INSTITUTO FEDERAL DE PERNAMBUCO

CAMPUS BELO JARDIM

BACHARELADO EM ENGENHARIA DE SOFTWARE

ANA THAMYRES SANTANA SANTOS

Estratégias de Gerenciamento de Riscos em Empresas de TIC: Metodologias e Benefícios para o Desenvolvimento de Software

Belo Jardim, Pernambuco

26/08/2024

ANA THAMYRES SANTANA SANTOS

Estratégias de Gerenciamento de Riscos em Empresas de TIC: Metodologias e Benefícios para o Desenvolvimento de Software

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Engenharia de Software do Instituto Federal de Pernambuco de Belo Jardim como requisito parcial à obtenção do grau de Bacharel Engenharia de Software.

Banca de Qualificação

José Fernando Silva – IFPE – Campus Belo Jardim
Elton Bezerra Torres – IFPE – Campus Belo Jardim
Wellyson Fernando Nunes Souza – IFPE – Campus Pesqueira

Belo Jardim, Pernambuco

26/08/2024

Dados Internacionais de Catalogação - CIP

S237e Santos, Ana Thamyres Santana

Estratégias de gerenciamento de riscos em empresas de TIC: metodologias e benefícios para o desenvolvimento de software / Ana Thamyres Santana Santos. – Belo Jardim-PE, 2024.

61f.: il.

Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Software) – Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco, Campus Belo Jardim- PE, 2024.

Orientador: Prof.º José Fernando da Silva.

Inclui referências.

1. Desenvolvimento de software. 2. Segurança da Informação. 3. Gerenciamento de riscos. 4. Tecnologia da Informação. I. Título. II. Silva, José Fernando da. III. Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco.

CDD 005

Ficha catalográfica elaborada pelo Sistema Integrado de Bibliotecas - SIBI/IFPE.
Bibliotecária: Louise Machado Freire Dias CRB – 4 /2267.

ANA THAMYRES SANTANA SANTOS

Estratégias de Gerenciamento de Riscos em Empresas de TIC: Metodologias e Benefícios para o Desenvolvimento de Software

Trabalho aprovado. Belo Jardim, 26/08/2024.

José Fernando da Silva

Professor Orientador

Wellyson Fernando Nunes Souza

Convidado 1

Elton Bezerra Torres

Convidado 2

Belo Jardim

2024

AGRADECIMENTOS

A conclusão deste Trabalho de Conclusão de Curso (TCC) representa a culminação de uma jornada acadêmica repleta de desafios e aprendizados. Gostaria de expressar minha sincera gratidão a todos que, de alguma forma, contribuíram para a realização deste trabalho.

Primeiramente, agradeço a Deus, pela força e inspiração concedidas ao longo deste percurso. Sua presença constante foi fundamental para que eu pudesse enfrentar cada desafio com resiliência e determinação.

Aos meus familiares, pelo amor incondicional, apoio e incentivo contínuos. Vocês sempre acreditaram em mim e me motivaram a buscar o melhor em todas as situações. Suas palavras de encorajamento e exemplo de dedicação são as bases do meu sucesso.

Ao meu orientador, Fernando Silva, pelo suporte técnico, orientação precisa e paciência durante todas as etapas deste trabalho. Sua expertise e conselhos foram essenciais para o desenvolvimento deste TCC. Sou profundamente grata pelo seu comprometimento e disponibilidade.

Aos meus colegas e amigos, em especial, Monique Tereza, que compartilharam comigo momentos de estudo, dificuldades e vitórias. A amizade e o companheirismo de vocês tornaram esta jornada mais leve e significativa.

Por fim, agradeço a todos que, direta ou indiretamente, participaram desta caminhada. Este trabalho é o resultado de um esforço coletivo e, por isso, sou grato a cada um de vocês. A todos, meu sincero muito obrigado.

RESUMO

Este Trabalho de Conclusão de Curso (TCC) aborda a importância do gerenciamento de riscos em empresas de Tecnologia da Informação e Comunicação (TIC) e propõe uma estrutura de suporte para incentivar a adoção de metodologias robustas de gerenciamento de riscos. Inicialmente, uma revisão abrangente da literatura foi realizada para explorar os principais frameworks e padrões, como PMBOK, PRINCE2, ISO 31000, NIST e COBIT, destacando suas estruturas e enfoques específicos. Em seguida, foi apresentada uma proposta detalhada para auxiliar as empresas de TIC na implementação dessas metodologias, enfatizando os benefícios de proteção de ativos, conformidade regulatória, continuidade dos negócios e vantagem competitiva. A pesquisa utilizou a técnica de pesquisa bibliográfica para fundamentar teoricamente a análise e a proposta apresentada. Foram detalhadas as etapas de definição do tema, identificação e seleção de fontes de informação, leitura e análise crítica, síntese dos resultados e citação das fontes utilizadas. Além disso, trabalhos relacionados foram explorados para fornecer um contexto mais amplo e identificar lacunas na literatura existente. As sugestões para pesquisas futuras destacam a importância de desenvolver novas tecnologias para a gestão de riscos, criar políticas e estruturas de governança robustas e considerar aspectos humanos e culturais. A conclusão reafirma a relevância do investimento em práticas eficazes de gerenciamento de riscos para garantir o sucesso e a sustentabilidade das empresas de TIC.

Palavras-chave: Gerenciamento de Riscos, Tecnologia da Informação e Comunicação (TIC); Metodologias de Gerenciamento de Riscos; PMBOK; PRINCE2; ISO 31000; NIST; COBIT; Proteção de Ativos; Conformidade Regulatória; Continuidade dos Negócios; Vantagem Competitiva; Pesquisa Bibliográfica; Governança de TI; Segurança da Informação.

ABSTRACT

This Undergraduate Thesis (TCC) addresses the importance of risk management in Information and Communication Technology (ICT) companies and proposes a support structure to encourage the adoption of robust risk management methodologies. Initially, a comprehensive literature review was conducted to explore major frameworks and standards such as PMBOK, PRINCE2, ISO 31000, NIST, and COBIT, highlighting their specific structures and focuses. Subsequently, a detailed proposal was presented to assist ICT companies in implementing these methodologies, emphasizing the benefits of asset protection, regulatory compliance, business continuity, and competitive advantage. The research employed the bibliographic research technique to theoretically underpin the analysis and the proposed framework. The stages of defining the theme, identifying and selecting information sources, critical reading and analysis, synthesis of results, and citation of utilized sources were detailed. Additionally, related works were explored to provide a broader context and identify gaps in the existing literature. Suggestions for future research emphasize the importance of developing new technologies for risk management, creating robust governance policies and structures, and considering human and cultural aspects. The conclusion reaffirms the relevance of investing in effective risk management practices to ensure the success and sustainability of ICT companies.

Keywords: Risk Management; Information and Communication Technology (ICT); Risk Management Methodologies; PMBOK; PRINCE2; ISO 31000; NIST; COBIT; Asset Protection, Regulatory Compliance; Business Continuity; Competitive Advantage; Bibliographic Research; IT Governance, Information Security.

LISTA DE ABREVIATURAS

TIC: Tecnologia da Informação e Comunicação
PMBOK: Project Management Body of Knowledge
PRINCE2: Projects in Controlled Environments
ISO: International Organization for Standardization
NIST: National Institute of Standards and Technology
COBIT: Control Objectives for Information and Related Technologies
CMMI: Capability Maturity Model Integration
IT: Information Technology (Tecnologia da Informação)
IoT: Internet of Things (Internet das Coisas)
COSO-ERM: Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management
APA: American Psychological Association
MLA: Modern Language Association

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A Gestão de Riscos de Tecnologia da Informação (TI) é um dos principais desafios enfrentados pelas organizações de desenvolvimento de software nos dias de hoje. A complexidade crescente dos sistemas e a necessidade de entrega rápida de software estão levando as empresas a buscarem métodos eficazes para gerenciar os riscos associados a seus projetos de TI. Estudos indicam que a falha em gerenciar esses riscos pode levar a atrasos significativos, aumento de custos e até falhas catastróficas nos projetos (Meredith & Mantel, 2012).

Nesse contexto, diversas metodologias têm sido propostas para ajudar as empresas a gerenciarem os riscos de TI em seus projetos de software. Algumas das metodologias mais populares incluem o PMBOK (Project Management Body of Knowledge), que fornece uma estrutura de melhores práticas para o gerenciamento de projetos, incluindo gestão de riscos; o PRINCE2 (Projects in Controlled Environments), que integra o gerenciamento de riscos em todas as fases do ciclo de vida do projeto; o ISO 31000 (Risk Management - Principles and Guidelines), que oferece princípios e diretrizes para a gestão holística de riscos; o COBIT (Control Objectives for Information and Related Technology), que foca na governança de TI e gerenciamento de riscos alinhados aos objetivos estratégicos da organização.

Cada uma dessas metodologias oferece abordagens distintas para o gerenciamento de riscos de TI em desenvolvimento de software, mas todas têm como objetivo ajudar as organizações a identificarem, avaliar e mitigar os riscos associados aos seus projetos (Schwalbe, 2015). Contudo, a crescente complexidade dos sistemas de software e a necessidade de entregas rápidas estão desafiando a eficácia das metodologias tradicionais. Por isso, novas abordagens estão emergindo. Novas metodologias de gestão de riscos de TI, como o Agile Risk Management (ARM), que integra o gerenciamento de riscos com metodologias ágeis de desenvolvimento, o Threat Modeling, que foca na identificação e mitigação de ameaças específicas ao sistema, e o Risk-Based Testing, que prioriza os testes com base nos riscos identificados, estão sendo implementadas por organizações ao redor
do mundo (Smith, 2019).

Esta pesquisa tem como objetivo apresentar um estudo comparativo das metodologias tradicionais e novas aplicadas à gestão de riscos de TI em desenvolvimento de software. A pesquisa incluirá uma revisão da literatura sobre as

metodologias existentes, uma análise crítica dessas abordagens e a apresentação das novas metodologias propostas e sua aplicabilidade em projetos de software. Fontes recentes apontam para a necessidade de adaptação e evolução das estratégias de gestão de riscos para lidar com a natureza dinâmica e incerta dos projetos de TI modernos (Jones & Ashenden, 2019).

Ao explorar tanto as abordagens tradicionais quanto as emergentes, esta pesquisa visa contribuir para o avanço do conhecimento e das práticas no campo da gestão de riscos de TI, fornecendo insights sobre como as organizações de desenvolvimento de software podem melhorar suas estratégias de mitigação de riscos e, assim, aumentar a probabilidade de sucesso de seus projetos.

1.1 Metodologia de gerenciamento de riscos em projetos de desenvolvimento de software

A metodologia de gerenciamento de riscos em projetos de desenvolvimento de software visa identificar, analisar e mitigar potenciais eventos adversos que podem impactar o sucesso do projeto. Seguindo as diretrizes do guia PMBOK, várias ferramentas são sugeridas para esse propósito. A análise de listas de verificação, por exemplo, identifica riscos com base em experiências passadas.

Destaca-se a Matriz SWOT, uma ferramenta abrangente criada por Albert Humphrey na década de 60. Essa matriz categoriza atributos do projeto sendo ela as seguintes:

- **Forças:** Refere-se aos atributos únicos do negócio ou do projeto que proporcionam vantagens competitivas ou recursos valiosos.
- **Fraquezas:** Representa as áreas em que a empresa ou o projeto não apresentam desempenho satisfatório ou onde há deficiências que podem prejudicar o sucesso.
- **Oportunidades:** São áreas não exploradas ou potenciais de crescimento e desenvolvimento que podem ser aproveitados para benefício do projeto ou negócio.
- **Ameaças:** Engloba fatores externos que podem prejudicar o desempenho do projeto ou negócio, como concorrência acirrada, mudanças no mercado ou regulamentações adversas.

Esses atributos proporcionam uma visão holística e estratégica dos riscos envolvidos. Na Figura 1 abaixo, exemplificamos a Matriz SWOT.

Figura 1: Análise SWOT

Fonte: GROWTHLOVERS(2023)

Além da Matriz SWOT, outras ferramentas e técnicas, como os 5 porquês, diagrama de causa e efeito, matriz de riscos e softwares de gestão de projetos, também são valiosas para identificar, avaliar e gerenciar riscos de forma eficaz durante o ciclo de vida do projeto de desenvolvimento de software. Essa abordagem sistemática contribui para a redução de incertezas e aumenta a probabilidade de sucesso na entrega do projeto.

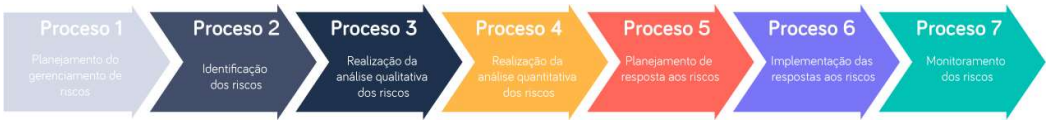
Com base nos processos estabelecidos pelo PMBOK (Project Management Body of Knowledge). Cada processo será detalhado, destacando suas atividades e importância para a eficácia do gerenciamento de riscos em projetos de TI.

1. **Planejamento do Gerenciamento dos Riscos:** O processo de planejamento do gerenciamento dos riscos envolve a definição de como o gerenciamento será executado, monitorado e controlado ao longo do projeto. Serão discutidos os aspectos-chave desse processo, incluindo a escolha da metodologia de gerenciamento de riscos mais adequada, a definição de funções e responsabilidades dos envolvidos e o estabelecimento de orçamentos e cronogramas relacionados ao gerenciamento de riscos.

2. **Identificação dos Riscos:** Esta seção abordará a importância da identificação detalhada de todos os riscos aos quais o projeto de desenvolvimento de software está exposto. Serão discutidos os métodos e técnicas utilizados para mapear os riscos, incluindo a análise de causas e efeitos, a identificação de atividades afetadas e a determinação de gatilhos para cada risco identificado.
3. **Análise Qualitativa dos Riscos:** Será apresentada uma análise detalhada do processo de análise qualitativa dos riscos, que envolve a priorização dos riscos com base em sua probabilidade de ocorrência e no impacto potencial no projeto. Serão discutidas as escalas de probabilidade e impacto, bem como a utilização de matrizes de probabilidade e impacto para priorizar os riscos identificados.
4. **Análise Quantitativa dos Riscos:** Esta seção abordará a avaliação quantitativa do impacto dos riscos priorizados no projeto de desenvolvimento de software. Será discutida a importância de expressar o impacto dos riscos em números e a utilização de métodos quantitativos para avaliar os impactos financeiros e cronogramas decorrentes dos riscos identificados.
5. **Planejamento das Respostas aos Riscos:** Serão discutidas as estratégias e planos de ação desenvolvidos para tratar dos riscos identificados no projeto de desenvolvimento de software. Será destacada a importância de investir na prevenção de problemas e na atribuição de responsáveis pelo gerenciamento de cada risco, visando minimizar os impactos negativos no projeto.
6. **Implementação das Respostas aos Riscos:** Será abordada a implementação prática das respostas planejadas para os riscos identificados, destacando a importância de seguir as etapas de planejamento definidas anteriormente. Serão discutidas as melhores práticas para garantir a eficácia da implementação das respostas aos riscos ao longo do projeto.
7. **Monitoramento dos Riscos:** Esta seção discutirá a importância do monitoramento contínuo dos riscos ao longo do projeto de desenvolvimento de software.

Será destacada a necessidade de acompanhar o projeto para identificar novos riscos e implementar respostas planejadas conforme necessário, garantindo que o gerenciamento de riscos seja um processo contínuo e cíclico.

Figura 2: 7 Etapas do Gerenciamento de Riscos em Projetos



Fonte: Artia(2023)

O gerenciamento de riscos é crucial para o êxito dos projetos de uma organização, sendo imperativo que se busque adquirir o mais amplo conhecimento possível sobre o assunto.

1.2 Objetivo

1.2.1 Objetivo Geral

Este trabalho tem como objetivo geral explorar a importância do gerenciamento de riscos para o sucesso dos projetos em organizações, enfatizando a necessidade de adquirir conhecimento substancial sobre o tema.

1.2.2 Objetivos Específicos

Os objetivos específicos deste trabalho de Trabalho de Conclusão de Curso (TCC) são direcionados, principalmente, a compreender e descrever fenômenos específicos dentro de um contexto delimitado, utilizando fontes de dados secundários como principal técnica de coleta de informações. Nesse sentido, os objetivos específicos podem ser delineados da seguinte forma:

1. **Identificar fontes de dados secundários pertinentes:** Localizar e selecionar fontes de informações relevantes para garantir a abrangência e qualidade dos dados.

2. **Analisar criticamente as fontes de dados selecionadas:** Avaliar a veracidade e precisão das informações para assegurar a confiabilidade dos dados.

3. **Realizar análise documental:** Analisar detalhadamente documentos relevantes para extrair informações significativas que contribuam para a compreensão do tema.

4. **Explorar e descrever aspectos específicos do objeto de estudo:** Finalmente, os objetivos específicos visam explorar e descrever detalhadamente os aspectos identificados durante a pesquisa, proporcionando uma compreensão mais profunda do fenômeno em análise.

Por meio da consecução desses objetivos específicos, espera-se atingir o propósito geral da pesquisa exploratória, que é o de ampliar o conhecimento sobre o tema investigado e subsidiar futuras análises e pesquisas na área.

1.3 Justificativa e Motivação do Estudo

No cenário competitivo atual, empresas de Tecnologia da Informação e Comunicação (TIC) enfrentam desafios complexos e crescentes relacionados ao gerenciamento de riscos. O desenvolvimento de software de qualidade é imperativo para o sucesso empresarial, mas os riscos inerentes ao processo de desenvolvimento – como falhas de segurança, atrasos nos cronogramas, e problemas de conformidade – podem comprometer não apenas a eficácia, mas também a segurança e a reputação das organizações. Estudos indicam que uma má gestão de riscos pode resultar em perdas financeiras significativas, danos à reputação e até mesmo falências (Hubbard & Seiersen, 2016).

Para mitigar esses riscos, a implementação de metodologias eficazes de gerenciamento de riscos é essencial. Este estudo foca nas cinco principais metodologias: NIST (National Institute of Standards and Technology), COBIT (Control

Objectives for Information and Related Technology), ISO 31000 (Risk Management - Principles and Guidelines), PRINCE2 (Projects in Controlled Environments) e PMBOK (Project Management Body of Knowledge). Cada uma dessas metodologias oferece frameworks robustos que ajudam as organizações a identificarem, avaliarem e mitigarem riscos de maneira estruturada e eficaz.

Complexidade e Crescimento das Soluções TIC

A complexidade das soluções de TIC tem aumentado exponencialmente, conforme destaca Hanseth e Ciborra (2007). A integração de diferentes sistemas, embora necessária para a funcionalidade e inovação, também amplifica os riscos associados. Medidas de controle tradicionais podem, paradoxalmente, aumentar os riscos, em vez de reduzi-los.

Importância Econômica do Gerenciamento de Riscos

O gerenciamento de riscos de segurança da informação é uma questão econômica crítica para as organizações. O investimento contínuo em medidas de segurança é necessário para minimizar perdas potenciais causadas por ataques cibernéticos e falhas no sistema. Bojanc e Jerman-Blazic (2008) enfatizam a importância de modelar economicamente esses investimentos para garantir a alocação eficiente de recursos.

Melhoria da Competitividade e Sustentabilidade

Investir em metodologias de gerenciamento de riscos, como NIST, COBIT, ISO 31000, PRINCE2 e PMBOK, não apenas minimiza impactos negativos, mas também maximiza oportunidades de inovação e melhoria contínua. Empresas que implementam essas abordagens de forma eficaz estão mais bem posicionadas para competir no mercado, pois são capazes de responder mais rapidamente às demandas dos clientes e adaptar-se às mudanças do ambiente de negócios. Estudos indicam que o uso de frameworks de gerenciamento de riscos estruturados ajuda a identificar

riscos potenciais antes que eles se materializem, permitindo uma resposta proativa e estratégica (Hillson, 2019).

A implementação do NIST, por exemplo, é fundamental para empresas que buscam proteger suas infraestruturas críticas contra ameaças cibernéticas, aumentando assim a confiança dos clientes e parceiros na segurança de suas operações (NIST, 2018). Este framework de segurança cibernética é amplamente reconhecido e utilizado globalmente, destacando-se como um padrão essencial para empresas que desejam se manter competitivas em um mercado cada vez mais focado na proteção de dados e privacidade.

O COBIT, por sua vez, oferece um conjunto de práticas para a governança de TI, alinhando a gestão de riscos aos objetivos estratégicos da organização. A adoção do COBIT ajuda a otimizar a utilização dos recursos tecnológicos e melhora a eficiência operacional, aspectos críticos para a competitividade das empresas de TI (ISACA, 2019). Empresas que utilizam o COBIT conseguem integrar o gerenciamento de riscos com a governança corporativa, garantindo que todas as decisões de TI estejam diretamente ligadas ao sucesso empresarial.

Com o uso da ISO 31000, as organizações são capazes de adotar uma abordagem holística para a gestão de riscos, promovendo uma cultura de risco integrada em todos os níveis da empresa. Isso não só melhora a resiliência organizacional como também fortalece a sustentabilidade a longo prazo, ao garantir que as decisões de negócio sejam informadas por uma análise robusta de riscos e oportunidades (ISO, 2018).

PRINCE2 e PMBOK são particularmente eficazes para organizações que gerenciam múltiplos projetos simultaneamente. Esses frameworks fornecem estruturas claras para a integração do gerenciamento de riscos no ciclo de vida do projeto, desde a concepção até a conclusão. Ao aderir a esses padrões, as empresas podem melhorar a previsibilidade dos resultados dos projetos e a satisfação dos stakeholders, uma vez que os riscos são gerenciados de forma contínua e eficaz (Axelos, 2017; PMI, 2017).

A implementação de práticas de gerenciamento de riscos baseadas nessas metodologias aumenta a previsibilidade dos resultados, aprimora a confiança dos stakeholders e promove um ambiente de negócios mais seguro e adaptável. Além disso, ao antecipar e mitigar riscos, as empresas não apenas evitam perdas potenciais, mas também identificam novas oportunidades de crescimento e inovação, o que é essencial para a sustentabilidade a longo prazo (Hubbard & Seiersen, 2016).

Exemplos de Sucesso

Empresas líderes no setor de tecnologia, como IBM, Amazon e Oracle, têm implementado com sucesso metodologias robustas de gerenciamento de riscos, utilizando frameworks como NIST, COBIT, ISO 31000, PRINCE2 e PMBOK, para aprimorar seus processos de desenvolvimento de software e proteger seus ativos.

IBM: A IBM adota um mix de metodologias para gestão de riscos, destacando- se pelo uso do **COBIT** e **ISO 31000**. A empresa realiza análises detalhadas de riscos em todos os seus projetos de desenvolvimento de software, seguindo práticas descritas no PMBOK para garantir uma abordagem estruturada ao gerenciamento de riscos. Através do COBIT, a IBM assegura que sua governança de TI esteja alinhada com os objetivos estratégicos, melhorando a eficiência operacional e a segurança da informação (ISACA, 2019). Além disso, ao aplicar ISO 31000, a IBM promove uma cultura de gestão de riscos que permeia toda a organização, aumentando a resiliência e a capacidade de resposta a crises (ISO, 2018).

Amazon: A Amazon incorpora práticas de **NIST** e **PRINCE2** em suas operações para garantir a confiabilidade e a segurança de suas plataformas de e-commerce e serviços em nuvem (AWS). O NIST é fundamental para o gerenciamento de riscos cibernéticos da Amazon, permitindo a detecção e mitigação proativas de ameaças e vulnerabilidades, especialmente em suas operações de grande escala (NIST, 2018). Paralelamente, a Amazon utiliza PRINCE2 para gerenciar seus projetos de forma ágil e eficiente, integrando o gerenciamento de riscos em todas as fases do ciclo de vida do projeto. Essa abordagem permite à Amazon adaptar-se rapidamente às mudanças do mercado e inovar continuamente (Axelos, 2017).

Oracle: A Oracle aplica o **PMBOK** e o **COBIT** para gerenciar os riscos em seus processos de desenvolvimento de software e proteção de dados. O PMBOK é utilizado para padronizar a identificação e mitigação de riscos nos projetos de software da Oracle, garantindo que todos os riscos sejam abordados de maneira sistemática e eficaz (PMI, 2017). O uso do COBIT ajuda a Oracle a alinhar suas práticas de gerenciamento de riscos com a governança corporativa, melhorando a confiabilidade e segurança de seus produtos e serviços. A empresa também adota a ISO 31000 para desenvolver planos de contingência robustos, assegurando que suas operações possam continuar mesmo em face de incidentes adversos (ISO, 2018).

Esses exemplos de sucesso demonstram como as grandes empresas de tecnologia têm se beneficiado da implementação de metodologias de gerenciamento de riscos, não apenas para proteger seus ativos e operações, mas também para manter uma vantagem competitiva em um mercado global dinâmico e desafiador. A adoção dessas práticas permite que essas empresas inovem com confiança, sabendo que estão preparadas para enfrentar e mitigar quaisquer riscos que possam surgir (Hillson, 2019).

Benefícios Tangíveis

Conforme apontado por Sommerville (2016), os benefícios tangíveis do gerenciamento de riscos incluem:

- Minimização de Impactos Negativos: Redução de falhas e atrasos, garantindo entregas eficientes e dentro do prazo.
- Maximização de Oportunidades: Identificação de oportunidades de inovação e melhoria contínua.
- Aumento da Confiança dos Stakeholders: Compromisso com transparência, responsabilidade e qualidade.
- Redução de Custos a Longo Prazo: Prevenção de falhas e retrabalhos, economizando tempo e recursos.
- Melhoria da Competitividade: Adoção de práticas eficazes para competir de maneira mais eficaz no mercado.

Dado o contexto e os desafios do setor de TIC, este estudo justifica-se pela necessidade imperiosa de implementar metodologias de gerenciamento de riscos que garantam a segurança, eficiência e competitividade das empresas. Ao focar na mitigação de riscos e na maximização de oportunidades, as organizações podem não apenas sobreviver, mas prosperar em um mercado cada vez mais complexo e dinâmico.

1.4 Estrutura do Trabalho

No Capítulo 1, são apresentados os desafios de gestão de riscos em TI e as principais metodologias: PMBOK, PRINCE2, ISO 31000, COBIT e NIST. Este capítulo também introduz novas abordagens, como Agile Risk Management e Threat Modeling, que atendem às necessidades de ambientes ágeis. O Capítulo 2 oferece uma análise detalhada dessas cinco metodologias, explorando como elas ajudam a identificar, avaliar e mitigar riscos em projetos de desenvolvimento de software. No Capítulo 3, propõe-se uma estrutura de suporte para que empresas de TIC adotem essas metodologias, destacando benefícios como proteção de ativos, conformidade regulatória e melhoria da competitividade. O Capítulo 4 descreve a metodologia de pesquisa bibliográfica utilizada, incluindo a seleção e análise de fontes relevantes para o estudo. No Capítulo 5, são explorados estudos relacionados, abordando práticas de gestão de riscos empresariais, definição de termos fundamentais e controle de riscos. O Capítulo 6 sugere direções para futuras pesquisas, destacando a importância de novas tecnologias, políticas de governança e considerações sobre aspectos humanos e culturais no gerenciamento de riscos. Finalmente, no Capítulo 7, são apresentadas as considerações finais, discutindo as contribuições da pesquisa, desafios encontrados e sugestões para trabalhos futuros.

2 REFERENCIAL SOBRE GERENCIAMENTO DE RISCOS

Neste capítulo, será apresentada uma revisão da literatura sobre as principais metodologias de gerenciamento de riscos no contexto de Tecnologia da Informação (TI), focando especialmente em desenvolvimento de software. Serão discutidas as abordagens e diretrizes fornecidas pelo PMBOK (Project Management Body of Knowledge), PRINCE2 (Projects in Controlled Environments), ISO 31000 (Risk Management - Principles and Guidelines), COBIT (Control Objectives for Information and Related Technology) e NIST (National Institute of Standards and Technology). Cada uma dessas metodologias oferece estruturas e enfoques distintos para o gerenciamento de riscos, adequando-se às diferentes necessidades e contextos de projetos de TI.

- **PMBOK:** Desenvolvido pelo Project Management Institute, o PMBOK fornece um conjunto abrangente de práticas para gerenciamento de projetos, incluindo uma abordagem sistemática para o gerenciamento de riscos. O PMBOK destaca processos como identificação, análise qualitativa e quantitativa, planejamento de respostas, monitoramento e controle de riscos, aplicáveis a qualquer tipo de projeto (PMI, 2017).

- **PRINCE2:** Este método de gerenciamento de projetos é amplamente utilizado na Europa e integra o gerenciamento de riscos em todos os estágios do ciclo de vida do projeto. PRINCE2 enfatiza a identificação precoce de riscos e a tomada de decisões baseada em dados, garantindo que os riscos sejam monitorados continuamente e que as respostas sejam adaptadas conforme necessário (Axelos, 2017).

- **ISO 31000:** Uma norma internacional que oferece princípios e diretrizes gerais para o gerenciamento de riscos. A ISO 31000 é aplicável a qualquer organização, independentemente do tamanho ou setor, e promove uma abordagem holística que integra o gerenciamento de riscos na cultura organizacional e nos processos de tomada de decisão. Ela enfatiza a criação de valor e a proteção dos ativos organizacionais (ISO, 2018).

- **COBIT:** Desenvolvido pela ISACA, o COBIT é um framework voltado para a governança e gestão de TI, com foco em alinhar os riscos de TI aos objetivos estratégicos da organização. COBIT ajuda a garantir que os processos de TI não apenas suportem, mas também aumentem o valor para o negócio, por meio de uma gestão de riscos eficaz e eficiente (ISACA, 2019).

- **NIST:** O NIST fornece diretrizes especificamente voltadas para a gestão de riscos cibernéticos e a proteção de infraestruturas críticas. Este framework é particularmente relevante para empresas que precisam assegurar a segurança e a resiliência de suas operações contra ameaças cibernéticas. O NIST destaca a importância de identificar, proteger, detectar, responder e recuperar de incidentes cibernéticos (NIST, 2018).

Essas metodologias não apenas ajudam a identificar e mitigar riscos, mas também promovem a criação de estratégias robustas que garantem a segurança, a eficiência e a eficácia dos projetos de desenvolvimento de software. Ao explorar e comparar essas metodologias, este capítulo contribuirá para uma compreensão mais profunda de como as empresas de TI podem implementar práticas de gerenciamento de riscos para enfrentar os desafios do ambiente de negócios atual.

2.1 PMBOK (Project Management Body of Knowledge)

O PMBOK (Project Management Body of Knowledge) é um guia amplamente utilizado na área de gerenciamento de projetos, especialmente em projetos de Tecnologia da Informação (TI). Desenvolvido e publicado pelo Project Management Institute (PMI), o PMBOK oferece um conjunto de melhores práticas, princípios e diretrizes que ajudam os gerentes de projeto a planejarem, executar, controlar e encerrar projetos de forma eficaz e eficiente (PMI, 2017). Reconhecido globalmente como uma referência fundamental, o guia é essencial para profissionais que buscam assegurar a qualidade e o sucesso de seus projetos, independentemente do setor ou da indústria em que atuam.

O PMBOK estrutura o gerenciamento de projetos em dez áreas de conhecimento, sendo o gerenciamento de riscos uma delas. No contexto de gerenciamento de riscos, o PMBOK descreve um processo sistemático que inclui:

- **Planejamento do Gerenciamento de Riscos:** Definição de como o gerenciamento de riscos será conduzido durante o projeto.
- Identificação dos Riscos: Determinação dos riscos que podem afetar o projeto e documentação de suas características.
- **Análise Qualitativa dos Riscos:** Avaliação dos riscos identificados para priorizar os que merecem mais atenção.
- **Análise Quantitativa dos Riscos:** Quantificação do impacto dos riscos nos objetivos do projeto.
- **Planejamento de Respostas aos Riscos:** Desenvolvimento de opções e ações para melhorar as oportunidades e reduzir as ameaças aos objetivos do projeto.
- **Implementação das Respostas aos Riscos:** Assegurar que as respostas planejadas sejam executadas conforme necessário.
- **Monitoramento e Controle dos Riscos:** Acompanhar os riscos identificados, monitorar riscos residuais, identificar novos riscos e avaliar a eficácia das respostas aos riscos ao longo do projeto (PMI, 2017).

Esses processos são inter-relacionados e oferecem um framework estruturado que permite aos gerentes de projeto gerenciarem riscos de forma contínua, adaptativa e pró-ativa, utilizando ferramentas e técnicas apropriadas em cada fase do projeto. O uso do PMBOK em gerenciamento de riscos ajuda a aumentar a previsibilidade dos resultados dos projetos, melhorar a comunicação entre stakeholders e minimizar potenciais impactos negativos que poderiam comprometer o sucesso do projeto (Hillson, 2019).

A abordagem do PMBOK para o gerenciamento de riscos é amplamente adotada por sua flexibilidade e aplicabilidade em diferentes tipos de projetos, desde projetos de desenvolvimento de software até grandes iniciativas de infraestrutura. Ao seguir as diretrizes do PMBOK, os gerentes de projeto podem não apenas proteger seus

projetos contra ameaças potenciais, mas também aproveitar oportunidades que possam surgir ao longo do ciclo de vida do projeto, promovendo um ambiente de projeto mais seguro e eficiente (Schwalbe, 2015).

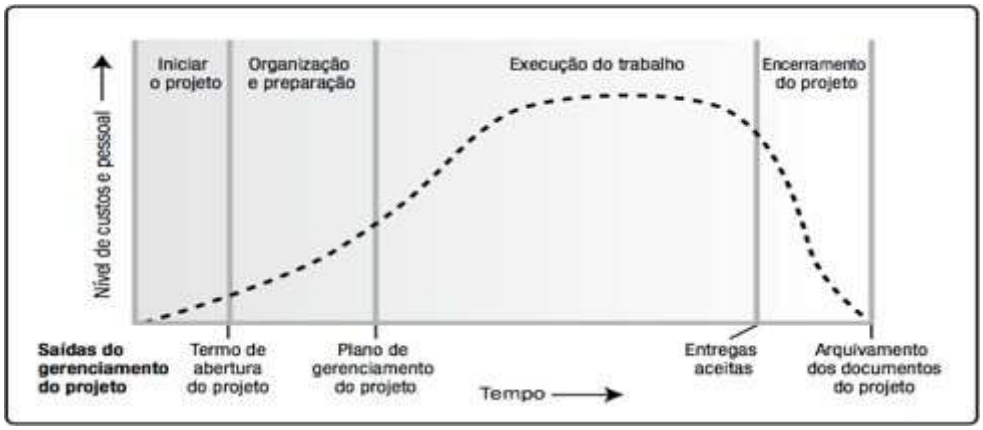
2.1.1 Ciclo de vida e organização dos projetos

O gerenciamento de projetos é realizado em um contexto mais amplo do que o próprio projeto e é dividido em grandes etapas conhecidas como ciclo de vida. A equipe envolvida no projeto precisa compreender esse contexto e selecionar as técnicas e ferramentas mais adequadas para cada etapa específica.

Cada etapa do ciclo de vida do projeto envolve a entrega de resultados ou produtos que devem ser verificados para garantir sua conclusão antes de iniciar o trabalho na próxima etapa. No entanto, é possível iniciar uma etapa antes da conclusão de outra, desde que os riscos envolvidos sejam adequadamente tratados. Embora o número de etapas possa ser padronizado em várias organizações,
o ciclo de vida de cada projeto é único, pois as durações de cada etapa podem variar de um projeto para outro.

De acordo com o PMBOK, os projetos podem variar em termos de tamanho e complexidade, mas todos eles podem ser mapeados para uma estrutura padrão de ciclo de vida. Como ilustrado na Figura 3 abaixo:

Figura 3: Nível típico de custos e pessoal ao longo de seu ciclo de vida



Fonte: Moraes, 2012 (2023)

Diante disso, os projetos possuem diferentes tamanhos e níveis de complexidade. No entanto, todos eles podem ser divididos em quatro fases principais, independentemente de sua escala ou dificuldade:

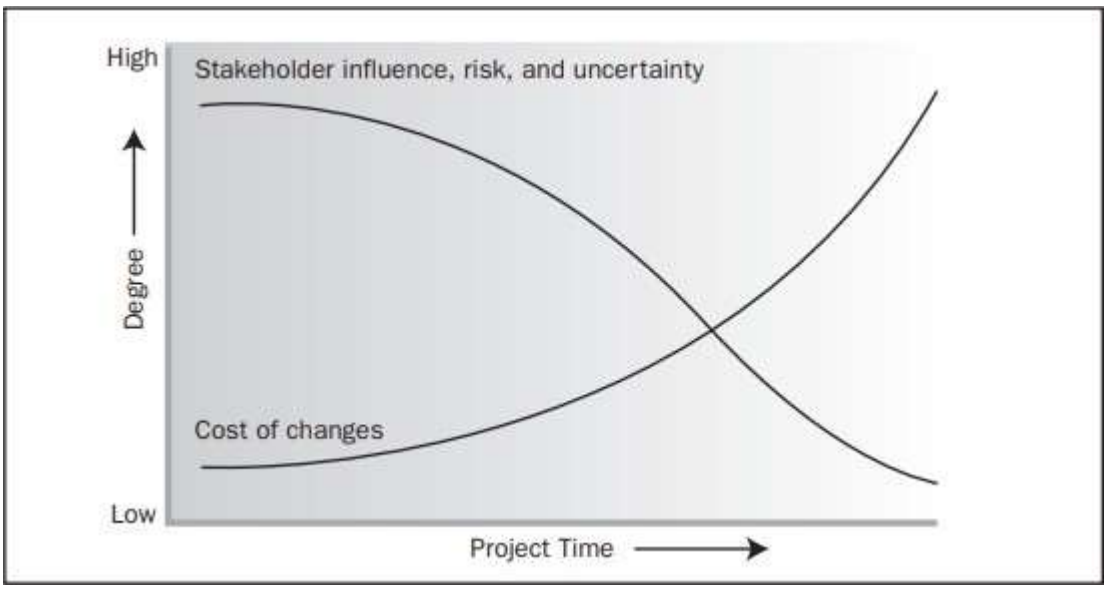
- Iniciar o projeto;
- Organizar e preparar;
- Executar o trabalho do projeto;
- Encerrar o projeto;

Essa estrutura de ciclo de vida geral é comumente utilizada ao se comunicar com a alta gerência ou outras partes envolvidas menos familiarizadas com os detalhes do projeto. Essa visão abrangente serve como um ponto de referência comum para comparar projetos, mesmo que sejam distintos em sua natureza. A estrutura genérica do ciclo de vida geralmente exibe as seguintes características:

- No início do projeto, os custos e o número de funcionários são baixos, atingindo

  o pico durante a execução do trabalho e diminuindo rapidamente à medida que o projeto se aproxima do final. Isso é ilustrado pela linha tracejada na Figura 3;
- As influências das partes interessadas (stakeholders), os riscos e a incerteza (conforme mostrado na Figura 4.) são maiores no início do projeto. Esses fatores diminuem ao longo do tempo;
- A capacidade de influenciar as características finais do produto do projeto, sem afetar significativamente o custo, é maior no início do projeto e diminui à medida que o projeto avança em direção à conclusão. A Figura 4 mostra que o custo de fazer mudanças e corrigir erros geralmente aumenta consideravelmente à medida que o projeto se aproxima do fim.

Figura 4: Impacto de Variáveis Baseado no Tempo do Projeto



Fonte: GUIDE, 2001 (2023)

Dentro do contexto da estrutura genérica do ciclo de vida, um gerente de projeto pode perceber a necessidade de um controle mais eficaz sobre certas entregas. Especialmente em projetos grandes e complexos, pode ser necessário um nível adicional de controle. Nesses casos, dividir formalmente o trabalho realizado para atingir o objetivo do projeto em fases pode trazer benefícios significativos.

2.1.2 Fases do Projeto

As fases do projeto são divisões dentro do projeto onde é necessário um controle adicional para gerenciar efetivamente a conclusão de uma entrega importante. Essas fases são geralmente executadas em sequência, mas em algumas situações podem ocorrer sobreposições. As fases do projeto fazem parte do ciclo de vida do projeto e não devem ser confundidas com os Grupos de Processos de Gerenciamento de Projetos.

A estrutura de fases permite segmentar o projeto em subsets lógicos para facilitar o gerenciamento, planejamento e controle. O número de fases, a necessidade de fases e o nível de controle aplicado dependem do tamanho, complexidade e impacto potencial do projeto. Independentemente do número de

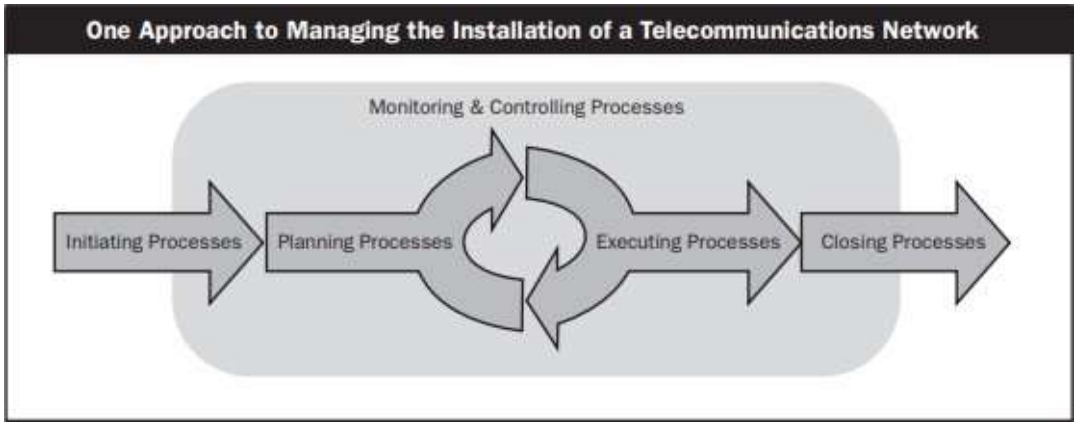
fases que compõem um projeto, todas as fases possuem características semelhantes:

- Quando as fases são executadas sequencialmente, o encerramento de cada fase ocorre com uma transferência ou entrega do trabalho produzido como resultado da fase. Esse encerramento de fase representa um momento oportuno para reavaliar o andamento do projeto e tomar decisões de continuidade ou encerramento, se necessário. Esses pontos são conhecidos como marcos de fase, pontos de decisão ou pontos de encerramento.
- Cada fase possui um foco distinto que difere das outras fases. Isso geralmente envolve diferentes organizações e conjuntos de habilidades específicas.

A entrega principal ou objetivo da fase requer um controle adicional para ser alcançada com sucesso. A repetição dos processos em todos os cinco Grupos de Processos de Gerenciamento de Projetos (Iniciação, planejamento, execução, monitoramento e controle e encerramento), proporciona esse controle adicional e define os limites da fase.

Embora muitos projetos possam ter fases com nomes semelhantes e entregas similares, poucos projetos são idênticos. Alguns projetos podem ter apenas uma fase, como ilustrado na Figura 5, enquanto outros podem ter múltiplas fases. A duração e extensão de cada fase podem variar de projeto para projeto.

Figura 5: Exemplo de um Projeto de Única Fase



Fonte: GUIDE, 2001 (2023)

Segundo o PMBOK, não existe uma única forma de definir a estrutura ideal para um projeto. Embora as práticas comuns da indústria frequentemente levem ao uso de uma estrutura preferida, projetos na mesma indústria - ou até mesmo na mesma organização - podem apresentar variações significativas.

As estruturas de projeto podem variar significativamente, dependendo da organização e da equipe de projeto envolvida.

Um exemplo utilizado no PMBOK (GUIDE, 2001) é que um estudo de viabilidade pode ser visto por uma organização como uma atividade pré-projeto rotineira, enquanto outra pode considerá-lo como a primeira fase do projeto, e ainda outra pode tratá-lo como um projeto separado e independente. Da mesma forma, a equipe de projeto pode optar por dividir um projeto em múltiplas fases, enquanto outra equipe pode escolher gerenciar todo o trabalho como uma única fase. A escolha da estrutura de projeto é influenciada pela natureza específica do projeto e pelo estilo de trabalho da equipe ou organização envolvida.

O guia PMBOK é organizado em dez áreas de conhecimento, que abrangem os processos e práticas fundamentais do gerenciamento de projetos:

- **Integração do Projeto:** Inclui os processos necessários para coordenar os diversos elementos do projeto de forma coesa;
- **Escopo do Projeto:** Define e controla o que está incluído e excluído do projeto;
- **Cronograma do Projeto:** Envolve a definição das atividades do projeto, sequenciamento, estimativa de duração e desenvolvimento do cronograma;
- **Custos do Projeto:** Abrange a estimativa, orçamento e controle dos custos do projeto;
- **Qualidade do Projeto:** Inclui as atividades e processos necessários para garantir que o projeto atenda aos requisitos e padrões de qualidade;
- **Recursos Humanos do Projeto:** Trata do gerenciamento das equipes de projeto, incluindo seleção, desenvolvimento e gestão de recursos humanos;
- **Comunicações do Projeto:** Abrange o planejamento, distribuição, armazenamento e recuperação das informações do projeto;
- **Gerenciamento de Riscos do Projeto:** Envolve a identificação, análise, planejamento e controle dos riscos do projeto;
- **Aquisições do Projeto:** Abrange o planejamento, aquisição e gerenciamento de fornecedores e recursos externos ao projeto;

- **Partes Interessadas do Projeto:** Trata do gerenciamento das partes interessadas, identificando-as, envolvendo-as e gerenciando suas expectativas.

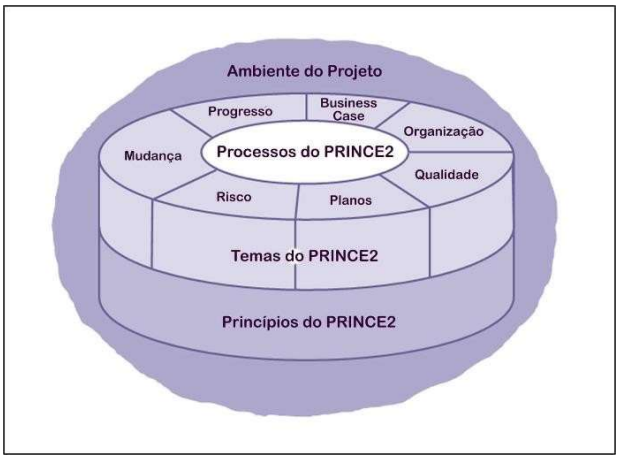
O PMBOK é uma referência valiosa para profissionais de gerenciamento de projetos, fornecendo uma estrutura e terminologia comuns que podem ser aplicadas em diferentes projetos e organizações. No entanto, é importante destacar que o PMBOK é um guia e não um método prescritivo, e os gerentes de projeto devem adaptar suas abordagens às necessidades específicas de cada projeto. Cada um desses processos acima desempenha um papel fundamental em diferentes estágios do ciclo de vida do projeto e contribui para a entrega bem-sucedida do projeto.

2.2 PRINCE2 (Projects in Controlled Environments)

O PRINCE2 é uma metodologia de gerenciamento de projetos amplamente adotada, especialmente no contexto de TI. Ele fornece uma estrutura estruturada para o gerenciamento de riscos em projetos de desenvolvimento de software, enfatizando a importância do controle e da governança. Segundo a AXELOS (organização que mantém o PRINCE2), o PRINCE2 enfoca a identificação e análise de riscos em todas as fases do projeto, estabelecendo processos claros para a gestão de riscos e a definição de responsabilidades. Ele também enfatiza a necessidade de atualizar e revisar continuamente o plano de gerenciamento de riscos à medida que o projeto avança.

O PRINCE2 possui uma estrutura bem definida, composta por sete princípios, sete temas e sete processos. Esses elementos trabalham em conjunto para fornecer uma abordagem abrangente e controlada para o gerenciamento de projetos. Como ilustrado na Figura 6, a estrutura do PRINCE2 é a seguinte:

Figura 6: Estrutura PRINCE2



Fonte: GOVERNMENT COMMERCE, 2011 (2023)

2.2.1 Principios do PRINCE2 (Projects in Controlled Environments)

Os princípios do PRINCE2 fornecem a base essencial para orientar o planejamento, execução e controle de projetos de maneira eficaz e eficiente. Esses princípios, que refletem as melhores práticas da indústria e a experiência acumulada ao longo do tempo, são fundamentais para garantir o sucesso do projeto e a entrega de resultados satisfatórios para todas as partes interessadas.

Nesta seção, exploraremos os sete princípios do PRINCE2, destacando sua importância e aplicação no contexto do gerenciamento de projetos. Ao compreender e aplicar esses princípios, os gerentes de projeto podem melhorar significativamente as chances de alcançar os objetivos do projeto e atender às expectativas das partes interessadas. São elas:

Justificativa contínua do negócio (Business Justification): O princípio da justificativa contínua do negócio assegura que o projeto esteja sempre alinhado aos objetivos estratégicos da organização. Ele requer uma análise regular da viabilidade do projeto em termos de benefícios esperados, riscos envolvidos, custos e impacto nas operações organizacionais. A justificativa contínua do negócio garante que o projeto permaneça viável e que as decisões sejam baseadas em informações atualizadas.

Aprendizado de lições (Learn from Experience): Esse princípio enfatiza a importância de aprender com as experiências anteriores de projetos. É essencial documentar as lições aprendidas e aplicá-las no planejamento e execução do projeto

atual. O aprendizado de lições contribui para a melhoria contínua do desempenho do projeto, evitando erros repetidos e aproveitando as melhores práticas identificadas em projetos anteriores.

Papeis e responsabilidades definidos (Defined Roles and Responsibilities): O PRINCE2 enfatiza a definição clara dos papéis e responsabilidades de cada membro da equipe do projeto. Isso evita ambiguidade e conflitos, garantindo que todos saibam suas responsabilidades e autoridades dentro do projeto. A definição precisa dos papéis também facilita a comunicação e a tomada de decisões eficazes.

Gerenciamento por estágios (Manage by Stages): Esse princípio divide o projeto em estágios gerenciáveis. Cada estágio tem seus objetivos claros, produtos entregáveis e critérios de controle. O gerenciamento por estágios permite uma abordagem incremental, com revisões regulares para avaliar o progresso, a viabilidade e a justificativa contínua do projeto. Essa abordagem permite que decisões informadas sejam tomadas a cada estágio, com base em informações atualizadas.

Gerenciamento por exceção (Manage by Exception): O princípio do gerenciamento por exceção estabelece limites claros de autoridade para a tomada de decisões. Os limites são definidos para os níveis de tolerância de cada aspecto do projeto, como custo, prazo e qualidade. Isso permite que a equipe do projeto tome ações corretivas dentro dos limites estabelecidos sem a necessidade de relatar a cada detalhe. O gerenciamento por exceção promove a delegação eficiente de autoridade e responsabilidade.

Foco no produto (Focus on Products): Esse princípio coloca o produto como o ponto central do projeto. Ele enfatiza a importância de entender claramente os requisitos e especificações do produto e garantir que os produtos entregues estejam em conformidade com esses requisitos. O foco no produto envolve a definição precisa dos produtos, sua qualidade esperada e a atribuição clara de responsabilidade.

Adaptação ao ambiente do projeto (Tailor to Suit the Project Environment): O último princípio do PRINCE2 destaca a importância de adaptar a metodologia às características e complexidades específicas do projeto. Cada projeto é único, e é necessário ajustar o PRINCE2 para atender às necessidades e restrições específicas do ambiente do projeto. Isso envolve a seleção e aplicação

adequada dos processos, temas e técnicas do PRINCE2 de acordo com a escala, riscos e complexidade do projeto. A adaptação ao ambiente do projeto garante que o PRINCE2 seja flexível e aplicável em diferentes contextos de projeto.

2.2.2 Temas do PRINCE2 (Projects in Controlled Environments)

Nesta seção, serão apresentados estudos e casos que abordam a aplicação da Análise Preliminar de Riscos (APR) em diferentes setores. A APR é uma metodologia utilizada para identificar riscos potenciais em um projeto, processo ou atividade antes que ocorram problemas. Ela envolve a avaliação sistemática de cada etapa do processo para identificar possíveis perigos, analisando as consequências e as probabilidades de ocorrência de eventos indesejados.

Serão discutidos os benefícios da APR, como a identificação precoce de riscos, o que permite a implementação de medidas de controle eficazes e a mitigação de potenciais impactos negativos. A aplicação da APR é fundamental para garantir a segurança, a conformidade e a eficiência operacional, reduzindo a possibilidade de acidentes e prejuízos.

Business Case (Caso de Negócio): É fundamental para o PRINCE2, pois define e justifica os benefícios esperados do projeto. Ele envolve a identificação dos objetivos e resultados desejados, bem como a análise dos custos, benefícios e riscos associados ao projeto. O Business Case fornece a base para a tomada de decisões ao longo do projeto, garantindo que o projeto continue a ser viável e alinhado com as metas estratégicas da organização.

Organization (Organização): Define a estrutura de papéis e responsabilidades no projeto. Isso inclui a designação de uma equipe de gerenciamento do projeto, composta pelo Gerente de Projeto, Patrocinador e outros stakeholders relevantes. Além disso, o tema Organization também aborda a identificação e envolvimento das partes interessadas, a definição das interfaces entre as equipes e a clara atribuição de responsabilidades. Uma estrutura organizacional bem definida é essencial para garantir uma comunicação eficaz e uma governança adequada do projeto.

Quality (Qualidade): Abrange a definição dos critérios de qualidade para os produtos do projeto e os processos para garantir a conformidade. Isso envolve a

identificação dos requisitos de qualidade, a definição dos padrões a serem seguidos e a implementação de atividades de controle de qualidade. O tema Quality assegura que os produtos entregues pelo projeto atendam aos padrões e requisitos estabelecidos, garantindo a satisfação do cliente e a excelência na entrega.

Plans (Planos): Envolve o desenvolvimento de planos detalhados para orientar a execução do projeto. Isso inclui a criação de planos de projeto que descrevam as atividades, cronogramas, recursos e riscos envolvidos. Além disso, o tema Plans também aborda o monitoramento e controle dos planos, ajustando-os conforme necessário à medida que o projeto avança. Os planos fornecem uma visão clara das atividades e recursos necessários, permitindo um gerenciamento eficiente e uma comunicação eficaz durante o projeto.

Risk (Riscos): O tema Risk no PRINCE2 tem como objetivo identificar, avaliar e controlar os riscos associados ao projeto. Isso envolve a identificação de eventos incertos que possam impactar o projeto, a avaliação dos riscos em termos de probabilidade e impacto, e o desenvolvimento de estratégias para mitigar ou responder aos riscos identificados. O tema Risk visa garantir que os riscos sejam gerenciados de forma proativa, minimizando possíveis impactos negativos no projeto.

Change (Mudanças): Aborda a gestão das mudanças no escopo, requisitos e produtos do projeto. No PRINCE2, reconhece-se que as mudanças são inevitáveis durante o ciclo de vida do projeto e é importante gerenciá-las de forma eficaz. Isso inclui estabelecer um processo formal de solicitação e avaliação de mudanças, definir critérios para aprovação ou rejeição de mudanças, e garantir que as mudanças sejam devidamente implementadas e controladas. O tema Change visa garantir que as mudanças sejam gerenciadas de forma controlada, minimizando os impactos negativos e garantindo que o projeto continue alinhado aos objetivos e requisitos definidos.

Progress (Progresso): O tema Progress diz respeito ao monitoramento e controle do progresso do projeto em relação ao plano. Isso envolve o estabelecimento de mecanismos de monitoramento, a definição de indicadores de desempenho, a avaliação contínua do progresso em relação às metas estabelecidas e a implementação de medidas corretivas quando necessário. O tema Progress fornece uma visão clara do estado atual do projeto, permitindo que os gerentes

tomem decisões informadas e realizem ajustes para garantir o cumprimento dos prazos, orçamentos e entregas planejadas.

É importante destacar que a estrutura dos temas do PRINCE2 fornece uma abordagem abrangente e consistente para o gerenciamento de projetos. A adoção desses temas ajuda a garantir que aspectos críticos, como benefícios, organização, qualidade, planejamento, riscos, mudanças e progresso, sejam devidamente considerados ao longo do ciclo de vida do projeto, contribuindo para o sucesso geral da iniciativa.

2.2.3 Processos do PRINCE2 (Projects in Controlled Environments)

A estrutura do PRINCE2 é composta por sete processos que abrangem o ciclo de vida completo de um projeto. Cada processo tem um propósito específico e define as atividades e responsabilidades necessárias para alcançar seus objetivos. Vamos explorar cada um desses processos:

Starting up a Project (Iniciar um Projeto): O processo de Starting up a Project é realizado no início do projeto e tem como objetivo preparar os documentos iniciais, estabelecer os objetivos e o ambiente de controle do projeto. Nesse processo, são identificados o patrocinador do projeto, o executivo responsável e os membros da equipe de gerenciamento do projeto. Também são estabelecidos os limites e as restrições iniciais do projeto, como o escopo e o prazo. Além disso, são produzidos documentos como o Mandate (Mandato) e o Project Brief (Resumo do Projeto).

Directing a Project (Direcionar um Projeto): O processo de Directing a Project é executado durante todo o ciclo de vida do projeto e é responsável por fornecer orientação e tomada de decisões estratégicas para o projeto. Nesse processo, são definidos o Business Case (Caso de Negócio) e a estratégia de gerenciamento do projeto. O Comitê Diretor do Projeto, composto por representantes-chave do projeto, é responsável por revisar o progresso, aprovar planos e tomar decisões importantes para o projeto.

Initiating a Project (Iniciar um Projeto): O processo de Initiating a Project é realizado no início do projeto e tem como objetivo definir o escopo, estabelecer as bases do projeto e criar o Plano de Gerenciamento do Projeto. Nesse processo, são

desenvolvidos o Project Initiation Documentation (Documento de Iniciação do Projeto) e o Business Case completo. Também são identificados os produtos e suas respectivas entregas, além de estabelecer os critérios de controle de qualidade.

Controlling a Stage (Controlar uma Etapa): O processo de Controlling a Stage é executado durante cada etapa do projeto e tem como objetivo monitorar e controlar o progresso da etapa atual. Nesse processo, são definidas as atividades a serem realizadas, os recursos necessários e os responsáveis por cada uma delas. O Gerente de Estágio é responsável por garantir que a etapa esteja sendo executada de acordo com o Plano de Estágio aprovado, monitorando o progresso, lidando com exceções e tomando medidas corretivas quando necessário.

Managing Product Delivery (Gerenciar a Entrega de Produtos): O processo de Managing Product Delivery é responsável por gerenciar a produção e a entrega dos produtos do projeto. Nesse processo, o Gerente de Entrega do Produto trabalha em conjunto com a equipe de fornecedores para criar os produtos de acordo com as especificações e prazos estabelecidos. São estabelecidos acordos contratuais, monitorado o progresso da entrega dos produtos é garantida a qualidade de cada um deles.

Managing Stage Boundaries (Gerenciar os Limites da Etapa): O processo de Managing Stage Boundaries ocorre no final de cada etapa do projeto e é responsável por planejar e preparar a transição para a próxima etapa. Nesse processo, é revisado o desempenho da etapa atual, avaliando se os objetivos foram alcançados e se os produtos foram entregues conforme o esperado. São atualizados os registros de lições aprendidas e preparado o Plano de Próxima Etapa, que descreve as atividades e recursos necessários para a próxima fase do projeto. O Comitê Diretor do Projeto revisa e aprova o Plano de Próxima Etapa antes de autorizar o início da próxima etapa.

Closing a Project (Encerrar um Projeto): O processo de Closing a Project é executado no final do projeto e tem como objetivo formalizar o encerramento do projeto de forma controlada. Nesse processo, são realizadas atividades como avaliação do desempenho do projeto em relação aos objetivos estabelecidos, registro de lições aprendidas, arquivamento de documentos e comunicação do encerramento aos interessados relevantes. O objetivo é garantir que todos os aspectos do projeto sejam concluídos adequadamente e que as lições aprendidas possam ser aplicadas em projetos futuros.

3 METODOLOGIA DA PESQUISA

A metodologia adotada nesta pesquisa baseia-se na técnica de pesquisa bibliográfica, essencial para a construção do conhecimento acadêmico. Esta seção detalha os procedimentos metodológicos utilizados, destacando a relevância, as etapas e as boas práticas para a condução eficaz da pesquisa bibliográfica.

3.1 Pesquisa Bibliográfica

A pesquisa bibliográfica é uma técnica fundamental e amplamente utilizada na investigação acadêmica. Segundo Gil (2008), ela desempenha um papel crucial no processo de construção do conhecimento, fornecendo uma base sólida de informações e insights a partir de estudos anteriores sobre o tema em questão. De acordo com Marconi e Lakatos (2017), a pesquisa bibliográfica envolve a seleção e análise de obras já publicadas, permitindo ao pesquisador identificar, reunir e avaliar o conhecimento acumulado sobre um determinado assunto.

Além disso, a pesquisa bibliográfica é essencial para a fundamentação teórica de trabalhos científicos, como os relacionados às estratégias de gerenciamento de riscos em empresas e Tecnologias da Informação e Comunicação (TIC), baseadas nas principais normas e frameworks, como ISO 31000, PRINCE2, COBIT, NIST e PMBOK. Como destacado por Lakatos e Marconi (2003), a pesquisa bibliográfica oferece um panorama das principais abordagens teóricas e práticas, facilitando a compreensão das metodologias e práticas de gerenciamento de riscos já validadas e aplicadas em diferentes contextos.

Por fim, conforme afirma Creswell (2014), a pesquisa bibliográfica deve seguir boas práticas que incluem a seleção criteriosa das fontes, a leitura crítica e a síntese das informações, garantindo que o estudo seja conduzido com rigor e relevância.

3.2 Relevância da Pesquisa Bibliográfica

No contexto acadêmico, a pesquisa bibliográfica cumpre diversas funções essenciais:

1. Contextualização do Estudo: Permite ao pesquisador situar seu estudo dentro do contexto mais amplo da literatura existente, oferecendo um panorama das principais teorias, conceitos e debates relacionados ao tema de interesse.

2. Identificação de Lacunas: Ao examinar as contribuições de estudos anteriores, o pesquisador pode identificar lacunas no conhecimento existente e formular questões de pesquisa que contribuam para o avanço do campo de estudo.
3. Base Teórica: Oferece uma base teórica sólida para o desenvolvimento do problema de pesquisa, hipóteses e objetivos do estudo. A revisão crítica da literatura relevante ajuda a identificar diferentes enfoques teóricos e selecionar os que melhor se alinham com os objetivos da pesquisa.

3.3 Etapas da Pesquisa Bibliográfica

Embora a pesquisa bibliográfica não possua fases tão distintas quanto algumas técnicas de coleta de dados, ela pode ser dividida em etapas que orientam o processo de maneira eficiente. As principais etapas são:

1. Definição do Tema e Escopo da Pesquisa: Nesta fase, o pesquisador identifica o tema específico a ser investigado e delimita o escopo da pesquisa. Isso envolve definir os principais conceitos a serem abordados e os limites temporais e geográficos da pesquisa.
2. Identificação de Fontes de Informação: O pesquisador busca identificar fontes de informação relevantes para o tema em questão. Isso inclui pesquisa em bancos de dados acadêmicos, catálogos de bibliotecas, revistas científicas, livros, teses, dissertações, entre outros.
3. Seleção de Fontes: Uma vez identificadas as fontes de informação, o pesquisador avalia sua relevância e confiabilidade. Isso pode envolver a leitura de resumos, análise de conteúdo, e avaliação da reputação do autor e da publicação.
4. Leitura e Análise Crítica: Nesta fase, o pesquisador realiza a leitura crítica das fontes selecionadas, identificando os principais argumentos, conceitos, teorias e evidências apresentadas. Avalia também a consistência e qualidade do material encontrado, identificando lacunas, contradições ou pontos de interesse.
5. Síntese e Organização dos Resultados: Com base na leitura e análise crítica, o pesquisador sintetiza as informações relevantes e organiza os principais conceitos, teorias e descobertas em um formato compreensível. Isso pode incluir resumos, sínteses, mapas conceituais ou esquemas.

6. Citação e Referenciação: Por fim, o pesquisador deve citar corretamente todas as fontes utilizadas, seguindo as normas de referência bibliográfica adequadas (por exemplo, ABNT, APA, MLA, etc.). Isso garante a integridade acadêmica do trabalho e dá crédito aos autores das obras consultadas.

3.4 Boas Práticas para Realização da Pesquisa Bibliográfica

- Planejamento Cuidadoso: Definir claramente os objetivos e o escopo da pesquisa, e planejar a busca de informações com antecedência.
- Critérios de Seleção Rigorosos: Utilizar critérios rigorosos para a seleção das fontes, considerando relevância, confiabilidade e atualidade.
- Análise Crítica: Realizar uma leitura crítica e detalhada das fontes, destacando os principais pontos de interesse e identificando possíveis lacunas na literatura existente.
- Organização e Síntese: Organizar de forma lógica e coerente os dados e informações obtidas, facilitando a compreensão e utilização no desenvolvimento do trabalho de pesquisa.

3.5 Classificação Metodológica

A metodologia adotada nesta pesquisa baseia-se na técnica de pesquisa bibliográfica, essencial para a construção do conhecimento acadêmico. Esta seção detalha os procedimentos metodológicos utilizados, destacando a relevância, as etapas e as boas práticas para a condução eficaz da pesquisa bibliográfica.

Tabela 1: Quadro Metodológico

Quanto à Natureza	Pesquisa Básica
Objetivos	Exploratório
Procedimentos	Pesquisa Bibliográfica
Forma de abordagem	Qualitativa

Fonte: Próprio Autor (2024)

3.5.1 Quanto à Natureza

Pesquisa Básica, esta pesquisa busca gerar conhecimentos novos e teóricos sobre os riscos de TI, ampliando o entendimento sobre o tema e contribuindo para o avanço do conhecimento na área.

3.5.2 Quanto ao Objetivo

Em relação ao objetivo, a metodologia é exploratória, buscando proporcionar maior familiaridade com o problema dos riscos de TI, tornando-o explícito e construindo hipóteses que possam guiar investigações futuras. Essa abordagem é especialmente útil para esclarecer conceitos, identificar problemas e propor novas questões de pesquisa.

3.5.3 Quanto aos Procedimentos

A pesquisa bibliográfica é o método adotado, baseando-se na revisão crítica da literatura existente sobre os riscos de TI. Isso inclui a análise de livros, artigos científicos, teses, dissertações e outras fontes acadêmicas relevantes para o tema em questão.

3.5.4 Quanto a Abordagem

A abordagem qualitativa é focada na compreensão aprofundada dos conceitos, teorias e práticas relacionadas aos riscos de TI. Isso envolve uma análise interpretativa dos dados coletados, sem a intenção de quantificá-los, buscando compreender a complexidade do fenômeno em estudo.

3.6 Conclusão

No capítulo 3, a metodologia da pesquisa foi detalhadamente abordada, destacando a importância da pesquisa bibliográfica como técnica fundamental para garantir a qualidade e a validade dos resultados obtidos. A escolha dessa abordagem foi fundamentada na necessidade de revisar e analisar criticamente o conhecimento existente sobre os riscos de TI.

4. PROPOSTA DE APOIO A EMPRESAS DE TIC PARA INVESTIR EM METODOLOGIAS DE GERENCIAMENTO DE RISCOS

No cenário altamente dinâmico e competitivo da Tecnologia da Informação e Comunicação (TIC), o gerenciamento eficaz de riscos é essencial para garantir a continuidade dos negócios e proteger os ativos empresariais. Investir em metodologias de gerenciamento de riscos permite às empresas de TIC identificar, avaliar e mitigar riscos potenciais, minimizando impactos negativos e maximizando oportunidades. Esta proposta visa oferecer um suporte estruturado para incentivar as empresas de TIC a adotarem práticas robustas de gerenciamento de riscos, utilizando referenciais reconhecidos internacionalmente, como ISO 31000, NIST e COBIT.

O objetivo desta proposta é fornecer um plano abrangente para empresas de TIC sobre como implementar e investir em metodologias de gerenciamento de riscos, utilizando padrões e frameworks reconhecidos como ISO 31000, NIST, e COBIT, além de promover uma cultura organizacional voltada para a gestão proativa de riscos.

4.1 Justificativa

A adoção de metodologias de gerenciamento de riscos oferece diversos benefícios para empresas de TIC, incluindo:

- **Proteção dos Ativos**: Minimiza a exposição a ameaças e vulnerabilidades (Sommerville, 2016).
- **Conformidade Regulatória**: Assegura o cumprimento de normas e regulamentos, evitando penalidades (Aven, 2016).
- **Continuidade dos Negócios**: Garante operações contínuas, mesmo diante de incidentes imprevistos (Ross et al., 2018).
- **Vantagem Competitiva**: Melhora a confiança dos clientes e stakeholders, promovendo uma imagem de resiliência e responsabilidade (De Haes et al., 2020).

4.2 Dados sobre a adoção de metodologias de gerenciamento de riscos em empresas de TIC

A adoção de metodologias de gerenciamento de riscos em empresas de TIC é uma prática amplamente reconhecida. De acordo com o relatório "Pulse of the Profession" de 2020 do Project Management Institute (PMI),

aproximadamente 77% das organizações reconhecem a importância do gerenciamento de riscos como uma competência crítica para o sucesso do projeto. Outro estudo da ISACA de 2018 revelou que cerca de 60% das organizações de TI utilizam algum tipo de framework formal de gerenciamento de riscos, como COBIT ou ISO 31000. Um relatório de 2019 da Gartner indicou que mais de 70% das grandes empresas de TIC adotam metodologias formais de gerenciamento de riscos, embora a eficácia varie dependendo da maturidade organizacional e do nível de integração dessas práticas nos processos de negócios.

4.3 ISO 31000

A ISO 31000 é um padrão internacional que fornece princípios e diretrizes para o gerenciamento de riscos. Segundo Aven (2016), a ISO 31000 oferece uma abordagem estruturada para o gerenciamento de riscos, abrangendo três componentes principais:

- **Princípios**: Estabelecem uma abordagem sistemática, estruturada e oportuna para o gerenciamento de riscos.
- **Estrutura**: Integra o gerenciamento de riscos na estrutura organizacional, assegurando que a gestão de riscos esteja alinhada com os objetivos estratégicos.
- **Processo**: Envolve a identificação, avaliação, tratamento, monitoramento e revisão contínua dos riscos.

4.4 NIST (National Institute of Standards and Technology)

O NIST oferece uma estrutura para melhorar a segurança cibernética e a resiliência das infraestruturas críticas. Conforme Ross et al. (2018), o framework do NIST é composto por:

- **Framework Core**: Conjunto de atividades e resultados desejados divididos em cinco funções: Identificar, Proteger, Detectar, Responder e Recuperar.
- **Implementation Tiers**: Níveis que indicam a maturidade do programa de segurança cibernética.
- **Profiles**: Descrição das posturas atuais e desejadas em relação ao gerenciamento de riscos cibernéticos.

4.5. COBIT (Control Objectives for Information and Related Technologies)

O COBIT é um framework para a governança e gerenciamento de TI corporativa. De acordo com De Haes et al. (2020), seus principais elementos são:

- **Principles**: Diretrizes para uma governança eficaz de TI.
- **Governance and Management Objectives**: Objetivos que ajudam a alinhar a TI com os objetivos de negócios.
- **Components**: Recursos necessários para atingir os objetivos de governança e gerenciamento.

4.6 Metodologias de Gerenciamento de Riscos

4.6.1 Análise de Riscos em Ativos de TIC

A análise de riscos em ativos de TIC envolve a identificação e avaliação de riscos associados aos ativos de TI, como redes, hardware, software e recursos humanos. De acordo com Dadmarz (2019), essa análise deve considerar os seguintes aspectos:

- **Identificação de Ativos**: Inclui rede, hardware, software e recursos humanos.
- **Avaliação de Riscos**: Confidencialidade, integridade, disponibilidade e vulnerabilidades.
- **Metodologias**: Adoção de frameworks como COBIT e ISO/IEC 17799 para planejar e implementar medidas de segurança.

4.6.2 Modelagem Econômica para Gestão de Riscos de Segurança da Informação

A modelagem econômica para gestão de riscos de segurança da informação envolve a avaliação do investimento necessário em tecnologia de segurança e a análise de riscos para determinar os melhores investimentos. Segundo Bojanc e Jerman-Blazic (2008), os principais componentes incluem:

- **Avaliação Econômica**: Investimento necessário em tecnologia de segurança.
- **Métodos de Identificação**: Ameaças e vulnerabilidades dos sistemas de TIC.
- **Seleção de Investimentos**: Análises quantificadas de risco para determinar os melhores investimentos.

4.6.3 Metodologia Intuitiva para Seleção de Abordagens de Gerenciamento de Riscos

A metodologia intuitiva para seleção de abordagens de gerenciamento de riscos utiliza métodos gráficos-vetoriais para facilitar a tomada de decisão e a implementação simplificada em projetos de TIC. Segundo Rodríguez et al. (2017), essa abordagem envolve:

- **Método Gráfico-Vetorial**: Facilitação da tomada de decisão.
- **Processos Intuitivos**: Implementação simplificada em projetos de TIC.

4.6.4 Controle de Riscos com Pensamento de Opções Reais

O controle de riscos com pensamento de opções reais utiliza técnicas qualitativas para o gerenciamento de riscos em projetos de TIC, baseando-se em estudos de caso reais. De acordo com Angelou e Economides (2007), essa abordagem inclui:

- **Técnicas Qualitativas**: Gerenciamento de riscos em projetos de TIC.
- **Estratégias de Implantação**: Baseadas em estudos de caso reais.

4.7 Empresas Pioneiras no Gerenciamento de Riscos

4.7.1 IBM

Figura 7: Logo IBM

Fonte: Wikipedia.org (2023)

Reconhecida por sua expertise em desenvolvimento de software e serviços de consultoria em TI, a IBM aplica metodologias de gerenciamento de riscos em suas soluções de software. A empresa realiza análises detalhadas de riscos e implementa estratégias de mitigação para garantir o sucesso de seus projetos. Segundo Dittmann et al. (2020), a IBM integra práticas como a análise de risco contínua e a

implementação de controles de segurança robustos em seus processos de desenvolvimento de software, seguindo padrões reconhecidos como ISO 31000 e COBIT.

4.7.2 Amazon

Figura 8: Logo Amazon

Fonte: Wikipedia.org (2023)

Líder em serviços de computação em nuvem e desenvolvimento de software, a Amazon adota abordagens ágeis e incorpora metodologias de gerenciamento de riscos em seus processos de desenvolvimento. Isso garante a confiabilidade e segurança de suas plataformas e serviços. De acordo com Villarroel et al. (2019), a Amazon utiliza frameworks como NIST e PRINCE2 em seu processo de gerenciamento de riscos, especialmente para assegurar a conformidade com regulamentos e a resiliência de seus serviços em nuvem.

4.7.3 Oracle

Figura 9: Logo Oracle

Fonte: Wikipedia.org (2023)

Oferecendo uma ampla gama de soluções de software empresarial, a Oracle aplica metodologias de gerenciamento de riscos em seus produtos e serviços. Isso inclui análises detalhadas de riscos, planos de contingência e medidas de segurança para proteger os dados e sistemas de seus clientes. Segundo Henderson (2018), a Oracle segue práticas de gerenciamento de riscos baseadas em frameworks como PMBOK

e ISO 31000, garantindo que suas soluções atendam aos mais altos padrões de segurança e desempenho.

4.8 Benefícios do Investimento em Gerenciamento de Riscos

Sommerville (2016) destaca a importância do gerenciamento de riscos como uma parte intrínseca do processo de desenvolvimento de software. Ele enfatiza que as empresas devem adotar abordagens proativas para identificar e mitigar riscos, reconhecendo a inevitabilidade da incerteza no desenvolvimento de software e a necessidade de um gerenciamento eficaz para lidar com essa incerteza. Ao investir em metodologias de gerenciamento de riscos, as empresas de TIC podem colher uma série de benefícios:

- **Minimização de Impactos Negativos**: A identificação proativa e a mitigação de riscos potenciais ajudam a reduzir a probabilidade de falhas e atrasos nos projetos de desenvolvimento de software, garantindo uma entrega mais eficiente e dentro do prazo (Sommerville, 2016).
- **Maximização de Oportunidades**: Além de mitigar riscos, as metodologias de gerenciamento de riscos auxiliam na identificação e aproveitamento de oportunidades. Ao analisar o ambiente do projeto e os possíveis cenários futuros, as empresas podem descobrir oportunidades de inovação e melhoria que, de outra forma, poderiam passar despercebidas (Aven, 2016).
- **Aumento da Confiança dos Stakeholders**: O investimento em gerenciamento de riscos demonstra compromisso com a transparência, responsabilidade e qualidade. Isso aumenta a confiança dos stakeholders, incluindo clientes, investidores e parceiros comerciais (Ross et al., 2018).
- **Redução de Custos a Longo Prazo**: Embora o investimento inicial em metodologias de gerenciamento de riscos possa exigir recursos adicionais, a longo prazo, pode resultar em uma redução significativa de custos. Evitar falhas, retrabalhos e atrasos resultantes de riscos não gerenciados economiza tempo e recursos valiosos (De Haes et al., 2020).
- **Melhoria da Competitividade**: Empresas que adotam abordagens eficazes de gerenciamento de riscos estão melhor posicionadas para competir no mercado.

Reduzindo a incerteza e aumentando a previsibilidade em seus projetos, essas empresas podem responder mais rapidamente às demandas do mercado, adaptar-se a mudanças e oferecer produtos e serviços de alta qualidade (Sommerville, 2016).

4.9 Conclusão

O investimento em metodologias de gerenciamento de riscos é essencial para o sucesso a longo prazo das empresas de TIC. Além de minimizar os impactos negativos dos riscos, essas metodologias capacitam as empresas a identificarem e aproveitar oportunidades, aumentar a confiança dos stakeholders, reduzir custos e melhorar sua competitividade no mercado. Portanto, as empresas de TIC que desejam prosperar e crescer devem priorizar o desenvolvimento e implementação de práticas eficazes de gerenciamento de riscos em seus processos de desenvolvimento de software.

5 TRABALHOS RELACIONADOS

Neste capítulo, iremos explorar **pesquisas acadêmicas**, exploraremos os termos fundamentais relacionados aos riscos empresariais e à gerência de riscos, além de oferecer uma visão abrangente sobre como as empresas podem abordar efetivamente esses desafios, a discussão sobre riscos empresariais e sua gestão tem sido um tema de interesse constante ao longo dos anos. No entanto, a falta de clareza e precisão na terminologia relacionada a esse campo tem sido um obstáculo significativo. Para enriquecer ainda mais o capítulo sobre gerenciamento de riscos empresariais, podemos incluir referências a pesquisas relevantes, como o estudo *"Tecnologias Consagradas de Gestão de Riscos" (De Cicco & Fantazzini, 2003)*. Este estudo oferece uma análise aprofundada das práticas estabelecidas na gestão de riscos, fornecendo insights valiosos sobre as metodologias e ferramentas tradicionais utilizadas pelas empresas para lidar com os desafios relacionados aos riscos empresariais.

Ao incorporar essa pesquisa, podemos destacar a importância de compreender não apenas os conceitos fundamentais, mas também as abordagens práticas e as tecnologias disponíveis para a gestão eficaz de riscos nas organizações modernas.

5.1 Definição dos Termos Fundamentais Perigo e Risco

- Perigo (Hazard): Refere-se a uma ou mais condições com potencial para causar danos, como lesões pessoais, danos materiais, perda de material ou redução de desempenho. O perigo implica na possibilidade de efeitos adversos.
- Risco (Risk): Expressa a probabilidade de danos dentro de um período específico ou número de operações. Pode ser calculado pela probabilidade de um acidente multiplicado pelo dano esperado.
- Segurança: Embora seja frequentemente definida como a ausência de perigos, é praticamente impossível eliminar completamente todos os perigos. Segurança refere-se, portanto, a um compromisso de proteção relativa contra exposição a perigos, sendo o oposto do nível de perigo.
- Nível de Perigo (Danger): Indica a exposição relativa a um perigo, aumentando a probabilidade de danos.

- Dano: Refere-se à gravidade da perda humana, material ou financeira que pode ocorrer se o controle sobre um perigo for perdido.
- Causa: A origem, seja humana ou material, de um evento catastrófico, resultando em danos.
- Perda: O prejuízo sofrido por uma organização, sem garantia de ressarcimento por seguro ou outros meios.
- Sinistro: O prejuízo sofrido por uma organização, com garantia de ressarcimento por seguro ou outros meios.
- Incidente: Qualquer evento com potencial para causar danos, mesmo que não resulte em danos visíveis.

5.2 Considerações Adicionais

A gestão de riscos é uma prática fundamental no ambiente corporativo, especialmente diante dos desafios enfrentados no mundo dos negócios, como evidenciado pelas recentes crises financeiras e pela pandemia global. A compreensão dos riscos envolvidos nas operações de uma empresa é essencial para a implementação eficaz de controles internos e para a garantia da segurança organizacional.

- Controles Internos e Gestão de Riscos: Os controles internos desempenham um papel crucial na gestão de riscos corporativos, assegurando processos definidos pela alta administração e mitigando ameaças potenciais. A integração entre controles internos, compliance e segurança da informação fortalece a estrutura de gestão de riscos, tornando-a mais eficiente.
- Desafios na Implementação: A implementação eficaz de controles internos e gestão de riscos enfrenta diversos desafios, incluindo a falta de conhecimento do negócio por parte de alguns profissionais e a complexidade das operações empresariais. Além disso, questões como a segurança da informação em ambientes de home office representam desafios adicionais que exigem atenção e medidas adequadas.
- Melhores Práticas e Normas: Normas reconhecidas internacionalmente, como o COSO-ERM e a ISO 31000, fornecem diretrizes valiosas para a gestão de riscos corporativos. Além disso, a adoção de melhores práticas de mercado e

a implementação de metodologias específicas podem contribuir para a eficácia dos processos de gestão de riscos.

- Revisões Periódicas: A revisão periódica dos sistemas de controles internos e gestão de riscos é essencial para garantir sua eficácia contínua. Diante das mudanças no ambiente empresarial e das novas ameaças emergentes, é fundamental que as organizações estejam preparadas para adaptar e aprimorar seus processos de gestão de riscos.

5.3 Visão sobre Gerência de Riscos

A Gerência de Riscos é uma disciplina que visa proteger os recursos humanos, materiais, ambientais e financeiros de uma empresa. Isso pode ser alcançado através da eliminação ou redução de riscos e do financiamento dos riscos remanescentes, de acordo com a viabilidade econômica.

5.4 Evolução e Contexto

A percepção crescente dos perigos potenciais decorrentes do progresso tecnológico, juntamente com preocupações ambientais e uma postura mais crítica dos consumidores, tem destacado a importância da Gerência de Riscos. As empresas estão cada vez mais conscientes de que as perdas, sejam elas de natureza financeira, humana ou ambiental, podem impactar significativamente seus objetivos e até mesmo sua existência.

5.5 Origens e Desenvolvimento

A Gerência de Riscos teve origem nos Estados Unidos e na Europa após a Segunda Guerra Mundial, quando os responsáveis pela segurança das empresas começaram a explorar maneiras de reduzir os gastos com seguros e aumentar a proteção contra riscos de acidentes. Isso levou à necessidade de uma análise detalhada das situações de risco, considerando tanto a probabilidade de perda quanto os custos e benefícios das medidas de proteção.

5.6 Abordagem Integrada

A abordagem da Gerência de Riscos proposta neste trabalho é uma combinação de teorias lógicas e objetivas, derivadas de diversas áreas, incluindo a Engenharia de

Segurança de Sistemas. Isso envolve uma análise cuidadosa dos riscos, a determinação de medidas de proteção adequadas e a consideração dos aspectos econômicos da gestão de riscos.

5.7 Conclusão

Em suma, a Gerência de Riscos é essencial para as empresas enfrentarem os desafios associados aos riscos empresariais. Ao adotar uma abordagem integrada e considerar os diversos aspectos dos riscos, as organizações podem proteger seus ativos e garantir sua sustentabilidade a longo prazo. Este capítulo fornece uma base sólida para futuras pesquisas e práticas na área de Gerência de Riscos Empresariais.

6. TRABALHOS FUTUROS

A conclusão deste trabalho apresenta uma série de insights valiosos sobre os riscos de TI e suas implicações no ambiente corporativo. No entanto, como toda pesquisa acadêmica, este estudo também revela lacunas e áreas que necessitam de investigação adicional. Este capítulo delineia as sugestões de trabalhos futuros, destacando a importância de expandir o conhecimento e a compreensão sobre os riscos de TI, suas estratégias de mitigação, e a integração de novas tecnologias e metodologias na gestão de riscos empresariais.

6.1 Áreas para Pesquisa Futura

6.1.1 Desenvolvimento de Novas Tecnologias para Gestão de Riscos

Uma área promissora para futuras pesquisas é o desenvolvimento e a aplicação de novas tecnologias na gestão de riscos de TI. Com o avanço constante das tecnologias emergentes, como a inteligência artificial, machine learning, blockchain, e IoT (Internet das Coisas), há um vasto campo a ser explorado sobre como essas tecnologias podem ser utilizadas para prever, detectar e mitigar riscos de TI de maneira mais eficaz. Estudos futuros podem se concentrar em:

- **Inteligência Artificial e Machine Learning**: Investigar como algoritmos de machine learning podem ser aplicados para identificar padrões de risco e prever possíveis falhas ou ataques cibernéticos.
- **Blockchain**: Explorar o uso de blockchain para garantir a integridade e a segurança dos dados, além de sua aplicação em sistemas de auditoria e compliance.
- **Internet das Coisas (IoT)**: Avaliar os riscos específicos associados aos dispositivos IoT e desenvolver frameworks para sua gestão eficaz.

6.1.2 Políticas e Estruturas de Governança

Outra área que merece atenção é a elaboração de políticas e estruturas de governança robustas que possam apoiar a gestão de riscos de TI. Pesquisas futuras podem focar em:

- **Governança de TI**: Estudo de frameworks e modelos de governança que possam ser implementados para assegurar uma gestão de riscos de TI alinhada com os objetivos estratégicos da organização.
- **Compliance e Regulações**: Analisar o impacto das regulamentações governamentais e da conformidade com normas internacionais na gestão de riscos de TI e como as empresas podem melhor se preparar para atender a essas exigências.

6.1.3 Aspectos Humanos e Culturais

A gestão de riscos de TI não depende apenas de tecnologias e políticas, mas também dos aspectos humanos e culturais dentro das organizações. Áreas de pesquisa futuras podem incluir:

- **Cultura Organizacional**: Investigar como a cultura organizacional influencia a percepção e a gestão de riscos de TI, e como uma cultura de segurança pode ser promovida.
- **Capacitação e Treinamento**: Estudar a eficácia de programas de capacitação e treinamento em segurança da informação e gestão de riscos de TI, bem como o desenvolvimento de currículos educacionais focados nessas áreas.

6.2 Metodologias de Pesquisa para Estudos Futuros

Para abordar as áreas mencionadas, é crucial que futuras pesquisas adotem metodologias robustas e variadas, que possam incluir:

- **Estudos de Caso**: Análise detalhada de empresas que implementaram com sucesso (ou falharam na implementação de) tecnologias e políticas de gestão de riscos de TI.
- **Pesquisas Quantitativas e Qualitativas**: Utilização de métodos quantitativos para medir a eficácia de novas tecnologias e políticas, e métodos qualitativos para compreender os aspectos culturais e humanos.
- **Revisões Sistemáticas da Literatura**: Realizar revisões sistemáticas da literatura existente para identificar tendências, lacunas e oportunidades de pesquisa na área de gestão de riscos de TI.

6.3 Conclusão

Este capítulo apresentou diversas direções para pesquisas futuras na área de gestão de riscos de TI. Ao explorar novas tecnologias, políticas de governança, e aspectos humanos e culturais, futuras investigações podem não apenas ampliar o entendimento sobre os riscos de TI, mas também oferecer soluções práticas e inovadoras para mitigar esses riscos. A continuidade da pesquisa neste campo é essencial para garantir que as empresas estejam preparadas para enfrentar os desafios de um ambiente tecnológico em constante evolução, protegendo seus ativos e garantindo a sustentabilidade a longo prazo.

7. CONCLUSÃO

O gerenciamento de riscos em empresas de Tecnologia da Informação e Comunicação (TIC) é uma área crucial para garantir a continuidade e a sustentabilidade dos negócios, especialmente em um ambiente dinâmico e repleto de incertezas. Este trabalho de conclusão de curso explorou as principais metodologias de gerenciamento de riscos e propôs uma estrutura de suporte para a adoção dessas práticas nas empresas de TIC.

7.1 Importância do Gerenciamento de Riscos

Ao longo deste trabalho, evidenciou-se a importância de uma abordagem estruturada e integrada para o gerenciamento de riscos. As empresas que investem em metodologias robustas conseguem não apenas minimizar os impactos negativos de potenciais riscos, mas também identificar e aproveitar oportunidades, aumentando assim sua competitividade no mercado. As metodologias discutidas, incluindo PMBOK, PRINCE2, ISO 31000, NIST e COBIT, oferecem frameworks valiosos que auxiliam na identificação, avaliação e mitigação de riscos, proporcionando uma base sólida para a tomada de decisões informadas e estratégicas.

7.2 Benefícios e Desafios

Os benefícios de investir em gerenciamento de riscos são claros: proteção dos ativos, conformidade regulatória, continuidade dos negócios e vantagem competitiva. No entanto, a implementação dessas práticas não está isenta de desafios. As empresas precisam lidar com a complexidade crescente dos sistemas de TI e a necessidade de adaptação rápida às mudanças tecnológicas e de mercado. Além disso, a cultura organizacional desempenha um papel fundamental na eficácia do gerenciamento de riscos, destacando a necessidade de uma abordagem que envolva todos os níveis da organização.

7.3 Metodologias e Tecnologias Emergentes

O trabalho também destacou a importância de novas tecnologias e metodologias emergentes, como inteligência artificial, machine learning, blockchain e Internet das Coisas (IoT). Essas tecnologias oferecem novas maneiras de prever, detectar e

mitigar riscos de forma mais eficiente, abrindo novas frentes de pesquisa e aplicação prática no campo do gerenciamento de riscos.

A pesquisa bibliográfica foi descrita em suas etapas essenciais, desde a definição do tema e escopo da pesquisa até a citação e referenciação das fontes utilizadas. A relevância dessa abordagem foi ressaltada, pois ela proporciona uma base sólida de informações e insights a partir de estudos anteriores sobre o tema em questão. Além disso, boas práticas para a realização da pesquisa bibliográfica foram apresentadas, incluindo o planejamento cuidadoso, critérios de seleção rigorosos, análise crítica e organização eficiente dos resultados.

Na classificação metodológica, a pesquisa realizada foi categorizada de acordo com diferentes critérios. Quanto à natureza, foi classificada como pesquisa básica, buscando gerar conhecimentos novos e teóricos sobre os riscos de TI. Em relação ao objetivo, foi classificada como exploratória, visando proporcionar maior familiaridade com o problema dos riscos de TI e construir hipóteses para investigações futuras. Quanto aos procedimentos, a pesquisa bibliográfica foi o método adotado, baseando- se na revisão crítica da literatura existente. Quanto à abordagem, foi classificada como qualitativa, focalizando na compreensão aprofundada dos conceitos, teorias e práticas relacionadas aos riscos de TI, sem a intenção de quantificar os dados coletados.
Essa metodologia proporciona uma base sólida para o desenvolvimento da pesquisa, garantindo sua relevância, rigor e contribuição para o avanço do conhecimento na área de riscos de TI.

7.4 Direções para Pesquisas Futuras

A pesquisa realizada apontou várias áreas promissoras para investigações futuras, incluindo o desenvolvimento de novas tecnologias para gestão de riscos, a criação de políticas e estruturas de governança robustas, e a consideração dos aspectos humanos e culturais na gestão de riscos de TI. Estudos de caso, pesquisas quantitativas e qualitativas, e revisões sistemáticas da literatura são metodologias recomendadas para aprofundar o conhecimento e desenvolver práticas inovadoras nesta área.

7.5 Considerações Finais

Em resumo, o investimento em práticas eficazes de gerenciamento de riscos é essencial para o sucesso e a sustentabilidade das empresas de TIC. Este trabalho contribuiu para a compreensão das principais metodologias de gerenciamento de riscos, destacando a importância de uma abordagem integrada e adaptativa que considere tanto os avanços tecnológicos quanto os fatores humanos e culturais. A continuidade da pesquisa nesta área é fundamental para que as empresas estejam preparadas para enfrentar os desafios de um ambiente tecnológico em constante evolução, protegendo seus ativos e garantindo sua sustentabilidade a longo prazo.

REFERENCIAS

ALFF, Chico. **Análise de Requisitos**. Disponível em: https://analisederequisitos.com.br/autor/chicoalff/. Acesso em: 27 nov. 2023.

ANGELOU, George N.; ECONOMIDES, Anastasios A. A real options approach for prioritizing ICT business alternatives: A case study from broadband technology business field. **Journal of the Operational Research Society**, v. 58, n. 10, p. 1340-1350, 2007. Disponível em: https://www.tandfonline.com/doi/abs/10.1057/palgrave.jors.2602254. Acesso em: 10 jan. 2024.

AVEN, Terje. Risk assessment and risk management: Review of recent advances on their foundation. **European Journal of Operational Research**, v. 253, n. 1, p. 1-13, 2016. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0377221716302535. Acesso em: 12 jun. 2024.

BOJANC, Rok; JERMAN-BLAZIC, Borka. An economic modelling approach to information security risk management. **International Journal of Information Management,** v. 28, n. 5, p. 413-422, 2008. Disponível em: https://www.sciencedirect.com/science/article/pii/S026840120800070X. Acesso em: 5 jan. 2024.

CICCO, F.; FANTAZZINI, D. Tecnologias Consagradas de Gestão de Riscos. **Revista Brasileira de Gestão de Negócios**, v. 5, n. 13, p. 47-58, 2003.

CRESWELL, J. W. **Research Design**: Qualitative, Quantitative, and Mixed Methods Approaches. Thousand Oaks, CA: Sage Publications, 2014.

DE HAES, Steven; VAN GREMBERGEN, Wim; DEBRECENY, Roger S. COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. **Journal of Information Systems**, v. 34, n. 1, p. 29-41, 2020. Disponível em: https://aaajournals.org/doi/10.2308/isys-52564. Acesso em: 10 dez. 2023.

DE HAES, Steven; VAN GREMBERGEN, Wim; DEBRECENY, Roger S. COBIT 2019: New Concepts and Their Implementation. **ISACA Journal,** 2020. p. 18-25. Disponível em: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5. Acesso em: 12 jun. 2024.

DEAL, Terrence E.; KENNEDY, Allan A. **Corporate Cultures**: The Rites and Rituals of Corporate Life. Reading: Addison-Wesley, 1982.

DADMARZ, Mohammad. **Information Security Management**: A Case Study of an Information Security Culture Change Programme. *In:* Information Security Management: Global Challenges in the New Millennium. Springer, 2019. p. 93-108. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-15731-0_5. Acesso em: 20 dez. 2023.

DITTMANN, L.; WOJCIK, R.; GELLER, J. Risk Management in Software Development: A Case Study of IBM. **Journal of Systems and Software**, 170, 110736, 2020.

GARTNER. **Gartner's IT Risk Management Framework**. Disponível em: https://www.gartner.com/en/documents/3977197/gartner-s-it-risk-management- framework. Acesso em: 12 jun. 2024.

GIL, A. C. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 2008.

HANSETH, Ole; CIBORRA, Claudio. **Risk, complexity and ICT**. Cheltenham: Edward Elgar Publishing, 2007. Disponível em: https://consensus.app/papers/risk-complexity-hanseth/316abe57007a561e9e265031e3c5703d/?utm_source=chatgpt. Acesso em: 13 jul. 2024.

HENDERSON, P. **Enterprise Risk Management with Oracle**: Aligning IT with Business Objectives. Oracle White Paper, Oracle Corporation, 2018.

HILLSON, D. **Practical Project Risk Management:** The ATOM Methodology.

Management Concepts, 2019

HUBBARD, D.; SEIERSEN, R. **How to Measure Anything in Cybersecurity Risk**. Wiley, 2016.

IBM. Disponível em: https://www.ibm.com/services. Acesso em: 16 jul. 2024.

ISACA. **State of Enterprise Risk Management 2018**. Disponível em: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpem. Acesso em: 12 jun. 2024.

ISO. **ISO 31000**: Risk Management – Guidelines, 2018.

JONES, R.; ASHENDEN, D. **Risk-Based Testing**: Prioritizing Testing Efforts Based on Risk Analysis. Journal of Software Testing, 2019.

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia científica**. São Paulo: Atlas, 2017.

LAKATOS, E. M.; MARCONI, M. de A. **Técnicas de pesquisa**. São Paulo: Atlas, 2003.

MEREDITH, J. R.; MANTEL, S. J. **Managing Risk in Information Technology Projects**. Wiley Online Library, 2012. Acesso em: 29 ago. 2024.

NIST. **Framework for Improving Critical Infrastructure Cybersecurity**, 2018.

ORACLE. Disponível em: https://www.oracle.com/security.

PMI (Project Management Institute). **A Guide to the Project Management Body of Knowledge (PMBOK Guide)**, 2017.

PROJECT MANAGEMENT INSTITUTE. **Pulse of the Profession**: 2020. Disponível em: https://www.pmi.org/learning/library/pulse-of-the-profession-2020-11972.

ROSS, Ron; MCEVILLEY, Michael; OREN, Janet. **Systems Security Engineering**: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. NIST Special Publication, 800-160, 2018.

Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf. Acesso em: 10 dez. 2023.