DESENVOLVIMENTO DE FERRAMENTA DE APOIO À GESTÃO E SIMULAÇÃO DE CENÁRIOS DE RISCO NO SC²EX

1º Sgt – AUDISON BATISTA DE MORAIS
1º Sgt – ANDERSON PEREIRA DA SILVA
1º Sgt – ANÍBAL PÓVOAS BARBOSA
1º Sgt – REGINALDO SOBREIRA DE MEDEIROS
2º Sgt – FELIPE MUNIZ DE MORAES

RESUMO

O projeto consiste na criação de uma ferramenta web de apoio à gestão e simulação de riscos para sistemas de comando e controle (SC²Ex). O objetivo principal é criar uma solução ágil que auxilie na identificação, análise e previsão de riscos em cenários críticos, otimizando a tomada de decisão e o planejamento de respostas estratégicas. O projeto foca em componentes-chave como a análise de requisitos dos utilizadores de C², integrando funcionalidades de simulação, monitoramento e gestão de cenários. Os objetivos específicos incluem aumentar a resiliência dos sistemas, melhorar a capacidade de resposta a incidentes e minimizar impactos negativos de eventos adversos. A ferramenta integrará funcionalidades de monitoramento, simulação e gestão de cenários para garantir a resiliência e eficiência dos SC²Ex em situações de adversidade e terá uma interface de gestão intuitiva, visando contribuir para a segurança e eficiência das operações, proporcionando um ambiente de gestão de riscos mais adaptável e robusto.

Palavras-chave: Comando e Controle, Riscos, Cenários, Vulnerabilidades.

1- INTRODUÇÃO

Há uma crescente dependência de sistemas digitais e redes de comunicação nas Forças Armadas. No contexto atual, a capacidade de antecipar, gerenciar e responder eficazmente a cenários de risco é uma necessidade. O estudo preencherá essa lacuna ao desenvolver uma ferramenta que não apenas gerencia riscos cibernéticos (identificação, avaliação), mas que simula a propagação e o impacto de ataques cibernéticos em tempo real ou quase real dentro do ambiente operacional modelado do SC²EX e oferecer uma capacidade de avaliação contínua e dinâmica de vulnerabilidades e da eficácia das defesas cibernéticas. Através da simulação de diferentes cenários de ataque.

1.1 JUSTIFICATIVA

O desenvolvimento de uma ferramenta de apoio à gestão e simulação de cenários de risco em Comando e Controle está na necessidade de melhoria na tomada de decisão e a resposta a incidentes cibernéticos, aumentando a segurança através da identificação, análise e mitigação de riscos. A simulação testa cenários simulados, resultantes da combinação de diferentes níveis de probabilidade e impacto, contemplando a diversidade de ativos, ameaças e vulnerabilidades dos Sistemas C².

1.2 CONTEXTUALIZAÇÃO

A gestão de riscos cibernéticos é crucial para proteger os ativos de informação e garantir a continuidade dos negócios. Automatizar a criação da tabela de riscos agiliza a identificação e priorização de ameaças, integrando dados como impacto, probabilidade e responsáveis. Isso transforma a segurança em um processo dinâmico, reduz erros manuais e permite uma resposta ágil às ameaças, tornando a proteção proativa e

eficiente.

1.3 DEFINIÇÃO DO PROBLEMA DE PESQUISA

A complexidade das ameaças cibernéticas impõe novos desafios à proteção de sistemas críticos. No âmbito do Exército Brasileiro, o Sistema de Comando e Controle desempenha papel essencial na coordenação de operações e no suporte à tomada de decisão. Entretanto, atualmente não há uma ferramenta integrada que permita realizar uma gestão de riscos, aliada à simulação de cenários realistas de ameaças comuns aos sistemas utilizados no Exército, o que gera uma lacuna no processo de gestão da segurança cibernética.

1.4 OBJETIVO DA PESQUISA

Desenvolver e validar uma ferramenta computacional de apoio à gestão e simulação de cenários de risco, voltada para o contexto operacional do Sistema de Comando e Controle, permitindo a identificação, análise, avaliação e tratamento automático de riscos com o intuito de aprimorar a tomada de decisão.

1.4.1. Objetivos específicos

Mapear os principais tipos de riscos enfrentados pelo Exército Brasileiro, considerando aspectos logísticos, operacionais, ambientais e cibernéticos, com base em dados históricos e projeções estratégicas.

Estudar o impacto da ferramenta na instituição, propondo inclusive sua utilização como recurso didático em treinamentos e cursos de formação.

Simular cenários de risco híbrido, como ataques cibernéticos combinados com ações físicas, para testar a resiliência das estruturas militares.

1.5 ESTRUTURA DO CONTEÚDO ESCRITO

Este trabalho está organizado da seguinte forma para facilitar a compreensão e a navegação do leitor:

Introdução: apresenta o contexto do problema, a justificativa para a pesquisa, os objetivos gerais e específicos, e a estrutura do trabalho.

Fundamentação Teórica: aborda os conceitos relacionados à gestão de riscos, cibersegurança, sistemas de apoio à decisão e técnicas de simulação, estabelecendo a base teórica para melhoria da ferramenta.

Metodologia: detalha a abordagem de pesquisa utilizada, incluindo as etapas de desenvolvimento da ferramenta, as tecnologias empregadas, os métodos de coleta e análise de dados, e a validação da proposta.

Desenvolvimento da Ferramenta: descreve a arquitetura da ferramenta proposta, suas principais funcionalidades, os módulos desenvolvidos e os desafios técnicos superados durante o processo.

Resultados e Discussão: apresenta os resultados obtidos com a ferramenta, incluindo exemplos de simulações de cenários de risco cibernético no ambiente SC²EX, e discute as implicações dos resultados.

Conclusão e Trabalhos Futuros: sintetiza os principais achados da pesquisa, reitera as contribuições do estudo, aponta suas limitações e sugere direções para futuros aprimoramentos da ferramenta.

2 - DESENVOLVIMENTO

2.1 REVISÃO DA LITERATURA

A revisão da literatura abrange a gestão de riscos no contexto militar, sendo que a literatura existente destaca a crescente formalização da gestão de riscos nas Forças Armadas, inclusive no Exército Brasileiro (EB).

O EB possui diretrizes e manuais técnicos que regulam a política e a metodologia de gestão de riscos (ex: EB20-D-02.010 e EB20-MT-02.001), adaptando conceitos de normas internacionais (como ISO 31000) para o ambiente militar na ISO 27001, 27002 e 27005 por exemplo. Embora existam diretrizes gerais, há uma lacuna na literatura especializada sobre a aplicação de métodos

específicos e ferramentas de apoio para a gestão do risco em C². Além do contexto militar, a literatura referente a sistemas de C² nas operações militares, foca principalmente na infraestrutura de rede, operabilidade e influência de ameaças cibernéticas, em vez de ferramentas integradas de gestão de risco e simulação.

A literatura militar e civil descreve diversas ferramentas e métodos de análise de risco (FMEA, Análise Bow Tie, Matriz de Riscos, etc.). A análise de risco é reconhecida como uma ferramenta assessorial nos diferentes níveis decisórios.

A revisão sugere a necessidade de uma aplicação que integre as metodologias de gestão de risco existentes no EB com as capacidades de simulação de cenários (que hoje operam de forma separada) para fornecer uma análise de risco mais robusta e visual para os tomadores de decisão em tempo real ou no planejamento de operações. Em síntese a revisão da literatura indica que, embora a gestão de riscos e a simulação sejam práticas estabelecidas e regulamentadas no Exército, existe uma lacuna na integração dessas áreas. A criação de uma ferramenta específica que combine a gestão formal de riscos com a simulação de cenários operacionais e técnicos dos próprios sistemas C² representa uma área de pesquisa e desenvolvimento de grande relevância e ineditismo no contexto militar nacional.

2.2 MÉTODOS DE PESQUISA

Para conduzir um estudo da ferramenta de apoio à gestão e simulação de cenários de risco no SC²EX, a metodologia abrangerá o ciclo completo de engenharia de software, combinando abordagens qualitativas e quantitativas. O objetivo é assegurar que a ferramenta não só atenda às necessidades dos usuários, mas também se baseie em princípios robustos de gestão de riscos.

2.2.1 Desenho da pesquisa

O estudo seguirá um desenho de pesquisa aplicada, focado na criação de uma solução tecnológica para um problema prático. A abordagem será puramente qualitativa na fase inicial para entender as necessidades e desafios, e quantitativa na validação, para testar a eficácia e a usabilidade da ferramenta. A pesquisa pode ser dividida em quatro fases principais:

Fase de Análise: levantamento e análise detalhada dos requisitos do sistema e das necessidades dos usuários (gestores de risco).

Fase de Desenvolvimento: projeto e implementação da ferramenta de software para gestão de risco.
Fase de Validação: aplicação da ferramenta em cenários simulados para testar suas funcionalidades e avaliar a sua eficácia.

Fase de Avaliação: coleta de feedback dos usuários para medir a usabilidade e a satisfação com a ferramenta.

2.2.2 Amostra estudada

A amostra será composta por dois sistemas distintos, com o intuito de treinamento e avaliação do risco:

Sistema automatizado baseado em aplicação web utilizando FLASK e PYTHON para futuros riscos nos sistemas de C².

Sistema de simulação de cenários de riscos, baseado em aplicação web utilizando JSON e PYTHON.

2.2.3 Procedimentos de coleta de dados

Os dados serão coletados em diferentes etapas da pesquisa, utilizando uma combinação de técnicas qualitativas e quantitativas.

2.2.4 Fase de Análise (Coleta de Requisitos)

Observação participante: foram feitos testes de sessões da ferramenta de gestão de riscos para entender o fluxo de trabalho e as deficiências das atuais formas de calcular riscos e confeccionar matriz de risco.

Análise de Documentos: estudo de relatórios, manuais e procedimentos de gestão de riscos existentes para identificar dados relevantes e

modelos de análise utilizados.

Fase de Validação (Teste da Ferramenta)

Simulações de cenários: o grupo de trabalho, denominado usuários potenciais utilizará a ferramenta para simular cenários de risco predefinidos.

Aplicação: após as simulações, os participantes poderão utilizar o framework para mensurar a usabilidade, funcionalidade e eficácia da ferramenta.

2.2.6 Fase de Avaliação (Coleta de Feedback)

Grupo foco: reuniões do grupo do projeto para discutir as impressões gerais sobre a ferramenta, pontos fortes, fracos e sugestões de melhoria.

Testes de usabilidade: avaliação formal da interação dos usuários com a interface da ferramenta para identificar problemas de design e fluxos de trabalho.

2.2.7 Técnicas de análise

Análise de cenários: A funcionalidade da simulação de cenários foi testada usando dados simulados da realidade para verificar se os resultados da ferramenta correspondem aos eventos passados. Isso garantirá a confiabilidade dos modelos de risco.

Análise de riscos: Utilização de ferramentas como matriz de risco para avaliar as forças, fraquezas, oportunidades e ameaças da própria ferramenta desenvolvida.

Reprodutibilidade do estudo: Para garantir que outros pesquisadores possam reproduzir o estudo, os seguintes procedimentos serão detalhados na documentação final:

Manual de Instalação: descrição clara da metodologia de desenvolvimento de ferramenta utilizada, como JSON ou outra abordagem ágil, com as etapas de cada sprint e as entregas correspondentes.

Documentação da Ferramenta: depositório de código-fonte documentado, incluindo a arquitetura do sistema, os modelos de dados e a tecnologia utilizada (linguagens de programação, bancos de dados, etc.).

Manual de uso: Explicação passo a passo das técnicas de análise estatística e de conteúdo utilizadas, incluindo o software (por exemplo, JSON, Python) e os parâmetros de configuração, quando aplicável.

2.3 APRESENTAÇÃO E ANÁLISE DE DADOS

2.3.1 Contextualização: O SC²Ex e a gestão de riscos

O Sistema de Comando e Controle do Exército (SC²Ex) é o sistema estratégico do Exército Brasileiro responsável por comandar e controlar as operações militares. Sua eficácia depende da capacidade de tomar decisões rápidas e assertivas em ambientes complexos e incertos. O cenário de riscos no SC²Ex, ou seja, a gestão de riscos em um contexto militar, abrange diversos fatores:

Riscos operacionais: falhas de comunicação, equipamentos ou planejamento tático.

Riscos logísticos: interrupção na cadeia de suprimentos de equipamentos e materiais.

Riscos de inteligência: falhas na coleta ou análise de informações estratégicas.

Riscos externos: ameaças cibernéticas, sabotagem ou desastres naturais que afetam as operações.

2.3.2 Problema: Lacunas na gestão de riscos atual

A gestão de riscos tradicionalmente se baseia em análises manuais ou planilhas estáticas, que apresentam limitações significativas:

Reatividade: foco na resposta a eventos já ocorridos, e não na previsão e prevenção.

Complexidade: dificuldade em integrar grandes volumes de dados de diversas fontes

(terrestres, aéreas, navais) para uma visão completa do cenário.

Simulação limitada: ferramentas de simulação deficientes, que não permitem testar de forma eficaz os planos de contingência em múltiplos cenários.

Decisão lenta: a análise e comunicação de riscos demandam tempo, impactando a velocidade e a qualidade da tomada de decisão.

2.3.3 A solução: Ferramenta de apoio à gestão e simulação

O desenvolvimento de uma ferramenta especializada resolve as lacunas identificadas, oferecendo:
Interface intuitiva: visualização clara dos riscos em um painel interativo (dashboard).

Mecanismo de simulação: modelos que permitem testar o impacto de diferentes eventos de risco sobre as operações, como interrupções na cadeia de suprimentos ou ataques cibernéticos.

Recomendação de ações: sugestões de estratégias de mitigação com base nos resultados das simulações.

2.3.4 Análise de dados: Metodologia e fontes

Metodologia:

Identificação de riscos (qualitativa): uso de técnicas como Matriz SWOT e Análise Preliminar de Risco (APR) para listar ameaças e vulnerabilidades.

Análise de risco (quantitativa): avaliação da probabilidade de ocorrência e do impacto de cada risco.

Modelagem preditiva: uso de algoritmos de aprendizado de máquina para prever a probabilidade de eventos de risco com base em dados históricos.

Fontes de dados:

Dados históricos: registros de incidentes passados, falhas em equipamentos e interrupções logísticas.

Dados operacionais: informações em tempo real dos sistemas de comunicação e monitoramento do SC²Ex.

Dados de inteligência: relatórios sobre ameaças externas e potenciais pontos de vulnerabilidade.

Análise dos dados:

Identificação das principais ameaças: quais são os riscos mais prováveis e de maior impacto?

Padrões de vulnerabilidade: há padrões recorrentes que podem ser explorados por adversários?

2.4 ANÁLISE DA FERRAMENTA DE ANÁLISE DE RISCO

2.4.1 Justificativa para a Escolha do *Framework* Flask

O desenvolvimento da ferramenta de gestão de riscos requer uma plataforma que equilibre simplicidade, flexibilidade e capacidade de expansão. A escolha do *micro-framework* **Flask**, baseado em Python, justifica-se pelos seguintes fatores:

Leveza e Minimalismo: o Flask é um *micro-framework* que fornece apenas os componentes essenciais para o desenvolvimento *web*, como roteamento de URLs e renderização de templates. Isso permite que a arquitetura da aplicação seja construída de forma modular, adicionando apenas as bibliotecas e funcionalidades necessárias para a gestão de riscos, evitando a complexidade desnecessária de *frameworks* mais robustos.

Flexibilidade e Controle: a filosofia "One Drop at a time" do Flask oferece total controle sobre a arquitetura do projeto. Para um sistema de gestão de riscos, isso é crucial, pois permite a personalização exata dos fluxos de trabalho (identificação, análise, planejamento de respostas, monitoramento) sem as restrições de um *framework* "completo" (*full-stack*).

Ecossistema Python: o Python é amplamente utilizado e possui um vasto ecossistema de bibliotecas para análise de dados, aprendizado de máquina e integração de sistemas, que podem ser valiosas para futuras expansões da ferramenta, como a implementação de análises preditivas de riscos.

Curva de Aprendizagem Suave: a simplicidade do Flask facilita o desenvolvimento e a manutenção por parte da equipe, agilizando o processo de implementação.

2.4.2 Arquitetura Baseada em Flask

A arquitetura da ferramenta será baseada no padrão WSGI (Web Server Gateway Interface) que o Flask suporta nativamente, permitindo uma comunicação eficiente entre o servidor web e a aplicação. A estrutura adotará uma abordagem modular, separando as responsabilidades em diferentes camadas:

Camada de Apresentação (Frontend): utilizará tecnologias *web* padrão (HTML, CSS, JavaScript) para criar a interface do usuário, onde os gestores de risco irão interagir com a aplicação. O Flask facilitará a renderização de templates e a manipulação de requisições assíncronas para uma experiência de usuário fluida.

Camada de Aplicação (Backend): implementada em Python com Flask, será responsável por processar a lógica de negócios da gestão de riscos, como o cálculo da matriz de risco (probabilidade x impacto), registro de mitigações e monitoramento de status.

Camada de Dados: será utilizada uma solução de banco de dados relacional, gerenciada através de uma biblioteca ORM (Object-Relational Mapper) como o SQLAlchemy, que se integra perfeitamente ao Flask.

APIs RESTful: o Flask é excelente para a criação de APIs RESTful leves. A ferramenta utilizará esse recurso para permitir a troca de dados em formato JSON entre o frontend e o backend, e também para facilitar futuras integrações com outros sistemas corporativos (ex: sistemas de gerenciamento de projetos).

2.4.3 Segurança e Escalabilidade

A flexibilidade do Flask permite a integração de extensões robustas para segurança, como o Flask-WTF para formulários seguros e o Flask-Login para gerenciamento de sessões e autenticação. Em termos de escalabilidade, embora seja um micro-framework, o Flask pode ser dimensionado para aplicações complexas através de uma arquitetura modular e da implementação de boas práticas de engenharia de software.

Em suma, o Flask é a ferramenta ideal, fornecendo a base técnica necessária para construir uma ferramenta de gestão de riscos eficaz, personalizável e com potencial para crescimento futuro.

2.5 SIMULAÇÃO DE CENÁRIOS

O desenvolvimento da ferramenta Web baseada em Python e JSON de simulação de cenários de risco resultou em uma aplicação flexível e eficiente, projetada para auxiliar na tomada de decisões estratégicas e na análise quantitativa de riscos. A arquitetura modular e o uso de bibliotecas consagradas de Web foram fundamentais para superar os desafios técnicos inerentes à modelagem de incertezas.

2.5.1 Arquitetura da Ferramenta

A arquitetura da ferramenta é dividida em camadas lógicas e se baseia na integração eficiente de Web, como motor de processamento, e do JSON, como formato de armazenamento e intercâmbio de dados de configuração e cenários.

Camada de Interface (Front-end): uma interface de usuário, desenvolvida utilizando bibliotecas como streamlit ou dash permite a interação intuitiva, visualização de dados e configuração de parâmetros.

Camada de Lógica de Negócio (Back-end/Core): o coração da ferramenta, desenvolvido em Web, onde a lógica de simulação e os algoritmos de análise de risco são executados. Utiliza bibliotecas como pandas para manipulação de dados, numpfi para cálculos numéricos scipy ou statsmodel para estatística.

Camada de Dados (Persistência): utiliza

arquivos JSON para armazenar e carregar as configurações dos cenários de risco, parâmetros de distribuição de probabilidades e dados históricos. Isso facilita a portabilidade e a fácil modificação dos cenários sem alterar o código-fonte.

Camada de Visualização: módulos que utilizam plotly para gerar gráficos e visualizações dos resultados das simulações, como histogramas e distribuições de probabilidade.

2.5.2 Principais Funcionalidades

A ferramenta oferece um conjunto de funcionalidades destinadas a uma gestão de risco abrangente:

Modelagem de Cenários Flexível: permite a definição de múltiplos cenários de risco e suas respectivas probabilidades de ocorrência através de arquivos JSON de fácil configuração.

Simulação de Monte Carlo: implementa o método de Monte Carlo para simular milhares de iterações, gerando uma distribuição de resultados possíveis com base nas incertezas modeladas.

Análise Quantitativa de Risco: calcula métricas chave de risco, como VaR (Valor em Risco), Expected Shortfall, e desvio padrão, fornecendo uma base sólida para a tomada de decisão.

isualização e Relatórios: gera visualizações gráficas interativas e relatórios automatizados (em PDF ou CSV) dos resultados das simulações e métricas de risco.

2.5.3 Módulos Desenvolvidos

A ferramenta é composta por módulos interconectados que gerenciam diferentes aspectos da simulação:

app.py: Módulo responsável por carregar e validar os dados de entrada e configurações a artir dos arquivos JSON.

start.sh: Módulo que processa os resultados brutos da simulação e calcula as métricas de risco quantitativas.

utils.py: Módulo de funções utilitárias compartilhadas, como geradores de números aleatórios e manipuladores de erros.

2.5.4 Desafios Técnicos Superados

O desenvolvimento da ferramenta de simulção enfrentou alguns desafios técnicos:

Modelagem de Incerteza Complexa: traduzir cenários de risco do mundo real, muitas vezes subjetivos, em distribuições de probabilidade e estruturas JSON concretas exigiu um design cuidadoso da arquitetura de dados e validação extensiva.

Validação de Dados de Entrada: garantir que os arquivos JSON de configuração estivessem corretamente formatados e contivessem dados válidos foi um desafio, superado com a implementação de um robusto módulo de validação de esquemas JSON.

Integração e Visualização: integrar os resultados numéricos com bibliotecas de visualização interativa, garantindo uma experiência de usuário fluida e responsiva, exigiu expertise no uso dessas bibliotecas.

2.6 DISCUSSÃO DOS RESULTADOS

2.6.1 Desempenho da ferramenta e usabilidade

Validação da ferramenta: a discussão de resultados valida se a ferramenta de apoio conseguiu auxiliar na aprendizagem e na aplicação de prática relacionada ao gerenciamento de riscos em C².

Identificação de falhas: foi discutido se a ferramenta, durante seu desenvolvimento, permitiu à equipe identificar defeitos e pontos de melhoria, como a priorização das funcionalidades mais críticas.

isibilidade de funcionalidades: a análise dos resultados aborda se o sistema, mesmo em fase inicial, proporcionou visibilidade sobre a execução de funcionalidades críticas.

2.6.2 Aderência ao contexto específico (SC²Ex)

Identificação dos riscos: os resultados evidenciam como a ferramenta possibilitou

uma abordagem estruturada para identificar e classificar os riscos inerentes ao contexto militar.

Avaliação do impacto: a avaliação mostra como a ferramenta foi capaz de avaliar o impacto e a probabilidade de riscos específicos no âmbito de C^2, chegando à matriz de risco, gráficos de risco e sugerindo soluções e mitigação.

Análise de cenários: é crucial analisar a capacidade da ferramenta de simular diferentes cenários de risco, permitindo que os gestores de TIC possam testar estratégias contra eventos incertos e planejar ações preventivas.

2.6.3 Fortalecimento da resiliência e tomada de decisão

Aumento da resiliência: os resultados demonstram que a ferramenta contribui para aumentar a resiliência da instituição, preparando-a para eventos inesperados e permitindo a recuperação e continuidade das operações.

Melhora da tomada de decisão: uma discussão de resultados bem-sucedida evidencia como a ferramenta melhora a tomada de decisões ao permitir que os usuários simulem o resultado de alterações e avaliem as condições necessárias para atingir os objetivos.

2.6.4 Desafios e lições aprendidas

Integração e transparência de dados: a discussão aborda os desafios enfrentados, como a falta de uma visão centralizada dos riscos e ameaças, e como a ferramenta ajudou ou poderia ajudar a superar essa dificuldade.

Lições para o futuro: a análise dos resultados inclui as lições aprendidas com o desenvolvimento e a implementação da ferramenta, fornecendo insights para futuros projetos e aprimoramentos.

2.6.5 Contribuições e benefícios

Inovação tecnológica: a ferramenta incorpora tecnologias como aprendizado de máquina ou análise de dados avançada, a discussão explora como essas inovações beneficiam a gestão de riscos.

Vantagem competitiva: para o contexto militar, a discussão enfatiza como a ferramenta, ao aumentar a capacidade de recuperação e a continuidade das operações, se traduz em uma vantagem estratégica.

Planejamento e análise simplificados: a discussão realça como a ferramenta simplifica a análise e o planejamento complexo de C^2, tornando as informações mais acessíveis e fáceis de interpretar.

3 - CONCLUSÃO

Segundo De Bakker, Boonstra e Wortmann (2010) é possível situar a gestão de riscos dentro da tradição positivista, portanto pode-se esperar que seus resultados possam ser medidos e avaliados de forma objetiva e instrumental, no intuito de melhorar os resultados de alguma empresa ou projeto.

O projeto teve como objetivo principal desenvolver e propor uma ferramenta de gestão de riscos especificamente adaptada aos complexos e críticos Sistemas de Comando e Controle (C^2) do Exército Brasileiro.

A premissa central da pesquisa foi sobre uma ferramenta digital poder otimizar a identificação, análise, mitigação e monitoramento contínuo dos riscos operacionais e de segurança da informação em sistemas C^2 do EB, garantindo a prontidão e a eficácia das operações militares.

Os resultados da pesquisa demonstram que a gestão de riscos, embora já regulamentada no âmbito do Exército, carecia de uma solução tecnológica integrada e dedicada para os sistemas, que possuem características e vulnerabilidades únicas.

A ferramenta proposta, baseada nas diretrizes da ISO 27001, 27002 e 27005 e nas normas internas do EB (como o EB20-MT-02.001), permitiu a identificação de riscos críticos que vão desde falhas de comunicação e segurança cibernética até erros humanos na tomada de decisão em cenários de alta pressão. A utilização de uma matriz de riscos e controles integrada na ferramenta facilitou a priorização visual dos riscos mais relevantes

("extremos"), orientando o tratamento prioritário e respostas tempestivas por parte dos gestores. Verificou-se que a automação de etapas como a coleta de dados e o monitoramento contínuo (Etapa 5 do gerenciamento de riscos) demonstrou potencial para aumentar significativamente a eficiência e a precisão do processo em comparação com métodos manuais ou fragmentados.

Do ponto de vista prático, a principal implicação deste estudo é a capacidade de fornecer aos comandantes e suas equipes uma visão holística e em tempo real do perfil de risco de seus sistemas C². Isso permite uma tomada de decisão mais informada e resiliente, aumentando a probabilidade de sucesso das missões e a proteção dos recursos e vidas envolvidos.

A ferramenta contribui diretamente para a "geração de poder de combate", ao mitigar ameaças que poderiam comprometer a capacidade operacional da Força Terrestre.

Teoricamente, a pesquisa contribui para a literatura ao propor um modelo híbrido de gestão de riscos que adapta metodologias civis (ISO 31000) a um ambiente militar específico, validando a aplicabilidade de princípios universais de gestão de riscos em contextos de segurança e defesa.

Demonstrou-se que a gestão de riscos deve ser um processo dinâmico, adaptável e integrado à governança e à administração do Exército. Apesar dos resultados promissores, o estudo possui limitações. A ferramenta proposta foi desenvolvida em um ambiente de simulação e com dados parciais, onde o grupo do projeto possuía um grau de conhecimento limitado sobre designer web, a pesquisa se limitou aos próprios integrantes do grupo, e a eficácia plena depende de uma implementação e de um treinamento adequado dos usuários finais.

Além disso, a natureza em constante evolução das ameaças cibernéticas exige atualizações frequentes da base de dados de riscos da ferramenta. Com base nos resultados e limitações, aponta-se recomendações práticas para trabalhos futuros.

3.1 Trabalhos Futuros:

3.1.1 Implementação Piloto: recomenda-se a implementação da ferramenta em uma Organização Militar (OM) com autonomia administrativa e que possua um sistema C2 ativo, para validação em um cenário real.

3.1.2 Treinamento Contínuo: o sucesso da ferramenta depende crucialmente da capacitação dos operadores e gestores de risco, que devem ser treinados para identificar eventos (riscos e vulnerabilidades) e utilizar a matriz de riscos de forma eficaz.

3.1.3 Cultura de Segurança: reforçar a cultura de gestão de riscos e segurança em todos os níveis da hierarquia militar, promovendo atitudes e comportamentos seguros.

Em suma, este trabalho "fecha o círculo argumentativo", confirmando que a criação de uma ferramenta de gestão de riscos dedicada é um passo fundamental para modernizar e fortalecer os sistemas de C2 do Exército Brasileiro. A pesquisa não apenas respondeu à questão central, mas também pavimentou o caminho para o avanço do conhecimento na área de gestão de riscos em ambientes militares, oferecendo um arcabouço sólido para futuras inovações e garantindo que o Exército esteja preparado para os desafios.

ABSTRACT

The project consists of creating a web-based tool to support risk management and simulation for command and control systems (C² systems). The main objective is to create an agile solution that assists in the identification, analysis, and prediction of risks in critical scenarios, optimizing decision-making and the planning of strategic responses. The project focuses on key components such as the analysis of user requirements for C² systems, integrating simulation, monitoring, and scenario management functionalities. Specific objectives include increasing system resilience, improving incident response capabilities, and minimizing the negative impacts of adverse events. The tool will integrate monitoring, simulation, and scenario management functionalities to ensure the resilience and efficiency of C² systems in adverse situations and will have an intuitive management interface, aiming to contribute to the security and efficiency of operations, providing a more adaptable and robust risk management environment.

REFERÊNCIAS

BAKKER, Karel de; BOONSTRA, Albert; WORTMANN, Hans. Does risk management contribute to IT project success? A meta-analysis of empirical evidence. International Journal of Project Management, Oxford: Elsevier, v. 28, n. 5, p. 493-503, July 2010.

ABNT. NBR ISO 31010:2011 – Gestão de Riscos: Técnicas para o processo de avaliação de riscos. Associação Brasileira de Normas Técnicas, 2011.

BRASIL. Ministério da Defesa. MD31-A-MA-03A: Doutrina para o Sistema Militar de Comando e Controle (SC²Ex). 3. ed. Brasília, DF, 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000: Gestão de riscos – Diretrizes. Rio de Janeiro, 2018.

BRASIL. Comando do Exército. EB20-MT-02.001: Manual Técnico da Metodologia de Gestão de Riscos do Exército. Brasília, DF: Estado-Maior do Exército, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR IEC 31010: Gestão de riscos – Técnicas para o processo de avaliação de riscos. Rio de Janeiro, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001: segurança da informação, segurança cibernética e proteção à privacidade: sistemas de gestão da segurança da informação. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 27002: Tecnologia da informação — Técnicas de segurança — Controles de segurança da informação. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 27005: Orientações para a gestão de riscos de segurança da informação. Rio de Janeiro, 2023. Rio de Janeiro, 2022.