INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
CAMPUS JOÃO PESSOA
DIRETORIA DE ENSINO SUPERIOR
UNIDADE ACADÊMICA DE GESTÃO E NEGÓCIOS
CURSO SUPERIOR DE BACHARELADO EM ADMINISTRAÇÃO

JACKSON MANOEL RAMOS DA CRUZ

APLICAÇÃO DA GESTÃO DE RISCO PARA REDUZIR INCIDENTES DE SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES

JOÃO PESSOA
2025

JACKSON MANOEL RAMOS DA CRUZ

APLICAÇÃO DA GESTÃO DE RISCO PARA REDUZIR INCIDENTES DE SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES

Unidade Acadêmica de Gestão e Negócios

TRABALHO DE CONCLUSÃO DE CURSO apresentado ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), curso Superior de Bacharelado em Administração, como requisito institucional para a obtenção do Grau de Bacharel(a) em **ADMINISTRAÇÃO**.

Orientador(a): Dra. Amanna Ferreira Peixoto.

JOÃO PESSOA
2025

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca Nilo Peçanha do IFPB, *campus* João Pessoa

C957a Cruz, Jackson Manoel Ramos da.

Aplicação da gestão de risco para reduzir incidentes de segurança da informação em organizações / Jackson Manoel Ramos da Cruz. – 2025.

36 f. : il.

TCC (Graduação – Bacharelado em Administração) – Instituto Federal de Educação da Paraíba / Unidade Acadêmica de Gestão e Negócios, 2025.

Orientação: Profa. Dra Amanna Ferreira Peixoto.

1.Gestão de riscos. 2. Segurança da informação. 3. Tecnologia da informação. 4. ISO 27001. 5. Cibersegurança. I. Título.

CDU 005:331.461(043)

Bibliotecária responsável: Lucrecia Camilo de Lima – CRB 15/132

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

FOLHA DE APROVAÇÃO

JACKSON MANOEL RAMOS DA CRUZ

20191460019

APLICAÇÃO DA GESTÃO DE RISCO PARA REDUZIR INCIDENTES DE SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO apresentado em **26/02/2025** no Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), curso Superior de Bacharelado em Administração, como requisito institucional para a obtenção **do Grau de Bacharel(a) em ADMINISTRAÇÃO.**

Resultado: APROVADO

João Pessoa, 28 de fevereiro de 2025.

BANCA EXAMINADORA:

(assinaturas eletrônicas via SUAP)

Dra. Amanna Ferreira Peixoto (IFPB)

Orientador(a)

Dra. Karoline Fernandes Siqueira Campos (IFPB)

Examinador(a) interno(a)

Dra. Arielle Pinto Silva (IFPB)
Examinador(a) interno(a)

Documento assinado eletronicamente por:

- **Amanna Ferreira Peixoto**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 09/03/2025 21:04:37.
- **Karoline Fernandes Siqueira Campos**, **COORDENADOR(A) DE CURSO - FUC1 - CCSBA-JP**, em 09/03/2025 21:22:02.
- **Arielle Pinto Silva**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 10/03/2025 09:52:25.

Este documento foi emitido pelo SUAP em 28/02/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código 676650
Verificador: 8c040ec9a4
Código de Autenticação:

AGRADECIMENTOS

Primeiramente, agradeço a Deus, por me dar força, saúde e sabedoria para enfrentar cada desafio ao longo desta caminhada. Sem Ele, nada disso seria possível. Sua presença foi constante em cada momento de dificuldade e conquista, me guiando e iluminando o caminho até aqui.

Agradeço também à minha família, que esteve ao meu lado em todos os momentos, oferecendo apoio incondicional, incentivo e compreensão. O suporte de vocês foi essencial para que eu pudesse enfrentar os obstáculos e seguir em frente com determinação. Cada palavra de encorajamento e cada gesto de carinho foram fundamentais para minha trajetória.

Aos meus amigos King Lions, Geiciel, Lindemberg e Jacob, que compartilharam comigo os desafios e as alegrias dessa jornada. O companheirismo e a amizade de vocês tornaram essa caminhada mais leve e inspiradora, provando que, mesmo nos momentos mais difíceis, nunca estamos sozinhos.

Aos meus professores e orientadores, que, com dedicação e paciência, me guiaram durante este trabalho, fornecendo conhecimento e direcionamento valiosos.

Por fim, sou grato a todos que, direta ou indiretamente, contribuíram para que este momento fosse possível. Essa conquista não é apenas minha, mas de todos que acreditaram em mim e me ajudaram a chegar até aqui.

Muito obrigado!

RESUMO

A Gestão de Riscos desempenha um papel fundamental na segurança da informação, especialmente em organizações de Tecnologia da Informação (TI), onde a proteção de dados e a continuidade dos negócios são prioridades estratégicas. Este estudo teve como objetivo analisar como a Gestão de Riscos pode ser utilizada para reduzir incidentes de segurança da informação, adotando uma abordagem qualitativa e exploratória. A metodologia consistiu na realização de uma entrevista semiestruturada com o gestor da área de Governança, Riscos e Conformidade (GRC), cujas respostas foram analisadas por meio da técnica de análise de conteúdo. Os principais resultados indicam que a organização implementa práticas estruturadas de Gestão de Riscos, utilizando frameworks como a ISO 27001 e metodologias como análise SWOT e matriz de probabilidade e impacto. A pesquisa revelou que, sem a aplicação dessas práticas, a empresa enfrentaria um número significativamente maior de incidentes cibernéticos, comprometendo a segurança dos ativos digitais. Além disso, destacou-se a importância da capacitação contínua dos funcionários e do monitoramento constante dos sistemas como fatores determinantes para a eficácia da Gestão de Riscos. Conclui-se que, ao adotar uma abordagem estruturada e proativa, as organizações conseguem reduzir vulnerabilidades, otimizar a alocação de recursos e fortalecer a resiliência diante das ameaças cibernéticas. Recomenda-se o investimento em tecnologias emergentes, como inteligência artificial e aprendizado de máquina, para aprimorar a detecção e resposta a riscos. Assim, a Gestão de Riscos se consolida como um diferencial competitivo para as empresas, garantindo maior segurança, conformidade regulatória e continuidade operacional.

Palavras-chave: Gestão de Riscos. Segurança da Informação. Tecnologia da Informação. ISO 27001. Cibersegurança.

ABSTRACT

Risk Management plays a fundamental role in information security, especially in Information Technology (IT) organizations, where data protection and business continuity are strategic priorities. This study aimed to analyze how Risk Management can be used to reduce information security incidents, adopting a qualitative and exploratory approach. The methodology consisted of a semi-structured interview with a manager from the Governance, Risk, and Compliance (GRC) area, with responses analyzed using content analysis techniques. The main results indicate that the organization implements structured Risk Management practices, using frameworks such as ISO 27001 and methodologies like SWOT analysis and probability and impact matrix. The research revealed that, without the application of these practices, the company would face a significantly higher number of cyber incidents, compromising the security of digital assets. Additionally, continuous employee training and constant system monitoring were highlighted as key factors for the effectiveness of Risk Management. It is concluded that by adopting a structured and proactive approach, organizations can reduce vulnerabilities, optimize resource allocation, and strengthen resilience against cyber threats. Investment in emerging technologies, such as artificial intelligence and machine learning, is recommended to enhance risk detection and response. Thus, Risk Management is established as a competitive advantage for companies, ensuring greater security, regulatory compliance, and operational continuity.

Keywords: Risk Management. Information Security. Information Technology. ISO 27001. Cybersecurity.

SUMÁRIO

1 INTRODUÇÃO

A gestão de riscos é como uma bússola que orienta as organizações na navegação por um ambiente de incertezas, garantindo que os desafios sejam enfrentados de forma ordenada e eficiente. Com um método bem estruturado, é possível estabelecer diretrizes que iluminam o caminho para identificar e mitigar ameaças, sempre alinhadas às metas organizacionais. Essa prática dinâmica se adapta às constantes mudanças do cenário de riscos, fortalecendo a segurança e a resiliência operacional das empresas (SHOEMAKER *et al.*, 2017).

As raízes da gestão de riscos remontam ao Renascimento, quando matemáticos como Blaise Pascal e Pierre de Fermat desenvolveram a teoria da probabilidade, introduzindo um olhar científico sobre a incerteza. Durante séculos, até meados do século XX, o foco esteve na proteção contra prejuízos financeiros, com modelos tradicionais de seguro servindo como principal ferramenta. No entanto, com os avanços tecnológicos e a crescente complexidade dos mercados, surgiram estratégias mais sofisticadas, como o autosseguro e novos mecanismos de proteção contra perdas (PRZETACZNIK, 2022).

A partir dos anos 1970, a gestão de riscos passou por uma evolução significativa, impulsionada pela volatilidade econômica e pelo advento de instrumentos financeiros como os derivativos. Apesar desse avanço, o modelo tradicional de "gestão em silo" ainda predominava, tratando os riscos de forma isolada e sem considerar seus impactos cruzados na estratégia organizacional. Esse formato limitava a capacidade das empresas de enxergar o risco de maneira integrada (PRZETACZNIK, 2022).

Nos anos 1990, o conceito de Enterprise Risk Management (ERM) emergiu, promovendo uma abordagem integrada e proativa da gestão de riscos. A crescente complexidade dos mercados e eventos de grande impacto, como os ataques de 11 de setembro e a crise financeira de 2008, destacaram a necessidade de um modelo mais abrangente. Normas como o COSO ERM e a ISO 31000 consolidaram a importância do ERM, estabelecendo diretrizes para a gestão estruturada dos riscos empresariais (PRZETACZNIK, 2022).

Integrar a gestão de riscos aos processos estratégicos não apenas melhora a tomada de decisão, mas também otimiza o uso dos recursos. Compreender os riscos vai além da mera prevenção de prejuízos; trata-se de antecipar problemas e construir defesas robustas contra vulnerabilidades. A implementação de frameworks reconhecidos globalmente, como os da NIST, fornece um alicerce sólido para garantir a segurança e a conformidade organizacional (SHOEMAKER *et al*., 2017).

No atual cenário digital, caracterizado por um volume crescente de dados e ameaças cibernéticas cada vez mais sofisticadas, a gestão de riscos enfrenta desafios que demandam agilidade e precisão. Um programa eficaz deve ser capaz de identificar, avaliar e responder rapidamente às novas ameaças, garantindo o uso estratégico dos recursos para minimizar impactos. Para isso, é essencial adotar uma estrutura de gestão de riscos coesa, promovendo a uniformidade das práticas em toda a organização (SHOEMAKER *et al*., 2017).

A gestão de riscos desempenha um papel fundamental na segurança da informação, protegendo os ativos digitais e assegurando a continuidade das operações. A adoção de um Sistema de Gestão de Segurança da Informação (SGSI), baseado no ciclo "planejar-fazer-verificar-agir", melhora a capacidade organizacional de lidar com riscos de forma proativa e eficaz (ANTON; NEDELCU, 2018). Diante desse cenário, surge a seguinte questão: como a gestão de riscos pode ser utilizada para reduzir incidentes de segurança da informação em organizações?

O fortalecimento das práticas de gestão de riscos é suportado por frameworks amplamente reconhecidos, que ajudam a alinhar a gestão de riscos aos objetivos estratégicos. Assim, a gestão de riscos se consolida como uma ferramenta essencial para reduzir incidentes de segurança e reforçar a resiliência dos sistemas corporativos (SHOEMAKER *et al*., 2017).

A transformação digital trouxe inúmeros benefícios para as organizações, mas também ampliou os desafios relacionados à segurança da informação. A crescente dependência de sistemas digitais e o alto volume de dados aumentaram a exposição das empresas a ataques cibernéticos. Para mitigar esses riscos, é fundamental ir além da tecnologia, combinando medidas técnicas com estratégias organizacionais e culturais. A segurança deve ser um compromisso coletivo, permeando todos os níveis da organização e reforçando a confiança de colaboradores, clientes e parceiros (GEBREMESKEL *et al*., 2023). Dessa forma, a gestão de riscos se torna um

diferencial competitivo, permitindo reações rápidas a incidentes e minimizando impactos negativos (HEY, 2017).

O gerenciamento de riscos organizacional, quando aplicado de forma integrada, capacita as lideranças a equilibrar as demandas internas com as constantes transformações do panorama de ameaças. Cabe à alta gestão estabelecer diretrizes claras e adaptáveis, que não apenas cumpram exigências regulatórias, mas também protejam os ativos essenciais da empresa. A implementação de controles compartilhados entre diferentes níveis hierárquicos favorece a eficiência operacional e reduz custos, garantindo a resiliência organizacional (BROAD, 2021).

No Brasil, os desafios em cibersegurança são agravados pela ausência de uma estrutura regulatória unificada. Enquanto setores como o financeiro e de telecomunicações demonstram avanço, outras áreas carecem de maturidade na implementação de boas práticas. Pequenas e médias empresas enfrentam dificuldades adicionais devido à escassez de recursos e de expertise especializada. Investir em políticas consistentes e iniciativas de conscientização é essencial para fortalecer a segurança cibernética nacional (CMM, 2023).

1.1 Objetivos

Diante do contexto apresentado e da crescente complexidade do ambiente digital, este estudo busca compreender a importância da Gestão de Riscos na minimização de incidentes de segurança da informação. Em um cenário onde as ameaças cibernéticas se tornam cada vez mais sofisticadas e frequentes, torna-se essencial investigar como as organizações podem fortalecer suas estratégias de proteção, utilizando métodos eficazes de gestão de riscos para garantir a continuidade dos negócios e a proteção de seus ativos digitais. Assim, este estudo tem como objetivos:

1.1.1 Objetivo Geral

Analisar como a Gestão de Risco é utilizada para reduzir os incidentes de segurança da informação em organizações.

1.1.2 Objetivos Específicos

1. Identificar e analisar como a Gestão de Riscos é aplicada em organizações de TI, com base em práticas e conceitos descritos na literatura;
2. Verificar a utilização de ferramentas e metodologias descritas na literatura para administrar riscos relacionados à segurança da informação;
3. Investigar as práticas de gestão de riscos adotadas por uma organização, com base em uma entrevista com um gestor da área de Governança, Riscos e Conformidade (GRC);
4. Propor recomendações baseadas em boas práticas documentadas na literatura para aprimoramento da Gestão de Riscos em organizações de TI, considerando o cenário atual de ameaças digitais.

1.2 Justificativa

A crescente digitalização dos processos organizacionais e a expansão da conectividade global trouxeram inúmeros benefícios para as empresas, mas também aumentaram significativamente os riscos associados à segurança da informação. Nesse cenário, a gestão de riscos emerge como uma abordagem essencial para minimizar incidentes que possam comprometer a integridade, a confidencialidade e a disponibilidade dos dados, protegendo tanto os ativos da organização quanto a privacidade de clientes e parceiros.

A importância desse tema se justifica, primeiramente, pela necessidade de garantir a continuidade dos negócios como: violações de segurança, ataques cibernéticos e vazamentos de dados podem resultar em perdas financeiras expressivas, impactar a reputação das empresas e comprometer a confiança dos clientes. Além disso, o cumprimento das regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, exige que as organizações adotem medidas robustas para gerenciar riscos e assegurar conformidade.

Outro fator relevante é a constante evolução das ameaças cibernéticas. A sofisticação dos ataques e a multiplicidade de vulnerabilidades exigem que as empresas adotem estratégias dinâmicas e proativas na identificação, avaliação e mitigação de riscos. A implementação de frameworks reconhecidos internacionalmente, como a ISO 27001 e o NIST Cybersecurity Framework, possibilita uma abordagem estruturada e eficaz para fortalecer a resiliência organizacional diante dessas ameaças.

A gestão de riscos desempenha um papel fundamental na segurança da informação, indo além da simples prevenção de ameaças. Ao permitir uma alocação mais eficiente de recursos, ela contribui diretamente para a resiliência organizacional, garantindo que as empresas estejam melhor preparadas para enfrentar cenários adversos. Quando bem implementadas, as metodologias de gestão de riscos não apenas reduzem a probabilidade de incidentes, mas também fortalecem a capacidade da organização de responder e se recuperar rapidamente diante de crises. Esse aprimoramento na resposta a incidentes não só minimiza impactos operacionais e financeiros, como também garante uma vantagem competitiva no mercado, permitindo que a empresa se mantenha sustentável e confiável no atual ambiente digital, cada vez mais dinâmico e desafiador..

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Gestão de Riscos

A gestão de riscos destaca-se como uma ferramenta estratégica fundamental para organizações que desejam prosperar em um cenário empresarial repleto de desafios e incertezas. Esse processo proativo busca identificar, avaliar e responder a ameaças que podem afetar os objetivos e operações de uma empresa. As fontes de risco são variadas, incluindo oscilações de mercado, instabilidade política, falhas operacionais, desastres naturais e ataques cibernéticos (FREITAS, 2020).

Quando adotada de forma estratégica, a gestão de riscos permite às organizações proteger seus ativos e recursos enquanto identificam oportunidades escondidas nas incertezas. Esse entendimento abrangente das ameaças inerentes ao negócio facilita o desenvolvimento de planos de contingência eficazes e estratégias de mitigação, que não apenas minimizam impactos negativos, mas também abrem espaço para o crescimento e a inovação (FAGUNDES *et al*., 2021).

Além disso, uma gestão de riscos bem estruturada transforma o processo de tomada de decisão, tornando-o mais assertivo e orientado. Isso possibilita que as organizações antecipem cenários adversos e fortaleçam sua resiliência. Ao mesmo tempo, promove uma cultura organizacional centrada na transparência, na responsabilidade e no aprendizado contínuo, características indispensáveis para enfrentar e se adaptar às constantes mudanças do ambiente empresarial (LIMA *et al*., 2021).

No universo da Tecnologia da Informação (TI), a gestão de riscos assume uma relevância estratégica ainda maior. Com processos, políticas e estruturas bem delineados, as empresas conseguem avaliar e controlar riscos tecnológicos de forma alinhada às necessidades do negócio, reduzindo custos operacionais e mitigando ameaças digitais. A Governança de TI (GTI), ancorada nos pilares de valor, risco e controle, atua como um complemento essencial à gestão de riscos, garantindo tanto o alinhamento estratégico quanto a continuidade das operações — aspectos vitais para uma governança eficaz (FREITAS, 2020).

Integrar a gestão de riscos em todas as áreas da organização não é apenas uma necessidade, mas um diferencial competitivo para assegurar sustentabilidade e geração de valor no longo prazo. Essa integração potencializa a resiliência organizacional e estimula a inovação, ao mesmo tempo em que alinha as operações aos interesses de todas as partes interessadas, criando um ambiente propício para o crescimento e a excelência organizacional (FREITAS, 2020; LIMA *et al.*, 2021).

2.1.1 Ferramentas e Metodologias em Gestão de Riscos

As ferramentas e metodologias em Gestão de Riscos desempenham um papel essencial no reconhecimento, análise, avaliação e controle dos riscos que podem impactar uma organização. Elas oferecem estruturas sistemáticas que auxiliam na tomada de decisões estratégicas, permitindo às empresas não apenas minimizar os efeitos negativos dos riscos, mas também aproveitar oportunidades associadas a eles. Abaixo, destacam-se algumas das ferramentas e metodologias mais utilizadas na Gestão de Riscos (LIMA *et al.*, 2021).

Uma das ferramentas mais amplamente aplicadas é a análise SWOT. Trata-se de um método estratégico que avalia os fatores internos e externos que influenciam uma organização. A análise é dividida em quatro dimensões principais: Strengths (Forças), que evidenciam os recursos e vantagens competitivas internas; Weaknesses (Fraquezas), que identificam as limitações ou áreas de melhoria dentro da organização; Opportunities (Oportunidades), que exploram condições externas favoráveis ao crescimento ou inovação; e Threats (Ameaças), que avaliam os riscos externos que podem comprometer os objetivos organizacionais. A SWOT é uma ferramenta crucial no planejamento estratégico, permitindo não só a identificação de riscos, mas também a formulação de estratégias para mitigá-los e maximizar os resultados (PUYT; LIE; WILDEROM, 2023).

Figura 1 – Análise Swot

Fonte: Meetime (2018)

- A Matriz de Probabilidade e Impacto é uma ferramenta amplamente utilizada na gestão de riscos para avaliar e classificar riscos com base na probabilidade de ocorrência e no impacto potencial. Essa matriz permite que as organizações priorizem riscos, concentrando esforços nos mais significativos (PROJECT MANAGEMENT INSTITUTE, 2021).

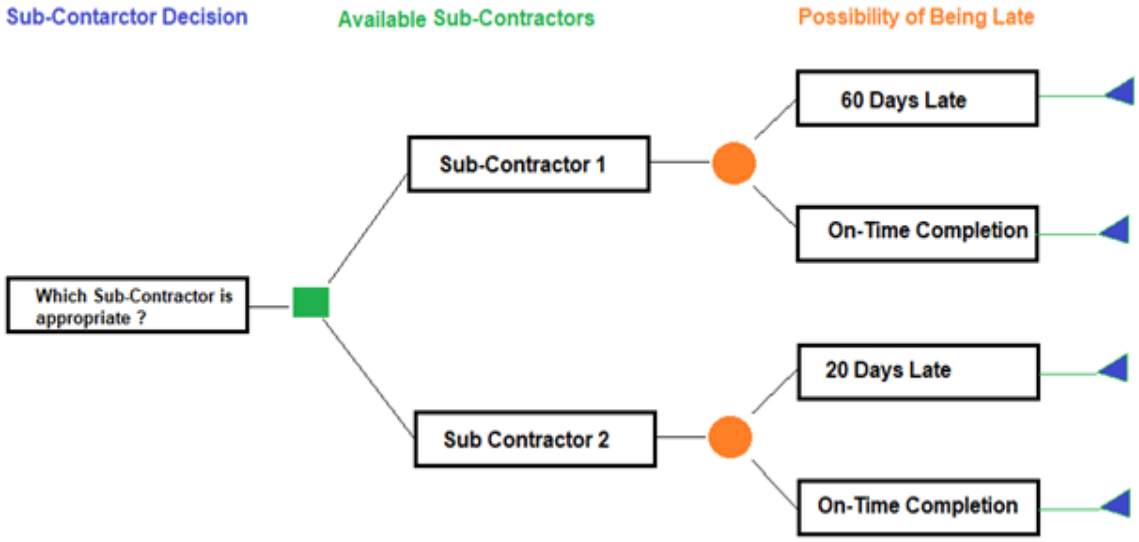
Figura 2 – Matriz de Probabilidade

Probabilidade / Impacto	Sem Impacto	Leve	Médio	Grave	Gravíssimo
Quase certo	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo	Risco Extremo
Alta	Risco Moderado	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo
Média	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo	Risco Extremo
Baixa	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo
Raro	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Elevado

Fonte: Frons (2020).

- A indução de árvores de decisão é uma técnica de aprendizado de máquina utilizada para classificar e organizar dados de forma hierárquica, facilitando a análise e a tomada de decisões. Essa abordagem foi inicialmente desenvolvida por Quinlan (1986), que propôs o algoritmo ID3, um modelo eficiente para segmentação de dados com base em critérios objetivos. Embora Quinlan tenha aplicado esse método principalmente ao aprendizado de máquina, a abordagem de árvores de decisão foi posteriormente adaptada para diversas áreas, incluindo a Gestão de Riscos, auxiliando na modelagem de cenários e na identificação das melhores estratégias para mitigação de ameaças.

Figura 3 – Análise de Árvores de Decisão



Fonte: ProjectCubicle (2024).

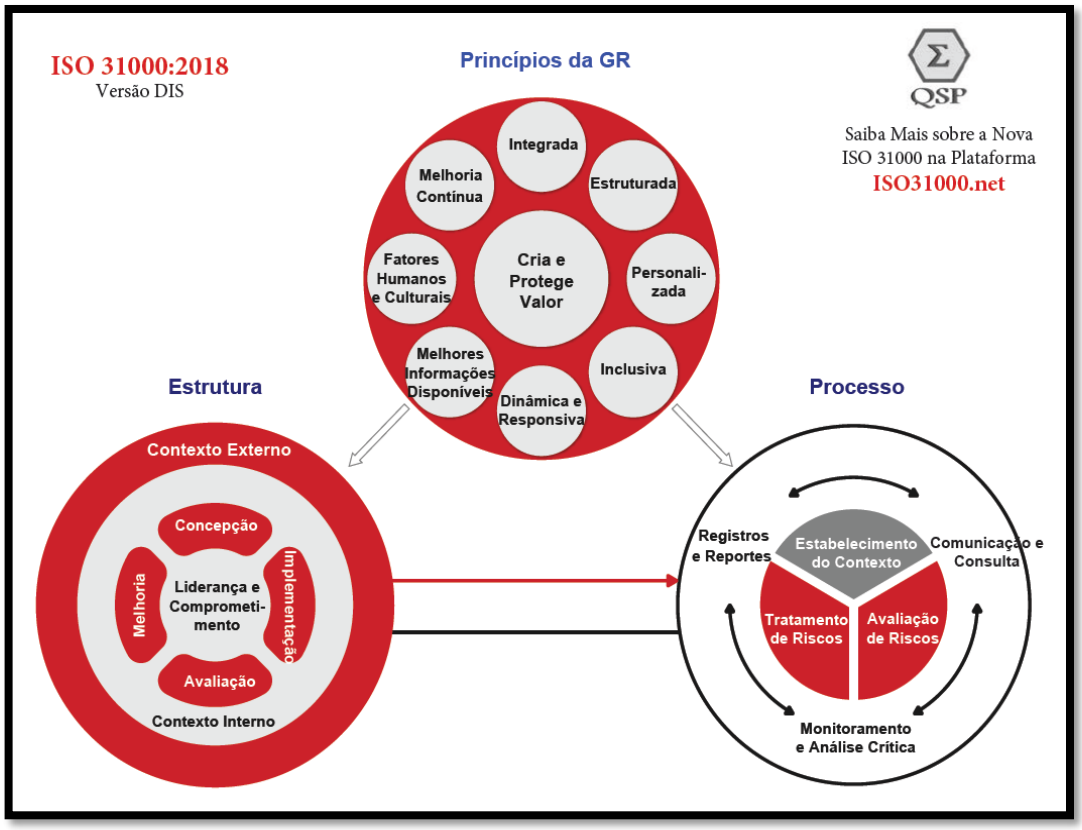
- FMEA (Failure Mode and Effects Analysis). Conforme Mikulak *et al*. (2009), a Análise de Modos de Falha e Efeitos (FMEA) é uma metodologia de análise preventiva que identifica os modos de falha possíveis de um processo ou sistema, avaliando seus efeitos e classificando os riscos associados. Ela é muito utilizada em indústrias para prevenir falhas e melhorar a qualidade e segurança.

Figura 4 – FMEA (Failure Mode and Effects Analysis)

Fonte: AuditComply (2020)

- ISO 31000: Gestão de Riscos. A ISO 31000 é uma norma internacional para a gestão de riscos. Ela fornece princípios e diretrizes para a criação de um processo de gestão de riscos em qualquer tipo de organização. A norma inclui práticas que cobrem a identificação, avaliação e tratamento dos riscos de forma sistemática (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018).

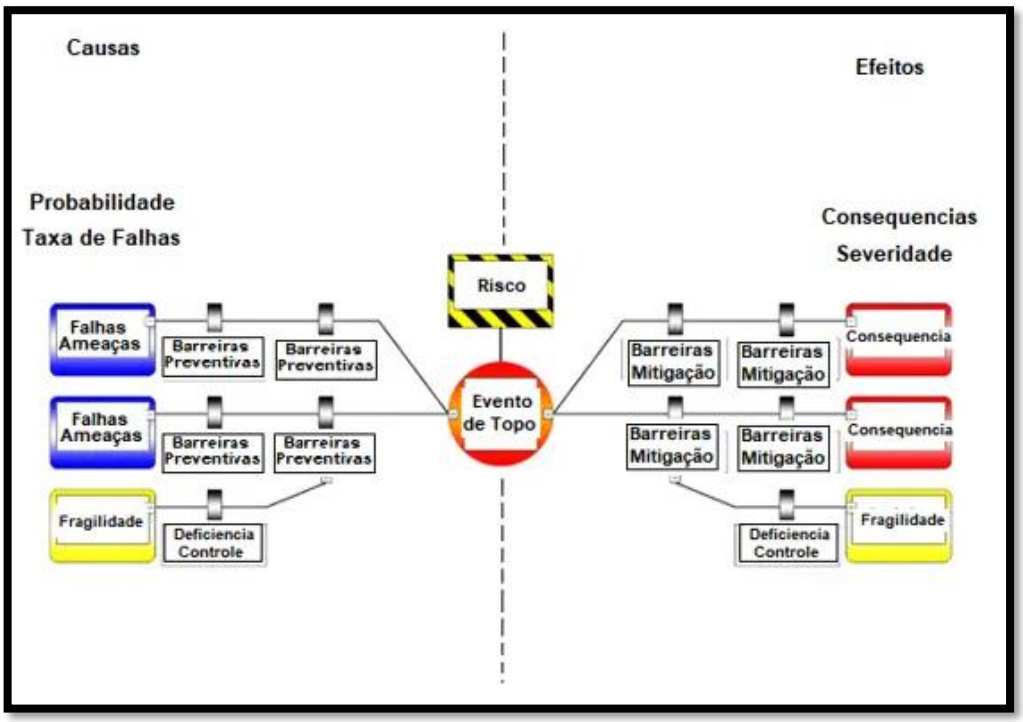
Figura 5 – ISO 31000



Fonte: ISO31000.net

- Bowtie Analysis. A Análise Bowtie (Gravata Borboleta) é uma técnica visual que permite mapear as causas, os eventos e as consequências de um risco. Ela combina aspectos da análise de causa raiz e da análise de consequências, permitindo visualizar como um evento de risco pode se expandir e afetar a organização. É muito utilizada em setores industriais e de engenharia. (CCPS; ENERGY INSTITUTE, 2021)

Figura 6 – Análise Bowtie



Fonte: Consultoria Engenharia (2018).

Dessa forma, as metodologias apresentadas – Análise de SWOT, Matriz de Probabilidade e Impacto, Árvores de Decisão, FMEA, ISO 31000 e Análise Bowtie – fornecem abordagens complementares para a identificação, avaliação e mitigação de riscos organizacionais. Cada uma dessas ferramentas possui aplicações específicas que auxiliam na tomada de decisão e no fortalecimento das estratégias de segurança. A adoção dessas técnicas permite que as organizações desenvolvam processos mais robustos, minimizando vulnerabilidades e garantindo maior resiliência diante das incertezas do ambiente corporativo.

2.2 Estudos Empíricos Sobre Gestão De Riscos Em Segurança Da Informação

Uma pesquisa realizada por Galegale *et al*. (2016) investigou as práticas de gestão de riscos em segurança da informação em uma instituição pública federal. O estudo revelou que muitas organizações ainda dependem de processos manuais e subjetivos para avaliar e mitigar riscos, com uma baixa utilização de ferramentas especializadas. Embora essa abordagem seja funcional em alguns casos, ela carece de eficiência e agilidade para lidar com as crescentes demandas do ambiente digital. A pesquisa destacou que a ausência de automação e padronização dificulta a resposta rápida a incidentes e compromete a eficácia das políticas de segurança da informação. Os autores sugerem que as organizações invistam em tecnologias modernas, como inteligência artificial e aprendizado de máquina, para melhorar a precisão e a proatividade na gestão de riscos. Além disso, enfatizam a importância de integrar a gestão de riscos de segurança da informação (GRSI) às estratégias corporativas para fortalecer a resiliência organizacional e garantir a proteção contínua contra ameaças emergente.

Hori (2020) propôs um modelo de gestão de riscos em segurança da informação que enfatiza a necessidade de integrar a segurança da informação aos objetivos estratégicos da organização. O estudo demonstrou que uma gestão de riscos eficaz depende não apenas de controles técnicos, mas também de uma abordagem holística que considere aspectos operacionais, mercadológicos e humanos. O modelo sugere que as organizações devem adotar uma estrutura flexível, permitindo ajustar os controles de segurança conforme as mudanças no ambiente organizacional e as novas ameaças.

Santos (2023), analisou a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) em uma empresa. A pesquisa revelou desafios específicos enfrentados por gestores de níveis hierárquicos inferiores, incluindo falta de treinamento adequado e comprometimento organizacional com a segurança da informação. A ausência de alinhamento estratégico entre os objetivos institucionais e as práticas de segurança resultou em vulnerabilidades críticas. O autor recomenda ações como capacitação contínua, maior envolvimento da alta gestão e a criação de

uma cultura organizacional focada em segurança. A pesquisa também destacou a importância de adaptar os controles de segurança às características específicas do setor educacional, considerando o ambiente dinâmico e colaborativo das empresas.

Bari *et al*. (2024) investigou o impacto da inteligência artificial (IA) na cibersegurança, especialmente por meio de análises preditivas. A pesquisa utiliza tanto abordagens quantitativas, analisando mais de 2.000 incidentes de segurança, quanto qualitativas, com estudos de casos de empresas que adotaram IA. A IA também permite automação, eliminando tarefas repetitivas e melhorando a eficiência das equipes de segurança. O estudo revela que a integração de IA preditiva fortalece a resiliência das organizações, transformando a abordagem de segurança cibernética de reativa para proativa, essencial no cenário pós-pandemia.

Coutinho *et al*. (2017) analisaram a implementação da Segurança da Informação em uma empresa de pequeno porte e identificaram falhas significativas, como a ausência de uma política formal, controle inadequado de acessos e regras pouco definidas para o uso da internet. Além disso, a falta de conscientização organizacional comprometia a proteção de dados e a continuidade dos negócios. Para mitigar essas vulnerabilidades, os autores recomendam a criação de uma política clara, a definição de regras específicas para redes e internet e a adoção de medidas preventivas para garantir a integridade e a disponibilidade das informações. O estudo destaca a importância de tratar a segurança da informação como um ativo estratégico, promovendo maior alinhamento com as melhores práticas descritas na ISO/IEC 27002:2005.

3 METODOLOGIA

A metodologia adotada neste trabalho foi delineada para proporcionar uma análise aprofundada sobre a aplicação da Gestão de Riscos na segurança da informação em uma organização situada na região Nordeste do Brasil. A pesquisa combinou uma abordagem qualitativa e exploratória, permitindo a identificação de padrões, desafios e boas práticas no gerenciamento de riscos cibernéticos.

3.1 Caracterização Da Pesquisa

Este estudo caracteriza-se como uma pesquisa qualitativa de natureza exploratória e descritiva. A abordagem qualitativa foi escolhida para permitir uma compreensão detalhada das percepções, experiências e estratégias adotadas na Gestão de Riscos aplicada à segurança da informação. O caráter exploratório se justifica pelo objetivo de investigar como essa prática é estruturada na organização estudada, enquanto a abordagem descritiva busca apresentar um panorama das metodologias, ferramentas e ações concretas implementadas.

3.2 Técnicas de Coleta de Dados

A coleta de dados foi realizada por meio de uma entrevista semiestruturada online, aplicada ao gestor responsável pela área de Governança, Riscos e Conformidade (GRC) da organização analisada. O objetivo da entrevista foi compreender como a Gestão de Riscos é aplicada na empresa e quais metodologias e ferramentas são utilizadas para minimizar incidentes de segurança da informação.

A entrevista foi conduzida remotamente via plataforma Microsoft Teams, garantindo flexibilidade ao entrevistado e possibilitando a gravação para análise posterior. O processo ocorreu durante cinco dias úteis, entre 12 e 16 de agosto de 2024, com um tempo médio de 40 a 60 minutos por sessão. O entrevistado foi previamente contatado por e-mail e telefone para agendamento e esclarecimento dos objetivos da pesquisa.

O instrumento de pesquisa consistiu em um questionário contendo 10 perguntas abertas, elaboradas com base em estudos prévios da literatura sobre Gestão de Riscos e Segurança da Informação. A formulação das perguntas seguiu como referência os modelos apresentados por ISO 31000 e NIST 800-39, garantindo alinhamento com boas práticas reconhecidas internacionalmente.

As respostas obtidas foram gravadas, transcritas integralmente e analisadas com o objetivo de identificar padrões, desafios e boas práticas adotadas pela organização. Essa abordagem qualitativa permitiu uma avaliação detalhada dos principais aspectos envolvidos na gestão de riscos, contribuindo para a compreensão das estratégias adotadas pela empresa para minimizar ameaças à segurança da informação.

3.3 Técnica Análise De Dados

Os dados coletados foram analisados por meio da técnica de análise de conteúdo, conforme proposta por Bardin (2011). Esse método consiste em um conjunto de procedimentos sistemáticos e objetivos que possibilitam a categorização e interpretação de dados qualitativos. A análise de conteúdo permite identificar padrões, inferir significados a partir das respostas obtidas e estruturar as informações coletadas em categorias temáticas. Dessa forma, foi possível extrair insights relevantes sobre a aplicação da Gestão de Riscos na segurança da informação, contribuindo para a compreensão de boas práticas, desafios e oportunidades de aprimoramento nas organizações estudadas.

A análise dos dados teve como objetivo identificar boas práticas, desafios enfrentados e oportunidades de aprimoramento, correlacionando os achados com diretrizes e frameworks estabelecidos na literatura. Dessa forma, foi possível construir uma visão estruturada sobre como a Gestão de Riscos pode contribuir para a redução de incidentes de segurança da informação em organizações do setor de tecnologia.

4 APRESENTAÇÃO E ANÁLISE DE RESULTADOS

A gestão de riscos é um elemento essencial para garantir a segurança da informação e a continuidade dos negócios nas organizações de Tecnologia da Informação. A partir da análise da entrevista realizada, foram identificadas as seguintes categorias temáticas: adoção de gestão de riscos, ferramentas e metodologias utilizadas, ações efetivas tomadas para mitigar os riscos identificados e alterações no sistema de gestão de riscos.

A Gestão de Riscos é uma prática essencial em organizações de Tecnologia da Informação, e a empresa em questão confirma a sua adoção para lidar com questões de segurança da informação. O respondente ressaltou que “essa prática é fundamental para proteger os ativos de informação e garantir a continuidade dos negócios, o que é amplamente reconhecido na literatura”. Almeida (2019) afirma que a gestão de riscos é crucial para proteger os ativos de informação e para a continuidade dos negócios. Além disso, Silva (2017) destaca que uma estratégia robusta de gestão de riscos ajuda a identificar e mitigar ameaças antes que elas possam causar danos significativos.

Quanto às ferramentas e metodologias utilizadas para implementar a Gestão de Riscos, o respondente mencionou que “a organização adota uma abordagem abrangente que inclui a análise de vulnerabilidades, a avaliação de impacto de segurança, a análise quantitativa e qualitativa de riscos e o Framework de Gerenciamento de Riscos da ISO 27001”. A análise de vulnerabilidades é considerada uma ferramenta crucial para identificar falhas de segurança de forma proativa, conforme destacado por Almeida (2019).

A avaliação de impacto de segurança, mencionada por Costa (2020), permite a priorização de ações de proteção, enquanto as análises quantitativa e qualitativa de riscos, conforme Melo (2018), fornecem uma visão abrangente e detalhada dos riscos. O Framework da ISO 27001, discutido por Silva (2017), é amplamente reconhecido como uma metodologia eficaz para a gestão de riscos, proporcionando uma abordagem estruturada e sistemática para enfrentar as ameaças.

Em relação às ações efetivas tomadas para mitigar os riscos identificados, o respondente afirmou que “a empresa implementa planos de ação baseados nas

análises de risco, os quais incluem medidas de segurança técnica, treinamento contínuo de funcionários e monitoramento constante". De acordo com Costa (2020), a criação de planos de ação baseados em análises de risco é fundamental para mitigar riscos de forma eficaz. Silva (2017) também enfatiza a importância do monitoramento contínuo e das atualizações regulares de sistemas para manter a segurança da informação. O respondente também indicou que, sem a implementação da Gestão de Riscos, a empresa teria enfrentado cerca de 15 ocorrências adicionais de segurança por ano, resultando em um total de 20 incidentes anuais. Isso demonstra claramente a eficácia da estratégia de gestão de riscos adotada pela organização.

Para melhorar ainda mais o sistema de Gestão de Riscos, o respondente sugeriu a conscientização e o treinamento contínuos dos funcionários, a implementação de controles de acesso adequados, a atualização regular de sistemas e a realização de auditorias frequentes. Melo (2018) destaca a importância da conscientização dos funcionários e do treinamento contínuo para promover uma cultura de segurança. Costa (2020) também reforça a necessidade de controles de acesso rigorosos e a atualização regular de sistemas, enquanto Silva (2017) salienta a importância da prontidão para responder rapidamente a incidentes de segurança.

Em relação às atitudes mais importantes para promover a segurança da informação, o respondente reiterou que a conscientização e o treinamento contínuos dos funcionários, a implementação de controles de acesso, a atualização regular de sistemas e a realização de auditorias de segurança regulares são essenciais para garantir a proteção das informações. Ferreira e Silva (2020) apontam que a conscientização e o treinamento constante são fundamentais para criar uma cultura de segurança sólida, enquanto Lima e Carvalho (2021) também enfatizam a necessidade de manter os sistemas atualizados e realizar auditorias regulares para identificar e corrigir vulnerabilidades antes que possam ser exploradas.

O respondente também afirmou que "a organização já adota essas práticas de forma proativa, realizando treinamentos regulares, mantendo os sistemas atualizados, implementando controles de acesso rigorosos e conduzindo auditorias frequentes". Lima e Carvalho (2021) destacam que essas ações são cruciais para garantir a proteção das informações e a integridade dos sistemas.

Sobre os pontos negativos provenientes de falhas na Gestão de Riscos, o respondente alertou para a exposição a ameaças e vulnerabilidades, o impacto

financeiro, os danos à reputação e a não conformidade regulatória. Santos e Almeida (2018) explicam que falhas na gestão de riscos podem resultar em custos financeiros elevados, como gastos com recuperação de dados, investigações forenses e multas por violações de regulamentações. Souza e Pereira (2019) também observam que a falta de uma gestão de riscos eficaz pode prejudicar a imagem da empresa, afetando a confiança de clientes e parceiros. Além disso, Lima e Carvalho (2021) ressaltam que a não conformidade regulatória pode resultar em penalidades legais, o que pode ter um impacto significativo na reputação e na saúde financeira da empresa.

Caso pudesse realizar alterações no sistema de Gestão de Riscos, o respondente sugeriu “a integração de tecnologias avançadas, como inteligência artificial, aprendizado de máquina e automação, para aprimorar a detecção e a resposta a ameaças em tempo real”. Machado e Costa (2022) enfatizam que a adoção dessas tecnologias inovadoras pode melhorar significativamente a segurança da informação. O respondente também destacou a necessidade de melhorar a comunicação e colaboração entre as equipes de TI e segurança, além de implementar um ciclo de melhoria contínua para revisar e atualizar regularmente as políticas e procedimentos de segurança.

Por fim, o respondente acredita que a implementação de um programa de conscientização em segurança da informação é fundamental para reduzir incidentes cibernéticos, educando os funcionários sobre as melhores práticas de segurança, a identificação e o relato de ameaças e a importância de proteger informações confidenciais. Oliveira e Mendes (2017) reforçam que funcionários bem-informados são mais capazes de reconhecer e evitar ameaças, fortalecendo as defesas cibernéticas da organização. Ferreira e Silva (2020) destacam que uma cultura de segurança eficaz reduz a probabilidade de comportamentos negligentes, que podem resultar em incidentes de segurança. Além disso, Nunes e Martins (2019) observam que a maioria dos ataques cibernéticos explora a falta de conhecimento e a inexperiência dos usuários finais, e um programa de conscientização pode ajudar a minimizar esses erros.

5 CONSIDERAÇÕES FINAIS

A Gestão de Riscos (GR) desempenha um papel essencial nas empresas de Tecnologia da Informação (TI), pois permite a identificação, avaliação e mitigação de ameaças que possam comprometer a segurança dos dados e a continuidade dos negócios. Em um cenário onde as ameaças cibernéticas se tornam cada vez mais sofisticadas, a implementação de práticas estruturadas de gestão de riscos é fundamental para garantir a proteção dos ativos digitais, minimizar vulnerabilidades e assegurar conformidade com regulamentações como a LGPD e a ISO 27001. Empresas que adotam um modelo eficiente de Gestão de Riscos conseguem reduzir incidentes, otimizar recursos e fortalecer a resiliência organizacional diante dos desafios da transformação digital.

Considerando o objetivo geral deste trabalho, que era analisar como a Gestão de Riscos é utilizada para reduzir os incidentes de segurança da informação em uma organização do Nordeste, juntamente com a análise documental da organização e baseando-se na entrevista realizada, pode-se concluir que a empresa estudada adota metodologias estruturadas de GR para minimizar impactos causados por ameaças cibernéticas. Através do uso de frameworks reconhecidos, como a ISO 27001 e a análise de vulnerabilidades, a organização demonstrou que uma abordagem preventiva e estratégica permite uma resposta mais eficiente a incidentes, reduzindo significativamente os riscos operacionais.

Com relação ao objetivo específico que trata das aplicações da Gestão de Riscos em organizações de TI, verificou-se que este foi alcançado, uma vez que, na Fundamentação Teórica, foram explorados diversos métodos e ferramentas utilizados para identificar e mitigar riscos, incluindo a análise SWOT, a matriz de probabilidade e impacto e a metodologia FMEA. Esses modelos foram fundamentais para compreender como as organizações podem estruturar seus processos de segurança da informação e alinhar as estratégias de proteção aos objetivos organizacionais.

No que se refere ao objetivo de verificar a utilização de ferramentas e metodologias descritas na literatura para administrar riscos relacionados à segurança da informação, os dados obtidos confirmam que a empresa estudada utiliza uma abordagem combinada, integrando metodologias qualitativas e quantitativas na

identificação e mitigação de riscos. A aplicação da análise de impacto de segurança e do Framework de Gerenciamento de Riscos da ISO 27001 reforça a relevância dessas ferramentas na construção de um ambiente digital mais seguro.

Já no que diz respeito ao objetivo de analisar, as práticas de gestão de risco em uma organização, constatou-se que a empresa analisada implementa ações concretas para mitigar ameaças, como a criação de planos de ação baseados na análise de risco, treinamentos contínuos para funcionários e monitoramento constante dos sistemas. A entrevista revelou que, sem essas iniciativas, a empresa teria enfrentado um número maior de incidentes de segurança, o que comprova a eficácia da GR na redução de vulnerabilidades.

Por fim, o objetivo de propor recomendações baseadas em boas práticas documentadas na literatura para o aprimoramento de sistemas de Gestão de Riscos em organizações de TI também foi atingido. A partir das análises realizadas, sugere-se a adoção de tecnologias emergentes, como inteligência artificial e aprendizado de máquina, para aprimorar a detecção e resposta a ameaças em tempo real. Além disso, recomenda-se o fortalecimento da comunicação entre as equipes de TI e segurança, garantindo maior alinhamento estratégico e operacional.

Dessa forma, conclui-se que a Gestão de Riscos é uma ferramenta indispensável para a segurança da informação, permitindo que as organizações se antecipem a possíveis ameaças e adotem medidas proativas para garantir a proteção de seus ativos digitais. A pesquisa reforça a necessidade de investimentos contínuos em capacitação, tecnologia e aprimoramento das estratégias de gestão de riscos, assegurando um ambiente organizacional mais seguro e resiliente diante dos desafios da era digital.

Entretanto, este estudo apresenta algumas limitações. A análise foi conduzida com base em uma única organização do setor de TI, o que pode limitar a generalização dos resultados para outras empresas com diferentes contextos operacionais. Além disso, a pesquisa se concentrou principalmente em metodologias e ferramentas existentes, não abordando de forma aprofundada os desafios específicos enfrentados na implementação dessas práticas. Para estudos futuros, sugere-se a realização de análises comparativas entre diferentes organizações e setores, bem como a investigação do impacto de novas tecnologias emergentes na

Gestão de Riscos, como blockchain e segurança baseada em zero trust, para aprimorar ainda mais a segurança da informação nas empresas.

REFERÊNCIAS

AMERICAN INSTITUTE OF CHEMICAL ENGINEERS. CENTER FOR CHEMICAL PROCESS SAFETY. **Bow ties in risk management: a concept book for process safety**. Hoboken, NJ: John Wiley & Sons, Inc, 2018.

ANTON, N.; NEDELCU, A. Security risk analysis and management. **MATEC Web of Conferences**, v. 178, p. 08015, 2018. DOI: https://doi.org/10.1051/matecconf/201817808015.

AUDITCOMPLY. FMEA - An Analysis Method to Mitigate Risk. 2020. 1 ilustração. Disponível em: https://www.auditcomply.com/2020/01/29/fmea-an-analysis-method-to-mitigate-risk/. Acesso em: 1 dez. 2024.

BROAD, J. **Risk management framework: a lab-based approach to securing information systems**. Waltham, MA: Syngress, An Imprint Of Elsevier, 2013.

CENTRO GLOBAL DE CAPACIDADE DE SEGURANÇA CIBERNÉTICA. Revisão das capacidades de segurança cibernética do Brasil 2023. Disponível em: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/cmm-report-brazil-2023_final_pt.pdf/view. Acesso em: 20 nov. 2024.

CONSULTORIA ENGENHARIA. Ferramenta de Gestão de Risco Bowtie. 2018. 1 ilustração. Disponível em: https://consultoriaengenharia.com.br/confiabilidade-e-risco/ferramenta-de-gestao-de-risco-bowtie/. Acesso em: 1 dez. 2024.

FAGUNDES, E. *et al*. Tolerância ao risco dos gestores: análise na tomada de decisão nos campos pessoal e organizacional**. Revista Evidenciação Contábil & Finanças**, v. 9, n. 1, p. 22-43, 2021. DOI: https://doi.org/10.22478/ufpb.2318-1001.2021v9n1.49966.

FREITAS, H. Análise de conteúdo: Faça Perguntas as Respostas obtidas com sua 'Pergunta'! RAC - **Revista de Administração Contemporânea**. Curitiba, v. 15, n. 4, p. 748-760, 2020. DOI: https://doi.org/10.1590/S1415-65552011000400011.

FRONS. Matriz de Probabilidade e Impacto. 2020. 1 ilustração. Disponível em: https://frons.com.br/blog/processos/matriz-probabilidade-impacto/. Acesso em: 1 dez. 2024.

GALEGALE, N. V.; FONTES, E. L. G.; GALEGALE, B. P. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. **Perspectivas em Ciência da Informação**, v. 22, n. 3, p. 75–97, set. 2017. DOI: https://doi.org/10.1590/1981-5344/2866.

GEBREMESKEL, B. K.; JONATHAN, G. M.; YALEW, S. D. Information Security Challenges During Digital Transformation. **Procedia Computer Science**, v. 219, p. 44–51, 2023. DOI: https://doi.org/10.1016/j.procs.2023.01.262.

HEY, R. B. Risk Management. **Elsevier eBooks**, p. 159–175, 1 jan. 2017. DOI: https://doi.org/10.1016/B978-0-12-810446-0.00011-6.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 31000:2018 - Risk Management – Guidelines**. Geneva: ISO, 2018.

ISO31000.NET. Nova ISO 31000. 2018. 1 ilustração. Disponível em: https://iso31000.net/nova-iso-31000/. Acesso em: 1 dez. 2024.

KOHNKE, A.; SIGLER, K.; SHOEMAKER, D. **Implementing cybersecurity: A guide to the national institute of standards and technology risk management framework.** London, England: Auerbach, 2022.

LIMA, E, *et al*. Balanço social e o “full disclosure” no terceiro setor. **Revista de Tecnologia Aplicada (RTA)**, v. 10, n. 1, p. 23-39, jan./abr. 2021. DOI: https://doi.org/10.48005/2237-3713rta2021v10n1p2339.

MCDERMOTT, R. E.; BEAUREGARD, M. R.; MIKULAK, R. J. **The Basics of FMEA**. 2. ed. Nova Iorque, NY, USA: Productivity Press, 2008.

MEETIME. Análise SWOT. 2018. 1 ilustração. Disponível em: https://meetime.com.br/blog/gestao-empresarial/analise-swot/. Acesso em: 1 dez. 2024.

PROJECT MANAGEMENT INSTITUTE. **A guide to the Project Management Body of Knowledge (PMBOK guide) and the Standard for project management**. 7. ed. Newton Square, PA, USA: Project Management Institute, 2021.

PROJECTCUBICLE. Importance of Decision Tree Analysis (Example). 2024. 1 ilustração. Disponível em: https://www.projectcubicle.com/importance-of-decision-tree-analysis-example/. Acesso em: 27 fev. 2024.

PRZETACZNIK, S. The evolution of risk management. **Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie**, v. 53, n. 1–2, p. 95107, 2022. DOI: https://doi.org/10.25944/znmwse.2022.01-2.95107.

PUYT, R. W.; LIE, F. B.; WILDEROM, C. P. M. The origins of SWOT analysis. **Long range planning**, v. 56, n. 3, p. 102304, 2023. DOI: https://doi.org/10.1016/j.lrp.2023.102304.

QUINLAN, J. R. Induction of decision trees. Machine Learning, v. 1, n. 1, p. 81-106, 1986. DOI: https://doi.org/10.1007/BF00116251.

S A MOHAIMINUL ISLAM *et al.* AI-driven Predictive Analytics for Enhancing Cybersecurity in a Post-pandemic World: a Business Strategy Approach. **International Journal For Multidisciplinary Research**, v. 6, n. 5, 5 out. 2024. DOI: https://doi.org/10.36948/ijfmr.2024.v06i05.28493.

TSIGA, Z.; EMES, M.; SMITH, A. Implementation of a risk management simulation tool. **Procedia Computer Science**, v. 121, p. 218–223, 2017. DOI: https://doi.org/10.1016/j.procs.2017.11.030.

ANEXO
ENTREVISTA/QUESTIONÁRIO

Analisar como a Gestão de Risco é utilizada para reduzir os incidentes de segurança da informação em uma organização do nordeste.

1. Há o uso de Gestão de Riscos em sua empresa?
2. Quais as ferramentas e/ou metodologias da Gestão de Riscos são utilizadas em sua organização?
3. Qual(is) a(s) mais relevante(s) ferramenta(s) e/ou metodologia(s) de Gestão de Riscos para empresas de TI em sua opinião?
4. Há as ações efetivas ou planos de ação, com base no emprego de ferramentas ou metodologias utilizadas pela organização para administrar os riscos que envolvem a segurança de informações?
5. Em sua opinião, quais seriam as atitudes mais importantes para promover a segurança de informações?
6. Na organização em que atua, há atitudes dessa natureza?
7. Quais os resultados concretos advindos destas ações?
8. Quais os pontos negativos provenientes de falhas na Gestão de Riscos para você e sua empresa?
9. Se pudesse fazer alterações livremente no sistema de Gestão de Riscos, quais seriam?
10. Como a implementação de um programa de conscientização em segurança da informação pode contribuir para a redução de incidentes cibernéticos em uma empresa?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus João Pessoa - Código INEP: 25096850
Av. Primeiro de Maio, 720, Jaguaribe, CEP 58015-435, João Pessoa (PB)
CNPJ: 10.783.898/0002-56 - Telefone: (83) 3612.1200

Documento Digitalizado Ostensivo (Público)

Entrega versão final TCC

Assunto:	Entrega versão final TCC
Assinado por:	Jackson Cruz
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Ostensivo (Público)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Jackson Manoel Ramos da Cruz**, **ALUNO (20191460019) DE BACHARELADO EM ADMINISTRAÇÃO - JOÃO PESSOA**, em 18/03/2025 21:36:24.

Este documento foi armazenado no SUAP em 18/03/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1424739
Código de Autenticação: 60c93706f5