonte e documentação de desenvolvimento têm baixa disponibilidade para verificação sua avaliação deve ser baseada na validação, na experiência operacional, em testes funcionais e avaliações anteriores.

***Software* configurável** - é que já existe e pode ser configurado de acordo com a demanda, sua vantagem é o controle exercido na modificação, para garantir que os processos adotados permitam a avaliação adequada. A avaliação é dividida, uma etapa para o *software* básico e outra para o *software* adicional ou versão modificada.

Validação - Conjunto de análises por meio de testes e revisão documental, realizadas via procedimentos que atestam se o *software* está de acordo com a especificação.

Verificação – É o processo que determina se o produto de cada fase do ciclo de vida do *software* atende ou não a todos os requisitos impostos pela fase anterior, ou seja, se as saídas de um processo refletem as entradas.

6. RESPONSABILIDADE

A responsabilidade por solicitar a aplicação do ProAS-NN é do requerente, cabe a esta fornecer uma amostra do *software* a ser avaliado, juntamente com os documentos necessários para a realização da avaliação, e opcionalmente estabelecer requisitos mínimos a serem verificados durante o processo. Se o *software* utilizar *hardware* específico, este também deve ser disponibilizado pelo requerente.

A responsabilidade pela execução do processo de avaliação, análise documental e testes é da equipe de avaliação constituída para tal, por meio de portaria de designação, sob a égide do organismo responsável pela Segurança e Qualidade Nuclear Naval, denominado avaliador, que cabe observar o cumprimento do estabelecido pelo ProAS-NN e de eventuais requisitos definidos pelo requerente, não se limitando a eles durante o processo de análise heurística e realização de testes, devendo relatar a percepção de qualquer anomalia ou necessidades.

A equipe designada para a execução do ProAS-NN, responsável por realizar a avaliação deve possuir quantitativo proporcional ao tamanho do sistema avaliado, ser livre, independente e não possuir qualquer envolvimento ou fazer parte de qualquer atividade ou processo de melhoria, requisição, especificação, desenvolvimento ou aquisição do *software* avaliado, além de ser independente hierarquicamente de qualquer setor ou pessoa ligada a algum dos processos listados. Possuir competência moral e profissional condizente com o nível da avaliação, domínio do ProAS-NN, comprovada formação técnica, observar a ética profissional, guardar sigilo sobre a avaliação e produto avaliado, não deter qualquer documento ou rascunho relativo ao processo de avaliação.

7. MÉTODO

A avaliação deve ocorrer de preferência durante o início do desenvolvimento ou modificação do *software* se estendendo as demais fases de produção, até a entrega do produto. O que torna possível descobrir erros em fases prematuras do projeto e apontar possíveis melhorias, com menores perdas em correções e atualizações menos danosa, entretanto, isso só é possível para *softwares* novos.

Contudo, o ProAS-NN pode ser aplicado em sistemas já finalizados e entregues, o que possivelmente não permitirá que sejam realizadas melhorias, apenas a verificação de fases

baseadas em testes e a identificação quanto a presença e eficiência dos atributos frente ao funcionamento e aos resultados obtidos.

A avaliação pelo ProAS-NN ocorre pela análise heurística, e realização de testes comportamentais e estressores, com os devidos registros documentais, da realização de todas as análises possíveis e previstas nos processos de verificação e validação, e a demonstração que falhas no funcionamento foram corrigidas e vulnerabilidades foram eliminadas, o que garante que o *software* atende os objetivos para que foi desenvolvido, com qualidade e segurança.

O ProAS-NN organiza a avaliação de acordo com o tipo de *software*, o que possibilita que diferentes fases do processo de verificação sejam realizadas, e que características e aspectos que definem o sistema, chamado no âmbito deste texto de atributos sejam validados. Estas fases e atributos devem ser especificados durante o planejamento da avaliação, pois poderão ser diferentes para cada *software* avaliado e não envolver todos, em função de sua especificidade e tipo.

Para a execução do ProAS-NN poderão ser considerados testes, ensaios e avaliações realizados por outras entidades, desde que contratados pelos fornecedores ou fabricantes e ajam de forma independente, ética, imparcial e confidencial. Caso isso ocorra, o que deve ser comprovada, através da documentação de realização dos testes, ensaios e avaliações., sua competência técnica deverá ser demonstrada por meio de acreditação, certificação ou outros mecanismos.

Também podem ser levadas em consideração avaliações em versões anteriores do software, caso em que deverá ser claramente apresentada a diferença da versão que se está submetendo, essa diferença deve ser analisada, e se necessário ser submetida a avaliação.

Durante todo o processo, a equipe fará registro das informações relativas aos ensaios, essas informações devem ser suficientes para garantir a rastreabilidade e repetibilidade dos ensaios executados, a qualquer momento, bem como a realização de auditorias.

A avaliação de *software* pelo ProAS-NN é elaborada pelas seguintes etapas:

a) Preparação para a avaliação;
b) Identificação do sistema avaliado;
c) Planejamento da avaliação;
d) Análise de riscos;
e) Verificação;
f) Validação;
g) Entrega da avaliação.

7.1.Preparação

Antes do início da avaliação é necessário que os envolvidos se preparem para o processo, que deve iniciar pela realização de um acordo ou contrato, que observe a imparcialidade e a confidencialidade, estabeleça papeis, atores e compromissos.

O requerente deve utilizar o ProAS-NN para conhecer seu papel e responsabilidades durante o processo. Após caracterizar o tipo do *software*, deve preparar a documentação a ser entregue ao avaliador, de acordo com o tipo de *software* avaliado e com a fase do ciclo de vida

em que esse se encontra. Essa documentação deverá permanecer acessível durante toda avaliação, ser legível e estar no idioma português, inglês ou ambos.

Para *softwares* novos, a documentação e o *software* devem ser fornecidos à medida que forem sendo produzidos, de forma organizada, de acordo com o andamento de seu desenvolvimento.

Nos demais tipos de *software*, além da documentação, o avaliado deve preparar uma unidade do *software*, idêntico ao utilizado, havendo componentes e *hardwares* específicos para o correto funcionamento do *software* avaliado, esse também necessita ser entregue ao avaliador.

O avaliador deve nomear a equipe de profissionais que irá trabalhar na avaliação, reservar espaço físico e ferramentas necessárias para a avaliação, condizentes com o sistema (*software, hardware* e *firmware*) avaliado.

7.2.Identificação

O ProAS-NN é iniciado pela caracterização inicial do *software* avaliado, com a identificação do tipo, seu ambiente, conteúdo, funções, necessidades, possibilidades, objetivos e expectativa dos usuários, o que possibilita definir os limites do *software*, delimitar o escopo da avaliação, planejar o processo de avaliação e definir os processos de validação e verificação.

Primeiramente, deve-se entender qual será a utilização e objetivo do sistema, por meio de reuniões entre o avaliador e o requerente, onde deve ser apresentado o *software*, seu sistema, as finalidades, as funcionalidades e a aplicação, também poderá ser explicado o processo de avaliação e esclarecidas eventuais dúvidas. O anexo A do ProAS-NN é um modelo que auxilia a identificação e serve para a elaboração do relatório da avaliação.

Para *softwares* novos deverá ser apresentado o cronograma previsto para seu desenvolvimento para que sejam programadas as pausas para a verificação entre as fases do ciclo de vida, também devem ser programadas futuras reuniões para acompanhar o andamento da avaliação.

Para *softwares* proprietários, caso seja aplicado em computador convencional, será entregue a amostra do *software* para avaliação, por meio de dispositivos de armazenamento como pen drive ou cartão de memória, caso seja um sistema que utilize *hardware* dedicado, deve ser realizada a entrega acompanhada da unidade de *hardware* e sua estrutura física. Em ambos os casos todos os materiais recebidos deverão ser catalogados e registrados, com uma etiqueta que o identifique, de acordo com o apresentado no anexo A.

Deverão ser depositadas todas as ferramentas e recursos necessários para a realização de ensaios operacionais com o *software* avaliado, como ferramentas que o simulem/emulem e ferramentas de teste.

A documentação do *software*, deverá ser entregue, e catalogada de acordo com o previsto no modelo do anexo A, e passar por uma leitura prévia, para identificar sua pertinência, adequabilidade e aplicabilidade, bem como a necessidade de documentação complementar.

Esta leitura prévia, juntamente com as informações apresentadas na reunião inicial, fornecerá argumentos para definir o escopo da avaliação, selecionar quais atributos poderão ser

avaliados, como ocorrerão os ensaios, traçar as estratégias que serão utilizadas durante todo processo e montar a estrutura do plano, que será utilizada como guia para a avaliação.

7.3.Planejamento

Com base na identificação do *software* avaliado, é realizado o planejamento da avaliação, que orienta a aplicação do processo de avaliação de *software*, no atingimento dos seus objetivos, por isso é de suma importância que seja realizado de forma precisa e sólida para maior consistência das etapas seguinte de avaliação.

O nível de detalhe do plano deverá ser consistente com o tamanho, e a aplicação do *software*, o planejamento da avaliação pode ser realizado com base no modelo de plano de avaliação, constante no anexo A do ProAS-NN.

A depender do tipo de *software* será executada a verificação de um conjunto de fases, da mesma forma a depender das funções, local de instalação, *hardware* associado e demais características é executada a validação de um determinado conjunto de atributos.

Durante a realização da avaliação é possível revisar e alterar o planejamento, redefinir e aprimorar estratégias, adicionar e modificar os testes funcionais e estressores.

7.4.Análise de riscos

A interação entre o avaliador e o *software* no processo de avaliação do ProAS-NN ganha profundidade com a análise de riscos aos quais pode estar exposto. Existem diversas ferramentas para identificar, avaliar e propor soluções para os riscos que tenham potencial significativo para afetar adversamente o sistema, como a Árvore de Análise de Falhas (FTA), Análise de Modos de Falha e seus Efeitos (FMEA), dente outras.

Especificamente para a execução do ProAS-NN foi elaborado uma ferramenta baseada em métodos já consagrado na análise de riscos computacionais, o Guia para Modelagem de Ameaças, que faz a análise de riscos pela modelagem de ameaças, e segue no anexo B deste texto, sua execução possibilitará identificar, quantificar e ranquear os riscos baseado na probabilidade e consequências de sua ocorrência.

Caso já tenha sido realizada a análise de riscos ou modelagem de ameaças, anteriormente a avaliação, esta poderá ser considerada, desde que identificado quem a elaborou e sua competência técnica preferencialmente por meio de acreditação, certificação ou outro mecanismo semelhante. Os resultados da análise de riscos devem constar no relatório da avaliação.

7.5. Verificação

O processo de verificação consiste em analisar as informações ao longo do ciclo de vida do *software*, desde a fase de especificação dos requisitos do sistema, passando pelo projeto, até as fases de operação, manutenção e modificação, com o objetivo de confirmar, a cada fase, se os produtos gerados refletem os requisitos de entrada.

Cada tipo de *software* permite a realização da verificação de uma maneira diferente, em maior ou menor volume, e deve seguir o planejamento, o item 8 do ProAS-NN detalha como

estas devem ser realizadas. Todas as informações obtidas e observações devem ser registradas para compor o relatório de entrega da avaliação.

7.5.1. *Software* Novo

A verificação ocorre simultânea ao processo de desenvolvimento do *software*, entre suas fases, para cobrir as diversas fontes de falhas, e possibilita que sejam corrigidas antes do início da próxima fase. Sua principal fonte de informação é a documentação, também são realizados testes, se forem encontradas anomalias, elas serão registradas para a resolução imediata, as fases da verificação para *software* novo são:

a) Verificação da especificação dos requisitos do sistema;
b) Verificação das especificações do sistema;
c) Verificação de projeto de *software*;
d) Verificação do código;
e) Verificação da integração do sistema;
f) Verificação de teste de sistema;
g) Verificação do teste de validação e comissionamento;
h) Verificação de relatórios de entrega do sistema e de aceitação;
i) Verificação de relatórios de uso e manutenção.

7.5.2. *Software* Acessível

O acesso à grande parte da documentação oriunda do desenvolvimento e de aplicações anteriores possibilita verificar se a funcionalidade e o desempenho reivindicados para o sistema correspondam às informações documentadas, e se o mapeamento das funções do *software* foi realizado corretamente.

A verificação da funcionalidade e do desempenho ocorre da mesma forma que foi descrita para o *software* novo, seguindo o ciclo de vida de desenvolvimento, podem ser utilizados relatórios de verificações anteriores.

Se forem encontradas anomalias, elas serão registradas, não sendo resolvidas imediatamente como no ciclo de vida normal do desenvolvimento.

Abrange as etapas:

a) Verificação da especificação dos requisitos do sistema;
b) Verificação da especificação do sistema;
c) Verificação da especificação de desempenho do *software*;
d) Verificação do código fonte;
e) Verificação do relatório de integração do sistema;
f) Verificação do relatório de teste de sistema integrado;
g) Verificação do relatório de teste de aceitação de fábrica;
h) Verificação de relatório de teste de comissionamento;
i) Verificação do relatório de teste de aceitação do local; e
j) Verificação de relatórios de operação, manutenção e modificação.

Se o *software* tiver sido usado em um sistema de categoria de segurança semelhante, pode haver documentação extensa de processos realizados para uma avaliação independente.

7.5.3. *Software* Proprietário

A documentação disponível será revisada em relação a verificação dos requisitos, de forma semelhantes a *softwares* novos, dentro do possível, como a documentação completa normalmente não está disponível, a verificação será prejudicada, assim é dada mais ênfase na realização de testes assim como o *feedback* da experiência operacional e avaliações anteriores. Desta forma, devem ser executadas integralmente a verificação das seguintes atividades do ciclo de vida do sistema:

a) Verificação de especificação dos requisitos do sistema;
b) Verificação do relatório de ensaios do sistema;
c) Verificação do relatório de testes de validação e comissionamento;
d) Verificação do relatório de entrega do sistema;
e) Verificação de relatórios de operação, manutenção e modificação.

Devem ser utilizadas fontes de registros com controle de qualidade adequado, durante períodos adequados, como documentos dos testes do sistema integrado e os testes de validação e comissionamento, avaliações de terceiros e a justificativa feita para demonstrar a adequação ao propósito do *software* devem ser investigadas.

7.5.4. *Software* Configurável

Sua verificação é trabalhada em suas duas partes, o *software* básico e a parte de configuração específicos para a aplicação. A parte configurável, apesar de ser parte integrante do *software* total deve ser verificado como um *software* novo. O *software* básico pode ser tratado como *software* existente, podendo ser aplicada a verificação de acordo com a documentação apresentada, em muitos casos, o *software* básico já foi verificado, sendo necessário rever a verificação e decidir se é aceitável para a aplicação.

7.6. Validação

O objetivo da validação é demonstrar o atendimento as necessidades do usuário e a segurança do *software*, pelo atendimento aos requisitos estabelecidos pelo requerente e ao especificado em relação aos atributos avaliados, selecionados durante o planejamento.

A validação é realizada pela caracterização do *software* avaliado de forma clara, objetiva, completa e consistente, o que inclui seus aspectos conceituais, de projeto e implementação, da mesma maneira que a verificação, a validação ocorre de acordo com o tipo de *software*.

7.6.1. *Software* novo

O processo de validação de *softwares* novos é baseado nos requisitos do sistema, envolve análises documentais, simulações estáticas e dinâmicas de sinais de entrada, organizadas em modos que representam operação normal.

Os atributos devem ser analisados, medidos e confirmados por meio de testes representativos, para as ações causadas por cada parâmetro, isoladamente e em combinação. O relatório deve indicar o que foi aprovado, o que falhou e os motivos da falha. Todos os atributos devem ser cobertos pelos testes.

7.6.2. *Software* acessível

O processo de validação de *softwares* acessíveis existentes, envolve as mesmas etapas do *software* novo, na medida em que a documentação permita, para conferir se o *software* foi desenvolvido de acordo com as boas práticas de engenharia de *software*, seguindo um plano de controle de qualidade desenvolvido de acordo com padrões reconhecidos. Incluí a análise do histórico de operação documentado, e a análise da precisão do manual de usuário.

Se o código-fonte não estiver acessível, a seguinte documentação deve ser analisada para verificar o uso de interrupções, alocação de memória e recursão:

a) Especificações funcionais;
b) Especificação da interface;
c) Documentos de projeto;
d) Arquivos de teste

A realização dos testes irá mostrar que esses recursos funcionam corretamente.

7.6.3. *Software* proprietário

Normalmente, a avaliação de *softwares* proprietários não pode fazer uso de documentos de desenvolvimento e do código fonte, por isso o histórico operacional durante um período adequado deve ser avaliado, deve incluir:

a) Histórico de lançamento;
b) Número de licenciados e extensão de uso;
c) Histórico de erros e modificações para corrigir defeitos.

7.6.4. *Software* configurável

A validação do *software* básico seguirá as abordagens descritas para *softwares* acessíveis e proprietários existentes, os aspectos configuráveis do *software* devem ser validados como novo *software*.

7.7.Entrega da avaliação

Ao fim da avaliação do ProAS-NN será atribuído um relatório de ensaio, onde todas as informações registradas são organizadas, e juízo de valor é agregado, o objeto avaliado é classificado como aceito ou não, podem ser sugeridas modificações em seu *software* ou *hardware*, com o objetivo de reduzir ou eliminar eventual falha ou deficiência.

Todas as informações devem ser registradas ao longo da avaliação, de maneira lógica e organizada, mostrando o que na documentação analisada, o que é apresentado pela amostra estudada e seu comportamento, organizado por fase do ciclo de vida e por atributo avaliado, de acordo com o anexo C do ProAS-NN.

Vale ressaltar que o relatório não é confeccionado ao fim da avaliação, sua produção começa junto a primeira seção do ProAS-NN, quando o levantamento das informações iniciais define a estrutura do seu texto e é alimentado a cada observação realizada, fato levantado, e resultado de teste.

Caso sejam verificados erros e vulnerabilidades, o relatório identificará sua fonte, gravidade e sugestão para mitigar ou eliminá-la, devendo o instrumento passar por nova avaliação após sanada, sendo considerado aprovado após o encerramento de todos os ensaios, e não sejam identificados novamente.

Ao fim, é realizada a reunião de encerramento do ProAS-NN, com a entrega certificado e a apresentação dos pontos positivos e eventuais oportunidades de melhoria.

8. ENSAIOS

Os ensaios demonstram o atendimento aos atributos pela realização de um conjunto de testes e análises, são realizados de duas formas, cada uma associada a um conjunto de análises e que levam a um grau de confiança pela demonstração e construção das características desejadas, sendo:

a) Ensaio de Avaliação de Conceito;

b) Ensaio de Avaliação de Operação.

8.1.Ensaio de Demonstração de Conceito

A avaliação em termos de conceito, tem o objetivo verificar se a proposta conceitual do *software* apresentada permite seu funcionamento correto, atende as necessidades do usuário e aos princípios básicos de segurança consagrados na comunidade técnica e científica, e verificar se os riscos identificados foram mitigados.

O primeiro documento a ser trabalhado é a análise de riscos, que juntamente aos demais documentos recebidos, possibilitará levantar todas as informações referentes a algoritmos, ferramentas e mecanismos implementados no sistema.

A demonstração da conformidade ocorre por meio da análise textual de completude e consistência dos documentos:

a) Memorial descritivo, contendo as principais informações técnicas;
b) Manual operacional, contendo informações sobre o uso e manutenção;
c) Especificação dos dispositivos de armazenamento de dados utilizados;
d) Lista completa dos comandos;
e) Diagrama esquemático do *hardware* que comporta o *software*;
f) Diagrama de blocos que compõem o sistema e suas interfaces;
g) Descrição dos métodos de verificação de integridade dos programas embarcados;
h) Descrição dos métodos de proteção embarcados;
i) Descrição dos métodos de controle de acesso para todas as interfaces;
j) Descrição dos métodos de proteção e geração das chaves criptográficas;
k) Documentação fotográfica do dispositivo a ser avaliado;
l) Descrição do ambiente operacional onde o *software* será utilizado;
m) Análise de riscos do sistema.

A conformidade será alcançada se for evidenciada a caracterização conceitual, ou seja, se a documentação depositada permite verificar claramente, e de maneira consistente com a análise de riscos.

8.2.Ensaio de Demonstração em Operação

Em adição aos objetivos do ensaio de demonstração de conceito, o ensaio de demonstração da conformidade em operação tem como objetivo verificar se o comportamento do sistema cujo *software* é avaliado em condições operacionais é consistente com suas especificações.

Essa avaliação é feita por meio da execução de cenários de teste que permitam avaliar o comportamento, tanto em casos de uso típicos quanto em casos de abuso, que representem condições imprevistas às quais poderá eventualmente estar sujeito.

Em adição à documentação técnica listada, os ensaios devem ser realizados com base na documentação de testes do produto, incluindo planos de testes e relatórios de testes do instrumento, dentre outros que se considere relevante.

A conformidade será alcançada se o *software* avaliado apresentar, em todos os ensaios realizados, comportamento consistente com o previsto em documentação.

O ensaio é realizado com a inspeção do sistema e ambiente de execução, para verificar se o sistema se encontra em condições de operação conforme descrito em suas especificações.

Pela inspeção física da unidade sob avaliação, verifica-se a existência de consistência entre a amostra sob avaliação e as especificações descritas em sua documentação. A inspeção pode contemplar:

a) Inspeção visual;
b) Procedimentos de comunicação lógica com o ativo e seus módulos;
c) Procedimentos de monitoramento do ativo.

8.2.1. Testes Funcionais (Casos de Uso).

É a análise do comportamento do *software* em situações de operação real, por meio de procedimentos específicos, que devem ser elaborados tomando como subsídio as informações contidas na documentação do *software*.

Com o objetivo de que todas as funções que o *software* puder realizar sejam testadas, características e aspectos descritos nos memoriais e manual operacional também devem ser avaliadas de forma práticas de acordo com o contido na documentação.

Por esses ensaios, deve ser analisada a operação normal do *software*, todas as chaves ou teclas e combinações descritas devem ser empregadas e a reação do instrumento, interfaces gráficas de usuário, menus e demais elementos gráficos devem ser ativados e avaliados.

8.2.2. Testes de Segurança (Casos de Abuso).

Consiste na análise do comportamento do *software* avaliado, em situações atípicas de:

a) Testes de funcionalidade de segurança: permitem averiguar o comportamento de funcionalidades e serviços diretamente relacionadas à segurança, incluindo, mas não se limitando a mecanismos de autenticação, identificação de usuários, controle de acesso, registro de eventos e integridade de *software*;

b) Testes de exploração de vulnerabilidades: permitem demonstrar a existência de uma vulnerabilidade identificada ao longo do processo de avaliação;

c) Testes de penetração: são testes que reproduzem cenários de ataques típicos, permitindo avaliar o grau de explorabilidade de vulnerabilidades identificadas e impacto de ataques eventualmente bem-sucedidos;

d) Testes de sobrecarga: são testes que reproduzem cenários de sobrecarga a que poderá estar sujeito o ativo sob avaliação, sejam estes cenários legítimos ou maliciosos.

Estes testes devem ser planejados com base na documentação do *software*, realizados e documentados.

9. FASES DA VERIFICAÇÃO

A verificação é realizada entre as fases ao longo do ciclo de vida do *software*, para produtos novos acompanha seu desenvolvimento e para produtos já prontos resgata esse processo, com o objetivo de confirmar se o que é gerado em cada fase equivale ao requisito de início da fase, ou seja, se as saídas das fases condizem com suas entradas.

Na sequência são listadas todas as fases previstas no ProAS-NN para o processo de verificação relembrando que a depender do tipo do *software*, será verificado um conjunto diferente de fases.

9.1.Verificação da especificação dos requisitos do sistema

Ocorre no início do processo de desenvolvimento do *software*, seu objetivo é verificar se os requisitos especificados para a construção do *software*, satisfazem as necessidades explicitas dos usuários, expressas na documentação do conceito, e verificar se todas as funções foram claramente escritas e descritas.

É realizada por meio da revisão documental das especificações para a construção do *software* comparadas aos documentos de coleta das necessidades explicitas dos usuários.

9.2.Verificação da especificação do software

Tem como objetivo determinar se a especificação do *software* reflete o expresso nos requisitos para sua construção, e demostrar essa associação, além de verificar se todos os requisitos são testáveis.

Verifica os requisitos para que o *software* interaja com o *hardware*, usuários e outros *software*, avaliados em relação à completude, correção, consistência, precisão e legibilidade da especificação.

Verifica se as funções do *hardware* e *software* e sua integração foram claramente identificadas e alocadas, incluindo requisitos de teste, deve considerar aspectos como impacto na metodologia de projeto e, experiência anterior da equipe de projeto.

Verifica ainda a existência de requisitos de manutenção e se requisitos não funcionais foram introduzidos, como ferramentas de autoteste e diagnósticos internos.

Para garantir que todos os requisitos seguem para a próxima fase, estes devem estar documentados e justificados. É realizada por meio da verificação documental dos requisitos para a construção do e especificações do *software*.

9.3.Verificação da especificação do projeto de *software*

Tem como objetivo confirmar se a especificação do projeto do *software* é representada corretamente pelos requisitos da especificação de forma que o *software* funcione corretamente, satisfaça necessidades explicitas do usuário, e que seja rastreável.

Verifica se estão presentes na documentação a descrição das partes que tornam possível o funcionamento do sistema, em que o *software* está inserido, como um todo, a comunicação entre todas suas partes e a infraestrutura que suporta e gerencia essa comunicação.

Para cada bloco do *software*, verifica se são descritos na documentação os recursos que suportam sua execução (memória e seu mapa, processador/microcontrolador), os aspectos estáticos (arquitetura de *software*, ambiente de desenvolvimento) e os dinâmicos (fluxos de execução) do *software* e as funcionalidades específicas do bloco que contribuem para o correto funcionamento.

Verificar se todas as funções alocadas ao *software* estão claramente incorporadas ao projeto, se informação ou ação não funcional oferecida são compatíveis com as especificações de requisitos de *software*, se incluí funções de autoteste, se nenhuma função extra foi adicionada, e se recursos que não eram previstos foram identificados e justificados.

Realiza a análise do fluxo de dados, fluxo de controle, completude dos comandos do *software*, e se esses estão de acordo com o aspecto dinâmico (fluxo de execução) especificado na descrição de cada bloco do sistema.

Verifica se os intervalos de valores das variáveis do programa estão respeitando os limites delas, caso não respeitem, deve-se inspecionar o comportamento e se violam o funcionamento do sistema.

Todos os módulos de *software* embarcados devem ser claramente especificados, incluindo descrição de função e serviços oferecidos, tecnologia, localização física, interfaces, canais de comunicação, controle de acesso e mecanismos de proteção, atualização e verificação de integridade.

A verificação deve determinar se os padrões, práticas e convenções de projeto estão sendo seguidos, deve considerar outros aspectos do projeto julgados necessários e as necessidades de manutenção.

9.4.Verificação da codificação do *software*

O objetivo é determinar se o código-fonte e os dados de configuração refletem com precisão as funções alocadas no projeto de *software*.

Contempla a análise do código-fonte comentado, por meio de ferramentas de análise de código, com o objetivo de verificar a coerência na implementação do *software* em relação à documentação de projeto depositada, contempla o rastreamento das variáveis relevantes e da

análise de vulnerabilidades, bem como pode utilizar o exame dos resultados de testes de unidade ou análise de código concluída durante esta fase.

O que implica na análise de módulos, código-fonte e componentes quanto a integridade, correção, consistência, precisão e rastreabilidade a elementos específicos de projeto, para confirmar o atendimento aos requisitos.

Verifica se os intervalos de valores das variáveis do programa estão respeitando os limites delas, em caso negativo deve se verificar cada interface de comunicação envolvida na manipulação de dados, se estão descritos protocolos e algoritmos utilizados, a estrutura dos pacotes de dados transmitidos e a tecnologia empregada.

Contempla ainda a verificação da descrição da proteção dos módulos de software, mecanismos de atualização, soluções de verificação de integridade, os canais de comunicação e a sequência por onde as informações circulam.

Inspeciona o código-fonte em busca de todos os comandos descritos na lista completa de comandos, verificando se os parâmetros e seus respectivos tamanhos são iguais aos constatados na documentação, inspeciona o código em busca de comandos não descritos, caso existam, inspecionar o comportamento dos mesmos e se violam o funcionamento do sistema.

Realizar análise do código em busca de vulnerabilidades originadas em falhas de implementação, considerar as vulnerabilidades presentes nas principais listas para cada ambiente, tais como OWASP e CWE.

9.5.Verificação da integração do sistema

Tem o objetivo de verificar se funções alocadas ao *software* em seu projeto e na descrição da codificação estão corretamente demonstradas por testes no *software* integrado.

São realizados teste para verificar a integração de módulos e componentes de código-fonte, para demonstrar que os elementos de *softwares* integrados se comportam de forma correta, consistente e precisa, e que são funcionalmente completos, o que permite verificar se os módulos foram corretamente montados no projeto e confirmar que o *software* desempenha suas funções de projeto.

Também avalia se o desempenho predefinido e funções críticas são abordados e garantem que os padrões exigidos e convenções foram seguidas durante o processo de implementação.

Verifica a implementação dos módulos de *software* condizentes com as interfaces com o *hardware* e com outros módulos, avaliada quanto a completude, correção, consistência e precisão. A verificação deve levar em conta a necessidades decorrentes de futuras atividades de manutenção.

Verifica o esquemático do *hardware* com o objetivo de compreender a interação de todos os blocos do *software* avaliado e suas interfaces, e verificar se todos os blocos, interfaces de comunicação e os fluxos de informação estão representados e claramente indicados no esquemático, além da existência de outros dispositivos microcontrolados.

9.6.Verificação dos testes com o sistema integrado

É a verificação realizada quando o *software* é combinado com o *hardware* de destino, com o objetivo de demonstra o correto funcionamento do sistema, de acordo com sua documentação, observando as necessidades explicitas do usuário, os requisitos do projeto do *software* e os testes de integração do sistema.

Verifica por meio teste a realização das reais funções e o desempenho do sistema com relação aos requisitos especificados, confirma a completude, correção, consistência e precisão da interface do *hardware* com usuários e com outros sistemas.

Os testes também possibilitam verificar valores e intervalos calculados por suposições sobre a operação do sistema ou ambiente operacional, avalia se parâmetros de desempenho são alcançados, se as funções críticas funcionam com o necessário e se os requisitos de interface *hardware-software* foram satisfeitos.

9.7.Verificação dos testes de validação e comissionamento

É realizado com o *software* instalado no *hardware* de destino e alocado no ambiente em que deverá operar, com o objetivo de confirmar se o sistema foi instalado e comissionado corretamente, de modo que seu desempenho e as funções executadas sejam condizentes com a documentação de requisitos e de projeto, de modo a satisfazer as necessidades explicitas do usuário, que originaram a criação do *software*.

A parte essencial desta fase é verificar a realização dos testes de demonstração completa da funcionalidade e operação do sistema, e confirmar os resultados simulados, caso existam, e com a documentação.

Deve ser dada ênfase na medição dos tempos do sistema e desempenho, bem como a análise das interfaces externas e verificar se quaisquer erro e/ou anomalia identificados durante o processo de avaliação e desenvolvimento foram corrigidos.

Uma revisão da instalação deve ser realizada para garantir que o sistema foi instalado corretamente e executa com precisão as funções atribuídas.

9.8.Verificação dos testes desempenho do *software*

A verificação é realizada por meio de testes reais de desempenho do *software* com relação aos requisitos especificados em sua documentação, confirma a completude, correção, consistência e precisão dos valores obtidos com as estimativas calculadas por suposições sobre a operação do sistema.

Verifica se parâmetros de desempenho são alcançados e se as funções críticas funcionam como necessário sem deixar de satisfazer as necessidades do usuário.

9.9.Verificação dos testes de aceitação de fábrica

Tem o objetivo de verificar se o *software* foi testado corretamente quanto ao seu desempenho, com relação ao especificado na documentação de requisitos e projeto.

Verifica se as funções previstas na especificação dos requisitos do *software* foram testadas, com relação ao especificado na documentação de requisitos e projeto.

Verifica se os testes demonstraram a completa funcionalidade e operação do software, com relação ao especificado na documentação de requisitos e projeto.

9.10.Verificação dos testes de aceitação no local

Tem o objetivo de verificar se o sistema foi testado corretamente quanto ao seu desempenho com relação ao especificado na documentação de requisitos e projeto.

Verifica se as funções após a entrega e instalação correspondem ao previsto na especificação dos requisitos do *software*, com relação ao especificado na documentação de requisitos e projeto.

Verifica se os testes demonstraram a completa funcionalidade e operação do sistema, com relação ao especificado na documentação de requisitos e projeto.

9.11.Verificação da entrega do sistema

O objetivo é determinar se toda a documentação necessária para a operação e manutenção do sistema foi disponibilizada na entrega.

É realizada pela revisão sistemática da lista mestra de documentos do *software*, ou outro documento que contêm a lista da última versão da documentação atinente ao *software*, para verificar sua completude e consistência, envolve documentação do projeto, especificações e análises de engenharia, desenhos e diagramas, manuais, especificações e relatórios de teste.

9.12.Verificação de operação, manutenção e modificação

Ocorre em casos que a verificação é limitada à realização de testes e da experiência operacional. Compreende a realização dos testes previstos nas fases anteriores, complementado pelo acompanhamento de uso do software por seus usuários.

Verifica as necessidades de melhoria registradas pelos usuários e sua aplicabilidade.

10. ATRIBUTOS PARA VALIDAÇÃO

Os atributos da avaliação refletem as características da qualidade e aspectos de segurança que necessitam ter seus requisitos validados, devem descrever propriedades e comportamentos desejáveis e características aplicáveis, em busca da especificação clara, consistente e não ambígua implementada e a evidenciação de uma abordagem efetiva.

O ProAS-NN realiza a avaliação desses atributos, que refletem os diversos aspectos relacionados à concepção, implementação e operação do *software*, que refletem seu uso seguro e o atendimento às necessidades explicitas dos usuários.

Esse conjunto de atributos foi selecionado como forma de avaliar especificamente *softwares* aplicados em sistemas digitais empregados em meios navais com propulsão nuclear, para a avaliação pode ocorrer que alguns deles não estejam presentes ou não sejam aplicados a

um sistema específico, a ocorrência desse atributo e sua necessidade de avaliação deve ocorrer de acordo a identificação do *software* e planejamento de sua avaliação.

A validação dos atributos não visa obter a perfeição, mas demonstrar que o *software* está em um nível suficiente para o contexto de uso especificado, de acordo com o estabelecido pelo usuário.

As observações quanto aos atributos, cumprimento ou descumprimento das especificações mínimas, necessidades de correções ou oportunidades de melhorias, devem ser registradas para compor o relatório de avaliação. A descrição dos atributos e a forma como deve ser avaliada são descritas na sequência.

10.1.Ambiente operacional e cenários de aplicação.

É o atributo que visa identificar a condição situacional (ambiente e cenário) em que o sistema que terá o *software* avaliado é designado para operar, leva em consideração aspectos técnicos, ambientais e humanos.

Esse atributo é semelhante ao atributo que avalia arquitetura de *hardware* e segurança física, diferenciado pelo ponto de vista, onde o ambiente operacional e cenário de aplicação tem foco nos fatores externos ao sistema, enquanto a arquitetura de *hardware* e segurança física tem foco nas propriedades do sistema.

O local físico onde o sistema irá operar deve ser claramente apresentado, com a identificação das principais ameaças que possam existir, sejam permanentes ou temporárias, e potenciais fatores agressivos e atacantes associados, bem como as principais contramedidas existentes para eliminar ou mitigar os efeitos maléficos destes e inferir sobre sua eficácia.

Deve-se considerar aspectos físico e lógicos apontados pela análise de riscos, com o objetivo de identificar a exposição do sistema a fatores que podem prejudicar seu bom funcionamento como:

a) Fatores climáticos (umidade, temperaturas elevadas, luz solar, poeira);
b) Radiação ionizante proveniente de materiais radioativos;
c) Animais que possam danificar elementos de *hardware* (roedores e insetos);
d) Poeira intensa;
e) Pessoas não autorizadas a ter acesso ao sistema ou suas partes;
f) Emissões eletromagnéticas;
g) Variações ou interrupções elétricas.

E apresentar as medidas adotadas contra essas, como:

a) Blindagem contra emissões eletromagnéticas;
b) Proteção contra radiação ionizante;
c) Vedação contra a entrada de poeira e umidade;
d) Proteção física que evite acesso de animais e pessoas não autorizadas ao sistema ou suas partes;
e) Mecanismo que atenue os efeitos da temperatura a qual instrumento está exposto;
f) Dispostos protetores de sobre cargas e quedas de energia.

Algumas dessas contramedidas também correspondem a aspectos avaliados no item a), e não pode haver a análise de um atributo alheio ao outro.

Deve se ter atenção ao sistema que não esteja instalado permanentemente, da mesma forma os que são portáteis, para que seu local de armazenagem não represente novas ameaças e riscos.

A avaliação desse atributo é realizada pela análise documental, pelo ensaio de demonstração de conceito, combinado com inspeção física da unidade de *hardware*.

10.2.Arquitetura de *hardware* e segurança física.

Reflete a arquitetura do *hardware* do sistema cujo *software* avaliado está embarcado, e aspectos da sua segurança física, incluindo elementos físicos, suas tecnologias e organização física.

O atributo é semelhante ao atributo ambiente operacional e cenário de aplicação, e a análise de seus requisitos são confluentes, de forma que não pode haver a análise de um atributo sem as considerações a respeito do outro. Com a diferença do ponto de vista, onde o ambiente operacional e cenário de aplicação tem como foco os fatores externos ao sistema enquanto a arquitetura de *hardware* e a segurança física tem foco nas propriedades do sistema.

A arquitetura de *hardware* e sua segurança física deve estar claramente especificadas, ser consistente e adequada aos fatores identificados na análise de riscos realizada.

Devem ser identificados aspectos como:

a) Exposição de componentes de *hardware* sem proteção, fora de painéis ou gabinetes;
b) Existência de portas e terminais sem os devidos bloqueios;
c) Arranjo do sistema quando instalado;

Deve-se descrever, aspectos relacionados ao isolamento e invólucro dos componentes, resinagem, selagem e lacres de *hardware* que além de medidas de segurança física, podem ser utilizadas como soluções de verificação de integridade em auditoria.

Identificada a boa implementação de ações, ferramentas e mecanismos para evitar que os fatores e elementos maléficos identificados na análise de riscos possam prejudicar o correto funcionamento de componentes de *software* e *hardware* do sistema.

A avaliação desse atributo é realizada pela análise documental, pelo ensaio de demonstração de conceito, combinado com uma inspeção física da unidade de *hardware*.

10.3.Interfaces de comunicação e interoperabilidade

Diz respeito as interfaces de comunicação internas do sistema que terá o *software* avaliado e as interfaces de comunicação com o mundo exterior, seja com outros sistemas ou com pessoas, e seus mecanismos de proteção física e lógica.

A documentação analisada deve permitir que todas as interfaces de comunicação sejam apresentadas, definidas e descritas de forma clara, consistente e não-ambígua.

Todos os serviços, recursos e funcionalidades acessíveis por meio de cada interface e os mecanismos de proteção física e lógica implementados em cada interface devem ser apresentados e claramente descritos. E todos os recursos que possibilitam a interoperabilidade entre o *software* avaliado e os outros que se comunicam e interagem com ele devem ser apresentados.

É avaliada a interoperabilidade com outros sistemas, sua capacidade de trabalhar em conjunto, importar e exportar dados, de funcionar em outros ambientes e a capacidade de operação em rede de maneira eficaz e eficiente deve ser considerada.

Por meio de testes avalia-se a clareza e nitidez das informações apresentadas nos mostradores e telas; se o tamanho, localização iluminação de telas e mostradores são condizentes com as condições do ambiente em que se encontra e a padronização da interface quanto a formato e localização de informações na tela, e se correspondem as descrições da documentação de comunicação.

Verificar se a arquitetura proposta não apresenta vulnerabilidades documentadas na literatura que possam ser exploradas por um atacante.

Avalia-se os canais de comunicação e a forma como a informação é transmitida, a capacidade de comunicação entre os sistemas, pontos fracos e fragilidades nesse processo que possam permitir a interceptação devem ser identificados.

A avaliação desse atributo é realizada pela análise documental, pelo ensaio de demonstração de conceito, combinado com a realização de testes.

10.4.Serviços e funcionalidades.

Esse atributo aborda o conjunto de serviços e funcionalidades oferecidos pelo *software*, tanto a um operador como a equipamento ou sistema. A avaliação desse atributo é realizada em suma pela execução dos testes funcionais, de acordo com a documentação do *software*.

Todos os serviços e funcionalidades devem estar descritos em seus manuais e catálogos, além de serem condizentes com a amostra do *software* depositada, de forma clara, consistente e não ambígua.

Avalia-se a capacidade do *software* executar as funções para as quais foi selecionado e se estas ocorrem corretamente, também possibilita identificar se existe alguma função não especificada na documentação.

Para a sua execução podem ser utilizadas informações geradas pelos testes realizados durante a verificação dos testes de integração, validação e comissionamento, de aceitação de fábrica e no local.

10.5.Usabilidade

A usabilidade é definida pelo conjunto dos aspectos que influenciam a capacidade do *software* de ser utilizado, compreendido e aprendido pelo usuário, sob condições específicas.

Todos os manuais e guias do usuário devem ser avaliados quanto a clareza e concisão, e devem ser escritos e apresentados de forma clara, consistente e não-ambígua, o mesmo deve ocorrer para as apresentações das interfaces, mostradores, telas e comandos do sistema.

A avaliação deve caracterizar a:

a)A possibilidade do usuário entender o *software* quanto ao seu uso; a existência de modos de auto demonstração, a facilidade de acessar os recursos durante a execução; a clareza e solidez de manuais e guias, com demonstração de como utilizar o equipamento e sanar eventuais dúvidas e dificuldades de uso; a diagramação, apresentação e organização da documentação sobre a sua utilização do software;

b)A facilidade com quero usuário pode utilizar o *software*, e aprender suas aplicações; devido a padronização das ações, interfaces e menus e a implementação de ações que facilitem ao usuário localizar informações no manual, e a possibilidade do usuário fazer mau uso do *software*;

c)O esforço necessário para o usuário operar e manter o controle da operação do sistema, acessar menus e executar funções, junto da verificação da descrição dos comandos e controles, seus acessos, iluminação e sensibilidade de forma condizentes com o ambiente em que este se encontra e com a descrição das interfaces.

A avaliação desse atributo é realizada pelos testes funcionais, de preferência por membros da equipe que não realizaram outras etapas do processo de avaliação, portanto não teriam conhecimento prévio do *software*, o que impactaria em sua cognição para utilizar, compreender e aprender o *software*.

10.6.Mecanismos de autenticação de usuário.

Nesse atributo, são avaliados os métodos que possibilite ao usuário se autenticar para a utilização do *software* avaliado, o que inclui mecanismos, tecnologias utilizadas e a caracterização de assertividade do processo.

Mecanismos de autenticação do usuário (senhas, *tokens*, cartões, chaves e biometria etc.), as etapas e sequência de autenticação, e os devidos índices de assertividade utilizados devem estar claramente definidos e rigorosamente caracterizados.

Deve ser realizada a caracterização da solidez e da capacidade dos algoritmos, protocolos, ferramentas e mecanismos de autenticação resistirem a ataques.

Mecanismos de *hash* criptográfico para armazenamento de senhas devem ser caracterizados.

Os algoritmos e protocolos devem seguir as boas práticas e recomendações consolidadas nos meios técnicos e científicos, eliminando-se quaisquer falhas conceituais.

A avaliação desse atributo é realizada pela análise documental e complementada pela realização dos testes de uso, que evidenciem o correto funcionamento do sistema de autenticação e por testes de segurança, que tentem quebrar a barreira de acesso.

10.7.Controle de acesso.

Esse atributo avalia a utilização de políticas de controle de acesso utilizadas.

Deve ser realizada a caracterização da política de controle de acesso ao *software* avaliado, incluindo o modelo (discricionário, mandatório, baseado em papéis etc.), tipos de agentes e recursos utilizados, modos de acesso dos usuários e outros detalhes a respeito das regras de acesso a objetos por parte de sujeitos.

Os modelos de controle de acesso implementados devem estar claramente definidos, com a descrição dos princípios básicos de controle de acesso, tais como privilégio mínimo e separação dos direitos.

As políticas para definição de usuários, papéis e responsabilidades devem estar claramente definidas.

A avaliação deve buscar por pontos falhos que possibilitem a usuários escalar privilégios, realizar tarefas além das necessárias e autorizadas.

Além da análise documental, a avaliação desse atributo é complementada pela realização de testes de uso e de segurança.

10.8.Criptografia e módulos criptográficos.

É o atributo que avalia a utilização de criptografia e de módulos criptográficos, como elemento de um mecanismo de segurança do *software*. Deve ser realizada a caracterização do conjunto de algoritmos e protocolos criptográficos utilizados pelo *software* avaliado, incluindo a descrição dos algoritmos, tamanhos de chaves e protocolo para gerenciamento de chaves.

Os algoritmos e protocolos utilizados devem ser de conhecimento público, seguir as boas práticas e recomendações consolidadas nos meios técnicos e científicos, eliminando-se quaisquer falhas conceituais nas arquiteturas criptográficas.

A avaliação desse atributo pode ser realizada pela análise documental, combinada com a realização de testes de segurança, que testem a possibilidade de quebra do algoritmo de criptografia.

10.9.Geração de números aleatórios.

Se avalia os procedimentos implementados para gerar números aleatórios utilizados nas aplicações de segurança. A avaliação leva em conta à existência de geradores de números verdadeiramente aleatórios (TRNG) ou pseudoaleatórios (PRNG) e suas aplicações.

Deve ser realizada a caracterização do conjunto de algoritmos e protocolos utilizado pelo *software* avaliado para gerar números aleatórios, incluindo fonte de entropia e algoritmos determinísticos.

Avalia-se se tais geradores seguem as boas práticas e recomendações consolidadas nos meios técnicos e científicos. Em particular, deve-se:

a) Elaborar modelos físicos para a fonte de entropia;
b) Possuir argumentos técnicos para justificar a qualidade da aleatoriedade;

c) Estimar/quantificar a entropia produzida por unidade de tempo gerada pelas fontes de entropia;

d) Usar algoritmos padronizados e validados pela comunidade técnica e científica para geração de números aleatórios.

10.10.Disponibilidade e eficiência.

É o atributo que descreve e avalia os aspectos de disponibilidade e eficiência em função do uso normal do *software*. Difere do atributo confiança e desempenho por não tratar do desempenho perante a ocorrência de falhas.

É medida pela capacidade de atendimento ao aumento das demandas originadas pela quantidade de usuários e aplicações em funcionamento legítimos e autorizados.

Deve estar definida e apresentada, na documentação do *software*, a política de prioridades entre processos e entre usuários, para o caso de demandas concorrentes, e caracterizadas as capacidades de atendimento a essas demandas e as devidas taxas de degradação em função do aumento da demanda.

Devem ser definidas e apresentadas características do *software* que influenciam na eficiência apropriada, relativo ao tempo e à quantidade de recursos, sob condições especificadas, pelo:

a) Comportamento em relação ao tempo: quanto ao tempo de resposta, processamento e eficiência na execução de funções, se são proporcionais aos recursos do sistema e suficientes para atender as necessidades do usuário.

b) Comportamento em relação aos recursos: avalia a quantidade de recursos utilizados para atingir o nível de eficiência de uma função desejada pelo *software*.

Deve demonstrar se as taxas de degradação em função do aumento da demanda, política de prioridades entre processos e usuários, dentre outros correspondem ao estimado, e como impactam no atendimento as necessidades do usuário.

A avaliação desse atributo pode ser complementada pela avaliação documental e pela realização de testes de segurança, que proporcionem o aumento das demandas do para caracterizar seu comportamento.

10.11.Confiabilidade e desempenho.

É o atributo que descreve e avalia os aspectos de confiabilidade e desempenho do *software* avaliado em função da ocorrência de falhas, difere do atributo disponibilidade e eficiência que trata de aspectos do *software* com relação às demandas de usuários e aplicações.

Permite avaliar características e aspectos do *software* que influenciam na capacidade de manter seu nível de desempenho sob condições e períodos específicos, com taxa de falhas dentro de limites aceitáveis.

A avaliação deve caracterizar a:

a) Maturidade do *software*, pela apresentação de mecanismos e ferramentas que demonstram a capacidade de evitar erros devido a falhas no *software*, intervenção de usuários,

queda de energia e falhas na execução, e manter a integridade dos dados na ocorrência de erros, deve estabelecer a probabilidade de ocorrer erros durante a execução de funções específicas, configuração e entrada de dados;

b) Tolerância a falhas, pela apresentação de mecanismos e ferramentas que demonstram a capacidade de resistir e manter seu funcionamento dentro de um nível específico de desempenho em casos de falhas, violação de interface específica, erros de preenchimento de campos ou de configuração, e exclusão de dados existentes, devido a capacidade do *software* tratar situações anormais que possam ocorrer durante sua execução;

c) Recuperabilidade, pela apresentação de mecanismos e ferramentas que demonstram a capacidade de restabelecer seu nível de desempenho e recuperar os dados diretamente afetados na ocorrência de falha, com o tempo e esforço necessários.

A avaliação desse atributo deve ser baseada na análise da sua documentação e complementada pela realização de testes de segurança.

10.12.Registro de eventos.

É o atributo que permite avaliar o conjunto de eventos que devem ser registrados pelo *software*, para uso em uma futura e possível auditoria.

A documentação apresentada deve definir o conjunto de eventos que devem ser registrados pelo *software* avaliado para posteriores ações de auditoria, assim como, as políticas e critérios para gerenciamento de tais eventos, incluindo permissões de leitura e exclusão, assim como, as políticas e critérios para gerenciamento de tais eventos.

Além da análise documental, a avaliação desse atributo realiza testes, como descreve, para confirmar as informações.

10.13.Temporalidade.

Por esse atributo é feita a caracterização e avaliação da temporalidade que avalia os aspectos de marcação de tempo utilizados na operação do *software* avaliado.

Por meio da avaliação da documentação apresentada, deve ser possível caracterizar os aspectos de uso de relógio, marcação de tempo e horário; incluindo exatidão, atrasos e autenticação de fonte de tempo, adotados na operação do *software* avaliado, na prestação de seus diversos serviços.

A avaliação desse atributo é realizada pela análise documental, e pelo ensaio de demonstração de conceito.

10.14.Manutenibilidade.

Permite avaliar o conjunto de características e aspectos que influenciam os recursos para modificar o *software*, com objetivo de corrigi-lo ou adaptá-lo, diferente da capacidade de configurá-lo. E que podem ser utilizados para a modificação sem a correta permissão. Deve ser realizada a caracterização da:

a)Modificabilidade, capacidade do *software* de permitir que uma modificação autorizada seja implementada, incluindo modificações no código, projeto e documentação. Todos os

recursos para implementar modificações específicas devem ser claramente especificados, incluindo funções, ferramentas de apoio, documentação específica, manuais e guias;

b)Analisabilidade, caracterizada pela capacidade do *software* de permitir o diagnóstico de deficiências ou causas de falha, bem como de identificar partes a serem modificadas. Todos os recursos utilizados para diagnosticar deficiências, causas de falhas, ou para identificação de partes a serem modificadas, devem ser claramente especificados;

c)Testabilidade, caracterizada pela capacidade do *software* de permitir, quando modificado, ser testado. Todos os recursos utilizados para facilitar e colaborar com a realização de análises e testes do *software* devem ser claramente especificados, incluindo ferramenta de apoio, documentação específica, manuais e guias;

d)Adaptabilidade, caracterizada pela capacidade do *software* de ser adaptado para diferentes ambientes, sem necessidade de aplicação de outras ações ou meios além daqueles fornecidos para essa finalidade pelo próprio software. Inclui a possibilidade de ajuste da capacidade interna. Todos os recursos utilizados para demonstrá-la, sem aplicar outros meios ou ações para atingir o propósito, incluindo documentação específica, manuais e guias devem ser claramente especificados.

10.15.Segregação de redes.

É o atributo que caracteriza como o *software* opera ao ser separação de qualquer tipo de redes de dados. De modo que as funções do *software* não sejam prejudicadas por falhas no processo de comunicação, funções e/ou interfaces de outro sistema.

Avalia se o *software* recebe, faz uso, depende de dados oriundos de outros dispositivos ligados à rede, se está disponível para enviar ou receber resposta ou mensagem de outro sistema ou *software*.

Deve ser demonstrado o isolamento da comunicação por uma separação física do sistema. A restrição deve ser por meio de desconexão física do cabo, ou por meio de chave de bloqueio que abre fisicamente o circuito de transmissão de dados.

Se em algum momento houver necessidade de ligação a uma rede de dados, deve ser caracterizado e demonstrado quais os mecanismos que foram idealizados e implementados para impedir o mau uso dela. E se as funções de segurança são ponto a ponto e utilizam um meio dedicado. Deve buscar por conectividade sem fio, que não deve ser implementada.

A avaliação desse atributo é realizada pela análise documental, pelo ensaio de demonstração de conceito, combinado com inspeção física da unidade de *hardware*.

10.16.Simplicidade

É o atributo que avalia se o *software* é o mais simples possível, e se realiza apenas as funções necessárias.

Projetos complexos devem ser evitados, caso sejam necessárias funções adicionais de segurança, mesmo que aumentem a confiabilidade, devem dar prioridade a execução fora do sistema.

A complexidade adicional do *software* associada ao desempenho de funções não diretamente relacionadas à sua função e ao recebimento de informações de apoio a essas funções não deve aumentar significativamente a probabilidade de erros de especificação de *software* ou codificação.

10.17.Redundância

Esse atributo tem como objetivo verificar a redundância implementada no *software*, para evitar a vulnerabilidade, em que, a falha de um componente pode ocasionar perda simultânea de múltiplas funções.

Todos os dados, funções e componentes redundantes devem ser apresentados e caracterizados de forma clara, consistente e não ambígua. Os tipos de redundância e sua rigidez na segurança devem ser caracterizados.

Formas, periodicidade e local de armazenamento de *backup*, devem ser apresentados e serem condizentes com a aplicação do software.

É avaliado se as partes duplicadas se mantêm equivalentes aos originais e se na ocorrência de fato maléfico não serão afetadas de forma simultânea.

A redundância não deve afetar profundamente a simplicidade do sistema.

11. **RELATÓRIO**

Todas as informações levantadas, os aspectos identificados e os resultados dos testes realizados devem ser apresentados no relatório da avaliação para demonstrar o atendimento aos requisitos das fases de verificação, e demonstrar a conformidade dos atributos validados, o modelo do relatório consta no anexo C.

O relatório começa a tomar sua forma durante a fase de planejamento, onde são verificadas as aplicações do sistema onde o *software* avaliado está contido, e são selecionados os atributos a serem avaliados, o relatório é dividido nas seções:

a) Identificação;
b) Objetivo da avaliação;
c) Responsabilidades;
d) Identificação de risco;
e) Verificação;
f) Validação;
g) Conclusão.

Deve conter a descrição da verificação das fases do ciclo de vida do *software*; a validação dos atributos presentes; as ameaças a que o *software* está exposto e as respectivas ferramentas e mecanismo que o instrumento e seu software possuem para protegê-lo, e as consequências e resultados dessa interação.

Todos as incoerências, divergências, e demais problemas detectados devem ser apresentados, de forma que evidencie os desvios e falhas no *software*.

O relatório final pode apresentar a necessidade de intervenções no software, que levarão a nova avaliação, com objetivo de verificar se esta foi sanada, não havendo mais deficiências, o processo avaliativo é encerrado e o certificado é emitido.

ANEXO A

Modelo de Plano de Avaliação

1. Identificação

1.1.Identificação do requerente

Com o nome da organização solicitante da avaliação, seu endereço, nome dos profissionais envolvidos na avaliação.

1.2.Identificação do público-alvo do sistema avaliado

Quem irá utilizar o sistema cujo *software* está sendo avaliado, sejam pessoas organizações e/ou outro sistemas.

1.3.Identificação do *software* avaliado

Qual o nome do sistema, do *software* e sua versão.

1.4.Tipo de *software*

	Software novo
	Software acessível existente
	Software proprietário existente
	Software configurável

1.5.Identificação do avaliador

Nome da organização avaliadora:

Endereço:

Local onde a avaliação ocorreu:

Identificação das equipes de avaliação:

Nome	Função	Formação técnica
	(avaliador líder, avaliador membro, avaliador do uso)	

2. Objetivos

Este capítulo deve fornecer uma declaração clara, sobre os objetivos da avaliação e do sistema avaliado. Bem como a aplicação pretendida para o software e quais as funções que deve desempenhar.

2.1.Objetivos da avaliação;
2.2.Objetivos do *software*;
2.3.Funções do *software*.

3. Itens recebidos

3.1.Documentos recebidos

Os documentos recebidos devem ser identificados e catalogados de forma simples, utilizando o quadro abaixo.

Item	Referência	Título	Língua	Autor	Ano de produção
1					
2					

3.2.Unidades físicas recebidas

As unidades físicas recebidas devem ser identificadas utilizando uma etiqueta fixada ao item. E catalogadas de forma simples, utilizando o quadro abaixo.

Item	Número de referência/série ou *part number*	Nome	Cor	Tipo
1				(CPU, painel, monitor, teclado, transdutor, interface sensível ao toque etc.)
2				

3.3.Unidades lógica recebidas

As unidades lógicas recebidas devem ser catalogadas utilizando o quadro abaixo. Mesmo que estejam associadas a uma mídia ou *hardware* dedicado.

Item	Nome	Mídia ou hardware integrado	Tipo
1		(CD, DVD, SD, pen drive) ou (unidade integrada, central, painel)	(software, firmware, app, SO)
2			

4. Definição de responsabilidades

Define todas as responsabilidades previstas e associadas com a implementação do Plano. Isto inclui toda a coleta de dados, tarefas de análise, a implementação de outros requisitos de apoio, relatos, acompanhamento e requisitos similares.

4.1.Requerente
4.2.Avaliador

5. Cronogramas

Este capítulo deve conter um cronograma para o acompanhamento das atividades do processo de avaliação, discutidas no processo de identificação do *software* avaliado. Incluindo a realização dos testes, as pausas no processo de desenvolvimento para a verificação, a previsão das entregas e as reuniões periódicas.

Deve fornecer um claro plano de metas com marcos e produtos estabelecidos para entrega. O quadro abaixo fornece um exemplo de cronograma.

Evento	Título	Data	Responsável	Local

6. Medições

Define as várias análises planejadas, tanto as realizadas no software quanto as planejadas para o sistema, estabelece em que fase do desenvolvimento estas medições serão executadas, com que frequência serão repetidas, quais técnicas ou ferramentas usadas para ajudar a captura e análise dos dados, e que ações estão previstas caso haja divergência dos objetivos estabelecidos, que podem ser em produtos intermediários ou final. Bem como ser executadas em várias fases do ciclo de vida do projeto.

6.1.Fases de verificação

Este tópico visa identificar quais as fases do processo de verificação devem ser realizadas, dependendo do tipo de *software* e do estágio de desenvolvimento em que este se encontra. Assinaladas as selecionadas.

Compreende	Fase de verificação
	Especificação dos requisitos do sistema
	Especificação do sistema
	Especificação do projeto do *software*
	Codificação do software
	Integração do sistema
	Testes do sistema integrado
	Testes de validação e comissionamento
	Desempenho do *software*
	Teste de aceitação de fábrica
	Teste de aceitação local
	Entrega do sistema
	Operação, manutenção e modificação

6.2.Atributos aplicáveis na validação

Este tópico visa identificar quais os atributos que devem ser avaliados. Por meio de evidências que as características que apoiam os objetivos prescritos, são identificadas, para a execução do processo de validação do *software*. Assinalados os identificados.

compreender	Atributo a ser validado
	Ambiente operacional e cenário de aplicação
	Arquitetura de *hardware* e segurança física
	Simplicidade

	Interface de comunicação e interoperabilidade
	Serviços e funcionalidades
	Usabilidade
	Mecanismos de autenticação do usuário
	Controle de acesso
	Criptografia e módulos criptográficos
	Geração de números aleatórios
	Disponibilidade e eficiência
	Registro de eventos
	Temporalidade
	Confiança e desempenho
	Manutenibilidade
	Segregação de redes
	Redundância

7. Uso e análise de dados

Define como os dados serão analisados e, caso existam, quais métodos serão empregados e quais técnicas de apresentação serão usadas. Faz referências a responsabilidades e ferramentas de apoio.

8. Outros requisitos

Este capítulo pode ser usado para incluir requisitos não considerados previamente. Fornece uma descrição das técnicas e métodos usados. Convém que esta seção, ou o material referido, seja clara e completa, de tal forma que possa ser facilmente compreendida e utilizada pelos interessados.

8.1.Ferramentas de apoio
8.2.Guias e normas relevantes

ANEXO B

Análise de risco

Guia para confecção do Modelo de Ameaças

Uma das ferramentas utilizadas para a análise de riscos de *softwares* é a modelagem de ameaças, que consiste é um artefato composto pela visão arquitetural de alto nível associada a lista de ameaças organizadas pela gravidade dos seus riscos.

O que possibilita a preparação para eventuais exposições, ajuda a identificar falhas, vulnerabilidades e ausências na proteção e controle da segurança, e observa pontos cegos do sistema, para que ações mitigadoras possam ser orquestradas de acordo com as prioridades.

A confecção desse modelo integrante do ProAS-NN utiliza o processo para modelagem de ameaças por meio dos 6 passos ilustrados na Figura 21.

Figura 21 – Método para criação do Modelo de Ameaças

Fonte: o autor.

Iniciado pela identificação dos ativos que se quer proteger e a criação da arquitetura geral do sistema, com objetivo de identificar o que o sistema se propõe a realizar e como ele usa e acessa os ativos que o compõe, o que resulta no diagrama da composição e estrutura do sistema e seus subsistemas, juntamente com as principais tecnologias utilizadas.

É feita a decomposição do sistema, em busca de uma visão mais profunda, em que é descrito o fluxo dos dados, identifica pontos de entrada, fronteiras de confiança, códigos, entradas do usuário, mecanismos de autenticação e autorização, gerenciamento de configuração, mecanismos de criptografia, manipulação de parâmetros, gerenciamento de exceções e mecanismos de auditoria e *logging*.

A identificação de ameaças é realizada pela técnica STRIDE, que utiliza a documentação do *software*, descreve a ameaça, seu alvo, o risco associado e o ataque utilizado para gerar o cenário de ameaça, que é classificada quanto a criticidade pelo método DREAD.

Como produto, surgi o modelo de ameaça composto pela visão arquitetural do sistema e pela lista de ameaças associadas, de forma categorizada e classificada de acordo com a severidade, que permite compreender os riscos, estabelecer prioridades e planejar maneiras de mitigá-las.

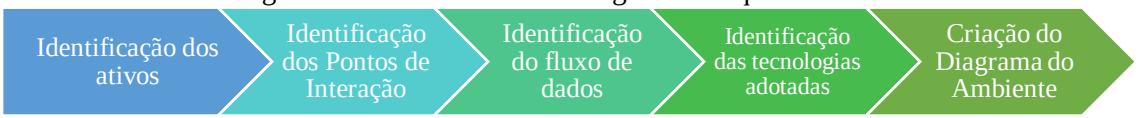
O modelo de ameaças é dividido em três partes principais, a primeira é a modelagem da arquitetura do ambiente, que possibilita conhecer o sistema para a execução da segunda parte, que identifica possíveis falhas existentes e vulnerabilidades associadas, e a terceira parte é a classificação da ameaça, de acordo com a severidade. Em complemento há a documentação do trabalho realizado, sob a forma de relatório.

1. Modelagem da arquitetura do ambiente

Tem como objetivo compreender o *software* que está sendo avaliado, para possibilitar a efetiva identificação de ameaças, para tal, é necessário entender quais são os componentes do sistema, como eles interagem, qual o fluxo de dados entre as principais entidades e quais os ativos que se deseja proteger, o que permite representar graficamente o sistema, pela visão macro e de alto nível.

Os documentos fornecidos permitem descrever tecnicamente o ambiente, como: documentações de arquitetura do sistema; diagramas UML; diagramas de caso de uso e de testes; manuais de instalação, manutenção e operação; dentre outros. A Figura 22 representa os passos deste processo.

Figura 22 - Processo de Modelagem da Arquitetura do Sistema



Fonte: o autor.

1.1.Identificação dos ativos do sistema

Os ativos são vistos como recursos de valor pelo seu detentor e por isso devem ser protegidos. Os ativos que formam o sistema, como sensores, atuadores, servidores, *software*, entidades na nuvem, *gateways*, banco de dados etc., devem ser identificados sob a forma de uma lista, que mais adiante será utilizada para mapear pontos de interação e fluxo de dados no sistema, e compor o seu diagrama arquitetural.

Por exemplo, o *software* que comanda e controla o sistema de climatização de um *Shopping Center*, possui sensores que identificam os valores de temperatura e umidade nos diversos ambientes, existem controladores das máquinas do sistema e há uma unidade central de gerenciamento que possui uma interface de comunicação com o usuário, de maneira geral esses são os ativos do sistema.

1.2.Identificação dos pontos de interação

Consiste na identificação da interação entre os ativos já identificados do sistema, entre si, com usuários, dispositivos e outros sistemas, as interfaces que permitem essas interações e sua comunicação.

É possível identificar tanto o fluxo de dados normal no ambiente quanto possíveis interfaces pelas quais um potencial atacante pode interagir com o sistema avaliado.

Utilizando o exemplo do sistema de climatização de um *Shopping Center*, e os ativos já levantados, identifica-se que os sensores, a interface e os controladores interagem diretamente com o *software*, mas não entre si.

1.3.Identificação do fluxo de dados

É o mapeamento das comunicações, com o objetivo de identificar o caminho das informações. Por meio do Diagrama de Fluxo de Dados (DFD) e pela análise dos pontos de

interação dos ativos identificados do sistema, observando por quais componentes os dados trafegam.

Voltando ao exemplo do sistema de climatização do *Shopping Center*, o *software* que gerencia o sistema, se comunica diretamente com os sensores diversos, interface e com os diversos controladores, como mostra o Quadro 13, há fluxo de dados unidirecional dos sensores para ele, e dele para os controladores, entre a unidade de *hardware* que contém o *software* e a interface é bidirecional.

Quadro 13 - Exemplo de DFD

Ativo	ativo com que se comunica
Sensor de temperatura do ar	*Software* de gerenciamento.
Sensor de umidade do ar	*Software* de gerenciamento
Sensor de temperatura da água	*Software* de gerenciamento
Software de gerenciamento	Interface, Controlador do ventilador, Controlador das bombas, Controlador do compressor
Interface	*Software* de gerenciamento

Fonte: o autor.

1.4.Identificação das tecnologias adotadas

Tem o propósito de identificar as diversas tecnologias que são utilizadas pelo *software* avaliado, em cada um dos seus componentes, identificando, por exemplo, fabricantes, sistemas operacionais, linguagens de desenvolvimento utilizadas etc., o que possibilita identificar ameaças relacionadas a estas tecnologias, inclusive em referências na literatura e listas especializadas.

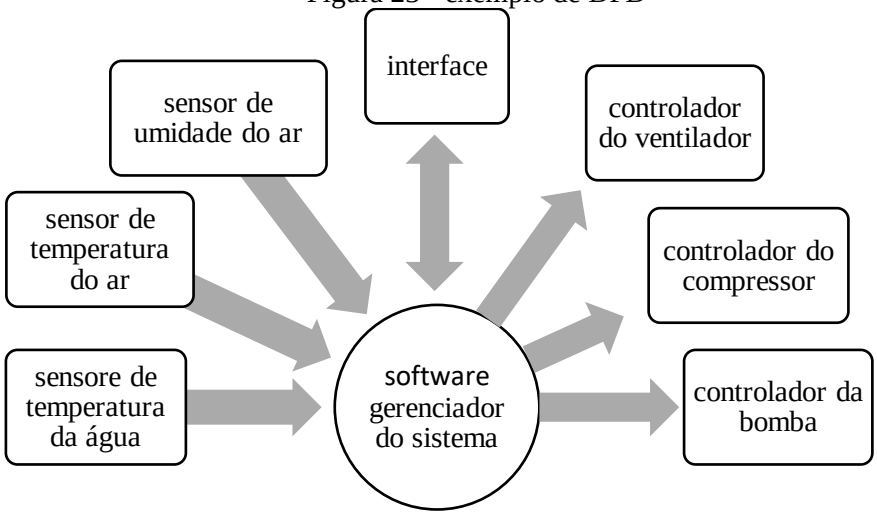
Usando o exemplo do texto, se identifica qual a tecnologia utilizada para o banco de dados, a comunicação dos dados, o sistema operacional do sistema e a interface com o usuário.

1.5.Criação do diagrama do ambiente

De posse das informações já levantadas, é possível criar o diagrama de representação da arquitetura do sistema, utilizando uma notação formal e de fácil entendimento, que permitirá a compreensão pelos envolvidos no processo de avaliação na busca de possíveis ameaças ao sistema.

Utilizando o exemplo já adota nesse texto, tem-se que o gerenciador do sistema recebe os dados dos diversos sensores, trata, analisa e toma decisões, encaminhando comandos para os controladores que permitem o funcionamento dos motores das máquinas, e a interface que troca dados com o gerenciador do sistema em ambos os sentidos, como ilustra a Figura 23.

Figura 23 - exemplo de DFD



Fonte: o autor.

2. Identificação de ameaças e vulnerabilidades

Ciente dos detalhes e características do sistema é possível realizar a identificação dos riscos sob a forma de ameaças e vulnerabilidades a que ele está susceptível.

2.1. Identificação de ameaça

É nessa etapa que se analisa o sistema em busca de possíveis riscos, pela identificação dos ativos e suas tecnologias, e a análise do diagrama de fluxo de dados e do ambiente, para elaborar e entregar uma lista de riscos associados aos ativos do sistema.

A técnica escolhida para ser utilizada no ProAS-NN é o STRIDE, em que se busca identificar a ameaça pelo dano que ela pode causar, como descrito pelo Quadro 14.

Quadro 14 - STRIDE

Ameaça	Prioridade	Definição
Spoofing	Autenticação	Personifica algo ou outra pessoa
Tampering	Integridade	Modifica dados ou códigos
Repudiation	Repúdio	Alega não ter realizado uma ação
Information disclosure	Confidencialidade	Expor informações a alguém não autorizado
Denial of servise	Disponibilidade	Negar ou degradar o serviço ao usuário
Elevation of Privilege	Autorização	Obter recursos sem a autorização adequada

Fonte: o autor.

a) **Autenticação**. Trata do acesso ilegal a ativos usando informações de autenticação, burlando a segurança do sistema, que depende da confiança na identidade, quando alguém ou um sistema afirma ser o que não é. Apenas usuários autorizados devem ser capazes de acessar um sistema ou seus dados preocupantes, já que muitos dispositivos no sistema estão conectados e confiam na identidade de outros.

b) **Integridade.** Envolve a modificação acidental ou mal-intencionada de ativos, com ou sem autenticação, deve se estender a todos os itens dos sistemas, sejam lógicos ou físicos. Leva em conta a codificação adequada das comunicações de dados, com a integração de ferramentas de análise de código estático de segurança para identificar *bugs* de segurança, uso de *firewalls*, armazenamento particionado e arquivos de *log* e notificações, métodos comuns para detectar

dados adulterados, armazenagem e localização em local seguro e abrigado e proteção de componentes.

c) **Repúdio.** Diz respeito aos usuários que negam a execução de uma ação sem que haja maneiras de provar o contrário, sua verificação visa a possibilidade de execução dessas auditorias e rastreamento, garante que o mau comportamento ou atividade não autorizada não possa ser escondido. Sistemas seguros devem incorporar mecanismos de não repúdio adequado, faz com que os dados e sua fonte possam ser confiáveis.

d) **Divulgação de Informação.** Envolve a exposição de informações a quem não necessitam ter acesso, dados privados e sigilosos podem ser expostos inadvertidamente devido a códigos com erros, ataques intencionais ou pelo armazenamento e acesso a dados e informações de sistemas, *backups* e arquivos em locais acessíveis, que podem incluir servidores, *laptops* ou unidades externas.

e) **Negação de Serviço.** É uma ação que torna um sistema inacessível, pode ocorrer pela falta de alimentação do *software* (eletricidade e dados), exploração exagerada e não autorizada dos recursos, de forma que não possam ser usados por usuários autorizados, sejam pessoas ou outros sistemas.

f) **Elevação de Privilégio**. Conhecido também por escalada de privilégio, ocorre quando um usuário sem privilégios obtém acesso privilegiado e altera o sistema, a falsificação se concentra na autenticação com privilégios sem autorização formal, um ataque deste tipo pode usar todas as outras áreas do STRIDE.

As ameaças podem ser físicas como a extração ou adulteração intencional ou degradação pela ação do tempo de um dispositivo do sistema, e a injeção ou a substituição de dispositivo legítimo por malicioso. E lógicas, que visam explorar aspectos peculiares da rede utilizada pelo sistema, análise de tráfego em que um ataque pode interceptar a comunicação da rede e inferi nos padrões de comunicação, podendo extrair informações sensíveis.

Há ainda ameaças que originam a negação de serviço por ataques com alto tráfego de rede, deixando o sistema indisponível a usuários legítimos, e ataques contra mecanismos de criptografia utilizados na comunicação.

E ameaças que utilizam *softwares* com capacidade de comprometer o sistema, os *malwares*, que podem ser vírus, *worms*, *spywares*, cavalo de Tróia, *ransomwares*, dentre outros, que podem ser utilizados para derrubar sistemas, roubar informações sensíveis, prover *backdoor*, apagar registros de *logs*, esgotar recursos de rede e processamento, sequestro do sistema etc.

O Quadro 15 contém exemplos de ameaças comuns, e pode ser usada durante o processo de identificação. O Quadro 16 apresenta mais ameaças possíveis cuja fonte é o ser humano.

Quadro 15 - Identificação de Ameaças

Tipo	Ameaças
Dano físico	Fogo
	Água/gelo

	Poluição
	Acidente grave
	Destruição de equipamento ou *mídia*
	Poeira, corrosão, congelamento
Eventos naturais	Fenômeno climático
	Fenômeno sísmico
	Fenômeno vulcânico
	Fenômeno meteorológico
	Inundação
Paralisação de serviços essenciais	Interrupção do suprimento de energia
	Falha do equipamento de telecomunicação
Distúrbio causado por radiação	Radiação eletromagnética
	Radiação térmica
	Pulsos eletromagnéticos
	Radiações ionizantes
Comprometimento da informação	Interceptação de sinais de interferência comprometedores
	Espionagem à distância
	Escuta não autorizada
	Furto de *mídia* ou documentos
	Furto de equipamentos
	Recuperação de mídia reciclada ou descartada
	Divulgação indevida
	Dados de fontes não confiáveis
	Alteração do *hardware*
	Alteração do *software*
	Determinação da localização
Ações não autorizadas	Uso não autorizado de equipamento
	Comprometimento dos dados
	Processamento ilegal de dados
	Abuso de direitos
	Forjamento de direitos
	Repúdio de ações

Quadro 16 – ameaças originadas por seres humanos

Origem das Ameaças	Motivação	Possíveis Consequências
Hacker, cracker	- Desafio; - Ego; - Rebeldia; - Status; - Dinheiro.	• Hacking • Engenharia social • Invasão de sistemas, infiltrações e entradas não autorizadas • Acesso não autorizado ao sistema
Criminoso digital	- Destruição de informações; - Divulgação ilegal de informações; - Ganho monetário Alteração de dados não autorizada	• Crime digital • Ato fraudulento por uma outra pessoa • Suborno por informação • *Spoofing* • Invasão de sistemas

Terrorista	- Chantagem - Destruição - Exploração - Vingança - Ganho político - Cobertura da mídia	• terrorismo • Guerra de informação • Ataque a sistemas • Invasão de sistema • Alteração do sistema
Espionagem (empresas, serviços de inteligência de governos estrangeiros, outros grupos de interesse)	- Vantagem competitiva - Espionagem	• Garantir a vantagem de umposicionamento defensivo • Garantir uma vantagem política • Exploração econômica • Furto de informação • Engenharia social • Invasão de sistema • Acesso não autorizado ao sistema
Pessoal interno (mal treinados, insatisfeitos, mal intencionados, negligentes, desonestos)	- Curiosidade - Ego - Obtenção de informações úteispara serviços de inteligência - Ganho monetário; - Vingança; - Erros e omissões não intencionais	• Chantagem • Vasculhar informação de propriedade exclusiva • Uso impróprio de recursocomputacional • Fraude e furto • Suborno por informação • Entrada de dados falsificados ou corrompidos • Interceptação • Código malicioso (vírus, *worm, trojan*) • Defeitos (“*bugs*”) no sistema • Invasão de sistemas • Sabotagem de sistemas • Acesso não autorizado ao sistema

Fonte: o autor.

2.2.Identificação de vulnerabilidades

A presença de vulnerabilidades por si só não causa danos, pois precisam de ameaças associadas para poderem ser exploradas, e geralmente estão ligadas a propriedades do ativo, mesmo assim, perante a presença de vulnerabilidade deve-se envidar esforços para combatê-la, mitigá-la e eliminá-la.

Em complemento a identificação dos riscos é realizada a identificação das vulnerabilidades, que são falhas que podem comprometer o *software* avaliado, ao serem exploradas.

Por meio da geração de árvores de falhas, que deve ocorrer para cada ameaça identificada na fase anterior, sendo possível realizar a análise passo a passo, desde a fonte até o resultado final, indicado pelo STRIDE, com a identificação das vulnerabilidades proeminentes de uma ameaça, como demonstra a Figura 24.

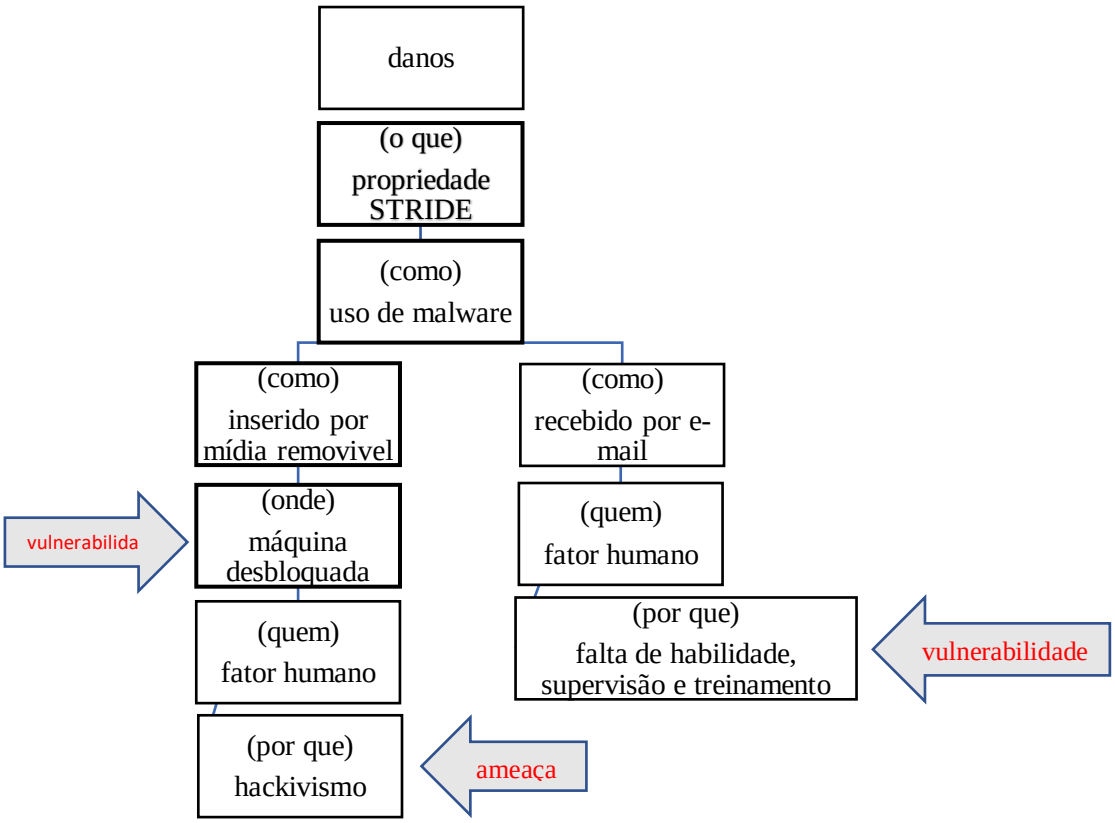
Figura 24 - Identificação de vulnerabilidades

Fonte: o autor.

A identificação de vulnerabilidades é realizada a partir das árvores de falhas, pode-se identificar vulnerabilidades que viabilizam o ataque, possibilitando a adoção de contramedidas de segurança para diminuir a probabilidade de exploração do sistema por um vetor de ataque.

A Figura 25 demonstra um modelo de montagem de uma árvore de análise de ameaças, que exemplifica o dano causado por malwares, em que se identificam duas vulnerabilidades.

Figura 25 - modelo de árvore de falha



Fonte: o autor.

O Quadro 17 traz diversos exemplos de vulnerabilidades.

Quadro 17 – exemplos de vulnerabilidades relacionadas a ameaças

Ativo	Exemplos de vulnerabilidades	Exemplos de ameaças
Hardware	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento
	Sensibilidade à radiação eletromagnética	Radiação eletromagnética
	Sensibilidade a variações de voltagem	Interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenômeno meteorológico
	Armazenamento não protegido	Furto de *mídia* e dados, acesso não autorizado
Software	Falhas conhecidas no *software*	Abuso de direitos
	Inexistência de uma trilha de auditoria	Abuso de direitos
	Atribuição errônea de direitos de acesso	Abuso de direitos
	Utilizar programas aplicativos com um conjunto errado de dados (referentes a um outro período)	Comprometimento dos dados

	Interface de usuário complicada	Erro durante o uso
	Documentação inexistente	Erro durante o uso
	Datas incorretas	Erro durante o uso
	Inexistência de mecanismos de autenticaçãoe identificação como, por exemplo, para a autenticação de usuários	Forjamento de direitos
	Tabelas de senhas desprotegidas	Forjamento de direitos
	Gerenciamento de senhas mal feito	Forjamento de direitos
	Serviços desnecessários permanecem habilitados	Processamento ilegal de dados
	Software novo ou imaturo	Defeito de *software*
	Inexistência de um controle eficaz de mudança	Defeito de *software*
	Inexistência de mecanismos de proteção física noprédio, portas e janelas	Furto de *mídia* ou documentos
	Inexistência de relatórios de gerenciamento	Uso não autorizado de equipamento
Rede	Inexistência de evidências que comprovem o envioou o recebimento de mensagens	Repúdio de ações
	Linhas de comunicação desprotegidas	Escuta não autorizada
	Tráfego sensível desprotegido	Escuta não autorizada
	Junções de cabeamento mal feitas	Falha do equipamento de telecomunicação
	Não identificação e não autenticação do emissor e do receptor	Forjamento de direitos
	Arquitetura insegura da rede	Espionagem à distância
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Local ou instalações	Localização em área suscetível a umidade, calor, poeira, radiação	Danos ao *hardware*
	Fornecimento de energia instável	Interrupção do suprimento de energia
	Inexistência de mecanismos de proteção física noprédio, portas e janelas	Furto de equipamentos
Organização	Inexistência de um mecanismo para registro e remoção de usuários	Abuso de direitos
	Inexistência de análise críticados direitos de acesso	Abuso de direitos
	Inexistência de mecanismos para realização de auditorias	Abuso de direitos
	Inexistência de mecanismos de registros de falha nos arquivos (*logs*)	Abuso de direitos
	Inexistência de procedimentos para a instalação de *software* nos instrumentos	Erro durante o uso
	Inexistência de procedimentos para a uso de *software* nos instrumentos	Erro durante o uso
	Inexistência de procedimentos para a operação de *software* nos instrumentos	Erro durante o uso
	Ausência de procedimento para atribuição das responsabilidades de	Erro durante o uso

	acesso de acordo com os cargos e funções	
	Inexistência de mecanismos para o monitoramento de violações da segurança	Furto de *mídia* ou documentos

As perguntas listadas abaixo auxiliam no levantamento dos riscos e na montagem de uma árvore de ameaças.

1)Como o sistema poderia funcionar mal de forma a criar um passivo econômico significativo?
2)Como o sistema poderia funcionar mal de uma forma que anularia a função de segurança?
3)A forma como o usuário irá interagir com o sistema difere significativa ou sutilmente da forma como o usuário interage com outro sistema existente?
4)O que aconteceria se o operador seguisse os procedimentos errados ao usar o sistema?
5)O que aconteceria se um técnico de manutenção seguisse os procedimentos errado no novo sistema?
6)O que aconteceria se um técnico de manutenção fizesse alterações online no sistema?
7)As entradas e saídas do sistema são incompatíveis (elétrica e mecanicamente) com as interfaces de planta correspondentes (ou seja, há um problema de interface)?
8)Existe alguma falha potencial do sistema (especialmente uma falha que cause um travamento do sistema) que não seja obviamente indicada ao operador?
9)Contenções de barramento e problemas de temporização são possíveis sob quaisquer condições de operação (dentro do ambiente de operação especificado na especificação de requisitos)?
10)Existe a possibilidade dos procedimentos de teste de sistema introduzirem perigos?
11)O autodiagnóstico do sistema é ativo? Como o autodiagnóstico afeta o sistema?
12)O sistema possui interrupções de *hardware* ou *software*? Se isso acontecer, como eles afetam o sistema? As interrupções de *hardware* não utilizadas estão vinculadas a um potencial de referência, como terra, ou são deixadas flutuando, o que pode resultar em uma falha do sistema?

3. Classificação dos riscos

Destina-se a classificar os riscos associados a cada ameaça identificada e a organização a partir de seu atributo de risco, o ProAS-NN utiliza o método de classificação DREAD. Em que as ameaças são ranqueadas de acordo com a pontuação obtida pela análise de suas características, o objetivo é fornecer uma ordem de gradação que possa estabelecer prioridades para as ações de tratamento das causas de tais ameaças.

O Quadro 18 apresenta os parâmetros que devem ser levados em consideração na análise das ameaças para se atribuir a devida pontuação, para classificá-las.

Quadro 18 – Parâmetros de classificação da ameaça (DREAD)

Classe / Valor atribuído	Muito baixo (0)	Baixo (1)	Médio (2)	Alto (3)
Damage (Danos)	Atividade sem danos	Vazamento trivial de informações acerca dos	Vazamento de informação sensível acerca dos ativos e/ou usuários, ou	Permite que o atacante controle um ativo ou obtenha autorização para

		ativos e/ou usuários	perda de qualquer tipo de informação	atuar como administrador do sistema
Reproducibility (Reprodução)	Para o componente afetado, existe mecanismos de proteção disponíveis contra-ataques	O ataque é difícil ou impossível de reproduzir	O ataque apenas pode ser reproduzido dentro de uma janela de tempo específica e em uma condição de particular	O ataque pode ser reproduzido a qualquer momento
Exploitability (Exploração)	Mesmo que haja probabilidades de exploração, o ataque requer diversos recursos que são provavelmente menos disponíveis	O ataque requer uma pessoa com profundo conhecimento técnico ou com conhecimento interno do sistema todas as vezes para realizar a exploração	Uma pessoa tecnicamente hábil, como um programador, pode realizar o ataque e, posteriormente, repetir os passos de exploração	Um programador iniciante ou pessoas sem conhecimento técnico pode realizar o ataque em tempo hábil seguindo um guia
Affected Things (Coisas afetadas)	O ataque não afeta coisa alguma	Um pequeno número coisas são afetadas	Um grupo de coisas são afetadas	Todos as coisas são afetadas
Affected Users (Usuários afetados)	A ameaça não põe vidas em risco ou danos diretos aos usuários do sistema	A ameaça fornece baixo risco a vida e/ou danos diretos aos usuários do sistema	A ameaça oferece risco consideráveis a vida e/ou danos diretos aos usuários do sistema	Alto risco de vida e/ou danos diretos aos usuários do sistema
Discoverability (Acobertamento)	Uma solução Alternativa é aplicada que corrige a vulnerabilidade	A vulnerabilidade tem comportamento difícil de ser entendido. É muito difícil compreender os possíveis danos potenciais de sua exploração	A vulnerabilidade pode ser acessada por apenas alguns usuários e seria necessário esforço para enxergar o uso malicioso	Guias publicados são disponíveis para ataque ou a vulnerabilidade é visível ou facilmente perceptível pela interface do usuário

Fonte: o autor

Após atribuir a pontuação de cada risco, é possível organizá-los de acordo com a gravidade, como mostra o Quadro 19, o que auxilia a organizar as formas de tratamento de acordo com prioridades.

Quadro 19 - Exemplo de soma dos pontos do DREAD

Ameaça	D	R	E	A	D	Total
(A)	X	Y	Z	A	B	SOMA
(B)	X’	Y’	Z’	A’	B’	SOMA’

ANEXO C

Modelo de Relatório de Avaliação

1. Identificação

Deve conter o capítulo 1 do plano de avaliação (anexo A). Acrescido de:

1.1. Identificação única do relatório;

1.2. Número de páginas do relatório;

1.3. Data de emissão do relatório;

1.4. Período de realização da avaliação.

Todas as páginas do relatório devem ser numeradas.

2. Objetivos da avaliação

Deve conter o capítulo 2 e 3 do plano de avaliação (anexo A).

3. Definição de responsabilidades

Deve conter o capítulo 4 do plano de avaliação (anexo A).

4. Riscos identificados

4.1. Identificação das ameaças

Deve conter o resultado do subitem 2.1 da modelagem dos riscos (anexo B).

4.2. Identificação das vulnerabilidades

Deve conter o resultado do subitem 2.2 da modelagem dos riscos (anexo B).

4.3. Classificação dos riscos

Deve conter o resultado do item 3 da modelagem dos riscos (anexo B).

5. Verificação

Devem ser descritos os fatos observados em cada fase da verificação, quais os documentos que comprovam o atendimento aos requisitos e de que forma.

De acordo com o tipo de software, a verificação envolverá as fases.

a) Verificação da especificação dos requisitos do sistema;
b) Verificação da especificação do sistema;
c) Verificação da especificação do projeto de *software*;
d) Verificação da codificação do *software*;
e) Verificação de integração do sistema;
f) Verificação de desempenho do software;
g) Verificação dos testes do sistema;
h) Verificação dos testes de validação e comissionamento;
i) Verificação de testes de aceitação de fábrica;
j) Verificação de testes de aceitação no local;
k) Verificação de ensaios do sistema;
l) Verificação da entrega do sistema;
m) Verificação de operação, manutenção e modificação.

6. Validação

6.1.Nível Conceitual

Elaborada de acordo com a análise heurística dos atributos identificados, devendo ser abordados apenas aqueles previstos no planejamento da avaliação. Todas os fatos positivos e negativos observados dos atributos devem ser registrados, principalmente os que forem afetos as falhas e vulnerabilidades apontadas na análise de riscos.

a) Ambiente operacional e cenário de aplicação;
b) Arquitetura de *hardware* e segurança física;
c) Interface de comunicação e interoperabilidade;
d) Serviços e funcionalidades;
e) Usabilidade;
f) Simplicidade;
g) Mecanismos de autenticação do usuário;
h) Controle de acesso;
i) Criptografia e módulos criptográficos;
j) Geração de números aleatórios;
k) Disponibilidade e eficiência;
l) Confiança e desempenho;
m) Registro de eventos;
n) Temporalidade;
o) Manutenibilidade;
p) Controle por software;
q) Segregação de redes;
r) Redundância.

6.2.Nível Operacional

6.2.3. Teste funcionais (casos de uso).

a) Arquitetura de *hardware* e segurança física;

Deve ser realizada inspeção visual da unidade física do sistema, quando se tratar de *hardware* dedicado.

b) Interface de comunicação e interoperabilidade;

Todas as interfaces gráficas de usuário, todos os menus e demais elementos gráficos devem ser ativados e avaliados.

c) Serviços e funcionalidades;

Todas as chaves ou teclas e combinações descritas devem ser empregadas e a reação do sistema deve ser avaliada.

d) Usabilidade;

De preferência, a equipe de avaliação deve ter um membro especialmente dedicado a avaliar esse atributo, de modo que ele não participe de outras partes do processo. Isso permite que sua capacidade cognitiva seja ativada e ele possa mensurar o entendimento, compreensão e aprendizagem sobre o software e sua utilização.

e) Geração de números aleatórios;

f) Registro de eventos;
g) Temporalidade;
h) Manutenibilidade;
i) Segregação de redes;
j) Redundância.

6.2.4. Teste de segurança (casos de abuso).

Os testes devem promover situações atípicas de uso, para mensurar o comportamento do software. Compreende a utilização de ferramentas de Testes de funcionalidade de segurança, Testes de exploração de vulnerabilidades, Testes de penetração e Testes de sobrecarga.

a) Mecanismos de autenticação do usuário;
b) Controle de acesso;
c) Criptografia e módulos criptográficos;
d) Disponibilidade e eficiência;
e) Confiança e desempenho.

7. Outros requisitos

Deve conter o capítulo 9 do plano de avaliação

8. Conclusões

APÊNDICE B

ProAS-NN

Questionário de qualificação do avaliador

- O propósito deste questionário é qualificar o respondente quanto ao conhecimento e experiência em avaliação de software;
- Informações pessoais não serão divulgadas, ou comporão o texto de qualquer trabalho
- Fique à vontade para responder as informações solicitadas.

Instituição a que o avaliador está ligado: _____

Nome do avaliador (opcional): _____

Escolaridade: ( ) técnico ( ) superior ( ) pós-graduação

Curso: _____

Função na Instituição: _____

Trabalha há quanto tempo na função: _____

Considera seu entendimento avaliação de *softwares*?
( ) insuficiente ( ) moderado ( ) suficiente ( ) muito bom

Realiza avaliações de *softwares* com frequência? ( ) sim ( ) não

Se considera capaz de avaliar *softwares* quando auxiliado por alguma ferramenta?( ) sim ( ) não

Qual sistema/método/ferramenta para avaliação de software costuma usar?
_____
_____

Qual sua maior demanda na avaliação de *softwares*?
_____
_____

APÊNDICE C

ProAS-NN

Questionário para avaliação das fases de verificação

- O propósito desse questionário é avaliar o estabelecido no ProAS-NN em relação as fases de verificação, considerando a descrição, importância, clareza e completude;
- Responda às perguntas de acordo com seu entendimento sobre o proposto no protocolo de avaliação apresentado;
- Responda às perguntas de forma franca e sincera, encare a avaliação como a possibilidade de melhorar o protocolo apresentado;
- Sua resposta será tratada estatisticamente junto a de outros avaliadores, como forma de avaliar as abordagens e o conteúdo do protocolo proposto
- Marque a quantidade de estrelas que corresponda à sua opinião, ou as apague e escreva o número, referente a: **5 - ótimo, 4 – bom, 3 – regular, 2 – déficit, 1 – ruim**
- Sua avaliação é muito importante para o desenvolvimento do trabalho.

Perguntas Fase do ciclo de vida	Acredita ser necessário a verificação da fase?	Está clara a maneira com que o protocolo busca realizar a verificação nesta fase do ciclo de vida?	O que o protocolo verifica é suficiente para possibilitar a transição para a fase seguinte?
Especificação dos requisitos do sistema	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Especificação do software	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Especificação do projeto do software	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Codificação	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Integração do sistema	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Testes com o sistema integrado	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Testes de validação e comissionamento	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Testes de desempenho do software	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Testes de aceitação de fábrica	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Testes de aceitação no local	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Entrega do sistema	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Operação, manutenção e modificação	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆

APÊNDICE D

ProAS-NN

Questionário para avaliação dos atributos s serem validados

- O propósito desse questionário é avaliar o estabelecido no ProAS-NN em relação as a validação, considerando a descrição, importância e método;
- Responda às perguntas de acordo com seu entendimento sobre o proposto no protocolo de avaliação apresentado;
- Responda às perguntas de forma franca e sincera, encare a avaliação como a possibilidade de melhorar o protocolo apresentado;
- Sua resposta será tratada estatisticamente junto a de outros avaliadores, como forma de avaliar as abordagens e o conteúdo do protocolo proposto
- Marque a quantidade de estrelas que corresponda à sua opinião, ou as apague e escreva o número, referente a: **5 - ótimo, 4 – bom, 3 – regular, 2 – déficit, 1 – ruim**
- Sua avaliação é muito importante para o desenvolvimento do trabalho.

Perguntas **Atributos**	Acredita ser necessário a análise do atributo?	Está claro como o protocolo busca abordar, entender e caracterizar o atributo?	Julga que a análise documental e a realização dos testes, especificados para cada atributo, possibilitam avaliá-lo?
Ambiente operacional e cenários de aplicação	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Arquitetura de hardware e segurança física	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Interface de comunicação e interoperabilidade	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Serviços e Funcionalidade	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Usabilidade	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Mecanismos de autenticação de usuário	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Controle de acesso	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Criptografia e módulos criptográficos	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Geração de números aleatórios	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Disponibilidade e eficiência	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Confiabilidade e desempenho	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Registro de eventos	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Temporalidade	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Manutenibilidade	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Segregação de redes	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Simplicidade	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
Redundância	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆

APÊNDICE E

ProAS-NN

Questionário para avaliação dos ensaios

- O propósito desse questionário é avaliar o estabelecido no ProAS-NN em relação as a validação, considerando a descrição, importância e método;
- Responda às perguntas de acordo com seu entendimento sobre o proposto no protocolo de avaliação apresentado;
- Responda às perguntas de forma franca e sincera, encare a avaliação como a possibilidade de melhorar o protocolo apresentado;
- Sua resposta será tratada estatisticamente junto a de outros avaliadores, como forma de avaliar as abordagens e o conteúdo do protocolo proposto
- Marque a quantidade de estrelas que corresponda à sua opinião, ou as apague e escreva o número, referente a: **5 - ótimo, 4 – bom, 3 – regular, 2 – déficit, 1 – ruim**
- Sua avaliação é muito importante para o desenvolvimento do trabalho.

Ensaio **Perguntas**	Avaliação Conceitual	Avaliação Operacional
considera que os documentos solicitados são consistentes com a avaliação proposta?	☆☆☆☆☆	☆☆☆☆☆
considera que existe clareza e facilidade de entendimento da avaliação proposta?	☆☆☆☆☆	☆☆☆☆☆
considera correta aplicação da avaliação proposta?	☆☆☆☆☆	☆☆☆☆☆
considera que existe aplicabilidade na avaliação?	☆☆☆☆☆	☆☆☆☆☆
considera que a avaliação permite verificar as funcionalidades oferecidas pelo software?	☆☆☆☆☆	☆☆☆☆☆
considera que a avaliação permite verificar a segurança o software?	☆☆☆☆☆	☆☆☆☆☆

Perguntas complementares (opcionais)

Concorda com o método utilizado no protocolo?

Concorda com a métrica estabelecida para qualificar o *software* avaliado?

Considera necessário acrescentar mais alguma fase no processo de verificação?

Considera necessário acrescentar a validação de mais algum atributo?

Considera necessário acrescentar mais algum aspecto ou procedimento em alguma fase da verificação?

APÊNDICE F

Relatório de Avaliação

1. Identificação

1.1. Identificação do software avaliado

Alguns meios de transporte como aviões, trem bala e navios observam fatores críticas à segurança, por estarem tecnologicamente equipados com diversos sistemas controlados e programados por equipamentos que utilizam a Tecnologia da Informação (TI), o que pode trazer vulnerabilidades, que os tornam um alvo substancial e plausível de ataques cibernéticos (MEDNIKAROV et. al., 2020), que conforme Bacellar (2018) podem afetar seus vários sistemas, como de navegação, suporte à vida, comunicação, propulsão, entre outros.

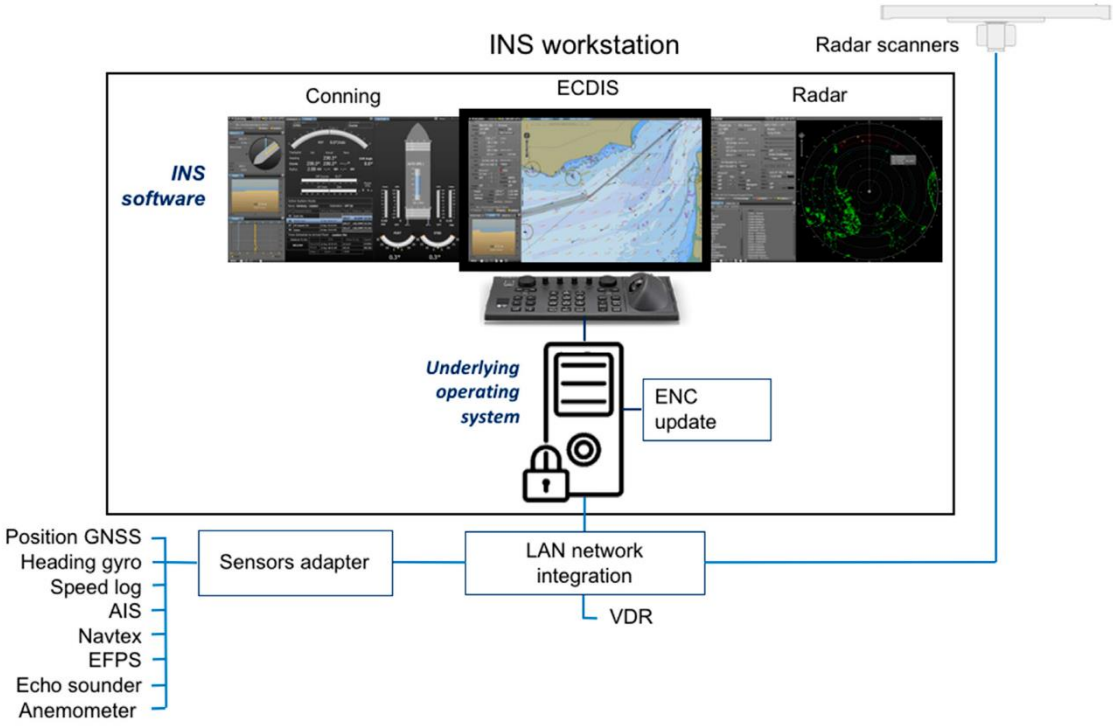
Os sistemas dos navios vêm se desenvolvendo intensivamente por meio de digitalização, com integração a sistemas de redes (SVILICIC, 2019c), ao mesmo tempo em que há aumento nos ataques cibernéticos, exploração de vulnerabilidades e ameaças à segurança cibernética provocadas por ações de criminosos, terroristas e espiões (KESSLER et. al., 2018), e na exploração de novos vetores de ataque, tornando necessário ampliar os esforços de pesquisa para negar as ameaça (JUNIOR et. al., 2021) (SVILICIC, 2019b).

As consequências dos ataques cibernéticos no ambiente marítimo podem resultar em acidentes de navegação, poluição, graves custos econômicos e perdas de vidas humanas, até agora os ataques trouxeram impactos e perdas limitados, mas tendem a crescer, com potencial de causar impacto na cadeia de suprimentos de classe mundial (JUNIOR et. a., 2021).

Dentro deste cenário em que o avanço da tecnologia possibilitou uma imensidão de aplicações para a automação, houve a integração de sistemas de radares, localização e de navegação, com a possibilidade do sistema ser ligado à web, trazendo mais segurança e praticidade a navegação, em contrapartida mais riscos de ataques, e a possibilidade de causar danos ao navio, ao encontrar vulnerabilidades nos sistemas (BACELLAR, 2018). Os principais sistemas de navegação de navios, como GPS, Sistema de Identificação Automática (AIS) e radares foram unificados ao sistema para visualização de cartas náuticas digitais, formando o Sistema Eletrônico de Exibição e Informação de Cartas (ECDIS), recebem dados via transmissão de radiofrequência, dessa forma, ficam vulneráveis (MUCCIN, 2018).

Sendo o ECDIS basicamente um pacote de software instalado em um computador com um sistema operacional (SVILICIC, 2019c), que recebe sinais de sensores e radares do navio de forma integrada, trazendo consigo ameaças de ataques cibernéticos, devido as vulnerabilidades dos sistemas de bordo (MEDNIKAROV et. al., 2020). A Figura 26 ilustra na forma de um diagrama a ligação de um ECDIS.

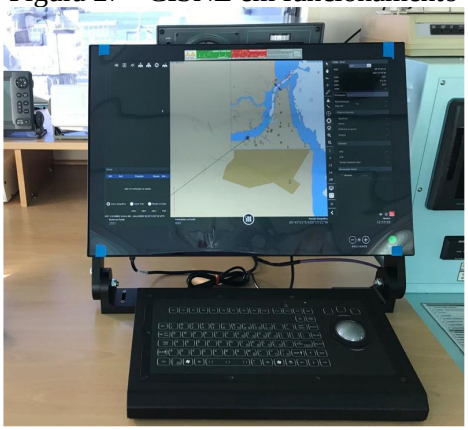
Figura 26 - Diagrama de um ECDIS.



Fonte: SVILICIC, 2019b.

A avaliação foi realizada em um sistema disponibilizado para estudo, o Centro de Integração de Sensores e Navegação eletrônica (CISNE), demonstrado pela Figura 27.

Figura 27 - CISNE em funcionamento

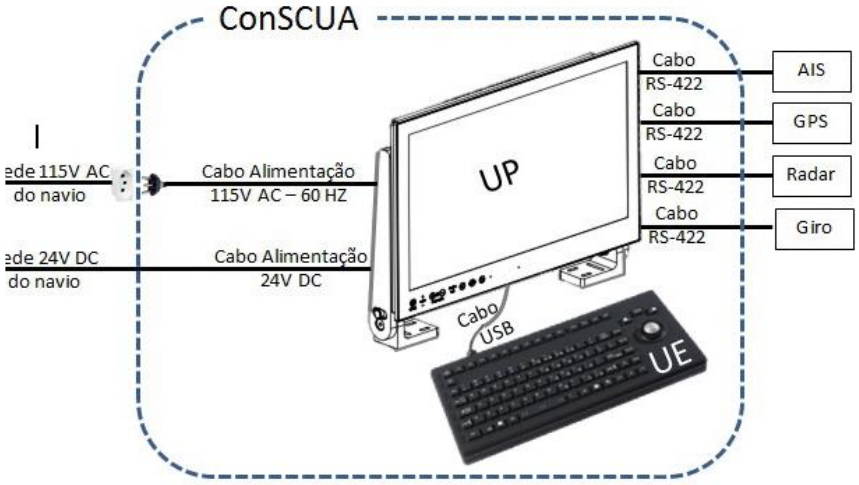


Fonte: Marinha do Brasil, 2020.

É um projeto iniciado em 2017 pela MB para apoio à navegação de navios militares, desenvolvido com uma arquitetura de sistema flexível, orientada a serviço e baseada em códigos abertos (CARNEIRO; JUNIOR, 2018). É um sistema baseado em apresentação gráfica, fundamentado para uso no auxílio à navegação, para exibir digitalmente cartas náuticas junto com a localização exata e a trilha do próprio navio, em uma tela interativa, juntamente às informações complementares, importantes à segurança da navegação, como velocidade e deslocamento, profundidade da água, velocidade do vento, posição geográfica em latitude e longitude e norte verdadeiro da Terra. Além de informar a existência de outros meios na área e sua identificação.

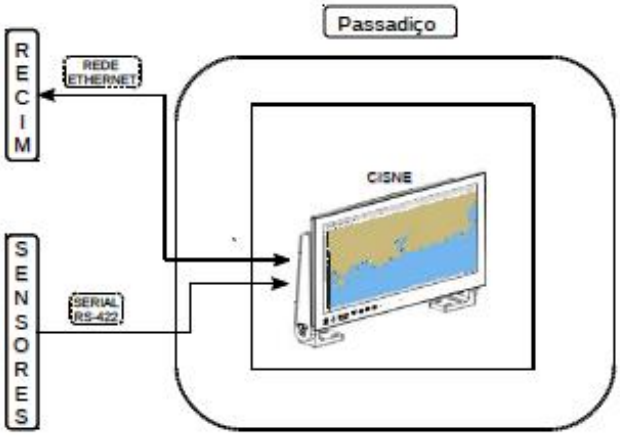
Seu principal objetivo é contribuir para a segurança da navegação, proporcionando ganhos significativos de segurança, graças ao desempenho e disponibilidade do sistema, sendo de grande ajuda por possibilitar a identificação, rastreamento e posicionamento de embarcações e prevenindo riscos de colisões e encalhe. Além de funcionalidades expressamente necessárias em missões militares como identificação, acompanhamento e interceptação de embarcações (SLIVICIC, 2019d). A Figura 28 representa na forma de diagrama a alimentação elétrica e de dados da primeira unidade do CISNE com alimentação de dados de GPS, AIS, radar e agulha giroscópica. A Figura 29 representa a interligação do CISNE a web e aos sensores.

Figura 28 - Alimentação da unidade CISNE no Navio Hidrográfico Sirius



Fonte: Marinha do Brasil, 2018.

Figura 29 - Ligação do CISNE a web e aos sensores.



Fonte: Marinha do Brasil, 2018.

De forma mais específica, o CISNE:

A. Integra informações provenientes de diversos sensores de bordo, tais como GPS, AIS, Giroscópio, Radar, Eco sondas e anemômetro;
B. Apresentar dados georreferenciados, tais como alvos provenientes de sensores (AIS e Radar), cartas náuticas eletrônicas (vetoriais e *rasters*), cartas de uso militar, *overlay* de vídeo bruto radar, *overlay* de imagens satelitais, *overlay* de dados climáticos e meteorológicos etc.;
C. Possibilita planejar, validar e monitorar derrotas de navegação;
D. Realizar fusão de alvos;

E. Realizar cálculos táticos básicos (ponto de maior aproximação, passar safo, manobra dado tempo, manobra dado velocidade etc.);
F. Realizar cálculos dinâmicos de interceptação de alvos;
G. Gravar dados históricos de alvos e do próprio navio (posição, rumo, velocidade etc.) provenientes de sensores (AIS e Radar) com o objetivo de permitir posterior análise de missões e/ou exercícios militares;
H. Disponibilizar, em tempo real e de forma segura, dados de alvos e do próprio navio (posição, rumo, velocidade etc.) provenientes de sensores (AIS e Radar) com o objetivo de prestar auxílio nas operações de busca e salvamento e promover incremento de consciência situacional do contexto militar naval.

1.2.Tipo de *software*

Seguindo o esquema do protocolo apresentado, foi possível identificar o CISNE como um *software* acessível, pois já foi desenvolvido, está sendo executado e possui vasta documentação. Foram caracterizados o ambiente físico e lógico onde é utilizado, sua funcionalidade, os recursos utilizados e sua aplicabilidade. Apesar de ser uma atividade acadêmica, buscou ser a mais fidedigna possível a uma avaliação formal.

2. **Objetivos**

2.1.Objetivos da avaliação

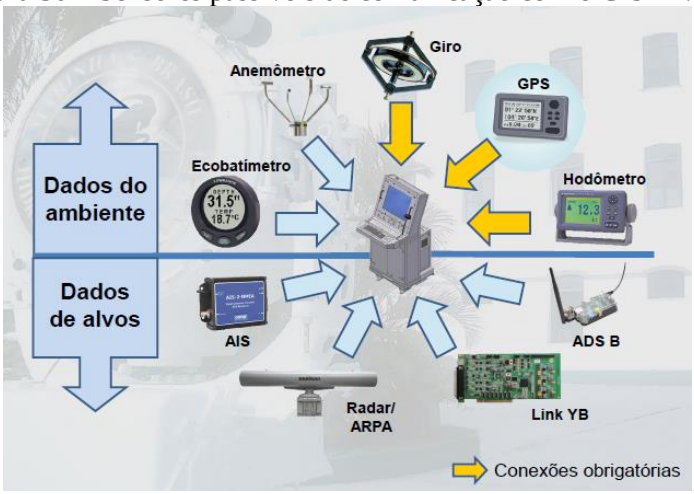
A avalição foi realizada como estudo de caso do trabalho de pesquisa.

2.1.Objetivos do software;

É um *Software* para a Exibição de Informações de Cartas Eletrônicas (ECDIS) desenvolvido pelo Instituto de Pesquisas da Marinha (IPqM) capaz de integrar em uma plataforma gráfica vários sensores do navio. Seu objetivo primário é o auxílio a navegação segura e consciente, por meio de cartas eletrônicas que possibilitam o planejamento e a monitoração de rotas, a percepção e identificação de outros navios em um modo imersivo de interação (MARINHA. 2021e).

É instalado em computador utiliza dados do Sistema de Posicionamento Global (GPS) para localizar pontos do globo terrestre em tempo real (SVILICIC, 2019c). Associado a informações recebidas do giroscópios, no incremento do deslocamento real que o navio sofre e corrige discrepâncias ou defasagens; junto a informações do radar e do Sistema Automático de Identificação (AIS), que compartilha informações entre embarcações por VHF, análogo ao *transponder* de aeronaves (MUCCIN, 2018); juntamente com informações da Eco Sonda sobre a profundidade do local em que se está trafegando (MARINHA, 2014), como ilustra a Figura 30. Segundo Carneiro e Junior (2018), tem acesso à Rede de Comunicações da Marinha (RECIM) para atualizações e envio de dados em tempo real ao Comando de Operações da MB. E pode estar sujeito a ataques (MEDNIKAROV; TSONEV; LAZAROV, 2020a).

Figura 30 – Sensores passíveis de comunicação com o CISNE.



Fonte: Marinha do Brasil, 2018

3. Itens recebidos

3.1. Documentos recebidos

Sua documentação foi disponibilizada, o que possibilitou a caracterização de seus atributos, a modelagem de suas possíveis ameaças, a análise de seus sistemas de proteção e defesa.

3.2. Unidades físicas recebidas

Também foi disponibilizada uma unidade operativa do CISNE nas instalações do IPqM, para a realização dos testes, que caracterizaram alguns dos atributos avaliados e possibilitaram a analisar o comportamento dele. Que junto a documentação permitiu realizar o processo de V&V descrito no ProAS-NN.

4. Planejamento

A identificação inicial permitiu delimitar o escopo da avaliação e realizar seu planejamento. Dentre os atributos especificados para validação, não foram selecionados os três abaixo listados, como previsto pelo método na inexistência do atributo.

- Geração de números aleatórios;
- Disponibilidade e eficiência;
- Confiabilidade e desempenho.

5. Análise de riscos

O passo seguinte foi realizar a análise de riscos aos quais o CISNE pode estar sujeito. Para tal, foi utilizada a técnica de modelagem de ameaças apresentada no ProAS-NN. A documentação fornecida pelo IPqM possibilitou a identificação dos ativos do sistema, sua interação e troca de informações, representados pela confecção do Diagrama de Fluxo de Dados (DFD), no qual foi utilizada a ferramenta *Threat Modeling Tool* 2016, de acordo com a Figura 31, onde são expostos os ativos do sistema, e o fluxo de informações entre esses sistemas, o que possibilitou o entendimento do funcionamento do CISNE com uma identidade visual.

Os principais ativos que compõem o CISNE são:

- Unidade Principal (Panel-PC 24” modelo HD24T22 da Hatteland Technology);
- Unidade de Entrada (teclado emborrachado e iluminado de 92 teclas; e um *trackball* de 25 mm de diâmetro; conexão USB);
- Agulha giroscópica
- GPS;
- Hodômetro de fundo;
- Ecobatímetro;
- Anemômetro;
- Sistema AIS;
- Radar;

A partir dos ativos que compõem o ambiente analisado, as seguintes informações sobre o fluxo de dados foram mapeados no Quadro 20.

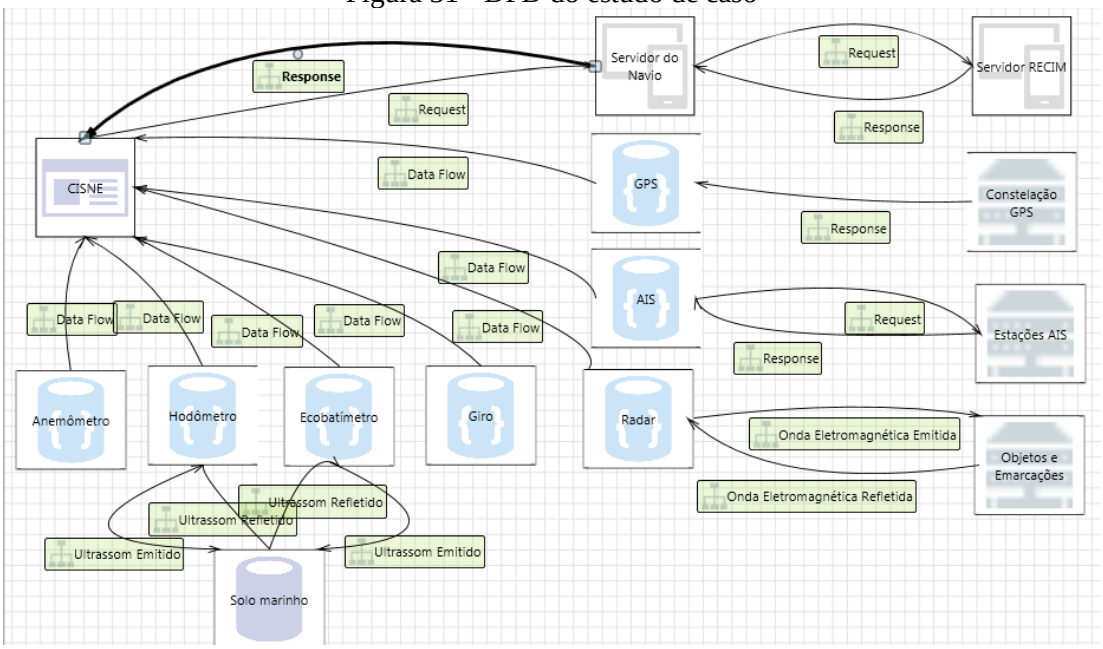
Quadro 20 – Identificação dos ativos que compõem o sistema

ativo	componente com que se comunica
Unidade Principal	Servidor interno; Agulha giroscópica; GPS; AIS; Hodômetro de fundo; Ecobatímetro; Radar e unidade de entrada.
Unidade de entrada	Unidade Principal
Servidor interno	Estação processadora;
Agulha giroscópica	Unidade Principal
GPS	Unidade Principal; Satélites da constelação GPS
AIS	Unidade Principal; outros pontos AIS
Hodômetro de fundo	Unidade Principal
Ecobatímetro	Unidade Principal
Anemômetro	Unidade Principal
Radar	Unidade Principal

Fonte: o autor

O fato do CISNE está instalado em um navio militar, especificamente em um ambiente fechado e com controle de acesso, temperatura, umidade e eletricidade, e sistemas que mitigam a ocorrência de incêndios e alagamento, como ilustra a Figura 32, e seus operadores serem treinados e qualificados para sua operação, diminui a incidência de riscos.

Figura 31 - DFD do estudo de caso



Fonte: o autor.

Figura 32 - CISNE instalado no passadiço do NOc ANTARES

Fonte: Marinha do Brasil, 2019.

A literatura retrata diversos tipos de ataques a sistemas digitais, como os direcionados a redes específicas com objetivo de penetração, acesso a informações confidenciais, obstrução do funcionamento normal dos sistemas, *malwares, phishing*, *ransoware*. E não direcionados, executados usando o ambiente da Internet e ferramentas de *software* para detectar componentes de comunicação desprotegidos, como força bruta, *man-in-the-middle* e *DoS*, diz Mednikarov et. al. (2020). Esses ataques basicamente são de três tipos, sabotagem, espionagem e subversão (RID apud BACELLAR, 2018). Visando destruir o sistema, interceptar informações e enfraquecer autoridade ou ordem estabelecida, atingindo valores sociais (intangíveis) e infraestrutura (tangível).

John Saul (2017) afirma que os riscos de ataques a sistemas de navegação via satélite estão cada vez maiores e mais perigosos, haja visto que na ocorrência de falhas, as embarcações sofrem o risco de encalhar, ou colidir com outros navios. E relata a ocorrência de uma série de interrupções nos sistemas de navegação marítima, apesar de não esclarecer o envolvimento de ataques.

Segundo Muccin (2018) ECDIS são privilegiados sob o aspecto da segurança, quando funcionam de forma independente, segregados física e logicamente de qualquer rede ou dispositivo externo ao seu sistema, mesmo utilizando sensores como GPS, AIS e radar, que dependem do envio e recebimento de sinais de satélite e outras fontes, os quais muitos especialistas consideram vulneráveis a interferências de atacantes. Mas quando eles estão ligados a uma rede ou tem acesso a dados baixados por uma fonte externa, seja por uma porta USB, cartão de memória ou via rede tornam-se susceptíveis a ataques e domínio.

A ação de um atacante, além do acesso e leitura, pode ser seguida da substituição, exclusão ou alteração de qualquer arquivo do ECDIS, de um navio ou de uma estação de terra. Que pode ser feito por meio de portas USB ou download de arquivo de rede. Em 2014, agentes do Grupo NCC estudaram a proteção cibernética do ECDIS, com ataques de penetração por porta USB e Internet, os agentes foram capazes de baixar, ler, modificar, substituir e excluir arquivos (MEDNIKAROV, 2020).

Da mesma maneira, atacantes podem implantar *malwares* no sistema com o objetivo de alterar os parâmetros e dados do sistema. A inserção desses *softwares* maliciosos pode ocorrer intencionalmente ou não, por mídia removível inserido na UP, por exemplo, um militar de

serviço no passadiço colocou um celular para carregar na porta USB do Panel-PC transferindo um *worm* (JUNIOR et. al., 2021).

Ou o *malware* pode realizar essas funções pré-programadas obedecendo a comandos do atacante enviados remotamente e recebidos pelos sistemas de radar e AIS. Como apresentado por Junior et. al. (2021) que expõe que uma atacante pode enviar mensagens forjadas ao AIS, que representa uma formação de cinco navios alinhados, que será reconhecido pelo malware como uma ordem para manipula os processos computacionais do sistema de acordo com o comando transmitido pelo atacante. Exemplos de possíveis ações prejudiciais executadas no sistema alvo durante este estágio são redefinir o sistema, gravar e reproduzir cenários, congelar a exibição do sistema etc.

Um *malware* ainda pode ser a ponte para um ataque *spoofing*, onde, um atacante pode acessar o sistema e *logar* como um usuário autêntico, descobrindo a senha porum ataque de força bruta, haja visto que a senha padrão que para o usuário normal de operação é fraca demais, bem como a senha de administrador pode ser descoberta e o atacante criar um usuário para si.

No ano de 2016, centenas de embarcações de pesca voltaram para o porto, na Coreia do Sul, após perderem o sinal de GPS, devido a ataques. A Guarda Costeira dos EUA relatou que a interferência no GPS dos navios interrompeu as operações em um porto por várias horas em 2014 e em outro terminal em 2015. Em junho de 2017 um navio no Mar Negro informou ao Centro de Navegação da Guarda Costeira dos EUA que seu sistema de GPS havia sido interrompido e que mais de 20 navios na mesma área tinham sido afetados de forma semelhante (SAUL, 2017). Junior et. al. (2021) apresentam em seu artigo um mecanismo em que um atacante utiliza o sistema de radar ou AIS como entrada no navio, enviando padrões específicos que servem de comandos a um malware implantado previamente no navio. Podendo também ativar um microchip previamente implantado no sistema, a exposição aumenta quando há conexão à internet para processamento ou análise de dados (BARROS, 2021).

Outro tipo de ameaça, não menos importante, é o elemento interno, que tem a capacidade de atuar no ciberespaço introduzindo uma vulnerabilidade operacionalmente por meio de ação humana direta, ou seja, por meio físico (NUNES, 2010).

ECDIS tem vulnerabilidades de segurança de *software* subjacentes que podem levar a resultados desastrosos para os navios no mar. Se o *malware* chega a bordo do navio poderá afetar sistemas críticos e, nesse cenário, é apenas uma questão de tempo antes que eles causem danos. Em redes rapidamente esse *malware* se espalhará, associado ao fato de que há muitos sistemas operacionais e *softwares* desatualizados que estão sendo executados (BARROS, 2021).

Neste tópico são apresentados os resultados da identificação de ameaças ao sistema. Com a análise do diagrama arquitetural do sistema foi possível apontar os principais cenários de ameaça.

Foram identificadas poucas ameaças, todas de origem externa, pela técnica STRIDE para a identificação das ameaças que foram classificadas de acordo a severidade, pela técnica DREAD, a saber:

a)Danos Físicos – com a adulteração da rota assumida ou dos dados do ambiente, a embarcação pode trafegar em águas muito rasas e encalhar ou abalroar em pedras e perigos submersos ou em outra embarcação em deslocamento;

b)Danos à Saúde – uma alteração da rota planejada, faz com que a embarcação realize deslocamentos desnecessariamente longos ou a velocidade baixa, fazendo com que o tempo da viagem aumente, e a tripulação passe mais tempo a bordo do navio, o que pode afetar-lhes a

moral e a saúde psicológica. Em uma ação de busca e salvamento (SAR) a adulteração da rota poderá prolongar o tempo de chegada ao local da ação, ou levá-la ao local errado;

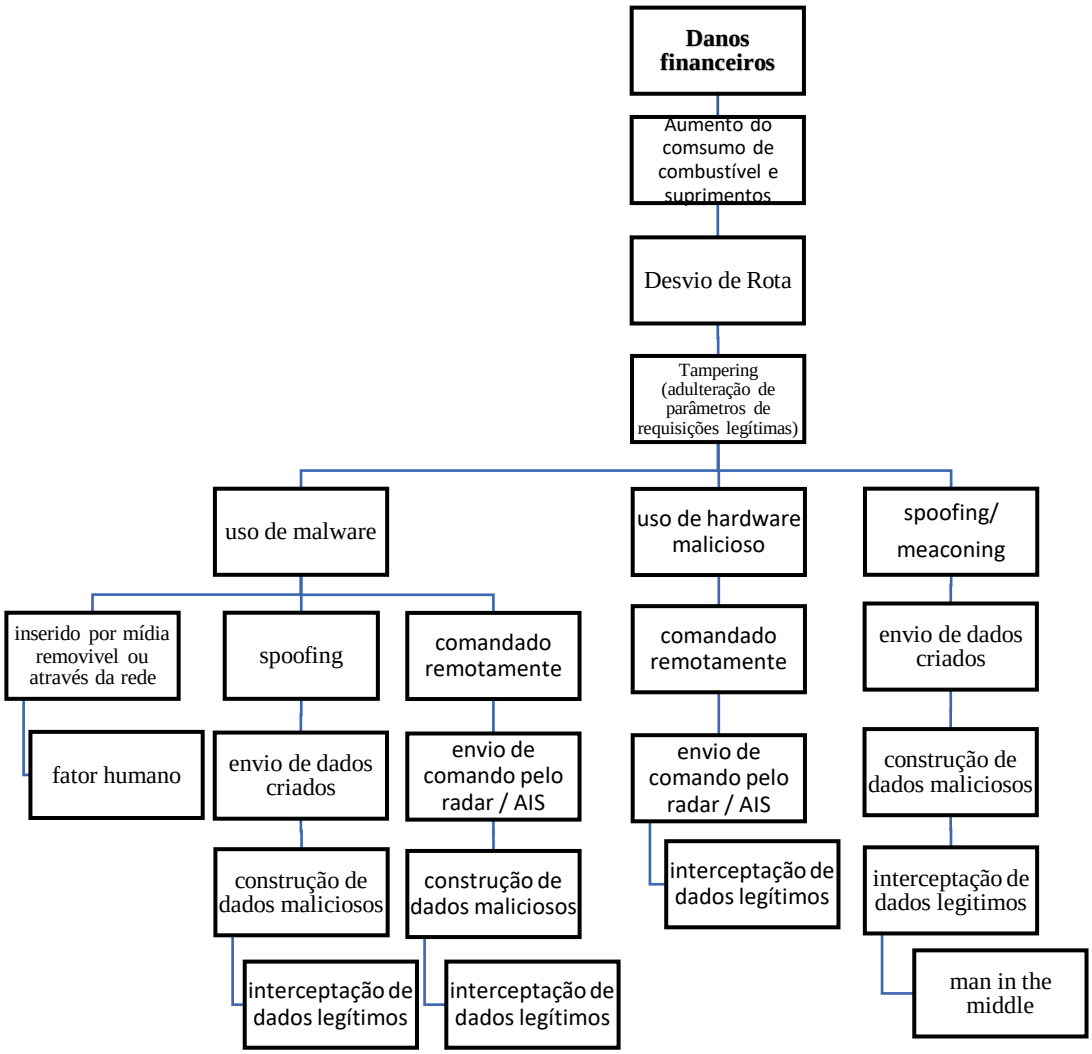
c)Danos Financeiros – os deslocamentos desnecessariamente longos ou a baixas velocidades causam danos financeiros pelo aumento do consumo de combustível, de suprimentos e água pela tripulação, encurta o intervalo entre as manutenções e a vida útil de componentes. Além de prejuízos na programação da viagem;

d)Falsa Identificação e Localização – um atacante poderá alterar a localização do navio, inserir falsos navios, adulterar a identificação dos mesmos e suprimi-los na carta náutica exibida. Dessa forma permite que um navio intercepte um alvo acreditando que seja outro, deixe de visualizar um alvo suspeito, ou acompanhe algo que não exista ou esteja em uma posição diferente da apontada.

De posse das ameaças, o ProAS-NN aborda a identificação das vulnerabilidades pela geração da árvore de falhas, que permite identificar as fontes dessas ameaças, e consequentemente sugerir medidas mitigadoras para elas.

A Figura 33 demonstra a árvore de falha traçada para a ameaça que resulta em dano financeiro, e possibilita entendê-la melhor ao identificar suas causas, autores e caminhos percorridos. E sugerir maneiras de mitigar ou eliminar a possibilidade de sua ocorrência. As outras ameaças identificadas têm árvores de causas semelhantes, e identificam os mesmos autores e causas.

Figura 33 - Árvore de análise de ameaça de danos financeiros



Fonte: o autor.

No papel de usuário autêntico, o atacante tem o poder de realizar a adulteração de dados legítimos com o objetivo de desviar a rota traçada após sua validação no CISNE, sem a percepção do operador. Ataques contemporâneos são realizados com novos e diversos malwares, que permitem a intervenção adicional dos invasores que podem acessar, ler, baixar, substituir ou excluir qualquer arquivo armazenado na UP do CISNE, bem como modifique ou exclua o conteúdo de arquivos e gráficos em computadores a bordo (MEDNIKAROV et. al., 2020).

Semelhante ao *software* malicioso, existe o *hardware* malicioso, que pode ser um microchip implantado fisicamente no sistema. Esse componente poderá varrer constantemente a tela do CISNE visando identificar um padrão específico, a procura de um comando remoto, gerada e transmitida por uma técnica de Memória de Rádio Frequência Digital (DRFM). Onde o comando é recebido e processado pelo radar ou AIS, exibido como uma imagem na tela, como qualquer outro alvo recebido (ALMSLMANY et. al. apud JUNIOR et. al., 2021). Como o exemplo da formação dos cinco navios alinhados, que da mesma forma corresponde ao comando de disparo enviado pelo invasor via AIS ou radar. Quando o padrão é reconhecido na tela, o chip interpreta a partida como um comando para desencadear uma ação maliciosa pré-programada que afeta o processo computacional do CISNE efetua as ações necessárias para desviar o navio da rota que deve traçar (ADEE, 2008).

O outro vetor de ataque ocorre quando um atacante consegue interceptar o sinal eletromagnético emitido pelo radar ou AIS e implanta obstáculos à navegação, fazendo com que a derrota do navio precise ser alterada pelo operador de forma consciente, para desviar do falso obstáculo, seja ele um banco de areia ou outra embarcação com rota coincidente, por exemplo.

O AIS é um dos sistemas do navio mais vulneráveis, pois não utiliza mensagens criptografadas nem autenticadas, o que faz com que as trocas de dados possam ser lidas por um atacante, que pode facilmente encontrar instruções, *hardwares* baratos e *softwares* abertos para construir um receptor AIS (KESSLER, et. al., 2018).

As mensagens transmitidas em texto simples, afetam a confidencialidade, integridade e disponibilidade das informações. Permitindo ataques de colisão intencional por piratas e terroristas, qualquer receptor AIS não autorizado dentro do alcance pode ler e encaminhar incontrolavelmente dados aos navios e estações de terra, além disso pode transmitir as informações do AIS para sites da Internet. Dando origem a cenários de ataque em áreas marítimas perigosas, onde piratas ou terroristas espreitam, além disso, a ausência de integridade de dados torna as mensagens AIS vulneráveis a modificações não autorizadas (GOUDOSSIS; KATSIKAS, 2019).

Essa facilidade permite ao atacante explorar, interceptar, transmitir, comprometer e adulterar os dados, se passar por autoridades marítimas para enganar a tripulação do navio e desativar o transmissor AIS, tornando-os invisíveis para qualquer um, exceto os próprios invasores. Pode ainda provocar uma enxurrada de dados no sistema visando a negação de serviço. Levando a modificação de todos os dados do navio em relação, posição, curso, carga, velocidade, nome do navio, (PARKER, apud KESSLER, et. al., 2018), além da criação de embarcações "fantasmas" em qualquer localização arbitrária no oceano, que seria reconhecida pelos receptores AIS como embarcações genuínas, disparar falso alerta de aviso de colisão, resultando em alteração de rota ou uma possível colisão. Enviar informações falsas de previsão do tempo de forma a forçar o desvio o curso devido a uma tempestade inexistente (MEDNIKAROV et. al., 2020).

A ausência de autenticação de origem torna o AIS vulnerável à falsificação de navios. Um navio virtual pode transmitir dados falsos, por exemplo, alarmes falsos, informações de tráfego falsas, informações de manobras falsas, para fazer o alvo mudar de rumo, um atacante envia mensagens AIS falsas para emular um barco inexistente no curso do alvo (GOUDOSSIS; KATSIKAS, 2019). Ao identificar e interceptar uma requisição legítima, levando em consideração que o sistema não utiliza nenhum mecanismo de autenticação, um atacante poderia então repetir esta requisição e executar comandos válidos no sistema.

Isto foi confirmado recentemente por várias fontes, incluindo Israel. Eles notaram que as embarcações que transmitem sinais espúrios de AIS não estavam nem perto da sua localização atual e em outras ocasiões também tinham aparecidos navios fantasmas que não puderam ser encontrados (MUCCIN, 2018).

O atacante pode ainda provocar a exclusão da mensagem AIS, por meio de interferência destrutiva ou construtiva, realizada produzindo um número significativo de erros de bits na mensagem, fazendo com que a parte receptora descarte a mensagem devido à corrupção de dados. A modificação da mensagem é iniciada alterando o fluxo de bits de uma mensagem, geralmente por inversão de bits (ou seja, alterando um 0 para 1 ou 1 para 0) ou ofuscamento (ou seja, usando uma fonte de transmissão de alta potência para substituir parte de, ou uma mensagem de destino inteira). (KESSLER, et. al., 2018)

O ataque *Meaconing* rastreia e registra a emissão eletromagnética dos satélites e a retransmite mais forte e com atraso para o alvo, que lê o sinal falso como dominante. Como verificado por agentes da UT Austin em ataque ao iate "*White Rose of Drax*" que navegava no mar mediterrâneo. Um sinal poderoso falso suprimindo o sinal de GPS autêntico é emitido até que o controle total sobre o sistema de navegação do navio seja alcançado (DIRENZO et. al. apud MEDNIKAROV et. al., 2020).

Com um rádio VHF o atacante pode explorar as fraquezas do AIS, interceptar os dados de identidade, tipo, posição, rumo e velocidade e marcação. De forma a modificar e comprometer todos os dados do navio, comprometer e adulterar os dados. Pode ainda criar embarcações "fantasmas" em qualquer local arbitrário no oceano, que seriam reconhecidos pelos receptores AIS como embarcações genuínas (MEDNIKAROV et. al., 2020).

O modelo de avaliação de ameaças estudado por Gauthier e Seker (2018) identifica três tipos principais de ataques cibernéticos a sistemas AIS. A Interrupção do sinal, o Bloqueio das comunicações e a Manipulação dos sinais de transmissões, posicionamento, deslocamentos. Pela injeção de mensagem (*spoofing*), exclusão e modificação de mensagem (alteração do conteúdo de dados (KESSLER, et. al., 2018).

O Quadros 21, 22, 23 e 24 apontam a pontuação da ameaça utilizando a ferramenta DREAD de classificação das ameaças.

Quadro 21 - Classificação da ameaça de danos financeiros

Propriedade	Valor	Justificativa
Damage	Baixo 1	O desvio da rota não provocará um aumento considerável do percurso
Reproducibility	Alto 3	Um atacante pode reproduzir os ataques necessários para concretização da ameaça a qualquer momento.
Exploitability	Baixo 1	Para a realização dos ataques envolvidos na concretização do cenário de ameaça, um atacante necessita interceptar e analisar o tráfego de comunicação entre o navio e a estação de terra e realizar o ataque ou envio de requisições maliciosamente criadas. Dado o conjunto de variáveis, exige-se uma alta expertise técnica para a concretização deste cenário.
Affected things	Médio 2	Equipamentos serão utilizados sem necessidade
Affected users	Baixo 1	A ameaça não trará grandes riscos as pessoas.
Discoverability	Médio 2	Dificilmente os operadores perceberão que estão operando em um sistema adulterado, por mais que o desvio malicioso da rota seja percebido, pouca será a desconfiança de adulteração no sistema, apenas o pessoal técnico ligado ao desenvolvimento do sistema poderá identificar ações de um atacante.
Risco	10	

Fonte: o autor.

Quadro 22 - Classificação da ameaça de danos à Saúde

Propriedade	Valor	Justificativa
Damage	Médio 2	O ataque poderá afetar a vida das pessoas que estão no navio, bem como as que eventualmente dependam desse para serem socorridas em uma situação de perigo ou emergência.
Reproducibility	Alto 3	Um atacante pode reproduzir os ataques necessários para concretização da ameaça a qualquer momento.
Exploitability	Baixo 1	Para a realização dos ataques envolvidos na concretização do cenário de ameaça, um atacante necessita interceptar e analisar o tráfego de comunicação entre o navio e a estação de terra e realizar o ataque ou envio de requisições maliciosamente criadas. Dado o conjunto de variáveis, exige-se uma alta expertise técnica para a concretização deste cenário.
Affected things	Baixo 1	Equipamentos serão utilizados sem necessidade
Affected users	Alto 3	Vidas podem deixar de ser salvas em uma missão de SAR.
Discoverability	Médio 2	Dificilmente os operadores perceberão que estão operando em um sistema adulterado, por mais que o desvio malicioso da rota seja percebido, pouca será a desconfiança de adulteração no sistema, apenas o pessoal técnico ligado ao desenvolvimento do sistema poderá identificar ações de um atacante.
Risco	12	

Fonte: o autor.

Quadro 23 - Classificação da ameaça por danos físicos a embarcação

Propriedade	Valor	Justificativa
Damage	Alto 3	O ataque poderá provocar acidentes sérios, que envolvam outras embarcações, por exemplo, um navio tanque que com um vazamento pode despejar centenas de toneladas de óleo no mar, afetando a vida marinha e a de habitantes do litoral
Reproducibility	Alto 3	Um atacante pode reproduzir os ataques necessários para concretização da ameaça a qualquer momento.
Exploitability	Baixo 1	Para a realização dos ataques envolvidos na concretização do cenário de ameaça, um atacante necessita interceptar e analisar o tráfego de comunicação entre o navio e a estação de terra e realizar o ataque. Dado o conjunto de variáveis, exige-se uma alta expertise técnica para a concretização deste cenário.
Affected things	Alto 3	Devido ao acidente o navio poderá quebrar, afundar ou tombar, bem como provocar danos o outros
Affected users	Alto 3	Vidas humanas do navio atacado e de outro que por ventura se envolva em um acidente podem ser perdidas.
Discoverability	Médio 2	Dificilmente os operadores perceberão que estão operando em um sistema adulterado, por mais que o desvio malicioso da rota seja percebido, pouca será a desconfiança de adulteração no sistema, apenas o pessoal técnico ligado ao desenvolvimento do sistema poderá identificar ações de um atacante.
Risco	15	

Fonte: o autor.

Quadro 24 - Classificação da ameaça de danos por falsa localização e identificação

Propriedade	Valor	Justificativa
Damage	Médio 2	O atacante poderá criar cenários que dificultarão a utilização do sistema e por consequência traçar e seguir a rota para o deslocamento do navio.
Reproducibility	Médio 2	O ataque apenas pode ser reproduzido dentro de uma janela de tempo específica e em uma condição de particular.
Exploitability	Baixo 1	Para a realização dos ataques envolvidos na concretização do cenário de ameaça, um atacante necessita interceptar e analisar o tráfego de comunicação entre o navio e a estação de terra e realizar o ataque. Dado o conjunto de variáveis, exige-se uma alta expertise técnica para a concretização deste cenário.
Affected things	Baixo 1	Equipamentos serão utilizados sem necessidade
Affected users	Baixo 1	A ameaça trará pequenos riscos às pessoas, aumentando a carga de estresse e o volume de trabalho envolvido.
Discoverability	Médio 2	Dificilmente os operadores perceberão que estão operando em um sistema adulterado, por mais que o desvio malicioso da rota seja percebido, pouca será a desconfiança de adulteração no sistema, apenas o pessoal técnico ligado ao desenvolvimento do sistema poderá identificar ações de um atacante.
Risco	9	

Fonte: o autor.

Após a classificação das ameaças e a atribuição dos seus valores devido aos riscos, os valores são organização em ordem crescente com relação ao valor do risco. O ranking das ameaças baseado em seus riscos é mostrado na Tabela 15.

Tabela 15 - Classificação das ameaças

Ameaça	Risco
Danos físicos a embarcação	15
Danos à saúde	12
Dano financeiro	10
Falsa posição/localização/identificação	9

Fonte: o autor.

Tendo apontado que a ameaça causadora de danos físicos a embarcação é a mais ofensiva.

6. Verificação

Identificado como *software* acessível existente, seu processo de verificação é realizado utilizando a documentação de desenvolvimento e de testes. Abrange as etapas:

a) Verificação da especificação dos requisitos do sistema – a documentação analisada permitiu verificar que os requisitos para o programa de criação do CISNE correspondem às necessidades que impôs a sua criação;

b) Verificação da especificação do sistema – com a análise da documentação foi possível determinar que a especificação do CISNE reflete com fidelidade os requisitos expressos no seu programa de criação, contempla requisitos de funcionalidades, testes, interação com os demais ativos do sistema;

c) Verificação da especificação de desempenho do *software* – a documentação permitiu demonstrar que a especificação de desempenho do CISNE corresponde as necessidades dos requisitos do sistema;

d) Verificação do código fonte – especificamente nessa etapa de verificação se realizou a verificação indireta, pelo relatório de revisão do código-fonte, que aponta a existência de alguns pontos falhos e sugere melhorias, que foram corrigidos e implementadas no desenvolvimento do CISNE;

e)Verificação do relatório de integração do sistema – verificado junto da fase seguinte;

f)Verificação do relatório de teste de sistema integrado – o relatório de integração do CISNE ao Panel PC, *hardware* adotado pela MB, contempla os testes de integração, e apontam o funcionamento correto do *software* em seu *hardware*, e o atendimento a todas as demandas;

g)Verificação do relatório de teste de aceitação de fábrica – os relatórios de teste do CISNE demonstraram a correta funcionalidade e operação;

h)Verificação de relatório de teste de comissionamento – a fase seguinte foi verificada em conjunto;

i)Verificação do relatório de teste de aceitação do local - foram analisados os relatórios de instalação do CISNE em dois navios da MB; não foram evidenciadas incoerências ou inconsistências no processo de instalação e operação; e

j)Verificação de relatórios de operação, manutenção e modificação – a documentação que encerra o programa de criação do CISNE prevê que sua constante melhoria, atualização do *software*, futura versão em *hardware* mais moderno e acompanha manuais de operação, instalação e treinamento.

7. Validação

Utilizou como subsídios apresentações que o IPqM realizou; especificações de alto nível; manuais de operação, instalação, configuração e do usuário; *data sheet* do *hardware*; o projeto de instalação do sistema em dois navios e o relatório da plataforma utilizada para seu desenvolvimento.

E a avaliação prática que possibilitou a complementação da avaliação documental, pela verificação complementar dos atributos que não foi possível de realizar na avaliação documental, seja por não estarem contidos nos documentos especificados ou não foram possíveis de serem verificados; além da realização de testes de uso e demais caracterizações físicas.

a)Ambiente operacional e cenários de aplicação – de acordo com os relatórios e projetos de instalação do CISNE foi possível caracterizar o ambiente em que o sistema opera como um ambiente controlado e seguro; livre de intempéries, animais e pessoas não autorizadas; com energia estabilizada. Assim pode-se considerá-lo conforme, pois atende o que se propõe;

b) Arquitetura de *hardware* e segurança física – pela análise da documentação e da unidade física disponibilizada foi possível caracterizar aspectos físicos do CISNE, por ser um *hardware* único é alcançada uma organização satisfatória com a vantagem de não haver cabos ou conexões, além do que o liga aos sensores. Entretanto, foi observada uma fragilidade que as portas USB e serial da unidade principal são acessíveis, e podem ser utilizadas para conexão com mídia removível e transmissão de malwares, o que pode ser resolvido com o bloqueio físico dessas portas, e alcançar a conformidade;

c) Interfaces de comunicação e interoperabilidade – foram analisados os documentos e verificou-se que as interfaces foram descritas de forma clara e consistente; foram testadas todas e teclas da unidade de *hardware* e analisado na tela os menus e janelas, que foram considerados condizentes com as condições do ambiente em que está empregado, como é possível ver na Figura 34. A interoperabilidade foi caracterizada pela comunicação do CISNE com os *softwares* e firmware dos sensores dos quais recebe dados, função para que foi desenvolvido, realizada de forma direta via cabo, o que pode ser uma fragilidade, apesar do CISNE realizar a verificação da autenticidade do sensor, um atacante a bordo do navio e conhecedor do sistema pode identificar o cabo de comunicação e interferir na transmissão de dados, uma hipótese possível, mas remota. Há também comunicação do CISNE com uma rede de dados externa ao navio, apenas com esse no porto, pelo cabo da RECIM, para atualização de cartas ou quando os técnicos do IPqM realizam a manutenção ou atualização do software, são observados todos os mecanismos de segurança da MB, como firewalls, criptografia e *antimalwares*. Não se observou vulnerabilidades que possam ser exploradas por um atacante, considerando conforme;

Figura 34 – CISNE em utilização em navio da MB

Fonte: Marinha do Brasil, 2019.

d) Serviços e funcionalidades – foram analisados os manuais de operação e usuário e realizados testes na unidade física disponibilizada; foram aplicados todos os recursos e funções, o CISNE respondeu de forma condizente aos comandos, não houve intercorrência nos testes e foi percebida clareza e nitidez das informações; não foram identificadas funções não documentadas. Considerando o CISNE conforme;

e) Usabilidade – esse atributo foi analisado pelo autor desse texto, que não havia tido contato com o sistema antes da pesquisa, como recomenda o ProAS-NN. Os manuais se mostraram claros e simples, com sua leitura foi possível entender e utilizar o CISNE com facilidade considerável. O layout e organização das telas foram considerados agradáveis e claros, convidativos a exploração do software e suas funções; houve um pouco de dificuldade na utilização do teclado e mouse, pela pressão que precisa se exercer nas teclas. A organização de menus e abas é intuitiva e há figuras que facilitam o entendimento e associação à uma função. Ao utilizar uma função de forma não convencional, que simbolize perigo ou com valores

exagerados, o CISNE alerta o usuário e informa a possibilidade de haver erro. De forma geral o sistema é considerado fácil de utilizar e aprender, o que o torna conforme;

f) Mecanismos de autenticação de usuário – pelo contido na documentação e nos testes da unidade física disponibilizada foi possível caracterizar o atributo, é utilizado o sistema de usuário e senha, como mostra a Figura 35. O manual do usuário define um usuário e sua senha para que seja feito o primeiro acesso e cadastrado novos usuários, onde se identifica uma falha, pois o CISNE não solicita que seja cadastrado um usuário ou que a senha seja modificada após esse acesso, ou seja, o primeiro acesso pode ser acessado sempre, para o ProAS-NN esse fato pode ser percebido como uma não conformidade e precisa ser tratado;

Figura 35 - Tela de login do CISNE

Fonte: Marinha do Brasil, 2019.

g) Controle de acesso - pelo contido na documentação e nos testes da unidade física disponibilizada foi possível caracterizar o atributo, é utilizado o modelo baseado em papéis, bem definidos quanto a funções e privilégios podendo considerar o CISNE conforme;

h) Criptografia e módulos criptográficos – a documentação fornecida não possibilitou a caracterização do uso de criptografia, contudo em entrevista com os desenvolvedores do CISNE foi possível identificar que o protocolo utilizado é o *blowfish*, e é utilizada no acesso aos arquivos e em eventuais comunicações pela RECIM. Assim, é considerado conforme;

i) Registro de eventos – pela experimentação prática do CISNE foi possível comprovar o registro de logs, atividades, percursos e alterações para posteriores verificações e auditoria. O que torna o CISNE conforme nesse atributo;

j) Temporalidade pela documentação e uso da unidade física disponibilizada verificou-se que o CISNE possui um relógio de horas, minutos e segundos, o utiliza no cálculo dos deslocamentos e registro de eventos. A referência de tempo são informações de hora recebidas do sistema GPS, podendo considerar o CISNE conforme nesse atributo;

k)Manutenibilidade – pela análise da documentação fornecida e com a experiência adquirida na realização da avaliação é possível afirmar que o CISNE permite o diagnóstico de causas de falha e permite ser testado, o eu considero-o conforme;

l) Segregação de redes – o entendimento do funcionamento do CISNE possibilita afirmar que seu funcionamento independente de qualquer rede de dados, ao mesmo tempo que depende totalmente da ligação com os sensores para seu funcionamento, por ser um sistema de integração de sensores, o que foi confirmado com a utilização da unidade física. Foi considerado como conforme por não necessita de comunicação externa ao navio;

m) Simplicidade - pelo entendimento da arquitetura e funcionamento do CISNE, associado a utilização prática da unidade física é possível garantir que ele foi construído para ser o mais simples possível, e se realiza apenas as funções necessárias, considerado conforme;

n) Redundância – foi caracterizada pela avaliação da documentação que aponta particionamento de HD para backup e armazenamento de cartas.

8. Conclusões

A análise heurística foi realizada para cada um dos 14 atributos selecionados, como descreve o procedimento para demonstração da conformidade de nível conceitual, cumprindo ainda e parte da demonstração de nível estrutural, apresentada e de operação.

Foram verificadas algumas possíveis vulnerabilidades, por exemplo, a exposição de entradas USB da unidade principal, que possibilita uma eventual conexão de uma mídia removível infectada.

E oportunidades de melhoria, como por exemplo a possibilidade de o usuário mostrar a senha digitada, para fim de conferência, como mostra a Figura 36.

Figura 36 - campo inserir senha

Fonte: o autor.

Após a realização da avaliação, os resultados foram apresentados, utilizando o conceito de mesa redonda, onde o desenvolvedor do sistema avaliado participava ativamente da apresentação dos resultados. Demonstrando seu entendimento da avaliação, e apresentando fatos que não foram evidenciados na avaliação heurística. Como por exemplo, que o terminal da unidade principal possui senha para acesso ao sistema operacional, o que incrementa em mais uma etapa o processo de autenticação do usuário.