UNIFACCAMP
Centro Universitário Campo Limpo Paulista

Método para Avaliação de Frameworks de Gestão de Risco Cibernético

Matheus de Andrade

Abril / 2025

Dissertação de Mestrado em Ciência da Computação

Método para Avaliação de Frameworks de Gestão de Risco Cibernético

Esse documento corresponde à Dissertação apresentada à Banca Examinadora no curso de Mestrado em Ciência da Computação da UNIFACCAMP - Centro Universitário Campo Limpo Paulista.

Campo Limpo Paulista, 13 de maio de 2025.

Matheus de Andrade

Prof. Dr. Ferrucio de Franco Rosa (Orientador)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

Ficha catalográfica elaborada pela

Biblioteca Central da Unifaccamp

A568m

Andrade, Matheus de

Método para avaliação de *frameworks* de gestão de risco cibernético / Matheus de Andrade. Campo Limpo Paulista, SP: Unifaccamp, 2025.
85 f.: il.

Orientador: Prof. Dr. Ferrucio de Franco Rosa
Coorientador: Prof. Dr. Amândio Ferreira Balcão Filho

Dissertação (Programa de Mestrado Profissional em Ciência da Computação) – Centro Universitário Campo Limpo Paulista – Unifaccamp.

1. Segurança cibernética. 2. Gestão de risco. 3. *Frameworks*. 4. Maturidade. 5. Análise comparativa. 6. Fator humano. 7. Conscientização. I. Rosa, Ferrucio de Franco. II. Balcão Fº., Amândio Ferreira. III. Centro Universitário Campo Limpo Paulista. IV. Título.

CDD - 005.75

Agradecimentos

Em primeiro lugar, agradeço a Deus por sua força, inspiração e resiliência ao longo desta jornada.

À minha família, que é a base de tudo em minha vida. Ao meu pai, Valdecir, minha mais profunda gratidão e admiração. Seu exemplo de dedicação, trabalho árduo e caráter moldou quem sou hoje. Seu apoio incondicional, seus conselhos sábios e sua fé inabalável em meu potencial foram fundamentais para que eu chegasse até aqui. Cada conquista minha carrega um pouco do seu esforço.

À minha mãe, Maria, e à minha noiva, Carolaynne, minha eterna gratidão por estarem ao meu lado em cada etapa desta caminhada. Vocês foram meu porto seguro, oferecendo compreensão, incentivo e amor mesmo nos momentos mais difíceis. Esta vitória é nossa.

Ao professor Ferrucio de Franco Rosa, meu orientador e mentor, por acreditar neste projeto desde o início. Sua dedicação, paciência e orientação foram essenciais para a realização deste trabalho. Sou grato por seu apoio, incentivo e comprometimento.

Agradeço aos professores Amândio Ferreira Balcão Filho e Rogerio Winter por suas contribuições essenciais no desenvolvimento desta dissertação e na construção da ideia central. Suas análises e sugestões foram fundamentais para tornar este trabalho mais sólido e consistente.

Não poderia deixar de prestar uma homenagem especial à minha querida tia Sil. Deus a chamou para junto Dele durante essa jornada, mas sua lembrança e seu exemplo de força, amor e generosidade permanecem vivos em meu coração.

Um agradecimento especial ao meu amigo Victor Kelven, que esteve ao meu lado em muitos momentos desafiadores, passando horas em chamadas comigo, ajudando a resolver problemas e oferecendo apoio técnico e emocional. Sua parceria e dedicação foram fundamentais para que eu conseguisse superar as etapas mais difíceis deste projeto.

Por fim quero agradecer ao colega Robson Bosse pela ajuda e apoio ao longo desta jornada e agradeço sinceramente a todos que, de alguma forma, fizeram parte desta jornada. Seu apoio e incentivo foram essenciais. Minha eterna gratidão!

Resumo.*A gestão de risco cibernético é uma preocupação central para instituições de todos os setores, impulsionada pelo aumento exponencial de ameaças digitais, como ransomware, phishing e ataques de negação de serviço. Em um ambiente cada vez mais digital e interconectado, proteger os ativos digitais e garantir a continuidade dos negócios é um desafio constante. Nesse contexto, frameworks de gestão de risco cibernético surgem como ferramentas fundamentais para orientar as organizações na identificação, avaliação e mitigação de ameaças. Esses frameworks oferecem diretrizes estruturadas para implementar práticas robustas de segurança da informação, garantindo que as organizações estejam preparadas para enfrentar riscos cibernéticos de forma eficaz. Contudo, a variedade de frameworks disponíveis, cada um com suas particularidades, gera um desafio significativo na seleção da abordagem mais apropriada para cada organização. Este trabalho propõe o método Evaluating Cyber Risk Frameworks (e-CRF), uma abordagem sistemática para avaliação de frameworks de gestão de risco cibernético. Integrando critérios como abrangência, adaptabilidade, eficácia e custo-benefício, o e-CRF visa padronizar o processo de avaliação e facilitar a escolha das melhores opções para atender às necessidades organizacionais específicas. Para validar o método, foi desenvolvido um protótipo de software que permite a avaliação prática dos frameworks. Esse protótipo foi testado com especialistas em segurança da informação, que utilizaram a plataforma para atribuir pesos e notas aos critérios definidos. Os resultados demonstram que o e-CRF facilita a padronização do processo de avaliação, destacando diferenças de desempenho e fornecendo insights valiosos para a seleção e melhoria contínua de frameworks. O principal objetivo deste estudo é fornecer uma abordagem prática para avaliar frameworks de gestão de risco cibernético, auxiliando as organizações na tomada de decisões informadas. Além disso, o trabalho contribui para a literatura acadêmica ao propor uma metodologia fundamentada em critérios bem definidos e aplicável a diferentes contextos organizacionais.*

Palavras-chaves*: Segurança cibernética, gestão de risco, frameworks, maturidade, análise comparativa, fator humano, conscientização.*

Abstract.*Cyber risk management has become a central concern for organizations across all sectors, driven by the exponential increase in digital threats such as ransomware, phishing, and denial-of-service attacks. In an increasingly digital and interconnected environment, protecting digital assets and ensuring business continuity is a constant challenge. In this context, cyber risk management frameworks emerge as fundamental tools to guide organizations in identifying, assessing, and mitigating threats. These frameworks provide structured guidelines to implement robust information security practices, ensuring that organizations are prepared to effectively address cyber risks. However, the variety of available frameworks, each with its specific characteristics, presents a significant challenge in selecting the most appropriate approach for each organization. This study proposes the Evaluating Cyber Risk Frameworks (e-CRF) method, a systematic approach to the evaluation of cyber risk management frameworks. By integrating criteria such as comprehensiveness, adaptability, effectiveness, and cost-benefit, the e-CRF aims to standardize the evaluation process and facilitate the selection of the best options to meet specific organizational needs. To validate the method, a software prototype was developed, enabling practical evaluation of selected frameworks. This prototype was tested by cybersecurity specialists who used the platform to assign weights and scores to the defined criteria. The results demonstrate that the e-CRF simplifies the evaluation process, highlights significant performance differences, and provides valuable insights for the selection and continuous improvement of security frameworks. The primary objective of this study is to offer a practical approach to evaluating cyber risk management frameworks, assisting organizations in making informed decisions. Furthermore, the study contributes to academic literature by proposing an evaluation methodology based on well-defined criteria applicable to various organizational contexts.*

Keywords*: Cybersecurity, risk management, frameworks, maturity, comparative analysis, human factor, awareness..*

Sumário

Glossário

API *Application Programming Interface*

CISO *Chief Information Security Officer*

CIS *Center for Internet Security*

COBIT Control Objectives for Information and Related Technologies

DoS/DDoS *Denial of Service / Distributed Denial of Service, ataques para sobrecarregar sistemas*

ETL *Extract, Transform and Load*

FAIR Factor Analysis of Information Risk

HCI International Conference on Human-Computer Interaction

HTTPS *Hypertext Transfer Protocol Secure*

IDS *Intrusion Detection System*

IES Instituições de Ensino Superior

INPI Instituto Nacional da Propriedade Industrial

IoT *Internet of Things*

ISO/IEC 27001 *International Organization for Standardization / International Electrotechnical Commission 27001*

ITNG *International Conference on Information Technology*

LGPD Lei Geral de Proteção de Dados

MFA *Multi-Factor Authentication*

NIST CSF *National Institute of Standards and Technology Cybersecurity Framework*

NoSQL *Not Only SQL*

OCTAVE *Operationally Critical Threat, Asset, and Vulnerability Evaluation*

PCI DSS *Payment Card Industry Data Security Standard*

SIEM	*Security Information and Event Management*
SIMS	*Strategic Information Monitoring System*
SQL	*Structured Query Language*
VM	*Virtual Machine*
VPN	*Virtual Private Network*

Lista de Tabelas

Lista de Figuras

1. Introdução

A gestão de risco cibernético tornou-se uma preocupação central para organizações de todos os setores, impulsionada pelo aumento exponencial de ameaças digitais, como ransomware, phishing e ataques de negação de serviço. Com a transformação digital acelerada, proteger os ativos digitais e garantir a continuidade dos negócios tornou-se um desafio estratégico para a sustentabilidade organizacional (Giuca et al.; 2021).

Nesse cenário, frameworks de gestão de risco cibernético surgem como ferramentas fundamentais para auxiliar as organizações na identificação, avaliação e mitigação de ameaças. No contexto deste trabalho, o termo Framework representa um conjunto de itens de avaliação ou diretrizes operacionais para análise e tomada de decisão. São exemplos de frameworks: padrões e normas técnicas (e.g., ISO/IEC 27001, NIST Cybersecurity Framework, COBIT), guias para avaliação (e.g., FAIR – Factor Analysis of Information Risk, OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation) e checklists (e.g., CIS Controls, PCI DSS – Payment Card Industry Data Security Standard). Esses frameworks fornecem diretrizes estruturadas para a implementação de práticas robustas de segurança da informação, garantindo que as empresas estejam preparadas para enfrentar riscos cibernéticos de forma eficaz. Entretanto, a diversidade de frameworks disponíveis no mercado, cada um com particularidades específicas, apresenta desafios complexos no momento da escolha do modelo mais adequado para cada organização (Palia et al.; 2021).

Diante dessa diversidade, torna-se essencial contar com um método que permita avaliar e comparar esses frameworks de maneira padronizada e objetiva. Este trabalho propõe o método *Evaluating Cyber Risk Frameworks* (e-CRF), uma abordagem sistemática e colaborativa que visa facilitar o processo de avaliação de frameworks de gestão de risco cibernético. O e-CRF integra critérios como abrangência, adaptabilidade, eficácia, custo-benefício e conformidade regulatória, oferecendo um mecanismo consistente para identificar as melhores opções disponíveis no mercado.

A proposta do e-CRF vai além da simples avaliação. Para garantir sua aplicabilidade prática, foi desenvolvido um protótipo de software que possibilita a realização de testes por especialistas em segurança da informação. Esse protótipo permite que os avaliadores

atribuam pesos e notas aos critérios estabelecidos, assegurando uma análise mais completa e personalizada. Os resultados obtidos até o momento demonstram que o e-CRF não apenas simplifica a avaliação dos frameworks, como também destaca diferenças significativas de desempenho, fornecendo insights valiosos para a tomada de decisão e melhoria contínua das práticas de segurança cibernética.

O principal objetivo deste estudo é oferecer uma abordagem robusta e prática para a avaliação de frameworks de gestão de risco cibernético, auxiliando as organizações a escolher soluções alinhadas às suas necessidades específicas e contextos operacionais. Além disso, o trabalho contribui para a literatura acadêmica ao propor uma metodologia fundamentada em critérios bem definidos, aplicável a diferentes setores e tamanhos de organizações, preenchendo lacunas existentes nos estudos anteriores.

Em suma, a pesquisa busca suprir a necessidade de um processo de avaliação mais objetivo e padronizado, contribuindo para fortalecer a resiliência das organizações frente às ameaças digitais em constante evolução.

1.1. Questão de Pesquisa, Objetivos e Contribuições

Este trabalho busca responder à seguinte **Questão de Pesquisa**: *Como aprimorar o processo de avaliação de frameworks de gestão de risco cibernético, considerando critérios como abrangência, eficácia e custo-benefício, para apoiar a tomada de decisões organizacionais de forma segura e eficiente?*

O **Objetivo Principal** deste estudo é desenvolver e validar o método *Evaluating Cyber Risk Frameworks* (e-CRF), que oferece uma abordagem sistemática e padronizada para a avaliação de frameworks de gestão de risco cibernético. A proposta visa auxiliar as organizações na identificação de frameworks mais adequados às suas necessidades específicas, melhorando a segurança cibernética e a continuidade dos negócios. Diferentemente de abordagens existentes, o e-CRF prioriza critérios customizáveis que podem ser ajustados conforme o contexto organizacional, garantindo maior flexibilidade e precisão na avaliação.

Antes de apresentar os objetivos específicos, é importante destacar que o e-CRF foi projetado para lidar com desafios recorrentes, como a dificuldade em comparar frameworks distintos devido à falta de uma metodologia unificada. A seguir, são descritos os principais

objetivos específicos deste trabalho.

Como **Objetivos Específicos**, destacam-se:

1. Realizar uma revisão sistemática da literatura para identificar os principais critérios utilizados na avaliação de frameworks de gestão de risco cibernético.
2. Propor um método que padronize a avaliação de frameworks, facilitando a comparação entre diferentes opções e destacando suas vantagens e limitações.
3. Desenvolver um protótipo de software que implemente o método e-CRF, oferecendo uma ferramenta prática para os avaliadores aplicarem as métricas propostas.
4. Validar o método por meio de um estudo de caso em um contexto organizacional real, utilizando dados concretos para analisar a eficácia do e-CRF na tomada de decisões.

As principais **Contribuições** técnico-científicas deste trabalho incluem:

- Desenvolvimento de um método sistemático de avaliação de frameworks de gestão de risco cibernético, aplicável a diferentes contextos organizacionais. O método destaca-se por permitir a atribuição de pesos personalizados a critérios específicos, garantindo uma análise adaptada às necessidades de cada organização.
- Criação de um protótipo de software que implementa o método e-CRF, facilitando a aplicação prática das avaliações. O protótipo inclui funcionalidades que permitem ajustes de critérios, personalização de pesos e geração de relatórios comparativos.
- Realização de um estudo de caso que demonstra a eficácia do método em melhorar a tomada de decisões relacionadas à segurança cibernética. O estudo evidencia como o uso do e-CRF pode otimizar a escolha de frameworks, garantindo maior eficiência na gestão de riscos.

1.2. Estrutura da Dissertação

A presente dissertação está estruturada em sete capítulos, organizados de forma a proporcionar uma compreensão clara e progressiva do tema abordado, desde a contextualização teórica até a apresentação dos resultados e considerações finais.

- **Capítulo 1** apresenta a introdução geral do trabalho, incluindo a motivação para a pesquisa, a questão de pesquisa, os objetivos principais e específicos, e

as contribuições esperadas. Também são descritos os principais desafios que motivaram a criação do método *Evaluating Cyber Risk Frameworks* (e-CRF).

- **Capítulo 2 -** é dedicado ao referencial teórico, abordando os conceitos fundamentais relacionados à gestão de risco cibernético, frameworks de avaliação, segurança da informação, e metodologias de análise de risco. Este capítulo fornece a base teórica necessária para o desenvolvimento do método proposto.
- **Capítulo 3 -** apresenta a revisão da literatura e os trabalhos relacionados. Este capítulo explora os principais estudos sobre frameworks de gestão de risco cibernético, destacando as lacunas existentes e as oportunidades para melhorias no processo de avaliação. A análise sistemática realizada contribui para a fundamentação do método e-CRF.
- **Capítulo 4 -** Este capítulo apresenta uma descrição detalhada do método e-CRF, abordando sua fundamentação teórica, os critérios utilizados para a avaliação de frameworks de gestão de risco cibernético e a justificativa para sua adoção. Além disso, são fornecidos exemplos práticos de aplicação do método, ilustrando o processo de cálculo e interpretação dos resultados, demonstrando sua aplicabilidade em diferentes contextos organizacionais.
- **Capítulo 5 -** este capítulo apresenta em detalhes as funcionalidades da aplicação desenvolvida para validar o método proposto. São descritas as principais características da ferramenta, incluindo sua interface, os módulos implementados e a forma como cada funcionalidade contribui para a avaliação dos frameworks de gestão de risco cibernético.
- **Capítulo 6 -** apresenta o estudo de caso realizado para validar o método e-CRF. Este capítulo contextualiza o ambiente organizacional onde o método foi aplicado, descreve a metodologia utilizada e analisa os resultados obtidos, destacando os benefícios e desafios identificados durante a implementação.
- **Capítulo 7 -** traz a discussão e análise sobre os resultados do estudo de caso. São apresentados insights obtidos a partir dos relatórios gerados pela aplicação, além de considerações sobre a eficácia do método na prática. Também são discutidos os principais desafios enfrentados durante o processo de avaliação.
- **Capítulo 8 -** apresenta as conclusões do trabalho, incluindo as limitações identifi-

cadas, propostas para trabalhos futuros e os resultados da pesquisa. Este capítulo reforça a relevância do método e-CRF e da aplicação desenvolvida, destacando sua contribuição para a área de gestão de risco cibernético.

A dissertação inclui ainda anexos com informações complementares, como detalhes técnicos sobre a configuração da aplicação e exemplos de relatórios gerados. Essas informações são fornecidas para auxiliar outros pesquisadores e profissionais interessados em aplicar o método e-CRF em seus contextos organizacionais.

2. Referencial Teórico

O referencial teórico é fundamental para estabelecer a base conceitual que orienta o desenvolvimento desta pesquisa, fornecendo o contexto necessário para a compreensão dos conceitos-chave relacionados à gestão de risco cibernético, frameworks de avaliação, segurança da informação e metodologias de análise de risco. Este capítulo busca explorar as principais teorias, definições e estudos que sustentam o método proposto, o *Evaluating Cyber Risk Frameworks* (e-CRF).

2.1. Gestão de Risco Cibernético

A gestão de risco cibernético refere-se ao processo contínuo de identificação, avaliação e mitigação de riscos associados ao uso de tecnologias digitais. Com a crescente digitalização das operações organizacionais, as ameaças cibernéticas tornaram-se um risco crítico para empresas de todos os setores. Segundo Giuca et al. (2021), as organizações precisam adotar práticas robustas de segurança da informação para proteger seus ativos digitais e garantir a continuidade dos negócios.

Entre as principais ameaças estão ataques de ransomware, phishing e negação de serviço, que podem comprometer dados sensíveis e interromper operações críticas. Para mitigar esses riscos, as organizações recorrem a frameworks de gestão de risco que oferecem diretrizes para implementar políticas de segurança e controles adequados.

2.2. Histórico da Gestão de Risco Cibernético

A gestão de risco cibernético evoluiu significativamente nas últimas décadas, acompanhando o avanço da tecnologia e o aumento das ameaças digitais. Nos anos 1990, as primeiras práticas de segurança da informação focavam na proteção de redes internas e sistemas corporativos. Com a popularização da internet, novos desafios surgiram, exigindo uma abordagem mais ampla e estratégica.

Na década de 2000, surgiram frameworks como o ISO/IEC 27001 e o NIST Cybersecurity Framework, que passaram a fornecer diretrizes estruturadas para a gestão de risco. Nos anos mais recentes, a evolução das ameaças cibernéticas, como ransomware e ataques de phishing avançados, levou ao desenvolvimento de frameworks dinâmicos que priorizam a resiliência organizacional.

Atualmente, a gestão de risco cibernético é vista como uma função crítica para a continuidade dos negócios, e frameworks como o e-CRF buscam padronizar a avaliação de diferentes soluções para garantir uma segurança mais eficaz.

2.3. Frameworks de Gestão de Risco

Os frameworks de gestão de risco cibernético são estruturas que auxiliam as organizações a identificar, avaliar e mitigar ameaças digitais. Alguns dos frameworks mais utilizados incluem:

- **NIST Cybersecurity Framework**: Desenvolvido pelo National Institute of Standards and Technology, oferece diretrizes para proteger ativos digitais por meio de cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar (Dias et al.; 2022; Moreira et al.; 2021).
- **ISO/IEC 27001**: Um padrão internacional que estabelece requisitos para sistemas de gestão de segurança da informação, com foco em políticas e procedimentos que garantem a proteção de dados sensíveis (Dias et al.; 2022; Valle; 2021).
- **COBIT**: Um framework que ajuda as organizações a alinhar seus objetivos de segurança com suas estratégias de negócios, fornecendo boas práticas para governança e gestão de TI (Noor & Ghazanfar; 2016).

Esses frameworks oferecem abordagens estruturadas para a gestão de risco cibernético, mas também apresentam desafios relacionados à sua implementação e adaptação a diferentes contextos organizacionais. O método e-CRF visa padronizar o processo de avaliação desses frameworks, facilitando a escolha da abordagem mais adequada para cada organização.

2.4. Segurança da Informação

A segurança da informação é um dos pilares da gestão de risco cibernético, abrangendo políticas, processos e tecnologias destinadas a proteger dados contra acessos não autorizados, alterações ou destruição. Segundo Saksonov et al. (2021), a segurança da informação deve garantir a confidencialidade, integridade e disponibilidade dos dados.

Os principais componentes da segurança da informação incluem:

- **Confidencialidade**: Garantir que apenas pessoas autorizadas tenham acesso às informações.
- **Integridade**: Garantir que os dados permaneçam precisos e não sejam alterados de forma não autorizada.
- **Disponibilidade**: Garantir que as informações estejam acessíveis sempre que necessário.

A implementação de frameworks de gestão de risco é uma das formas mais eficazes de garantir a segurança da informação nas organizações. Esses frameworks fornecem diretrizes para identificar vulnerabilidades, implementar controles e monitorar a eficácia das medidas de segurança.

2.5. Métodos de Análise de Risco

Os métodos de análise de risco (Zhao et al.; 2021) são técnicas utilizadas para identificar, avaliar e mitigar riscos em diferentes contextos, como segurança da informação, projetos, saúde e segurança ocupacional, e processos industriais. Esses métodos (de Paula et al.; 2019) auxiliam as organizações a compreender as ameaças potenciais e tomar decisões informadas para minimizar impactos negativos.

2.5.1. Classificação dos Métodos

Os métodos de análise de risco podem ser classificados em:

- **Análise Qualitativa:** Avalia os riscos com base em categorias descritivas, como baixo, médio e alto. É subjetiva e baseada em experiências e julgamentos de especialistas.
- **Análise Quantitativa:** Usa dados numéricos e estatísticos para calcular a probabilidade e o impacto dos riscos, proporcionando uma visão mais precisa e objetiva.

2.5.2. Métodos Qualitativos Comuns

- **Brainstorming:** Técnica colaborativa para identificar riscos potenciais com base na experiência da equipe.

- **SWIFT (Structured What-If Technique):** Analisa cenários hipotéticos baseados em perguntas "E se?" para explorar riscos potenciais e suas consequências.
- **Análise SWOT:** Avalia forças, fraquezas, oportunidades e ameaças, ajudando na compreensão dos riscos internos e externos.
- **Checklists e Entrevistas:** Utilizam listas de verificação padronizadas e entrevistas com stakeholders para identificar riscos.

2.5.3. Métodos Quantitativos Comuns

- **Análise de Árvores de Falhas (FTA):** Identifica a relação entre falhas e eventos que podem levar a um incidente crítico.
- **FMEA (Failure Modes and Effects Analysis):** Avalia potenciais falhas em um sistema ou processo, determinando sua gravidade, frequência e detectabilidade.
- **Simulação de Monte Carlo:** Usa distribuições de probabilidade para modelar incertezas e prever resultados de risco.
- **Matriz de Riscos:** Combina a probabilidade de ocorrência e o impacto dos riscos, classificando-os em categorias.
- **Análise Custo-Benefício (CBA):** Compara os custos de mitigação de riscos com os benefícios potenciais de sua redução.

2.5.4. Métodos Híbridos

Alguns métodos combinam aspectos qualitativos e quantitativos para fornecer uma visão mais equilibrada. Exemplos incluem:

- **ISO 31000:** Abordagem estruturada para a gestão de riscos organizacionais.
- **NIST Risk Management Framework (RMF):** Usado principalmente na segurança da informação para avaliar e mitigar riscos em sistemas de TI.

2.5.5. Fatores de Escolha do Método

A escolha do método de análise de risco depende de fatores como:

- Complexidade do sistema ou processo a ser analisado;

- Disponibilidade de dados históricos e quantitativos;
- Nível de experiência da equipe envolvida;
- Regulamentações e padrões aplicáveis ao setor (ex.: ISO 27001, NIST, COSO).

2.6. Fatores Humanos e Culturais na Segurança da Informação

A gestão de risco cibernético não se limita apenas a soluções tecnológicas; ela também envolve fatores humanos e culturais (AlHogail & Almalki; 2015). O comportamento dos colaboradores pode ser tanto uma barreira quanto uma defesa eficaz contra ameaças cibernéticas.

Campanhas de conscientização contínua, treinamentos regulares e políticas de boas práticas são essenciais para garantir que os colaboradores estejam cientes das ameaças e saibam como reagir a elas. Além disso, uma cultura organizacional que valorize a segurança da informação pode reduzir significativamente os riscos associados a erros humanos.

2.7. Ferramentas Tecnológicas de Apoio à Gestão de Risco

Diversas ferramentas tecnológicas podem ser utilizadas para apoiar a gestão de risco cibernético (Knowles et al.; 2015). Essas ferramentas automatizam processos de identificação, monitoramento e resposta a ameaças, facilitando a implementação de frameworks de segurança. Algumas das ferramentas mais comuns incluem:

- **Sistemas de Detecção de Intrusão (IDS)**: Identificam atividades suspeitas em redes e sistemas, alertando os administradores sobre possíveis ataques.
- **Firewalls de Última Geração**: Controlam o tráfego de rede com base em regras de segurança pré-definidas, protegendo contra acessos não autorizados.
- **Plataformas de Gestão de Identidades e Acessos (IAM)**: Garantem que apenas usuários autorizados tenham acesso a sistemas e dados sensíveis.

Essas ferramentas são fundamentais para garantir que as práticas de segurança sejam eficazes e estejam alinhadas com os frameworks adotados.

3. Revisão da Literatura e Trabalhos Relacionados

Uma revisão sistemática de literatura foi conduzida abrangendo a análise criteriosa de 30 artigos. Esta revisão de literatura teve como objetivo principal responder a seguinte questão de busca: *"Quais métodos e frameworks recentes têm sido propostos para avaliar e apoiar a gestão de riscos cibernéticos, considerando critérios como eficácia, custo-benefício e conformidade com normas regulatórias"*

3.1. Metodologia

A metodologia utilizada na revisão da literatura foi baseada nas diretrizes propostas por Kitchenham (2004). Esta revisão busca destacar os principais desafios e oportunidades associados a frameworks de gestão de risco cibernético. Foram realizadas buscas em três bases de dados científicas bem conhecidas da área de Computação (IEEE Xplore[1], ACM Digital Library[2] e Springer Link[3]).

A escolha dessas bases se justifica pelos seguintes motivos:

1. Reputação e Credibilidade: Essas plataformas são reconhecidas globalmente por sua contribuição significativa à pesquisa em Computação e áreas relacionadas. A qualidade dos artigos publicados nelas é rigorosamente avaliada, o que aumenta a confiabilidade das informações obtidas.
2. Diversidade de Conteúdo: Cada uma dessas bases de dados abriga uma variedade de publicações, incluindo artigos de conferências, periódicos e relatórios técnicos. Essa diversidade permite uma exploração abrangente dos desafios e soluções propostas na literatura sobre a questão pesquisada.
3. Foco em Inovação e Tendências: As três bases são conhecidas por incluir pesquisas de ponta que abordam as últimas inovações e tendências em tecnologia e métodos. Isso é fundamental para identificar não apenas os problemas existentes, mas também as novas abordagens e práticas recomendadas.

A combinação dessas três bases de dados possibilita uma revisão da literatura robusta e bem fundamentada.

[1]https://ieeexplore.ieee.org/Xplore/home.jsp

[2]https://dl.acm.org/

[3]https://link.springer.com/

O período de buscas estabelecido foi de 9 anos (2016 a 2024) e a seguinte string de busca geral foi utilizada, ajustando a sintaxe a cada base de dados: *”(”All Metadata”: cyber risk management) AND (”All Metadata”: frameworks) AND (”All Metadata”: evaluation) AND (”All Metadata”: method)”*.

A execução da busca considerou todos os artigos retornados. A busca inicial obteve um total de 210 artigos, nas 3 bases de pesquisas

Os critérios de inclusão e exclusão utilizados (Tabela 1) foram definidos durante a pesquisa exploratória, por meio de um processo iterativo de análise dos artigos relevantes ao tema. A triagem inicial considerou título, resumo e palavras-chave, resultando na seleção de 27 artigos. Dentre eles, 8 abordam soluções baseadas em conscientização contínua sobre segurança da informação (Seção 3.2.1), 6 tratam de soluções baseadas em monitoramento dinâmico (Seção 3.2.2) e 13 exploram métodos de avaliação de risco e métricas de desempenho (Seção 3.2.3). Os resultados da revisão de literatura que contribuem para a seleção de frameworks de gestão de risco cibernético são discutidos na Seção 3.4, enquanto os trabalhos relacionados estão organizados na Seção 3.5, oferecendo uma visão geral das práticas e desafios atuais na área.

Tabela 1. Critérios de inclusão e exclusão

Critérios de Inclusão	**Critérios de Exclusão**
(i.1) Artigos de periódicos ou anais de eventos científicos, com texto completo disponível	(ii.1) Área de pesquisa que não seja Ciência da Computação
(i.2) Publicações realizadas de 2016 a 2024	(ii.2) Trabalhos que não se relacionam com à pergunta norteadora
(i.3) Trabalhos publicados na língua inglesa ou na língua portuguesa	(ii.3) Artigos curtos e resumos

3.2. Qualidade e Avaliação de Frameworks

Esta seção apresenta uma análise sistemática de frameworks de gestão de risco cibernético, categorizados em três grupos principais: i) trabalhos que abordam soluções baseadas em conscientização contínua sobre segurança da informação; ii) trabalhos que

tratam de soluções baseadas em monitoramento dinâmico; e iii) trabalhos que exploram métodos de avaliação de risco e métricas de desempenho. Ressalta-se que a qualidade das diretrizes e a eficácia das práticas estão interligadas e se complementam, sendo ambas fundamentais para a seleção e aplicação de um framework eficaz.

Na avaliação de frameworks de gestão de risco cibernético, a qualidade refere-se à clareza, abrangência e conformidade regulatória das diretrizes fornecidas. Por outro lado, a eficácia está relacionada à capacidade do framework de atender às necessidades específicas de uma organização, promovendo a mitigação de riscos de forma prática e eficiente.

A Subseção 3.2.1 explora os frameworks que destacam a qualidade das diretrizes como um fator determinante, enquanto a Subseção 3.2.2 analisa os frameworks que enfatizam a eficácia na aplicação prática. Ambas as categorias são essenciais para uma avaliação completa e equilibrada, permitindo que as organizações selecionem o framework mais adequado ao seu contexto operacional.

A Tabela 2 apresenta uma síntese dos estudos analisados e está estruturada da seguinte forma: Objetivos: Identificação (I), Avaliação (A), Comparação (C), Sugestão (S). Domínio de aplicação: (1) Empresas (2) Financeiro (3) Governamental (4) Nuvem (5) Saúde (6) Educação. Classificação: Conscientização, Monitoramento, Desempenho.Dados.

Tabela 2. Síntese dos trabalhos analisados

Autores	Objetivos				Aplicação						Classificação
	I	A	C	S	1	2	3	4	5	6	
(Purkait & Damle; 2023)	X	X					X	X	X	X	Conscientização
(Din et al.; 2023)			X						X		Monitoramento
(Jain et al.; 2022)			X		X	X			X		Conscientização
(Savold et al.; 2017)				X	X						Desempenho
(Fitroh et al.; 2017)	X				X						Conscientização
(Khurana et al.; 2022)		X						X		X	Monitoramento
(Couretas; 2019)		X			X					X	Desempenho
(Romansky et al.; 2024)				X	X	X					Monitoramento
(Li; 2023)	X							X			Desempenho
(Feng et al.; 2017)		X			X						Monitoramento
(Billard; 2019)		X			X						Desempenho
(Khuvis et al.; 2019)	X						X				Monitoramento
(Naumov & Kabanov; 2016)		X			X						Desempenho
(Moreira et al.; 2021)		X			X	X					Conscientização
(Ayati & Naji; 2022)		X			X						Desempenho
(Manuja & Shekhawat; 2023)		X			X						Monitoramento
(Alghaithi et al.; 2022)		X			X						Desempenho
(Carmichael et al.; 2022)		X					X				Monitoramento
(Maneerattanasa et al; 2017)		X			X						Conscientização
(Levy; 2020)		X			X						Desempenho
(Waqdan et al;2023)		X							X		Monitoramento
(Datta; 2020)		X						X			Monitoramento
(Binyamini et al.; 2021)		X			X						Desempenho
(Rehman et al.; 2018)		X			X						Monitoramento
(Wu et al; 2023)		X			X						Desempenho
(Pandurang Gaikwad et al.; 2023)	X				X	X					Conscientização
(Giuca et al. 2021)		X			X	X					Monitoramento

3.2.1. Trabalhos que Abordam Soluções Baseadas em Conscientização Contínua sobre Segurança da Informação

A conscientização contínua sobre segurança da informação é fundamental para garantir a eficácia dos frameworks de gestão de risco cibernético. Investir em programas de conscientização que educam os funcionários sobre ameaças cibernéticas, melhores práticas de segurança e os protocolos estabelecidos pelo frameworks pode fortalecer a postura de segurança de uma organização. Esses programas não apenas capacitam os funcionários a reconhecer e relatar incidentes de segurança, mas também promovem uma cultura de segurança proativa em toda a organização.

Purkait & Damle (2023)abordam a crescente importância da segurança cibernética para as empresas, considerando o aumento significativo das atividades cibercriminosas. O autor propõe uma pesquisa para investigar informações sobre segurança cibernética, focando nas estruturas de frameworks atualmente em uso. Além disso, o estudo busca observar diversas ameaças cibernéticas e atividades de cibercriminosos que podem comprometer dados essenciais de sistemas.

Din et al. (2023) apresentam um sistema inovador de gerenciamento de confiança de memória cognitiva sensível ao contexto (CACMTM) adaptado para Sistemas Inteligentes de Transporte Ciber-Físico (ICPTS). Essa contribuição é significativa porque aborda o desafio crescente de garantir uma comunicação segura e robusta entre os diversos componentes e entidades interligados em sistemas de transporte inteligentes.

Jain et al. (2022) discutem a importância da proteção contra ataques cibernéticos, destacando como esses ataques podem comprometer a segurança de redes, programas e sistemas, levando à exclusão ou alteração de dados sensíveis, extorsão de dinheiro e interrupção das operações empresariais regulares. O autor também destaca a crescente complexidade dos dispositivos e a necessidade de medidas de segurança cibernética mais robustas, especialmente com o avanço da inteligência artificial. Além disso, o artigo ressalta a relevância da análise de *big data* na detecção precoce de ameaças cibernéticas e na compreensão das atividades que podem levar a ataques.

Savold et al. (2017) discutem a necessidade de um *framework* ágil para informar o desenvolvimento de soluções de segurança cibernética, destacando a importância de soluções que sejam adaptáveis a ameaças desconhecidas, práticas comerciais específicas e requisitos técnicos, além de serem traduzíveis em produtos de forma eficiente. O autor apresenta a Arquitetura de Referência de Defesa Cibernética da Northrop Grumman como um exemplo dessa abordagem, que vai além da higiene cibernética básica, focando em tarefas cognitivas através de implementações funcionais de análise avançada e automação.

Fitroh et al. (2017) apresentam uma metodologia para identificar problemas com base no COBIT 5, um framework amplamente utilizado na governança de tecnologia da informação (TI). Os autores destacam a importância de entender e abordar os problemas relevantes para as partes interessadas, alinhando-os aos objetivos da empresa e relacionados à área de TI. A metodologia proposta oferece um processo estruturado para identificar e priorizar problemas, permitindo que as organizações foquem em áreas-chave para melhorias.

Khurana et al. (2022) revisam um *framework* para o gerenciamento de riscos em projetos Scrum de grande escala, utilizando solicitações externas de metadados. O autor destaca a importância dessa estrutura para incentivar a comunicação e colaboração entre equipes em um ambiente de desenvolvimento ágil distribuído. A metodologia proposta visa mitigar os desafios específicos enfrentados na colaboração de equipes em projetos Scrum de grande escala, resistindo à falta de colaboração, ameaças e riscos para a conclusão bem-sucedida dos projetos.

Couretas (2019) apresenta uma estrutura para realizar uma análise de risco empresarial, com o objetivo de priorizar ativos de alto nível e modelar processos detalhados para avaliação estrutural. O autor destaca a importância de avaliar sistemas cibernéticos para garantir sua resiliência e oferece uma abordagem para desenvolver uma compreensão inicial dos níveis de segurança do sistema.

Romansky et al. (2024) abordam a relutância dos operadores de infraestrutura crítica em adotar práticas recomendadas de distribuição e instalação rápida de *patches* de software, devido a múltiplas barreiras que dificultam a validação e implantação desses *patches*. Em resposta a esse problema, Romansky propõe uma extensão para o *The*

Update Framework (TUF) que aborda especificamente o papel das decisões de implantação baseadas em risco necessárias para uso em sistemas de controle industrial. Essa extensão visa superar os desafios específicos enfrentados pelos sistemas de controle industrial, facilitando a implantação segura de *patches* de software e mitigando o risco de distribuição de software malicioso durante o processo de atualização. A contribuição deste trabalho é significativa, pois oferece uma solução potencial para melhorar a segurança dos sistemas de infraestrutura crítica por meio de práticas eficazes de gerenciamento de *patches* de software.

3.2.2. Trabalhos que Abordam Soluções Baseadas em Monitoramento Dinâmico

O monitoramento contínuo das atividades de segurança cibernética é essencial para avaliar a eficácia dos frameworks de gestão de risco. Isso envolve o uso de ferramentas e tecnologias para acompanhar constantemente o ambiente de TI em busca de atividades suspeitas ou anomalias. Ao implementar sistemas de monitoramento contínuo, as organizações podem identificar e responder rapidamente a incidentes de segurança, melhorar a detecção de ameaças e ajustar suas estratégias de segurança conforme necessário.

Li (2023) contribuiem propondo uma estrutura geral de segurança de rede baseada em tecnologia de inteligência artificial. Essa estrutura inclui métodos de modelagem de objetivos de segurança, limites de segurança, elementos do sistema de segurança e serviços de segurança, sugerindo uma abordagem abrangente para lidar com questões de segurança em redes.

Feng et al. (2017) propõem um *framework* de aprendizado de máquina centrado no usuário para centros de operações de segurança cibernética em ambientes empresariais reais. O artigo aborda o problema comum de sobrecarga de alertas nos centros de operações de segurança (SOCs), onde muitos alertas falsos positivos podem permitir que ataques maliciosos passem despercebidos. A estrutura desenvolvida visa reduzir a taxa de falsos positivos e melhorar a produtividade dos analistas SOC, aproveitando o aprendizado de máquina para processar e analisar os dados de segurança.

Billard (2019) apresentam o *framework* Security and Utility Risk Evaluation (SURE), um *framework* projetado para especificar e calcular riscos, permitindo decisões

dinâmicas e autônomas sobre segurança cibernética e risco de utilidade em sistemas computadorizados genéricos. O modelo de decisão do *framework* SURE oferece a capacidade de selecionar entre várias estratégias de mitigação alternativas, otimizando o risco de segurança e utilidade durante a operação de um sistema. O artigo destaca que o modelo de decisão do SURE proporciona uma adaptação superior em comparação com os modelos de decisão de segurança existentes, ao considerar o contexto da ação solicitada, os requisitos de segurança e utilidade, e a estratégia de mitigação selecionada, proporcionando maior flexibilidade tanto para os formuladores de políticas quanto para os usuários.

Khuvis et al. (2019) descrevem um *framework* baseado em integração contínua para gerenciamento de software no Ohio Supercomputer Center (OSC), com o objetivo de garantir a confiabilidade dos ambientes de software em computação de alto desempenho (HPC). Embora ferramentas como EasyBuild e Spack tenham agilizado a implantação de ambientes de software, as mudanças nesses ambientes precisam ser registradas e testadas para garantir a confiabilidade. O *framework* proposto integra ferramentas internas para automação de compilação e instalação de software, juntamente com o *framework* ReFrame, para configurar um sistema de teste contínuo acionado a cada *commit* em um repositório Gitlab local. Isso permite que os usuários do OSC implantem rapidamente e com confiança ambientes de software essenciais para suas operações de HPC, melhorando a eficiência e a confiabilidade do processo de gerenciamento de software.

Naumov & Kabanov (2016) abordam a necessidade urgente de avaliar adequadamente os riscos cibernéticos em ambientes dinâmicos, onde os frameworks atuais muitas vezes falham em se adaptar às mudanças. O autor propõe e valida um novo método que utiliza uma abordagem de dinâmica de sistemas para projetar um *framework* dinâmico de avaliação de riscos. Esse *framework* visa auxiliar as organizações a ajustarem seus métodos e processos de avaliação de riscos para permanecerem relevantes em um ambiente em constante evolução. Destacando a importância de abordar novas ameaças cibernéticas resultantes de mudanças internas ou externas, como expansão global ou presença digital, o artigo enfatiza a necessidade de novos instrumentos que possam aconselhar as empresas sobre quando e como ajustar suas estratégias de segurança cibernética. Este trabalho contribui significativamente ao introduzir uma abordagem dinâmica para o desafio da avaliação de riscos cibernéticos e identifica áreas para futuras pesquisas nesse campo em

constante evolução.

Moreira et al. (2021) tem como objetivo demonstrar como a criação de um plano de risco pode ser realizada com o auxílio do método multicritério construtivista. O autor aplica um estudo de caso utilizando o Método de Apoio à Decisão Multicritério Construtivista (MCDA-C), com os controles do *framework* de cibersegurança como referência. O estudo foi conduzido em um grande banco brasileiro. A relevância deste trabalho reside na demonstração de que a aplicação de métodos multicritérios pode ser utilizada no contexto da segurança da informação, recomendando o uso desses métodos para auxiliar na análise de riscos. A metodologia empregada neste estudo foi tanto quantitativa quanto qualitativa, obtendo dados primários por meio de *brainstorming* com tomadores de decisão e formulários respondidos por especialistas. Os dados secundários foram obtidos através do *Framework* para Melhoria da Cibersegurança em Infraestrutura Crítica, criado pelo NIST (National Institute of Standards and Technology). O problema foi estruturado de acordo com o método construtivista, e os dados coletados foram processados e analisados. O estudo concluiu que a categoria de controles de Monitoramento Contínuo de Segurança se destacou em comparação com outras categorias. Também demonstra a importância da aplicação do método construtivista para a gestão de riscos cibernéticos, oferecendo uma base sólida para a tomada de decisões. O trabalho contribui para uma melhor compreensão da gestão de riscos, incentivando a adoção do método construtivista como uma prática recomendada de gestão de riscos.

3.2.3. Trabalhos que Abordam Soluções baseadas em Métodos de Avaliação de Risco e Métricas de Desempenho

Os frameworks de avaliação de risco desempenham um papel crucial na determinação da eficácia da gestão de risco cibernético. Esses frameworks permitem que as organizações identifiquem e compreendam as ameaças potenciais, avaliem sua probabilidade de ocorrência e impacto nos ativos de informação, e implementem medidas adequadas de mitigação de risco. Ao empregar os frameworks de avaliação de risco robustos e adaptáveis, as organizações podem identificar vulnerabilidades, priorizar recursos e tomar decisões informadas para proteger seus ativos contra ameaças cibernéticas em constante evolução.

A distinção entre metodologia e framework reside no nível de detalhamento e orientação que cada um oferece. Uma metodologia é mais abrangente, fornecendo diretrizes claras sobre o que deve ser feito e como realizar as atividades de um projeto. Já um *framework* atua como uma estrutura básica ou ”esqueleto”, indicando o caminho a seguir, mas sem especificar exatamente como executar cada etapa. Ele oferece flexibilidade para ser combinado com outros processos e técnicas, servindo como suporte essencial, mas não prescritivo, para o desenvolvimento de projetos.

O estabelecimento e acompanhamento de métricas de desempenho relacionadas à segurança cibernética são essenciais para avaliar a eficácia dos frameworks de gestão de risco. Isso envolve a definição de indicadores chave de desempenho (KPIs) que medem o progresso da organização na implementação e manutenção das práticas de segurança recomendadas pelo frameworks. Ao utilizar métricas de desempenho, as organizações podem identificar áreas de melhoria, avaliar o impacto de suas iniciativas de segurança e demonstrar o valor de seus investimentos em segurança cibernética.

Ayati & Naji (2022) destacam a importância da eficácia dos controles em programas e projetos para alcançar seus objetivos. O autor propõe um *framework* adaptável de controles de programa e uma abordagem para definir métricas mensuráveis que visam garantir um programa com zero defeitos. Ao fornecer uma estrutura de medição de controles e criar métricas de eficácia, o artigo oferece uma contribuição significativa para melhorar a qualidade e o desempenho dos programas em diversas áreas.

Manuja & Shekhawat (2023) abordam a crescente importância da segurança da informação devido ao aumento significativo e à dependência organizacional da tecnologia da informação (TI). O autor destaca a necessidade de padrões que adaptem as melhores práticas para alcançar níveis adequados de segurança e gerenciamento de riscos de TI, reconhecendo a demanda por mudanças nos atuais frameworks de gerenciamento de riscos de TI. O artigo contribui examinando vários frameworks de gerenciamento de riscos de TI existentes por meio de uma pesquisa entre diferentes indústrias, líderes de equipe e membros de suas equipes de segurança de TI.

Alghaithi et al. (2022) investigam os frameworks de gerenciamento de risco e ferramentas de teste de segurança para garantir a segurança dos sistemas de software. O

autor destaca a importância de detectar eficazmente os riscos e defeitos potenciais durante o desenvolvimento do software para garantir sua segurança. O estudo demonstra que frameworks de gerenciamento de riscos, como segurança móvel e testes de segurança, são eficazes na detecção de riscos e defeitos em sistemas de software seguros.

Carmichael et al. (2022) discutem o crescente uso de métodos analíticos avançados, como inteligência artificial e aprendizado de máquina, para extrair valor de grandes conjuntos de dados. Esses métodos estão impulsionando novos padrões de processamento de dados e formas de colaboração em pesquisa, sustentadas pela partilha e processamento federados de dados. O autor destaca a necessidade de um quadro padrão de avaliação de riscos para a privacidade que possa abordar plenamente os riscos decorrentes desse novo contexto de processamento de dados.

Maneerattanasak & Wongpinunwatana (2017) propõem a apropriação de princípios e práticas na gestão de riscos de tecnologia da informação (ITRM), destacando a importância dessa abordagem devido aos vários padrões de ameaças cibernéticas contra sistemas e tecnologias de informação avançados. O autor destaca a contribuição do *framework* proposto para fornecer os fatores necessários para a avaliação apropriada no desenvolvimento e na prática dos princípios de ITRM.

Levy (2020) propõem um novo *framework* para a avaliação de riscos em locais de *data centers*, com o objetivo de oferecer uma compreensão abrangente dos riscos enfrentados por instalações de missão crítica. O autor destaca a importância dessa estrutura como uma ferramenta fundamental para a devida diligência em *data centers*, fornecendo um processo padronizado para quantificar e priorizar os riscos externos e permitir comparações entre diferentes instalações.

Waqdan et al. (2023) apresentam um *framework* de avaliação de risco específico para o ambiente de saúde, focado em tecnologias de Internet das Coisas (IoT). O autor destaca a importância dessa estrutura para ajudar as organizações do setor médico, especialmente nos serviços de urgência, a identificar, avaliar e gerenciar os riscos associados à implantação e uso de tecnologias IoT. O *framework* proposto é dinâmico e calcula a pontuação de risco para diferentes perfis de dispositivos, levando em consideração vários parâmetros relevantes, como protocolos de rede, atualizações de segurança, entre outros.

Datta (2020) apresentam o *framework* de segurança cibernética chamado DRAFT para plataformas IoT ponta a ponta, desenvolvido como resposta ao aumento dos ataques cibernéticos contra aplicativos e serviços IoT. O autor destaca a importância desse *framework* para aumentar a resiliência a ataques cibernéticos em plataformas IoT, oferecendo uma abordagem abrangente que inclui uma estrutura de avaliação de risco, uma ferramenta de monitoramento de incidentes e eventos de segurança (SIEM), além de uma estrutura resiliente a ataques cibernéticos.

Binyamini et al. (2021) apresentam um novo *framework* automatizado para modelar novas técnicas de ataque a partir de descrições textuais de vulnerabilidades de segurança, visando melhorar a eficiência do processo de avaliação de riscos em cibersegurança. Os grafos de ataque são uma técnica-chave nesse processo, mas a criação manual de novas regras de interação é demorada e limita a atualização dos grafos. O *framework* proposto inclui uma *pipeline* de ciência de dados com modelos linguísticos, de redes neurais e de regressão logística, que trabalham em conjunto para extrair entidades de ataque, completar informações ausentes e gerar novas regras de interação. Os resultados da avaliação demonstram a eficácia do *framework* na automação do processo de modelagem de técnicas de ataque, contribuindo para a atualização contínua dos grafos de ataque com informações relevantes e atualizadas sobre as ameaças cibernéticas.

Rehman et al. (2018) abordam os desafios de segurança enfrentados pelos sistemas ciberfísicos (CPS), que integram camadas físicas com sistemas de software, criando novos cenários de ataques. O autor analisa métodos estabelecidos de engenharia de requisitos de segurança para desenvolvimento de software, como UMLsec, CLASP, SQUARE e SREP, e propõe uma nova metodologia denominada *"CPS Framework"*. Esta metodologia combina os melhores aspectos dos métodos existentes e introduz parâmetros de segurança específicos para CPS, representando uma extensão do método SREP. Por meio de um estudo de caso e comparações com outros métodos importantes de segurança de requisitos, o artigo demonstra resultados promissores, contribuindo para avançar a pesquisa em segurança ciberfísica e fornecendo suporte significativo à comunidade de pesquisa nesta área em rápida evolução.

Wu et al. (2023)abordam os desafios enfrentados pela digitalização do transporte

marítimo, que expõe as empresas a crescentes riscos cibernéticos devido à integração de dispositivos de comunicação. Para enfrentar esse problema, Wu propõe um *framework* de segurança baseado em aprendizado profundo (DL) que integra a consciência de tipos de ataques para aprimorar a proteção de segurança da rede das empresas de transporte marítimo. O *framework* realiza monitoramento e análise em tempo real dos dados de rede para identificar vários tipos de ataques e tomar medidas de defesa correspondentes de forma oportuna. Testado no Grupo COSCO Shipping, o *framework* demonstrou melhorias significativas na proteção de segurança da rede, oferecendo uma abordagem eficaz para enfrentar os desafios cibernéticos associados à digitalização do transporte marítimo.

Pandurang Gaikwad et al. (2023) abordam a crescente dificuldade que as empresas enfrentam para defender seus sistemas de TI contra ataques cibernéticos, devido aos riscos residuais provocados pela interconectividade das redes e pelas decisões de segurança da informação. O autor aponta que a interdependência entre empresas compromete a eficácia das estratégias de proteção, como investimentos em autoproteção e ciberseguro[4] é cada vez mais relevante em ambientes digitais, especialmente quando as ameaças de segurança de TI são correlacionadas. O estudo analisa como esses métodos de gestão de risco de segurança são impactados por ameaças correlacionadas, utilizando uma perspectiva econômica para investigar as consequências gerenciais e políticas de riscos interrelacionados e propor soluções para aprimorar a segurança da informação. Além disso, técnicas de aprendizado de máquina foram aplicadas a dados de sites de *phishing*, comparando cinco técnicas diferentes e demonstrando que a rede neural (NN) é a mais eficaz para melhorar a cibersegurança. Os resultados indicam que a identificação de *phishing* pode ser automatizada e melhorada significativamente através de inteligência artificial, oferecendo insights práticos para a prevenção de *phishing*.

Giuca et al. (2021) realizam uma revisão sistemática da literatura sobre frameworks de gestão de risco cibernético, analisando diversas abordagens adotadas globalmente. O estudo classifica os frameworks segundo critérios como aplicabilidade, eficácia e conformidade com normas internacionais, fornecendo uma avaliação crítica das soluções

[4]Ciberseguro refere-se à capacidade de uma organização ou sistema de proteger suas informações e sistemas contra ameaças cibernéticas, garantindo a confidencialidade, integridade e disponibilidade dos dados.

existentes. Os autores destacam a crescente necessidade das organizações de aprimorar suas estratégias de cibersegurança, considerando o avanço das ameaças e o impacto da digitalização institucional. Além disso, a pesquisa evidencia desafios na seleção e implementação de frameworks, ressaltando a falta de diretrizes práticas para adaptação a diferentes contextos organizacionais. Embora o trabalho contribua para o entendimento das capacidades e limitações das abordagens analisadas, ele não propõe um modelo específico para avaliação de desempenho ou um método prático de implementação, limitando-se a um panorama comparativo das soluções existentes.

3.3. Análise e Considerações sobre a Literatura

Esta análise de literatura destaca as principais características, pontos fortes e desafios dos frameworks de gestão de risco cibernético, baseando-se em cinco critérios-chave: abrangência, adaptabilidade, eficácia, custo e conformidade. Observou-se uma tendência crescente na adoção de frameworks adaptáveis e a falta de evidências empíricas que comprovem a eficácia de frameworks de baixo custo em diferentes contextos organizacionais.

Os artigos revisados variam em escopo e aplicação, abrangendo desde soluções gerais para múltiplos setores até abordagens específicas para contextos particulares. Independentemente do enfoque, todos os frameworks revisados reforçam o compromisso com a proteção de ativos digitais e a mitigação de riscos cibernéticos.

Uma tendência significativa é a integração de tecnologias emergentes, como inteligência artificial e aprendizado de máquina, para aprimorar a detecção de ameaças e a adaptação das estratégias de mitigação de risco. Essas tecnologias, ao monitorarem comportamentos anômalos em tempo real, oferecem novas possibilidades para prevenir incidentes antes de sua materialização.

No entanto, persistem lacunas na literatura, especialmente quanto à validação empírica e à definição de métricas de desempenho claras para avaliar a eficácia dos frameworks. Métricas como tempo médio de resposta a incidentes, taxas de sucesso na mitigação de ataques e redução de vulnerabilidades detectadas poderiam fornecer bases comparativas mais robustas.

Ademais, a evolução das técnicas de ataque exige frameworks flexíveis e dinâmicos, capazes de incorporar rapidamente informações atualizadas. frameworks como o NIST

Cybersecurity Framework já implementam revisões periódicas, mas poderiam ser aprimorados com integração de inteligência em tempo real e *feedback loops* que ajustem estratégias conforme o cenário de ameaças.

3.4. Discussão Sobre os Resultado da Revisão da Literatura

A revisão da literatura conduzida permitiu identificar e categorizar diferentes abordagens utilizadas na avaliação de frameworks de gestão de risco cibernético. Os estudos analisados indicam que a avaliação desses frameworks frequentemente se baseia em critérios como eficácia, adaptabilidade, custo-benefício e conformidade com normativas regulatórias. No entanto, observa-se uma lacuna na padronização desses critérios, o que dificulta a comparação objetiva entre as diferentes metodologias propostas na literatura.

Outro aspecto relevante identificado na revisão foi a diversidade de abordagens aplicadas à avaliação dos frameworks, que variam entre métodos qualitativos, quantitativos e híbridos. Embora os métodos qualitativos sejam amplamente utilizados devido à sua flexibilidade e aplicabilidade em diferentes contextos organizacionais, eles tendem a ser subjetivos e carecem de métricas padronizadas. Por outro lado, métodos quantitativos oferecem maior precisão e reprodutibilidade, mas podem apresentar limitações quanto à disponibilidade de dados e complexidade de implementação. Alguns estudos sugerem abordagens híbridas como solução para essa dicotomia, combinando métricas qualitativas e quantitativas para oferecer uma avaliação mais equilibrada e contextualizada.

Além disso, identificou-se que poucos estudos abordam explicitamente a integração de fatores humanos na avaliação dos frameworks de gestão de risco cibernético. A influência da cultura organizacional, o nível de conscientização dos usuários e a resistência à adoção de novas práticas de segurança são fatores que impactam diretamente a efetividade dos frameworks, mas que ainda carecem de métricas sistemáticas na literatura analisada.

Com base nesses achados, a revisão da literatura reforça a necessidade de um método estruturado que permita a avaliação padronizada e comparativa dos frameworks de gestão de risco cibernético. A proposta do e-CRF busca preencher essa lacuna ao oferecer um modelo de avaliação que integra critérios técnicos e organizacionais, permitindo maior precisão na escolha de frameworks adequados às necessidades específicas das organizações.

3.5. Análise dos Trabalhos Relacionados

Nesta revisão, três trabalhos foram considerados relacionados, devido a apresentarem objetivos ou contribuições semelhantes, ou por abordarem o mesmo domínio de aplicação. A Tabela 3 apresenta uma síntese dos trabalhos relacionados, categorizando-os de acordo com seus objetivos (Identificação, Avaliação, Comparação, Sugestão) e aplicações (Empresas, Financeiro, Governamental, Nuvem e Educação). Nos parágrafos seguintes apresentamos uma análise comparativa desses estudos:

Palia et al. (2021) destacam a importância da eficácia dos controles em programas e projetos para garantir o alcance dos objetivos de forma consistente. Eles propõem uma estrutura adaptável de controles, acompanhada de métricas mensuráveis para avaliar o desempenho do programa. Os autores adotam uma abordagem baseada em estudo de caso para demonstrar a aplicabilidade da estrutura proposta em um ambiente corporativo. O artigo identifica um problema com modelos tradicionais de maturidade de controle, que muitas vezes focam na eficiência operacional, mas negligenciam a avaliação direta da eficácia dos controles. Como resultado, os programas podem falhar devido à falta de controles eficazes. A solução oferecida pelos autores visa superar essa limitação, fornecendo uma abordagem estruturada para melhorar os resultados e mitigar riscos. Diferentemente de (Radu et al.; 2020), que analisam múltiplas abordagens para avaliação de frameworks, (Palia et al.; 2021) concentram-se especificamente na aplicação de métricas em projetos individuais. Entretanto, o estudo não aborda a adaptação da estrutura para diferentes setores, o que pode limitar sua aplicabilidade em contextos variados.

Radu et al. (2020) analisam os frameworks de gestão de risco cibernético, destacando a importância de uma avaliação abrangente para garantir que as organizações selecionem a abordagem mais adequada às suas necessidades. Eles realizam uma análise comparativa entre métodos qualitativos e quantitativos de avaliação de risco, identificando as limitações de cada abordagem. Os autores utilizam uma revisão comparativa de frameworks existentes, considerando fatores como adaptabilidade, custo-benefício e conformidade regulatória. O artigo aponta que métodos qualitativos, embora amplamente utilizados, podem ser subjetivos e inconsistentes, enquanto os métodos quantitativos, apesar de mais precisos, podem ser complexos e exigir grande volume de dados. Como solução,

os autores propõem um modelo híbrido que combina os pontos fortes de ambas as abordagens, permitindo uma avaliação mais equilibrada e confiável. O estudo fornece diretrizes práticas para a escolha de frameworks, auxiliando as organizações na tomada de decisão informada. Diferentemente de (Palia et al.; 2021), que foca em métricas para projetos específicos, este trabalho adota uma abordagem mais ampla e comparativa. No entanto, a implementação prática do modelo híbrido ainda não foi realizada, o que representa uma limitação do estudo.

Wang et al. (2018) exploram a importância da conscientização contínua como um fator crítico na mitigação de riscos cibernéticos, reconhecendo que o fator humano é uma das maiores vulnerabilidades nas organizações. Os autores propõem um framework de conscientização em segurança cibernética, que integra treinamentos regulares, campanhas educativas e métricas de avaliação para medir o impacto das iniciativas. Os autores utilizaram uma abordagem baseada em pesquisas qualitativas e entrevistas com especialistas em segurança da informação para desenvolver o framework. O artigo identifica um problema com abordagens tradicionais de segurança, que geralmente focam em soluções técnicas e negligenciam o comportamento humano como elemento chave na prevenção de incidentes. A solução sugerida busca superar essa limitação ao fornecer uma abordagem sistemática que incentiva o envolvimento contínuo dos colaboradores e a criação de uma cultura organizacional voltada para a segurança. Embora o estudo de (Wang et al.; 2018) forneça um framework valioso para a conscientização em segurança cibernética, ele não aborda a integração direta com frameworks técnicos de gestão de risco, o que pode limitar sua aplicabilidade em ambientes altamente regulamentados.

Os estudos analisados foram categorizados com base em seus objetivos e domínios de aplicação, como mostrado na Tabela 3.

3.6. Diferenciais do e-CRF em Relação aos Trabalhos Relacionados

O método *Evaluating Cyber Risk Frameworks* (e-CRF) proposto neste trabalho apresenta inovações e diferenciais significativos em relação aos estudos anteriores, destacando-se nos seguintes aspectos:

Tabela 3. Resumo dos trabalhos relacionados

Autores	Objetivos				Aplicação						Classificação
	I	A	C	S	1	2	3	4	5	6	
(Palia et al. 2021)		X			X	X					Desempenho
(R. Radu, 2020)	X	X			X	X		X	X		Desempenho
(Wang, Yu, 2018)				X	X						Conscientização
Este Trabalho	X	X	X	X	X	X	X		X	X	Desempenho

Legenda: Objetivos: Identificação (I), Avaliação (A), Comparação (C), Sugestão (S). Aplicação: (1) Empresas, (2) Financeiro, (3) Governamental, (4) Nuvem, (5) Saúde, (6) Educação. Classificação: Conscientização, Monitoramento, Desempenho.

3.6.1. Personalização e Flexibilidade dos Critérios de Avaliação

O e-CRF permite a personalização de critérios e subcritérios de avaliação, possibilitando que cada organização atribua pesos conforme suas necessidades específicas.

Limitações dos trabalhos anteriores:

- Palia et al. (2021) foca na eficácia de controles, mas não oferece uma abordagem flexível para diferentes cenários organizacionais.
- Radu et al. (2020) apresenta uma abordagem híbrida, porém sem a capacidade de adaptação personalizada.

3.6.2. Avaliação Quantitativa e Qualitativa Integrada

O e-CRF combina métricas qualitativas (fatores humanos e organizacionais) com métricas quantitativas (desempenho e custo-benefício), proporcionando uma avaliação mais completa.

Limitações dos trabalhos anteriores:

- Wang et al. (2018) enfatiza a conscientização cibernética com foco no fator humano, negligenciando métricas quantitativas.
- Radu et al. (2020) sugere modelos quantitativos, mas sem considerar a perspectiva qualitativa das avaliações.

3.6.3. Plataforma Automatizada para Avaliação

O método proposto foi implementado em uma plataforma de software que automatiza o processo de avaliação, permitindo a entrada de dados, cálculo de pontuações e geração de relatórios detalhados para suporte à decisão.

Limitações dos trabalhos anteriores:

- Palia et al. (2021) sugerem processos manuais para avaliação, resultando em maior tempo e possibilidade de erro humano.
- Radu et al. (2020) não fornece uma implementação prática do modelo.

3.6.4. Enfoque na Comparação entre Frameworks

O e-CRF oferece funcionalidades específicas para comparação entre diferentes frameworks de gestão de risco, destacando suas vantagens e desvantagens em relação às necessidades organizacionais.

Limitações dos trabalhos anteriores:

- Trabalhos como Wang et al. (2018) concentram-se na aplicação individual dos frameworks, sem explorar comparações estruturadas.

A Figura 1 apresenta os resultados individuais obtidos por diferentes avaliadores utilizando a plataforma, permitindo observar a consistência das avaliações e a comparação entre os frameworks analisados.

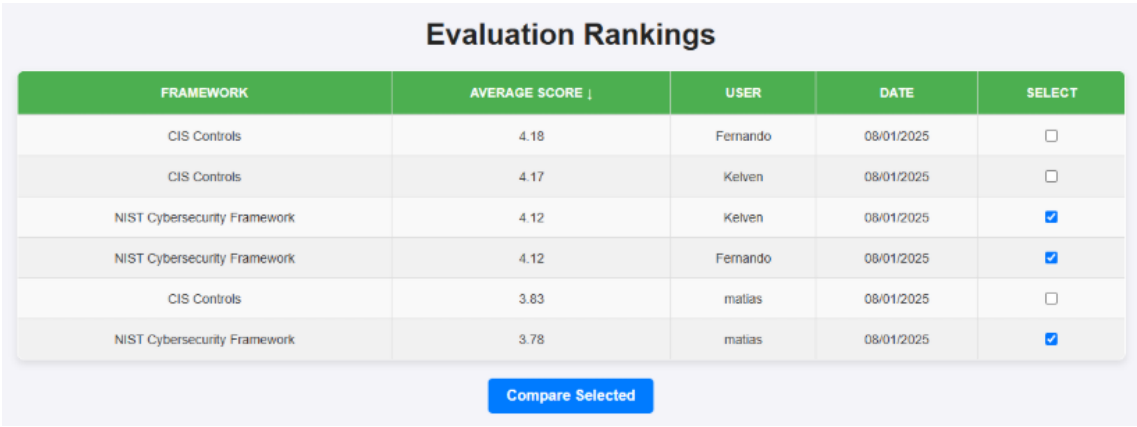


Figura 1. Interface da aplicação com os resultados das avaliações individuais por framework.

3.6.5. Abordagem Colaborativa

O método e-CRF permite que múltiplos avaliadores participem do processo, proporcionando uma visão colaborativa e reduzindo o viés individual na escolha do framework.

Limitações dos trabalhos anteriores:

- As abordagens analisadas normalmente são conduzidas por um único especialista ou uma equipe restrita, sem suporte colaborativo.

3.6.6. Inclusão do Fator Humano e Cultura Organizacional

Diferentemente dos frameworks tradicionais que se concentram em aspectos puramente técnicos, o e-CRF considera fatores humanos e a cultura organizacional como elementos essenciais na avaliação dos frameworks de segurança cibernética.

Limitações dos trabalhos anteriores:

- Wang et al. (2018)aborda a conscientização, mas não integra essa dimensão com métricas técnicas e operacionais de segurança.

3.6.7. Resumo Comparativo

A Tabela 4 apresenta um resumo das principais diferenças entre os trabalhos analisados e o método e-CRF proposto.

Tabela 4. Resumo comparativo dos trabalhos relacionados

Trabalhos	**PC**	**IM**	**AT**	**CF**	**AC**	**FH**
Palia et al. (2021)	Não	Qualit.	Não	Não	Não	Não
Radu et al. (2020)	Parcial	Quantit.	Não	Parcial	Não	Não
Wang et al. (2018)	Não	Qualit.	Não	Não	Não	Sim
Este Trabalho	Sim	Qualit. e Quantit.	Sim	Sim	Sim	Sim

Legenda: PC = Personalização de Critérios, IM = Integração de Métricas, AT = Automação, CF = Comparação de Frameworks, AC = Abordagem Colaborativa, FH = Fator Humano Considerado.

A comparação destaca como o e-CRF supera as limitações dos trabalhos existentes,

oferecendo uma solução mais abrangente e eficaz para a avaliação de frameworks de gestão de risco cibernético.

4. Método e-CRF

Propomos o Método para Avaliação de Frameworks de Gestão de Risco Cibernético (e-CRF), um método de avaliação colaborativa que envolve múltiplos avaliadores. Nesse método, cada critério C_i é ponderado e avaliado em diferentes frameworks M. O método permite que os avaliadores atribuam pesos específicos a cada subcritério, refletindo a importância relativa de cada aspecto, e utilizem uma média ponderada para calcular a pontuação final de cada framework com base nas avaliações recebidas.

4.1. Descrição do Método de Avaliação

Cada critério C_i é avaliado por A avaliadores em M frameworks. A pontuação ponderada final para cada critério é calculada como a média ponderada das notas atribuídas por todos os avaliadores. Para cada critério C_i, a pontuação ponderada $N(C_i, F_k)$ de um framework F_k é obtida utilizando a média das pontuações ponderadas atribuídas por A avaliadores, conforme descrito na Equação 1.

$$N(C_i, F_k) = \frac{1}{A} \sum_{a=1}^{A} \left(\frac{\sum_{j=1}^{n} \left(N_a(S_{ij}, F_k) \times P_a(S_{ij}) \right)}{\sum_{j=1}^{n} P_a(S_{ij})} \right) \tag{1}$$

Nesta equação, $N_a(S_{ij}, F_k)$ representa a nota atribuída pelo avaliador a ao subcritério S_{ij} no framework F_k. O valor $P_a(S_{ij})$ corresponde ao peso atribuído ao subcritério S_{ij} pelo avaliador a.

A nota final $NF(F_k)$ de um framework F_k, considerando todos os critérios e avaliadores, é calculada como descrito na Equação 2:

$$NF(F_k) = \frac{\sum_{i=1}^{m} \left(N(C_i, F_k) \times P(C_i) \right)}{\sum_{i=1}^{m} P(C_i)} \tag{2}$$

Aqui, $N(C_i, F_k)$ representa a nota ponderada média do critério C_i para o framework F_k, considerando todas as avaliações realizadas. O valor $P(C_i)$ refere-se ao peso geral do critério C_i, que pode ser atribuído de forma global ou calculado como a média dos pesos definidos por todos os avaliadores.

A Figura 2 apresenta o fluxograma do método e-CRF:

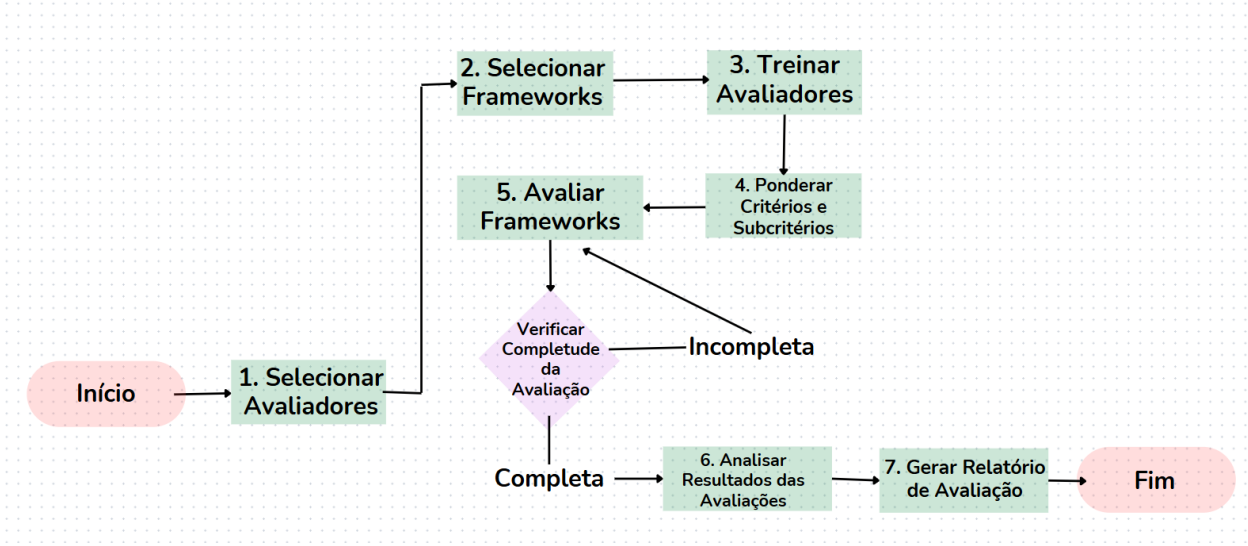


Figura 2. Fluxograma do e-CRF

A Figura 2 apresenta o fluxograma do método e-CRF, ilustrando o fluxo de etapas desde a seleção dos avaliadores até a geração do relatório de avaliação. O processo segue uma abordagem estruturada para garantir uma avaliação criteriosa dos frameworks analisados. As principais etapas do método são descritas a seguir:

1. **Selecionar Avaliadores**: São escolhidos os avaliadores que participarão do processo, garantindo que tenham experiência e conhecimento adequados.
2. **Selecionar Frameworks**: Definição dos frameworks que serão avaliados no processo.
3. **Treinar Avaliadores**: Os avaliadores passam por um treinamento para se familiarizarem com o método e os frameworks selecionados, assegurando uma padronização na atribuição de pesos e notas.
4. **Ponderar Critérios e Subcritérios**: Atribuição de pesos aos critérios e subcritérios, ajustando o modelo de avaliação conforme as necessidades do contexto.
5. **Avaliar Frameworks**: Aplicação do método para avaliar os frameworks de gestão de risco cibernético, atribuindo pesos e notas com base nos critérios definidos.
    - **Verificar Completude da Avaliação**: O sistema verifica se todas as avaliações foram concluídas corretamente. Nesta etapa, dois caminhos podem ser seguidos:
        - **Se a avaliação estiver completa**, o processo segue para a análise dos resultados.

- **Se a avaliação estiver incompleta**, retorna para a etapa de ponderação de critérios e subcritérios para ajustes necessários.

6. **Analisar Resultados das Avaliações**: Após a verificação de completude, os resultados são analisados para identificar padrões, comparar frameworks e extrair informações e indicadores para a tomada de decisão.
7. **Gerar Relatório de Avaliação**: O sistema gera automaticamente um relatório consolidando todas as avaliações, apresentando indicadores, tabelas e gráficos.

Esse fluxograma ilustra o fluxo lógico e as interações entre as diferentes etapas do método e-CRF, garantindo um processo sistemático e estruturado para avaliação de frameworks de gestão de risco cibernético.

4.2. Exemplo de Cálculo

Para ilustrar o processo de cálculo utilizando o método e-CRF, consideremos três critérios principais: Custo, Segurança da Informação e Eficiência. Esses critérios foram avaliados por dois avaliadores (A_1 e A_2), com os seguintes dados detalhados para os subcritérios:

- **Critério Custo:**
  - A_1: Notas 4 e 5, com pesos 2 e 3, respectivamente.
  - A_2: Notas 3 e 4, com pesos 1 e 2, respectivamente.
- **Critério Segurança da Informação:**
  - A_1 e A_2: Ambos atribuíram notas 3 e 4, com pesos iguais a 1.
- **Critério Eficiência:**
  - A_1: Notas 2 e 5, com pesos 2 e 1, respectivamente.
  - A_2: Notas 3 e 4, com pesos 1 e 2, respectivamente.

Os pesos gerais dos critérios são:

$$P(\text{Custo}) = 2, \quad P(\text{Segurança da Informação}) = 1, \quad P(\text{Eficiência}) = 1.$$

Cálculo das Notas dos Critérios

Custo: A nota ponderada média do critério Custo ($N(\text{Custo}, F_k)$) é calculada como:

$$N(\text{Custo}, F_k) = \frac{1}{2}\left(\frac{4\times 2+5\times 3}{2+3}+\frac{3\times 1+4\times 2}{1+2}\right) = \frac{1}{2}(4.6+3.67) = 4.14. \tag{3}$$

Segurança da Informação: A nota ponderada média do critério Segurança da Informação ($N(\text{Segurança da Informação}, F_k)$) é calculada como:

$$N(\text{Segurança da Informação}, F_k) = \frac{1}{2}\left(\frac{3\times 1+4\times 1}{1+1}+\frac{3\times 1+4\times 1}{1+1}\right) = \frac{1}{2}(3.5+3.5) = 3.5. \tag{4}$$

Eficiência: A nota ponderada média do critério Eficiência ($N(\text{Eficiência}, F_k)$) é calculada como:

$$N(\text{Eficiência}, F_k) = \frac{1}{2}\left(\frac{2\times 2+5\times 1}{2+1}+\frac{3\times 1+4\times 2}{1+2}\right) = \frac{1}{2}(3.0+3.67) = 3.34. \tag{5}$$

Nota Final do Framework A nota final ($NF(F_k)$) do framework F_k, considerando todos os critérios, é calculada como:

$$NF(F_k) = \frac{4.14\times 2+3.5\times 1+3.34\times 1}{2+1+1} = \frac{15.12}{4} = 3.78. \tag{6}$$

Com base na nota final calculada, o framework F_k obtém uma avaliação de 3.78, refletindo sua eficácia de acordo com os critérios avaliados e os pesos atribuídos.

Este exemplo demonstra a flexibilidade do e-CRF ao permitir ajustes nos pesos e critérios, adaptando-se às necessidades específicas de cada organização. Além disso, a inclusão de múltiplos avaliadores proporciona maior robustez ao processo de avaliação.

4.3. Justificativa para a Escolha da Função de Agregação

A função de agregação utilizada no método e-CRF foi definida com base na ampla aplicação da média ponderada em análises multicritério, devido à sua simplicidade,

flexibilidade e capacidade de refletir a importância relativa de cada subcritério na avaliação final.

A média ponderada permite que critérios com maior relevância tenham um impacto proporcionalmente maior no resultado, conforme os pesos atribuídos pelos avaliadores. Dessa forma, a agregação das notas mantém coerência com a hierarquia de importância estabelecida, garantindo uma análise equilibrada e representativa.

Embora existam diferentes métodos de agregação, sua aplicabilidade deve considerar as características da avaliação. Algumas abordagens alternativas incluem:

- **Soma Simples Ponderada**: Adequada para cenários onde os pesos dos critérios são fixos e previamente definidos, sem necessidade de normalização.
- **Funções de Maximização ou Minimização**: Utilizadas quando há interesse em otimizar critérios específicos, como minimizar custos ou maximizar segurança.
- **Outras Estratégias de Agregação**: Métodos baseados em análise estatística ou modelos híbridos podem ser explorados para contextos específicos.

A média geométrica foi considerada, mas sua aplicação foi descartada devido à sua inadequação para cenários onde há grande variação entre os valores, pois pode distorcer a representatividade dos dados.

Futuras versões do e-CRF poderão incluir a possibilidade de selecionar diferentes funções de agregação, permitindo maior personalização conforme o contexto organizacional e as preferências dos avaliadores.

4.4. Critérios e subcritérios

O método inclui um total de 12 critérios, cada um com 5 subcritérios específicos, que serão usados para avaliar *frameworks* de gerenciamento de risco cibernético. Cada *framework* é avaliado com base nesses critérios, levando em consideração o impacto de cada um em seu desempenho geral. Os critérios propostos para avaliação são:

Custo: Avalia os custos associados à implementação e manutenção do framework. Esse critério é essencial, pois frameworks de gestão de risco cibernético podem ter altos custos

operacionais, tornando necessário avaliar sua viabilidade financeira para diferentes tipos de organizações.

Subcritérios:

- **Implementação** – Refere-se ao custo inicial para configurar e integrar o framework na organização, incluindo a aquisição de hardware/software necessários.
- **Licença** – Refere-se aos custos associados ao licenciamento do framework, seja em formato proprietário de assinatura ou open-source com suporte pago.
- **Treinamento** – Refere-se ao investimento necessário para capacitar profissionais no uso do framework, incluindo treinamentos internos ou externos.
- **Manutenção** – Refere-se às despesas recorrentes para atualizações, correções de segurança e suporte técnico que garantam a funcionalidade do framework.
- **Consultoria** – Refere-se ao custo com especialistas externos necessários para implementação, adaptação ou melhoria contínua do framework na organização.

Segurança da Informação: Mede a eficácia do *framework* na proteção de informações críticas. Esse critério é fundamental, pois um *framework* de gestão de risco cibernético deve garantir a confidencialidade, integridade e disponibilidade dos dados, prevenindo ataques, vazamentos e falhas de segurança.

Subcritérios:

- **Proteção de Dados** – Avalia a capacidade do framework de garantir a confidencialidade e integridade das informações, protegendo contra acessos não autorizados e vazamentos.
- **Detecção de Intrusão** – Avalia a eficiência do framework na identificação de tentativas de ataque, uso indevido de credenciais e atividades suspeitas.
- **Resposta a Incidentes** – Avalia a capacidade do framework de responder rapidamente a ameaças e minimizar danos causados por ataques cibernéticos.
- **Recuperação** – Avalia os mecanismos disponíveis para restaurar sistemas e dados após um incidente de segurança, garantindo a continuidade operacional.
- **Prevenção** – Avalia as medidas proativas adotadas pelo framework, como políticas de segurança, controle de acesso e atualização contínua para evitar vulnerabilidades.

Eficiência: Refere-se à capacidade do framework de otimizar processos e recursos de segurança. Esse critério é essencial, pois um framework eficiente deve garantir máximo

desempenho com uso otimizado de recursos, reduzindo custos e tempo de resposta a incidentes.

Subcritérios:

- **Otimização de Recursos** – Avalia se o framework permite melhor aproveitamento dos recursos computacionais, reduzindo o consumo de hardware e processamento.
- **Tempo de Resposta** – Avalia a velocidade com que o framework detecta, analisa e responde a incidentes de segurança, minimizando impactos.
- **Automação** – Avalia a presença de mecanismos automatizados para identificação e mitigação de riscos, reduzindo a necessidade de intervenção manual.
- **Escalabilidade** – Avalia a capacidade do framework de se adaptar ao crescimento da organização sem comprometer a eficiência operacional.
- **Integração** – Avalia a compatibilidade do framework com outras ferramentas de segurança, garantindo um ecossistema coeso e eficiente.

Desempenho: Avalia o desempenho do framework em termos de resposta a incidentes e mitigação de riscos. Esse critério é essencial, pois um framework eficaz deve garantir respostas rápidas e eficientes a ameaças cibernéticas, minimizando impactos operacionais e maximizando a proteção.

Subcritérios:

- **Eficácia das Medidas de Segurança** – Avalia a efetividade das estratégias de defesa implementadas pelo framework para prevenir e mitigar ataques cibernéticos.
- **Taxa de Detecção de Ameaças** – Avalia a capacidade do framework de identificar riscos, garantindo maior precisão na identificação de ataques.
- **Mitigação de Riscos** – Avalia a eficiência do framework na redução do impacto de ameaças, minimizando danos à organização.
- **Impacto Operacional** – Avalia o quanto a adoção do framework interfere na rotina da organização, garantindo que sua aplicação não prejudique a produtividade.
- **Tempo de Recuperação** – Avalia a rapidez com que o framework possibilita a recuperação de sistemas e dados após um incidente de segurança.

Complexidade: Analisa a facilidade de implementação e uso do framework. Esse critério é crucial, pois frameworks muito complexos podem demandar mais tempo e recursos

para implementação, dificultando sua adoção por organizações com menor maturidade em segurança cibernética.

Subcritérios:

- **Facilidade de Implementação** – Avalia o quão simples ou burocrático é o processo de adoção do framework na infraestrutura da organização.
- **Curva de Aprendizagem** – Avalia o tempo e o esforço necessários para que a equipe compreenda e utilize o framework de maneira eficiente.
- **Requisitos Técnicos** – Avalia a necessidade de recursos computacionais específicos, como servidores, ferramentas ou expertise técnica para aplicação do framework.
- **Compatibilidade com Sistemas Existentes** – Avalia se o framework pode ser facilmente integrado aos sistemas e processos já adotados pela organização.
- **Complexidade de Manutenção** – Avalia o nível de esforço necessário para manter o framework atualizado, corrigir vulnerabilidades e garantir conformidade contínua.

Flexibilidade/Adaptabilidade: Avalia a capacidade do framework de se adaptar a diferentes tipos de organizações e setores. Esse critério é fundamental, pois um framework de gestão de risco cibernético deve ser versátil e ajustável para atender às necessidades de empresas de diversos segmentos e tamanhos.

Subcritérios:

- **Adaptação a Diferentes Setores** – Avalia a capacidade do framework de ser aplicado em diferentes áreas, como financeiro, saúde, tecnologia e governo.
- **Personalização** – Avalia se o framework pode ser ajustado para atender às necessidades específicas de uma organização, permitindo customizações em políticas e processos.
- **Escalabilidade** – Avalia se o framework pode crescer junto com a organização, garantindo que sua estrutura suporte operações de maior porte sem comprometer a eficiência.
- **Integração com Outras Ferramentas** – Avalia a facilidade de interação com outras soluções de segurança e gestão, como SIEMs, firewalls e sistemas ERP.

- **Ajustes de Configuração** – Avalia a flexibilidade do framework em permitir modificações em regras, políticas e processos sem a necessidade de grandes mudanças estruturais.

Compliance: Avalia o alinhamento do framework com padrões e regulamentações de segurança. Esse critério é essencial, pois frameworks de gestão de risco cibernético devem garantir conformidade com normas e regulamentações nacionais e internacionais, reduzindo riscos legais e operacionais para as organizações.

Subcritérios:

- **Regulamento** – Avalia se o framework segue padrões regulatórios reconhecidos, como GDPR, LGPD, ISO/IEC 27001 e NIST.
- **Políticas Internas** – Avalia a compatibilidade do framework com diretrizes e políticas de segurança adotadas pela organização.
- **Auditoria** – Avalia a capacidade do framework de fornecer rastreabilidade e transparência em processos de segurança, facilitando auditorias internas e externas.
- **Relatórios** – Avalia a capacidade do framework de gerar relatórios detalhados sobre conformidade e gestão de riscos, auxiliando na tomada de decisão.
- **Certificação** – Avalia se o framework facilita a obtenção de certificações de segurança exigidas por normas do setor, garantindo reconhecimento e credibilidade para a organização.

Suporte e Documentação: Avalia a qualidade e a disponibilidade do suporte técnico e da documentação do framework. Esse critério é essencial, pois uma documentação clara e um suporte eficiente facilitam a implementação, manutenção e uso adequado do framework, reduzindo falhas e otimizando sua adoção.

Subcritérios:

- **Qualidade da Documentação** – Avalia se o framework possui guias detalhados, manuais e materiais técnicos que facilitem sua implementação e configuração.
- **Disponibilidade de Suporte Técnico** – Avalia se há suporte técnico acessível, seja via provedores oficiais, consultorias ou fóruns especializados.
- **Comunidade de Usuários** – Avalia a presença e atividade de uma comunidade engajada que contribua com soluções, boas práticas e trocas de conhecimento sobre o framework.

- **Recursos de Aprendizagem** – Avalia a disponibilidade de treinamentos, cursos, webinars e materiais educacionais que ajudem na capacitação de profissionais que utilizarão o framework.
- **Atualizações de Documentação** – Avalia se a documentação do framework é mantida atualizada, refletindo novas versões, correções e aprimoramentos.

Escalabilidade: Avalia a capacidade do framework de crescer e se adaptar às necessidades da organização ao longo do tempo. Um framework escalável deve permitir que a gestão de riscos cibernéticos acompanhe a evolução dos desafios de segurança, regulamentações e estratégias organizacionais sem perder sua efetividade.

Subcritérios:

- **Capacidade de Crescimento** – Avalia se o framework pode ser aplicado em organizações de diferentes portes e setores, garantindo sua aplicabilidade mesmo em cenários de expansão organizacional.
- **Desempenho em Escala** – Avalia se o framework continua eficiente e gerenciável quando adotado por organizações maiores ou em ambientes corporativos complexos.
- **Flexibilidade de Expansão** – Avalia se o framework permite a incorporação de novos requisitos, regulamentações ou práticas sem comprometer sua estrutura original.
- **Gestão do Crescimento** – Avalia a capacidade do framework de fornecer diretrizes claras para que a segurança cibernética seja gerida de forma estruturada conforme a organização cresce.
- **Suporte Multinacional** – Avalia se o framework pode ser adotado em diferentes países, garantindo conformidade com regulamentações e normas internacionais.

Comunidade e Adoção: Avalia o tamanho e a atividade da comunidade de usuários e especialistas que utilizam o framework. Esse critério é essencial, pois frameworks amplamente adotados e respaldados por comunidades ativas tendem a ser mais confiáveis, dinâmicos e bem suportados, garantindo atualizações frequentes e a incorporação contínua de boas práticas de segurança.

Subcritérios:

- **Popularidade** – Avalia a aceitação do framework no mercado e sua relevância entre especialistas e organizações do setor.
- **Comentários da Comunidade** – Avalia o nível de engajamento dos usuários, fóruns de discussão e feedbacks sobre problemas e melhorias do framework.
- **Casos de Uso Reais** – Avalia a aplicação prática do framework em organizações e setores distintos, identificando sua eficácia no mundo real.
- **Colaborações e Parcerias** – Avalia o envolvimento do framework em projetos colaborativos, integração com outras soluções e apoio de instituições acadêmicas ou governamentais.
- **Desenvolvimento Contínuo** – Avalia a frequência de atualizações e contribuições da comunidade para manter o framework relevante e seguro.

Integração com Outras Ferramentas: Avalia a capacidade do framework de interagir com outras soluções e metodologias utilizadas na gestão de riscos cibernéticos. Esse critério é essencial, pois um framework eficaz deve ser compatível com o ecossistema organizacional, facilitando a adoção e a interoperabilidade com outras práticas de segurança.

Subcritérios:

- **Compatibilidade** – Analisa se o framework pode ser implementado em diferentes contextos organizacionais, permitindo sua utilização em conjunto com abordagens já adotadas.
- **APIs e Conectores** – Avalia se o framework oferece interfaces e mecanismos que possibilitam sua integração com ferramentas de análise, auditoria e monitoramento de segurança.
- **Interoperabilidade** – Mede a capacidade do framework de ser utilizado em conjunto com outras metodologias e práticas sem necessidade de adaptações extensivas.
- **Facilidade de Integração** – Examina a simplicidade do processo de adoção e incorporação do framework, considerando tempo, documentação e suporte disponíveis para sua implementação.
- **Suporte para Padrões Abertos** – Verifica se o framework adota padrões amplamente reconhecidos no setor, garantindo maior flexibilidade e reduzindo a dependência de abordagens proprietárias.

Inovação e Atualizações: Analisa a frequência de atualizações e a incorporação de novas tecnologias e práticas. Esse critério é essencial, pois frameworks de gestão de risco cibernético precisam evoluir constantemente para acompanhar as novas ameaças e regulamentações do setor.

Subcritérios:

- **Frequência de Atualização** – Avalia a regularidade com que o framework recebe atualizações, correções de segurança e melhorias em sua estrutura.
- **Incorporação de Novas Tecnologias** – Mede a capacidade do framework de adotar inovações, como inteligência artificial, automação e machine learning, para aprimorar a gestão de riscos.
- **Pesquisa e Desenvolvimento** – Examina o envolvimento do framework em iniciativas de P&D, garantindo que ele continue relevante e alinhado às tendências tecnológicas.
- **Feedback de Mercado** – Verifica se o framework evolui com base no retorno de especialistas, empresas e usuários, incorporando sugestões e melhorias identificadas na prática.
- **Melhorias Contínuas** – Analisa o compromisso dos desenvolvedores em manter o framework atualizado e seguro, garantindo que ele não fique obsoleto ao longo do tempo.

5. Aplicação Desenvolvida para Validação do Método e-CRF

A aplicação desenvolvida para validar o método e-CRF (de Andrade; 2025b) foi projetada com o objetivo de oferecer uma plataforma prática e eficiente para a avaliação de frameworks de gestão de risco cibernético. A seguir, a aplicação será detalhada em diversas subseções, abordando o software, sua arquitetura, os processos implementados, os serviços oferecidos e os papéis desempenhados pelos usuários.

5.1. Arquitetura da Aplicação

A aplicação foi estruturada utilizando uma abordagem modular, dividida em três camadas principais:

- **Camada de Apresentação (Front-end):** Desenvolvida com *React.js*, proporcionando uma interface interativa e responsiva. Componentes reutilizáveis foram criados para facilitar a navegação e a entrada de dados, além de gráficos gerados por meio da biblioteca *Chart.js*.
- **Camada de Aplicação (Back-end):** Implementada utilizando *Node.js* e *Express.js*, oferecendo uma API RESTful para gerenciar as operações do sistema. A autenticação dos usuários é realizada via *JWT (JSON Web Token)*, garantindo segurança no controle de acesso.
- **Camada de Persistência de Dados (Banco de Dados):** O banco de dados utilizado é o *Supabase (PostgreSQL-based)*, que permite escalabilidade e segurança, armazenando informações sobre usuários, frameworks, critérios e avaliações.

O fluxo de dados na aplicação segue a seguinte sequência:

1. O usuário realiza o login no sistema via interface web.
2. A API valida as credenciais e retorna um token de autenticação seguro.
3. O usuário acessa as funcionalidades de avaliação, atribuindo pesos e notas.
4. Os dados são armazenados no banco de dados e processados para a geração de relatórios.

5.2. Software

O desenvolvimento do software foi baseado em tecnologias de desenvolvimento web, garantindo robustez, escalabilidade e uma experiência de usuário intuitiva. A plataforma foi construída utilizando *React.js* para a interface do usuário, *Node.js* para o back-end e *PostgreSQL* como banco de dados.

O sistema possui as seguintes funcionalidades principais:

- **Cadastro e Login**: Os usuários podem criar contas utilizando e-mail e senha, com autenticação segura utilizando criptografia de senhas via *bcrypt*.
- **Gestão de Frameworks**: A aplicação permite o cadastro de frameworks avaliados, apresentados em abas específicas para fácil navegação.
- **Atribuição de Pesos e Notas**: Os avaliadores atribuem pesos aos critérios e notas com base na metodologia definida.

- **Geração de Relatórios**: O sistema exporta relatórios em formato XLSX e PDF, oferecendo gráficos comparativos gerados dinamicamente.
- **Interface Responsiva**: Compatibilidade com dispositivos móveis, tablets e desktops, garantindo acessibilidade ampla.

O código-fonte do software está disponível publicamente no repositório *GitHub* (de Andrade; 2025b), permitindo acesso e contribuições da comunidade acadêmica e profissional. Além disso, a aplicação encontra-se em funcionamento online, permitindo que usuários possam testar suas funcionalidades e realizar avaliações diretamente pela plataforma (de Andrade; 2025a).

Adicionalmente, a aplicação conta com uma página dedicada à explicação detalhada sobre seu funcionamento, incluindo instruções sobre o processo de avaliação, orientações para uso dos critérios e subcritérios, bem como exemplos práticos de preenchimento. Essa seção tem como objetivo facilitar a compreensão do método por parte dos avaliadores e promover uma utilização mais precisa e eficaz da ferramenta.

5.3. Processo

O processo de avaliação é conduzido de forma sistemática e padronizada, garantindo que todos os avaliadores sigam as mesmas etapas e critérios.

A Figura 3 apresenta o processo de avaliação do método e-CRF. As principais etapas do processo incluem:

1. **Identificação do Avaliador**: O avaliador se identifica no sistema e é direcionado para a página de frameworks disponíveis.
2. **Seleção do Framework**: O avaliador escolhe o framework que deseja avaliar e acessa uma aba específica contendo os critérios e subcritérios relacionados.
3. **Atribuição de Pesos**: Antes de começar a avaliação, o avaliador define o peso de cada critério com base na prioridade organizacional.
4. **Atribuição de Notas**: O avaliador atribui notas a cada subcritério, considerando a eficácia do framework.
5. **Geração de Relatório**: O sistema gera um relatório detalhado com os resultados, destacando pontos fortes e fracos do framework.

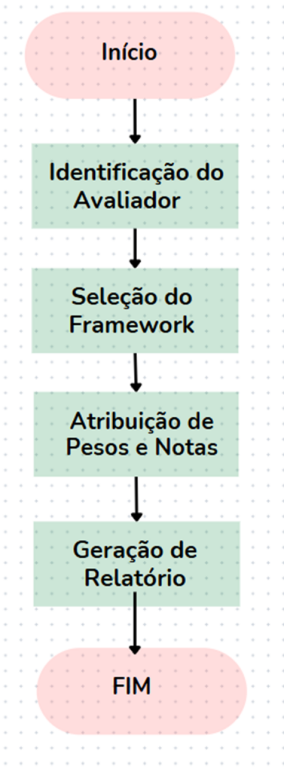


Figura 3. Processo do e-CRF

Para garantir uniformidade na avaliação dos subcritérios, foi utilizada a escala de Likert com cinco pontos, variando de 1 (Discordo Totalmente / Muito Baixo) a 5 (Concordo Totalmente / Muito Alto). Essa escala permitiu que os avaliadores expressassem seu grau de concordância ou percepção de adequação dos frameworks em relação a cada subcritério avaliado, proporcionando uma análise mais padronizada e comparável entre diferentes frameworks.

5.4. Serviço

A aplicação desenvolvida não apenas automatiza o processo de avaliação de frameworks de gestão de risco cibernético, como também oferece um conjunto abrangente de serviços integrados que visam melhorar a experiência do usuário, garantir a qualidade das avaliações e facilitar a tomada de decisões estratégicas. Esses serviços foram projetados para atender às necessidades de diferentes perfis de usuários, desde avaliadores técnicos até gestores e pesquisadores.

- **Relatórios Comparativos**: O sistema gera relatórios completos e comparativos entre os frameworks avaliados, com base nas notas atribuídas aos critérios e

subcritérios. Esses relatórios incluem tabelas, gráficos e rankings automáticos, possibilitando uma análise visual dos pontos fortes e fracos de cada framework. As informações podem ser exportadas em formatos como PDF e XLSX, o que facilita a documentação e a comunicação dos resultados para outros setores da organização. A Figura 4 apresenta um exemplo de relatório gerado pela aplicação e-CRF com visualização de notas e ranking dos frameworks avaliados.

Figura 4. Exemplo de relatório gerado pela aplicação e-CRF.

- **Suporte Técnico**: A aplicação conta com uma seção de suporte integrada que disponibiliza respostas para perguntas frequentes (FAQ), tutoriais de uso, vídeos explicativos e contato direto com a equipe de suporte. Esse serviço é essencial para orientar novos usuários, esclarecer dúvidas sobre o preenchimento das avaliações e garantir o correto funcionamento do sistema em diferentes dispositivos e navegadores.
- **Atualizações Contínuas**: Com base no feedback fornecido pelos usuários, a aplicação é constantemente atualizada para incorporar melhorias funcionais, correções de bugs e novos recursos. Essa prática garante que a plataforma esteja sempre alinhada com as demandas dos avaliadores e com a evolução das boas práticas em cibersegurança. As atualizações são comunicadas diretamente na interface da aplicação, e seus registros ficam disponíveis em um changelog público.

Esses serviços reforçam o caráter prático e escalável da ferramenta, contribuindo

para que o processo de avaliação seja mais eficiente, acessível e confiável em diferentes contextos organizacionais.

As demais capturas de tela da aplicação, como páginas de avaliação, cadastro, comparação entre frameworks e painéis administrativos, estão disponíveis na seção *e-CRF Dashboards*, no Apêndice B.

5.5. Perfis de Usuário

A aplicação foi projetada para atender a diferentes perfis de usuários, garantindo que cada grupo possua permissões e responsabilidades específicas no processo de avaliação dos frameworks de gestão de risco cibernético. Os perfis de usuário são os seguintes:

- **Avaliador**: Usuário responsável pela atribuição de pesos e notas aos critérios e subcritérios dos frameworks analisados. Esse perfil pode incluir especialistas em segurança da informação, gestores de risco e profissionais que aplicam frameworks no contexto organizacional. Os avaliadores têm acesso a um painel que permite a inserção e revisão de suas avaliações, seguindo a metodologia definida pela pesquisa.
- **Gestor**: Usuário que tem acesso aos relatórios gerados pelo sistema, podendo visualizar as avaliações realizadas pelos diferentes avaliadores. Esse perfil é geralmente ocupado por tomadores de decisão, como diretores de segurança, gerentes de TI ou líderes de equipes responsáveis pela adoção de frameworks de gestão de risco cibernético. O gestor pode analisar os resultados comparativos e utilizar os insights obtidos para fundamentar decisões estratégicas dentro da organização.
- **Administrador**: Usuário com permissões avançadas para gerenciar a plataforma. Suas funções incluem o cadastro e manutenção dos frameworks disponíveis para avaliação, a configuração de critérios e subcritérios, a gestão de usuários e o monitoramento do funcionamento do sistema. O administrador também pode supervisionar o ambiente tecnológico da aplicação, garantindo sua integridade, segurança e disponibilidade.

Cada perfil desempenha um papel fundamental para garantir a eficácia e a confiabilidade das avaliações realizadas, contribuindo para um processo estruturado e colaborativo na seleção e comparação de frameworks de gestão de risco cibernético.

5.6. Segurança

A segurança da aplicação é garantida por meio de:

- Criptografia de senhas utilizando algoritmos modernos (*bcrypt*).
- Controle de acesso por meio de autenticação JWT com expiração segura.
- Backups regulares e proteção de dados no banco de dados *Supabase*.

5.7. Validação e Resultados

Durante a fase de testes, especialistas em segurança da informação validaram a eficácia do sistema. Os feedbacks recebidos foram incorporados para aprimorar a interface e a usabilidade.

Os resultados indicaram que a plataforma simplificou o processo de avaliação, permitindo uma comparação clara entre frameworks e fornecendo relatórios detalhados que auxiliam na tomada de decisão.

6. Estudo de Caso

O estudo de caso foi realizado em uma instituição de médio porte do setor educacional, que lida diariamente com informações sensíveis de alunos, professores e colaboradores. A escolha dessa instituição se deve à relevância dos dados gerenciados e à necessidade constante de aprimorar suas práticas de segurança da informação, em conformidade com normas regulatórias, como a Lei Geral de Proteção de Dados (LGPD).

A organização possui um ambiente operacional complexo, composto por múltiplos sistemas legados que precisam ser integrados de maneira eficiente. Esse cenário torna a gestão de risco cibernético um desafio constante, especialmente no que diz respeito à interoperabilidade entre diferentes sistemas e à proteção de dados sensíveis. O estudo buscou avaliar como o método e-CRF e a aplicação desenvolvida poderiam auxiliar na seleção de frameworks que melhor atendam às necessidades específicas da organização, considerando critérios como custo-benefício, eficácia e conformidade regulatória.

Para validar o método, foram consultados três especialistas em segurança da informação, com perfis variados e ampla experiência na área:

- Especialista 1: Profissional de uma instituição pública de médio a grande porte, com profundo conhecimento nas práticas de segurança cibernética em órgãos governamentais.
- Especialista 2: Consultor de segurança de uma multinacional de grande porte, atuante em projetos de implementação de frameworks em diversos setores da indústria.
- Especialista 3: Profissional de um banco de grande porte, com vasta experiência na gestão de riscos relacionados a dados financeiros e regulatórios.

A diversidade dos especialistas permitiu uma análise mais ampla e completa das diferentes perspectivas e desafios enfrentados por organizações de distintos setores. O feedback fornecido por esses profissionais foi fundamental para avaliar a aplicabilidade e a flexibilidade do e-CRF em contextos organizacionais variados, além de identificar melhorias e ajustes necessários no método proposto.

6.1. Objetivo do Estudo de Caso

O principal objetivo do estudo de caso foi validar o método e-CRF em um ambiente real, analisando como a aplicação facilita o processo de avaliação de frameworks de gestão de risco cibernético. Além disso, o estudo buscou verificar se os relatórios gerados pelo sistema oferecem insights úteis para a tomada de decisão e se o uso da plataforma contribui para a padronização das práticas de segurança dentro da instituição.

Outros objetivos específicos incluíram:

- Avaliar a usabilidade da plataforma e sua capacidade de engajar os avaliadores no processo de atribuição de pesos e notas aos critérios.
- Identificar os principais desafios enfrentados durante a implementação prática do método.
- Analisar como os relatórios gerados podem auxiliar os gestores na priorização de investimentos em segurança cibernética.

6.2. Metodologia

A metodologia adotada para o estudo de caso foi estruturada em cinco etapas principais, conduzidas em um **workshop com especialistas** da área de segurança da informação. O workshop teve como objetivo validar a aplicação do e-CRF em um ambiente real, permitindo que os participantes utilizassem a plataforma e contribuíssem com feedbacks para aprimoramento do método. As etapas são descritas a seguir:

1. **Seleção dos Participantes**: Foram selecionados especialistas em segurança da informação de diferentes níveis hierárquicos dentro da instituição, incluindo analistas de TI, gestores de segurança e diretores de tecnologia. A escolha dos participantes buscou abranger diversas perspectivas e experiências no uso de frameworks de gestão de risco cibernético.
2. **Treinamento**: Antes da utilização da plataforma, os participantes passaram por um treinamento introdutório, no qual foram apresentados ao método e-CRF, sua estrutura e funcionalidades. Durante o treinamento, foram demonstrados exemplos práticos de atribuição de pesos e notas aos critérios avaliativos.
3. **Aplicação do Método**: Com o conhecimento adquirido no treinamento, os especialistas utilizaram a plataforma para avaliar frameworks de gestão de risco cibernético.

Cada participante realizou a avaliação de pelo menos três frameworks distintos, atribuindo pesos e notas conforme sua área de especialização e experiência.

4. **Geração de Relatórios**: Após a finalização das avaliações, o sistema gerou automaticamente relatórios analíticos, incluindo gráficos comparativos, tabelas de pontuação e insights sobre os frameworks analisados. Esses relatórios serviram como base para a análise de desempenho dos frameworks e a discussão posterior.
5. **Coleta de Feedback**: Para avaliar a usabilidade da plataforma e a eficácia do método, foi realizada uma coleta de feedback com os participantes. Foram utilizados questionários estruturados e entrevistas qualitativas para identificar pontos positivos, desafios enfrentados e sugestões de melhoria na aplicação e na metodologia adotada.

A realização do workshop possibilitou uma avaliação prática do e-CRF em um ambiente real, garantindo que os especialistas pudessem testar a plataforma e contribuir com ajustes para futuras implementações.

6.3. Frameworks Avaliados

Durante o estudo de caso, os seguintes frameworks de gestão de risco cibernético foram avaliados:

- **NIST Cybersecurity Framework**: Um framework amplamente adotado nos Estados Unidos, focado em proteger os ativos digitais e garantir a continuidade dos negócios. Inclui cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar.
- **ERM OECD (Enterprise Risk Management - Organization for Economic Co-operation and Development)**: Um framework desenvolvido pela Organização para a Cooperação e Desenvolvimento Econômico, que fornece diretrizes para a gestão de riscos empresariais, promovendo uma abordagem estruturada para a identificação, avaliação e mitigação de riscos cibernéticos e operacionais.
- **C2M2 (Cybersecurity Capability Maturity Model)**: Um modelo de maturidade que fornece uma abordagem sistemática para avaliar e melhorar as capacidades de segurança cibernética de uma organização. Ele ajuda as empresas a identificar lacunas de segurança e priorizar melhorias com base em níveis de maturidade.

- **CMMI (Capability Maturity Model Integration)**: Um framework que se concentra na melhoria de processos de gestão de riscos e governança de TI, oferecendo um modelo de maturidade integrado que auxilia as organizações na implementação de práticas eficazes de segurança e conformidade.
- **CIS Controls**: Um conjunto de controles recomendados para fortalecer a postura de segurança cibernética das organizações. Oferece diretrizes práticas e prioridades para proteger ativos digitais.

Cada framework foi avaliado com base nos critérios estabelecidos no e-CRF, considerando aspectos como abrangência, flexibilidade, custo de implementação e conformidade regulatória. As avaliações foram conduzidas de maneira a permitir a comparação objetiva entre os frameworks, destacando suas vantagens e limitações.

6.4. Síntese dos Resultados

Os resultados obtidos no estudo de caso demonstraram que o uso da aplicação facilitou significativamente o processo de avaliação de frameworks, permitindo uma comparação objetiva entre diferentes opções. Os relatórios gerados pelo sistema destacaram diferenças importantes entre os frameworks analisados, fornecendo insights valiosos para os gestores da instituição.

Os participantes relataram que a plataforma reduziu o tempo necessário para realizar as avaliações, aumentou a precisão das análises e garantiu maior transparência no processo. Além disso, os relatórios gerados auxiliaram os gestores na priorização de ações de segurança, identificando quais frameworks ofereciam o melhor custo-benefício.

A coleta de feedback indicou que o e-CRF pode ser uma ferramenta eficaz para padronizar o processo de avaliação de frameworks em diferentes contextos organizacionais. Entre os pontos fortes mencionados pelos participantes estão a facilidade de uso da plataforma, a clareza dos relatórios gerados e a possibilidade de personalizar os critérios de avaliação.

6.5. Desafios e Lições Aprendidas

Durante a realização do estudo de caso, alguns desafios foram identificados:

- **Resistência à Mudança**: Alguns participantes demonstraram resistência inicial em adotar a nova plataforma, preferindo métodos tradicionais de avaliação.

- **Tempo de Treinamento**: Embora o sistema seja intuitivo, foi necessário um tempo considerável de treinamento para garantir que todos os participantes compreendessem as funcionalidades da plataforma.
- **Personalização de Critérios**: Alguns participantes solicitaram a inclusão de critérios adicionais que fossem específicos para o contexto da instituição.

Como lições aprendidas, destaca-se a importância de fornecer suporte contínuo aos usuários durante a implementação da plataforma e de adaptar os critérios de avaliação às necessidades específicas de cada organização.

7. Discussão e Análise Sobre os Resultados do Estudo de Caso

Os resultados obtidos no estudo de caso demonstraram que a aplicação do método e-CRF, juntamente com a plataforma desenvolvida, proporcionou ganhos significativos no processo de avaliação de frameworks de gestão de risco cibernético. Através das avaliações realizadas, os participantes puderam comparar diferentes frameworks de forma estruturada e objetiva, permitindo a identificação de pontos fortes e fracos em critérios essenciais. A Tabela 5 apresenta a pontuação comparativa dos frameworks avaliados, abrangendo critérios como custo, segurança, eficiência, entre outros. Esses resultados fornecem uma visão clara das principais características de cada framework, auxiliando na priorização de investimentos em segurança cibernética e na escolha da abordagem mais adequada para cada organização.

Tabela 5. Pontuação comparativa dos frameworks em critérios de avaliação.

Framework	C	S	E	D	Cx	F	Cf	Sp	Es	Cm	I	In	e-CRF
NIST Cybersecurity Framework	3.67	4.80	3.93	4.80	3.73	3.80	4.20	4.60	3.67	4.00	4.22	4.60	4.17
CIS Controls	3.60	4.73	4.00	4.26	3.73	3.86	4.20	4.66	3.66	4.00	4.00	4.00	4.06
C2M2	3.12	4.00	4.02	3.86	4.00	3.13	5	4.00	3.00	3.85	3.00	4.00	4.01
CMMI	3.00	3.00	3.00	3.00	2.00	3.00	4.00	3.00	3.00	4.00	3.00	4.00	3.24
ERM OECD	3.00	3.00	3.00	4.00	2.00	3.00	4.00	3.00	3.00	3.00	3.00	3.00	3.10

Legenda: Custo (C), Segurança (S), Eficiência (E), Desempenho (D), Complexidade (Cx), Flexibilidade (F), Conformidade (Cf), Suporte (Sp), Escalabilidade (Es), Comunidade (Cm), Integração (I), Inovação (In), Nota do Evaluating Cyber Risk Frameworks (e-CRF).

A utilização do e-CRF permitiu que os avaliadores padronizassem o processo de análise, eliminando variações subjetivas e garantindo maior consistência nos resultados. Além disso, a plataforma facilitou o entendimento dos critérios e subcritérios de avaliação, proporcionando uma experiência de uso mais intuitiva. A seção de ajuda integrada no sistema foi apontada como um fator crucial para a compreensão dos parâmetros utilizados, o que contribuiu para um processo de avaliação mais ágil e preciso.

Um dos pontos mais relevantes identificados foi a capacidade do sistema de gerar relatórios automáticos e gráficos comparativos que destacavam diferenças de desempenho entre os frameworks avaliados. Esses relatórios forneceram insights valiosos para os gestores da organização participante, permitindo que identificassem os frameworks com melhor custo-benefício e priorizassem áreas críticas de segurança. Os relatórios gerados também

facilitaram a visualização das limitações de cada framework, oferecendo informações práticas para a melhoria contínua das práticas de gestão de risco.

A aplicação do método influenciou diretamente o processo de tomada de decisão dentro da organização. Os gestores relataram que a plataforma ajudou a visualizar de forma clara as principais lacunas nos frameworks analisados, possibilitando a identificação de pontos de melhoria e ajustes necessários para atender às necessidades específicas da organização. Além disso, o sistema destacou frameworks com maior flexibilidade e adaptabilidade, que se mostraram mais eficazes em ambientes dinâmicos e em constante evolução.

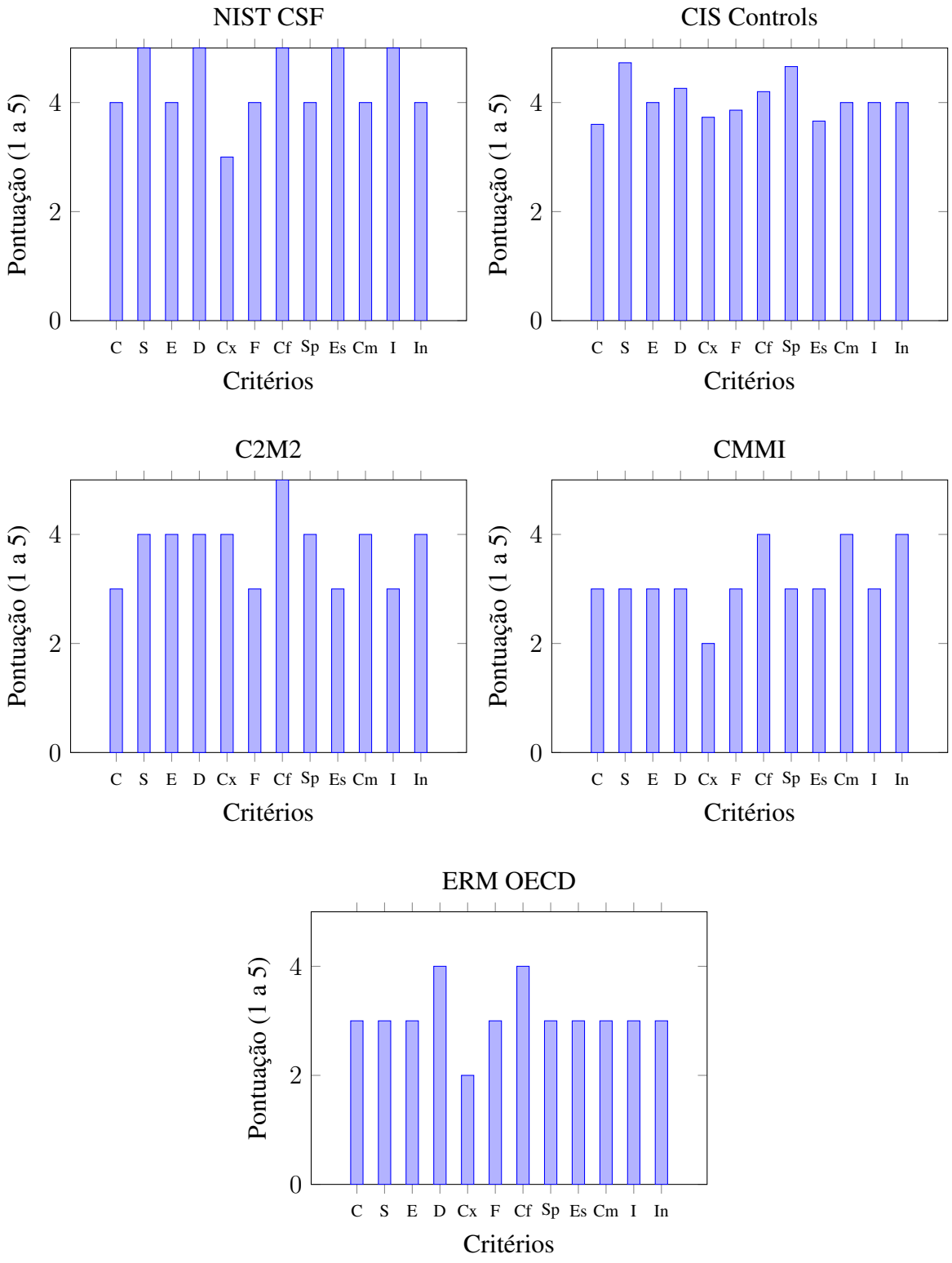
Apesar dos benefícios observados, alguns desafios foram identificados durante a implementação do e-CRF e o uso da plataforma. Entre os principais desafios estavam a resistência inicial por parte de alguns participantes em adotar um novo método de avaliação, a necessidade de treinamento para garantir que todos compreendessem as funcionalidades do sistema e a demanda por personalização de critérios adicionais que refletissem o contexto específico da organização.

Os resultados indicaram que o e-CRF contribui para a padronização da avaliação de frameworks, aumentando a confiabilidade das análises. No entanto, ficou claro que o método precisa ser adaptado às particularidades de cada organização para garantir uma aplicação mais eficaz. Foi destacada a importância de garantir suporte contínuo aos usuários durante o uso da plataforma, especialmente durante as primeiras etapas de implementação.

Além disso, o estudo de caso evidenciou que a plataforma desenvolvida contribuiu para reduzir o tempo necessário para realizar as avaliações e aumentou a precisão das análises. Os participantes relataram que o uso da plataforma facilitou a comparação entre diferentes frameworks e proporcionou maior confiança nas decisões tomadas com base nos relatórios gerados.

Para ilustrar os resultados, a Figura 5 apresenta as pontuações dos frameworks em cada critério, facilitando a comparação de desempenho e auxiliando na escolha mais adequada.

Figura 5. Comparação das pontuações dos frameworks em diferentes critérios de avaliação.



Legenda: C - Custo, S - Segurança, E - Eficiência, D - Desempenho, Cx - Complexidade, F - Flexibilidade, Cf - Conformidade, Sp - Suporte, Es - Escalabilidade, Cm - Comunidade, I - Integração, In - Inovação.

Em suma, a análise dos resultados demonstra que o método e-CRF e a plataforma desenvolvida são ferramentas eficazes para a avaliação de frameworks de gestão de risco cibernético. O estudo reforça a importância de utilizar uma abordagem padronizada e objetiva para a seleção de frameworks, contribuindo para o fortalecimento das práticas de segurança nas organizações. Apesar dos desafios enfrentados, os benefícios observados superam as dificuldades, destacando o e-CRF como uma solução prática e eficiente para a gestão de riscos cibernéticos.

8. Conclusão

O presente estudo apresentou o desenvolvimento e validação do método *Evaluating Cyber Risk Frameworks* (e-CRF), uma abordagem sistemática e padronizada para a avaliação de frameworks de gestão de risco cibernético. A aplicação prática do método, realizada por meio de um estudo de caso, demonstrou que o e-CRF é uma ferramenta eficaz para auxiliar organizações na seleção de frameworks que melhor atendam às suas necessidades específicas, promovendo maior segurança e continuidade dos negócios.

Os resultados obtidos reforçam a importância de utilizar um processo de avaliação padronizado para garantir consistência e confiabilidade nas análises. A plataforma desenvolvida mostrou-se uma solução prática e intuitiva, facilitando o entendimento dos critérios de avaliação e proporcionando relatórios detalhados que auxiliaram na tomada de decisão.

Embora os benefícios observados tenham sido significativos, algumas limitações foram identificadas durante o estudo de caso, conforme descrito a seguir.

8.1. Limitações e Trabalhos Futuros

Durante a realização do estudo de caso, foram identificadas **limitações** que impactaram a aplicação do método e a usabilidade da plataforma desenvolvida. Entre os principais desafios estão:

- **Adaptação ao Novo Modelo**: Alguns avaliadores demonstraram relutância na adoção do sistema, pois estavam habituados a métodos tradicionais baseados em planilhas.
- **Curva de Aprendizado**: Apesar da interface intuitiva, foi necessário um período de familiarização para que todos os usuários compreendessem as funcionalidades da plataforma.
- **Flexibilidade na Personalização**: A necessidade de ajustes nos critérios avaliativos foi apontada por alguns participantes, evidenciando a demanda por uma funcionalidade que permita a personalização sem modificações no código.
- **Ajuste nos Modelos de Cálculo**: A abordagem inicial utilizava a média geométrica, que se mostrou inadequada para avaliar cenários com valores extremos. Esse aspecto será revisado em versões futuras.

- **Revisão da Apresentação dos Dados**: Sugere-se uma reestruturação na exibição dos resultados, incluindo uma melhor separação entre avaliações individuais e síntese dos critérios, além da padronização dos nomes utilizados nos relatórios.

Como **trabalhos futuros**, pretende-se expandir a aplicação do e-CRF para diferentes setores, permitindo uma análise comparativa mais ampla. Além disso, estão previstas as seguintes melhorias:

- **Integração com Outras Ferramentas**: Viabilizar a compatibilidade com sistemas de gestão de risco amplamente utilizados.
- **Análise Preditiva**: Explorar o uso de inteligência artificial para prever tendências e padrões nos dados avaliados.
- **Personalização Direta**: Desenvolver uma interface que permita ajustes nos critérios de avaliação diretamente pelo usuário.
- **Validação Ampliada**: Realizar novos testes com um grupo maior de especialistas para refinar a metodologia e aprimorar a experiência do usuário.

8.2. Resultados da Pesquisa

A pesquisa realizada resultou na produção de um artigo científico aceito em uma conferência internacional de prestígio, evidenciando a relevância e a contribuição do trabalho desenvolvido para a área de segurança cibernética.

1. **Artigo Principal**: O artigo principal da pesquisa (de Andrade et al.; 2025), que apresenta em detalhes o método e-CRF, bem como os resultados obtidos no estudo de caso, foi aceito na conferência *Human-Computer Interaction International* (HCI) e será publicado em seus anais. A aceitação deste artigo em um evento de renome internacional demonstra a relevância da pesquisa e sua contribuição para a área de gestão de riscos cibernéticos.
2. **Registro do Protótipo de Software que implementa o Método Evaluating Cyber Risk Frameworks (e-CRF)**: O código da aplicação e-CRF, uma ferramenta essencial para a operacionalização do método proposto, foi registrado no Instituto Nacional da Propriedade Industrial (INPI) como programa de computador sob Código BR512025000938-0. Esse registro garantirá a proteção da propriedade intelectual, além de reforçar a aplicabilidade prática do método em diferentes

contextos organizacionais. O código-fonte está acessível no Repositório *GitHub* (de Andrade; 2025b), e a aplicação pode ser testada online em (de Andrade; 2025a).

A aceitação do artigo em uma conferência internacional reconhecida evidencia a contribuição técnico-científica deste estudo para o avanço da segurança cibernética. A validação prática do e-CRF e o desenvolvimento de uma plataforma eficiente para avaliação de frameworks representam avanços significativos para aprimorar as práticas de gestão de risco em ambientes organizacionais.

Em suma, o trabalho realizado oferece uma solução inovadora e eficiente para a avaliação de frameworks de gestão de risco cibernético, promovendo uma abordagem estruturada para fortalecer a segurança das organizações. Além disso, a pesquisa estabelece uma base sólida para investigações futuras, possibilitando a evolução contínua da área.

Referências

Alghaithi, S., Alkaabi, A., Al Hamadi, H., Al-Dmour, N. A. & Ghazal, T. M. (2022). A study of risk management frameworks and security testing for secure software systems, *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pp. 1–4.

AlHogail, A. & Almalki, A. H. (2015). Antecedents of perceived benefits of compliance towards information security policies: An empirical study, *2015 12th International Conference on Information Technology - New Generations*, pp. 725–730.
URL: *https://ieeexplore.ieee.org/document/7113575*

Ayati, S. A. & Naji, H. R. (2022). A novel it-based lightweight risk management framework for metering networks in smart grids, *2022 12th Smart Grid Conference (SGC)*, pp. 1–5.

Billard, A. K. (2019). Decision model for the security and utility risk evaluation (sure) framework, *Proceedings of the Australasian Computer Science Week Multiconference*, ACSW '19, Association for Computing Machinery, New York, NY, USA.
URL: *https://doi.org/10.1145/3290688.3290694*

Binyamini, H., Bitton, R., Inokuchi, M., Yagyu, T., Elovici, Y. & Shabtai, A. (2021). A framework for modeling cyber attack techniques from security vulnerability descriptions, *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, KDD '21, Association for Computing Machinery, New York, NY, USA, p. 2574–2583.
URL: *https://doi.org/10.1145/3447548.3467159*

Carmichael, L., Atmaca, U. I., Maple, C., Taylor, S., Pickering, B., Surridge, M., Epiphaniou, G., Le, A. T., Murakonda, S. K., Weller, S., Mcmahon, J., Hall, W. & Boniface, M. (2022). Towards a socio-technical approach for privacy requirements analysis for next-generation trusted research environments, *Competitive Advantage in the Digital Economy (CADE 2022)*, Vol. 2022, pp. 169–180.

Couretas, J. M. (2019). *Cyber Security – An Introduction to Assessment and Maturity Frameworks*, pp. 9–18.

Datta, S. K. (2020). Draft - a cybersecurity framework for iot platforms, *2020 Zooming Innovation in Consumer Technologies Conference (ZINC)*, pp. 77–81.

de Andrade, M. (2025a). Aplicação e-crf link, https://aplicacaomestrado.vercel.app/.
URL: *https://aplicacaomestrado.vercel.app/.*

de Andrade, M. (2025b). Avaliador de framework, https://github.com/TeteuSensei/avaliadorFramework.
URL: *https://github.com/TeteuSensei/avaliadorFramework*

de Andrade, M., Rosa, F. d. F. & Balcão Filho, A. F. (2025). Method for evaluating cybersecurity risk management frameworks (accepted), *27th International Conference on Human-Computer Interaction*.

de Paula, C. P., Cordeiro, G. A., Rampasso, I. S., Ordóñez, R. E. C. & Anholon, R. (2019). Métodos quantitativos para gestão de risco em projetos: Uma revisão da literatura, *GEPROS. Gestão da Produção, Operações e Sistemas* **14**(2): 129–148.
URL: *https://www.researchgate.net/publication/337436372*$_{M}etodos_{Q}uantitativos_{p}ara_{G}estao_{d}e_{R}isc$

Dias, A. L., Moreira, F. R. & Lima, E. d. O. (2022). A utilização dos frameworks nist csf e da série nbr abnt iso 27000 no contexto da gestão da segurança da informação, *ResearchGate* .
URL: *https://www.researchgate.net/publication/360082614*$_{AU}TILIZACAO_{D}OS_{F}RAMEWORKS$

Din, I. U., Awan, K. A. & Almogren, A. (2023). Secure and privacy-preserving trust management system for trustworthy communications in intelligent transportation systems, *IEEE Access* **11**: 65407–65417.

Feng, C., Wu, S. & Liu, N. (2017). A user-centric machine learning framework for cyber security operations center, *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 173–175.

Fitroh, Siregar, S. & Rustamaji, E. (2017). Determining evaluated domain process through problem identification using cobit 5 framework, *2017 5th International Conference on Cyber and IT Service Management (CITSM)*, pp. 1–6.

Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G. & Popescu, D. E. (2021). A survey of cybersecurity risk management frameworks, *in* V. E. Balas, L. C. Jain, M. M. Balas & S. N. Shahbazova (eds), *Soft Computing Applications*, Springer International Publishing, Cham, pp. 240–272.

Jain, A. K., Misra, T., Tyagi, N., Suresh Kumar, M. V. & Pant, B. (2022). A comparative study on cyber security technology in big data cloud computing environment, *2022*

5th International Conference on Contemporary Computing and Informatics (IC3I), pp. 235–241.

Khurana, S. K., Wassay, M. A. & Verma, K. (2022). A review on risk management framework for large scale scrum, *2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)*, pp. 394–400.

Khuvis, S., You, Z.-Q., Na, H., Brozell, S., Franz, E., Dockendorf, T., Gardiner, J. & Tomko, K. (2019). A continuous integration-based framework for software management, *Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (Learning)*, PEARC '19, Association for Computing Machinery, New York, NY, USA.
URL: *https://doi.org/10.1145/3332186.3332219*

Kitchenham, B. (2004). Procedures for performing systematic literature reviews, *Joint Technical Report, Keele University TR/SE-0401 and NICTA TR-0400011T.1* **33**.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P. & Jones, K. (2015). A survey of cybersecurity management in industrial control systems, *IEEE Transactions on Industrial Informatics* **11**(3): 767–800.
URL: *https://ieeexplore.ieee.org/document/7066248*

Levy, M. (2020). A novel framework for data center risk assessment, *2020 11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, pp. 0148–0154.

Li, X. (2023). Research on network information security service model based on user requirements under artificial intelligence technology, *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)*, pp. 1568–1572.

Maneerattanasak, U. & Wongpinunwatana, N. (2017). A proposed framework: An appropriation for principle and practice in information technology risk management, *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, pp. 1–6.

Manuja, P. & Shekhawat, R. S. (2023). It security frameworks: Risk management analysis and solutions, *Proceedings of the 4th International Conference on Information Management & Machine Intelligence*, ICIMMI '22, Association for Computing Machinery,

New York, NY, USA.

URL: *https://doi.org/10.1145/3590837.3590881*

Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T. & Nunes, R. R. (2021). Evaluating the performance of nist's framework cybersecurity controls through a constructivist multicriteria methodology, *IEEE Access* **9**: 129605–129618.

Naumov, S. & Kabanov, I. (2016). Dynamic framework for assessing cyber security risks in a changing environment, *2016 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–4.

Noor, U. & Ghazanfar, A. (2016). A survey revealing path towards service life cycle management in cobit 5, *2016 Eleventh International Conference on Digital Information Management (ICDIM)*, pp. 68–73.

Palia, A., Devlin, C., Yelorda, M. & Morrison, A. (2021). Program controls effectiveness measurement framework metrics, *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, pp. 369–373.

Pandurang Gaikwad, A., Balram Kakpure, K., Ambadas Landge, A., Gunderao Kulkarni, S., PramodJ adhav, M. & Tiwari, M. (2023). Cybersecurity risk management: A complete framework for it enterprises, *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, Vol. 10, pp. 602–607.

Purkait, S. & Damle, M. (2023). Cyber security and frameworks: A study of cyber attacks and methods of prevention of cyber attacks, *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, pp. 1310–1315.

Radu, R., Săndescu, C., Grigorescu, O. & Rughiniş, R. (2020). Analyzing risk evaluation frameworks and risk assessment methods, *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–6.

Rehman, S. u., Allgaier, C. & Gruhn, V. (2018). Security requirements engineering: A framework for cyber-physical systems, *2018 International Conference on Frontiers of Information Technology (FIT)*, pp. 315–320.

Romansky, B., Mazzuchi, T. & Sarkani, S. (2024). Extending the update framework (tuf) for industrial control system applications, *SoutheastCon 2024*, pp. 1571–1576.

Saksonov, E. A., Leokhin, Y. L. & Azarov, V. N. (2021). Information and functional security of distributed information processing systems, *2021 International Conference*

on Quality Management, Transport and Information Security, Information Technologies (ITQMIS), pp. 223–228.

Savold, R., Dagher, N., Frazier, P. & McCallam, D. (2017). Architecting cyber defense: A survey of the leading cyber reference architectures and frameworks, *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, pp. 127–138.

Valle, V. (2021). Metodologia para aplicação conjunta de frameworks de segurança, *Universidade Federal Fluminense - UFF* .

A. Manual de Instalação e Execução da Aplicação Web

Este manual descreve o processo de instalação e execução de uma aplicação web desenvolvida em React, integrada com o banco de dados Supabase.

Pré-requisitos:

- Sistema operacional Windows, macOS ou Linux.
- Node.js instalado na máquina.
- Conta no Supabase para configuração do banco de dados.
- Editor de texto recomendado: Visual Studio Code.

Passo 1: Clonando o Repositório

- Abra o terminal.
- Navegue até a pasta onde deseja clonar o projeto.
- Execute o comando: `git clone https://github.com/TeteuSensei/avaliadorFramework`
- Entre na pasta do projeto: `cd nome-do-projeto`

Passo 2: Instalando as Dependências

- Ainda no terminal, dentro da pasta do projeto, execute o comando: `npm install`

Passo 3: Configurando o Banco de Dados Supabase

- Acesse o site `https://supabase.io` e crie uma conta.
- Crie um novo projeto e copie a URL e a chave de acesso (API Key).
- No projeto, crie um arquivo `.env` na raiz e adicione as seguintes variáveis:

```
REACT_APP_SUPABASE_URL=\textit{sua-url-supabase}
REACT_APP_SUPABASE_KEY=\textit{sua-api-key}
```

Passo 4: Executando a Aplicação Localmente

- No terminal, execute o comando: `npm start`
- Acesse a aplicação no navegador através do endereço: `http://localhost:3000`

Passo 5: Publicando a Aplicação

- Para publicar a aplicação, use serviços como `Vercel` ou `Netlify`.
- Crie uma conta no serviço de sua escolha.

- Conecte o repositório do GitHub ao serviço.
- Configure as variáveis de ambiente no painel de controle do serviço.

Passo 6: Configuração de Segurança

- No painel do Supabase, configure as regras de segurança para permitir apenas acesso autenticado.
- Adicione provedores de autenticação, como e-mail/senha, Google, GitHub, entre outros.

Verificação e Monitoramento:

- Acesse o painel de controle do Supabase para monitorar o banco de dados.
- Utilize ferramentas como o `DevTools` do navegador para identificar possíveis erros na aplicação.

Dicas Finais:

- Mantenha as dependências do projeto atualizadas.
- Sempre utilize variáveis de ambiente para informações sensíveis.
- Realize testes locais antes de publicar a aplicação.

B. *e-CRF Dashboards*

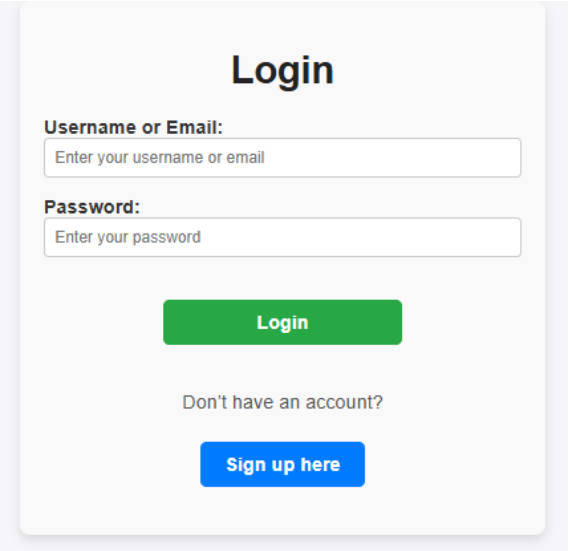


Figura 6. e-CRF Login

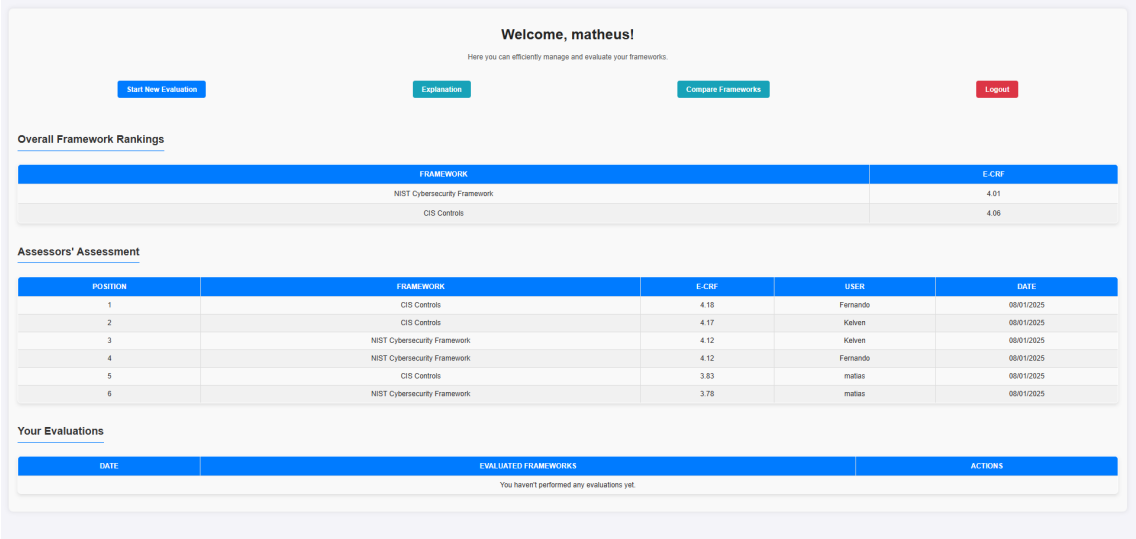


Figura 7. e-CRF Home

Figura 8. e-CRF Relatorio

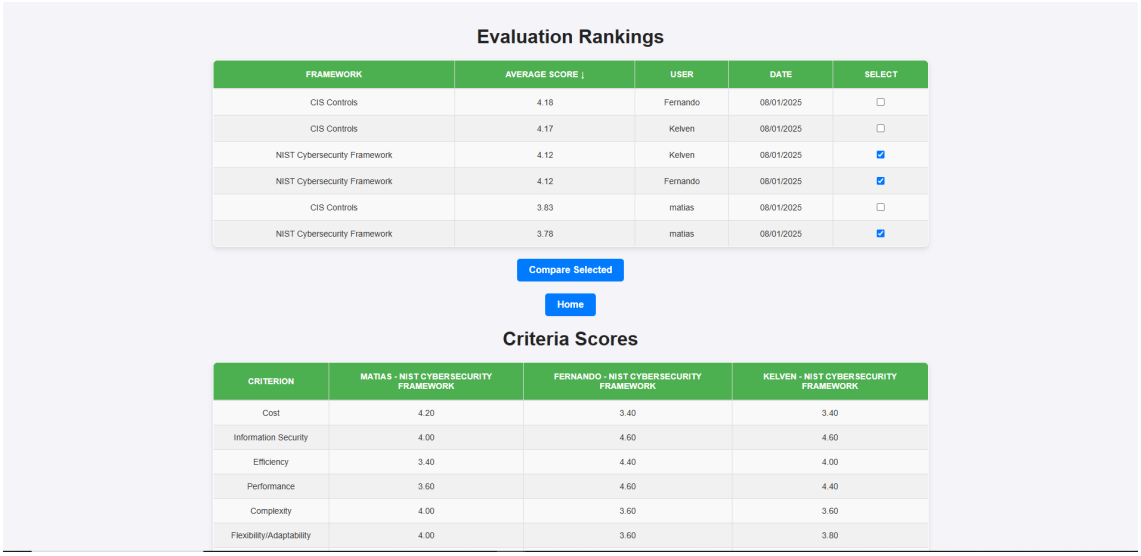


Figura 9. e-CRF tela de Comparação

C. Critérios e Subcritérios para Avaliação de Frameworks de Gestão de Risco Cibernético.

Tabela 6. Critérios e Subcritérios

Critério	**Subcritérios**
Custo	Implementação, Licença, Treinamento Manutenção, Consultoria
Segurança da Informação	Proteção de Dados, Detecção de Intrusão, Resposta a Incidentes Recuperação, Prevenção
Eficiência	Otimização de Recursos, Tempo de Resposta, Automação Escalabilidade, Integração
Desempenho	Eficácia das Medidas de Segurança, Taxa de Detecção de Ameaças Mitigação de Riscos, Impacto Operacional, Tempo de Recuperação
Complexidade	Facilidade de Implementação, Curva de Aprendizado Requisitos Técnicos, Compatibilidade, Complexidade de Manutenção
Flexibilidade/Adaptabilidade	Adaptação a Diferentes Setores, Personalização Escalabilidade, Integração com Outras Ferramentas, Ajustes de Configuração
Conformidade	Regulamento, Políticas Internas, Auditoria Relatórios, Certificação
Suporte e Documentação	Qualidade da Documentação, Disponibilidade de Suporte Técnico Comunidade de Usuários, Recursos de Aprendizagem, Atualizações
Escalabilidade	Capacidade de Crescimento, Desempenho em Escala Flexibilidade de Expansão, Gestão do Crescimento, Suporte Multinacional
Comunidade e Adoção	Popularidade, Comentários da Comunidade, Casos de Uso Reais Colaborações e Parcerias, Desenvolvimento Contínuo
Integração com Outras Ferramentas	Compatibilidade, APIs e Conectores Interoperabilidade, Facilidade de Integração, Suporte para Padrões Abertos
Inovação e Atualizações	Frequência de Atualização, Incorporação de Novas Tecnologias Pesquisa e Desenvolvimento, Feedback de Mercado, Melhorias Contínuas