DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de Modelo de Mensuração de Apetite a Riscos Cibernéticos: Uso do Método AHP e da Estrutura Básica de Segurança Cibernética

Marcus Aurélio Carvalho Georg

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Proposta de Modelo de Mensuração de Apetite a Riscos Cibernéticos: Uso do Método AHP e da Estrutura Básica de Segurança Cibernética

Marcus Aurélio Carvalho Georg

Orientador: Prof. Dr. Demétrio Antônio da Silva Filho, FIS/UnB
Coorientador: Prof. Dr. Rafael Rabelo Nunes, ADM/FACE/UnB

PUBLICAÇÃO: PPEE.MP.055 -
BRASÍLIA-DF, 29 DE JUNHO DE 2023.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de Modelo de Mensuração de Apetite a Riscos Cibernéticos: Uso do Método AHP e da Estrutura Básica de Segurança Cibernética

Marcus Aurélio Carvalho Georg

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Demétrio Antônio da Silva Filho, FIS/UnB _____
Orientador

Prof. Dr. Georges Daniel Amvame Nze, ENE/FT/UnB _____
Examinador Interno

Prof. Dr. João Souza Neto, UCB _____
Examinador Externo

Prof. Dr. Robson de Oliveira Albuquerque, ENE/FT/UnB _____
Suplente

FICHA CATALOGRÁFICA

GEORG, MARCUS AURÉLIO CARVALHO GEORG
Proposta de Modelo de Mensuração de Apetite a Riscos Cibernéticos: Uso do Método AHP e da Estrutura Básica de Segurança Cibernética [Distrito Federal] 2023.
xvi, 200 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Apetite a Risco	2. Segurança Cibernética
3. Gestão de Risco	4. Analytic Hierarchy Process - AHP
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

GEORG, M.A.C. (2023). *Proposta de Modelo de Mensuração de Apetite a Riscos Cibernéticos: Uso do Método AHP e da Estrutura Básica de Segurança Cibernética* . Dissertação de Mestrado Profissional, PPEE.MP.055 Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 200 p.

CESSÃO DE DIREITOS

Marcus Aurélio Carvalho Georg
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho ao meu querido pai, Mario Georg, (in memoriam), e à minha mãe, Maria Inez, que me ensinaram a buscar minhas próprias respostas por meio do estudo e da dedicação.

Dedico também à Renata, minha Pequena parceira, pela paciência pelas horas necessárias de dedicação à construção desse texto.

Por fim, dedico aos meus filhos, Daniela, Luiz e Júlia, que me proporcionaram a possibilidade de aprender um bocado sobre a vida.

AGRADECIMENTOS

À equipe de suporte da Secretaria do PPEE, Tayná Gabriela, Cristiana Rosa e Adriana Reis. Sem elas, o desafio seria muito maior.

Aos amigos e colegas que participaram dessa jornada (Solimar, Luiz, Zottmann, Leandro, Lucas, entre outros), seja por meio do tradicional incentivo moral, seja pelas horas que se dedicaram em compartilhar conhecimentos e corrigindo os textos construídos com o passar do tempo.

Aos colegas do Superior Tribunal de Justiça que se dispuseram a participar da pesquisa em debates acalorados e que deram um sentido prático para o trabalho: Adriana Cristina Bastos Pinto, Fernanda Klarmann Pôrto Silva, Leandro Gabriel Bastos Ferreira e Wilmar Barros de Castro.

Fica aqui um agradecimento especial ao Professor Doutor Rafael Nunes Rabelo pelo voto de confiança dado a um tema complexo e com muitos desafios. Torço para que muitos possam ter a felicidade de ser acompanhado por professores tão dedicados.

Por fim, agradeço ao Programa de Pós Graduação em Engenharia Elétrica (PPEE) da Universidade de Brasília, pela oportunidade que gera às pessoas em seus crescimentos pessoais e profissionais.

RESUMO

Realizar escolhas em relação aos desafios que o mundo cibernético tem apresentado tem sido uma das tarefas mais árduas dos gestores, sejam do setor privado como do setor público. Os prejuízos relacionados a não conformidade legal, à descontinuidade dos serviços prestados, às perdas de informações estratégicas, aos desafios relacionados à cadeia de suprimentos cibernéticos e aos custos relacionados aos controles com foco minimização de riscos, entre outros, têm trazido a necessidade, por parte de gestores, de escolhas mais adequadas, com critérios e alternativas que falem mais dos contextos em que se encontram. Este estudo visa à mensuração do apetite a risco cibernético proposto pela alta gestão, em um primeiro momento, assim como apontar uma estratégia de alcance desse objetivo por meio da implantação de uma série de controles que representem às decisões calcadas nos pesos de critérios e alternativas defendidas por seus gestores. O modelo foi aplicado à realidade de um órgão público brasileiro, o Superior Tribunal de Justiça (STJ), onde é possível observar o apetite a risco por meio da escolha de controles que se compreendeu desejados, assim como a identificação daqueles que ainda não estão sendo implementados. A pesquisa demonstrou que é possível mensurar quantitativamente o apetite a risco de uma organização e que a escolha adequada de critérios, alternativas e controles pode tornar o modelo proposto uma ferramenta de apoio à decisão bastante promissora, permitindo um alinhamento entre a alta gestão e a área operacional de uma empresa.

Palavras-chave: Apetite a Risco; Segurança Cibernética; Tomada de Decisão; AHP; Estrutura de Segurança cibernética

ABSTRACT

Making choices regarding the challenges the cyber world has presented has been one of the most arduous tasks for private or public sector managers. The losses related to legal non-compliance, discontinuity of services provided, loss of strategic information, challenges related to the cyber supply chain, and costs related to controls focused on risk minimization, among others, have brought about the need, by managers, for more appropriate choices, with criteria and alternatives that speak more to the contexts in which they find themselves. This study aims to measure the cyber risk appetite proposed by top management first and point out a strategy to reach this goal through implementing a series of controls that represent decisions based on the weights of criteria and alternatives defended by their managers. The model was applied to the reality of a Brazilian public agency, the Superior Court of Justice (STJ), where it is possible to observe the risk appetite through the choice of controls that are understood to be desired, as well as the identification of those that are not yet being implemented. The research demonstrated that it is possible to measure an organization's risk appetite quantitatively and that the appropriate choice of criteria, alternatives, and controls can make the proposed model a very promising decision-support tool, allowing for an alignment between top management and the operational area of a company.

Keywords:Risk Appetite; Cyber Security; Decision Making; AHP; Cybersecurity Framework

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

Siglas

ABNT	Associação Brasileira de Normas Técnicas
AHP	*Analytic Hierarchy Process*
ART	Alternativas de Transferência de Risco
ART	Alternative Risk Transfer
BM	*BitMort*
CA	Conselho de Administração
CAFe	Comunidade Acadêmica Federada
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CCG	Comissão de Coordenação-Geral
CGU	Controladoria Geral da União
CIO	*Chief Information Officer*
CNJ	Conselho Nacional de Justiça
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CPS	*Cyber-Physical Security*
CRMM	*Cybersecurity Resilience Maturity Measurement*
CS	*Cybersecurity*
CSA	*Cybersecurity Audit*
CSF	*Cybersecurity Framework*
CSID	Coordenadoria de Segurança da Informação e Defesa Cibernética
CSS	*Cyber Security Strategy*
DDoS	*Distributed DoS*
DNS	*Domain Name System*
DNSSEC	*Domain Name System Security Extensions*
DOS	*Denial of Service*
EDU4	Educação 4.0
ENAP	Escola Nacional de Administração Pública
ERM	*Enterprise Risk Management*
FSB	*Financial Stability Board*
FSF	*Financial Stability Forum*
G7	Grupo dos Sete
G7	*Group of Seven*
GARCH	*Generalized Autoregressive Conditional Heteroskedasticity*
GCN	Gerenciamento de Continuidade de Negócios
GRCorp	Gerenciamento de Riscos Corporativos

HTTP	*Hyper Text Transfer Protocol*
IBGC	Instituto Brasileiro de Governança Corporativa
ICCI	*International Classification of Cyber Incidents*
IDAC	*International Digital Asset Classification*
IoT	*Internet of Things*
IPS	*Intrusion Prevention System*
IRM	*Institute of Risk Management*
ISCI	*Information Security Climate Index*
ISO	*International Organization for Standardization*
KCFR	*Key Cyber Risk Factors*
LDA	*Loss Distribution Approach*
LGPD	Lei Geral de Proteção de Dados Pessoais
M2M	*Machine-to-Machine*
MAUT	Método de Utilidade de Múltiplos Atributos
MAUT	*Multi-Attribute Utility Theory*
MCDA	*Multi Criteria Decision Analysis*
MDCM	*Multi Criteria Decision Making*
MM	*MicroMort*
NICCS	*National Initiative for Cybersecurity Careers and Studies*
NIST	*National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia)
ÖffSchOR	*Öffentliche Schadenfälle OpRisk*
PMEs	Pequenas e Médias Empresas
POT	*Peaks Over Threshold*
PPEE	Programa de Pós-Graduação Profissional em Engenharia
RAF	*Risk Appetite Frameworks*
RDP	*Remote Desktop Protocol*
RMF	*Risk Management Framework*
SC	Segurança Cibernética
SRE	*Security Requirements Engineering*
STI	Secretaria de Tecnologia da Informação e Comunicação
STJ	Superior Tribunal de Justiça
TCP	*Transmission Control Protocol*
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TLS	*Transport Layer Security*
TVaR	*Tail Value-at-Risk*
UnB	Universidade de Brasília
VaR	*Value-at-Risk*
VPN	*Virtual Private Networks*
WEF	*World Economic Forum*

1 INTRODUÇÃO

Se você não pode medir, não pode gerenciar
Peter Drucker

Nas últimas décadas houve um grande aumento do uso da internet como ferramenta para apoiar as estratégias de negócio das empresas. Com esse aumento expressivo, as organizações passaram a ficar cada vez mais dependentes do mundo cibernético, e, com isso, expostas aos riscos que esse domínio apresenta. As organizações privadas focam a maximização dos lucros, e, embora relevantes, os investimentos em sistemas de segurança tendem a ser limitados, por não serem considerados lucrativos no curto prazo [1].

Os ataques que ocorrem no domínio cibernético visam aos ativos de software, objetivando comprometer e incapacitar a execução de serviços, podendo atingir as missões das organizações [2]. Entretanto, para Musman et al. [3], há uma dificuldade muito grande em determinar os impactos de um ataque em relação aos objetivos da missão.

As ações de defesa aos ativos requerem uma visão holística que levem em consideração aspectos tecnológicos, humanos e comerciais, mas, entretanto, as práticas de cibersegurança atuais acabam por tratá-los de forma separada, não explorando as relações entre eles [4].

Para o *World Economic Forum* (WEF) [5], no ano de 2020 houve um aumento de 435 % de ataques do tipo *ransomware*, houve uma carência de três milhões de profissionais no domínio da cibernética, até 2024 haverá um aumento de US$ 800 bilhões no comércio digital e o ser humano está relacionado a 95 % dos problemas de segurança cibernética. Os custos associados às ameaças não são apenas financeiros, envolvendo desde infraestruturas críticas, passando pela coesão social e o bem-estar mental das pessoas. O trabalho remoto, altamente alavancado pela COVID-19, acabou por aumentar a adoção de plataformas e dispositivos, com compartilhamento de dados confidenciais, saindo das tradicionais trocas digitais de escritórios para o envolvimento de redes residenciais, aumentando a variedade de dispositivos conectados com uma proteção menor em relação às intrusões cibernéticas, e o não investimento em proteções em suas infraestruturas digitais pode ser devastador para as empresas.

Os riscos de segurança e privacidade têm sido foco de preocupação das principais nações do mundo, em grande parte pelo aumento da complexidade de hardware, software, *firmware* e sistemas de informações, além da infraestrutura crítica nacional, o que tem ampliado a superfície de ataque a ser explorada por adversários [6]. O aumento da superfície de ataque em virtude de novas tecnologias associadas a uma demanda cada vez maior de conexão entre as estratégias de negócio e o uso da cibernética, tem sido foco de muitos estudos [7, 8, 9, 10, 11].

Como resposta aos desafios impostos pelo COVID-19 às organizações, houve um aumento acelerado de processos digitais e ofertas de serviços, seguido por um aumento na taxa de ataques cibernéticos. No setor financeiro o atual processo de gestão de riscos está sendo repensado devido ao seu alto grau de subjetividade, sendo necessárias abordagens com métricas mais refinadas voltadas para orientar essas atividades [12].

A sofisticação dos ataques cibernéticos e o aumento expressivo do uso da Internet das Coisas (IoT) têm levado os riscos do tradicional ambiente cibernético para ao ambiente físico, considerados como riscos

emergentes [13]. Para Mishina et. al [13, p.710], isso tem levado um aumento pela demanda de seguro cibernético, trazendo como um dos riscos emergentes mais graves o risco cibernético silencioso, "que é um risco desconhecido que não é explicitamente coberto ou isento por apólices de seguro de propriedade tradicionais". É possível observar, por meio de estudos promovidos pela academia, que a indústria de seguros tem buscado criar índices que associam os riscos cibernéticos com perdas financeiras, como a proposta de Lau et al. [14], com o *premium* Shapley, Belles-Sampera, Guillén e Santolino [15], com o GlueVaR, Carfora e Orlando [16], com o *Cyber Value at Risk*, eVaR e eTVaR, entre outros.

1.1 O PROBLEMA DE PESQUISA

As organizações se distribuem geograficamente (hemisférios, países, estados), em setores (financeiro, saúde, público, etc.), em dimensões (grandes, médias e pequenas), em relação aos mercados (globais, locais), e em diversas outras formas de classificação. Para Quinn et al. [17], pelo fato das empresas serem únicas, as lideranças empresariais podem buscar adaptações, em virtude de suas características, das suas declarações de apetite ao risco de segurança cibernética. O setor da indústria, o tamanho da empresa, os tipos de dados perdidos assim como o tipo de ataque cibernético acabam por influenciar tanto a frequência como a gravidade dos eventos de perdas relacionados à cibernética [18]. A ausência de limitações geográficas para os riscos cibernéticos e a natureza sistêmica desse risco são confirmadas por meio da análise da atividade de TI em diferentes países [19]. Nesse sentido, Malavasi et al. [18] indicam que a frequência e a gravidade dos eventos de perda cibernética são influenciadas por vários fatores, incluindo o setor da indústria, o tamanho da empresa, o tipo de dados perdidos e o tipo de ataque cibernético.

As declarações do apetite e da tolerância ao risco das organizações têm sido foco quando da execução de suas ações estratégicas, merecendo destaque os riscos cibernéticos, advindos da introdução, cada vez mais intensa, do uso da tecnologia que interconecta fornecedores, produtores e clientes. A assunção de riscos nessa esfera se, por um lado, permite o aproveitamento de oportunidades, por outro lado exige que sejam repensadas as abordagens na gestão de riscos, observando as limitações dos controles tradicionais [20].

A problemática dessa pesquisa relaciona-se à dificuldade atual de se traduzir uma declaração de apetite aos riscos cibernéticos, elaborada pela alta gestão, em forma de um indicador, e que esse indicador sirva de elemento propulsor de ações das áreas operacionais. Busca-se, com a pesquisa, o uso de conhecimentos já disponíveis, contribuindo e ampliando a compreensão do problema, trazendo novas questões a serem investigadas [21]. No gerenciamento dos riscos de segurança cibernética deve-se buscar um entendimento claro dos indicadores do negócio, sendo que os riscos, prioridades e sistemas são distintos em organizações, sendo múltiplos os métodos e as ferramentas utilizados [6].

A definição de um problema, para Matias-Pereira [22], se localiza uma área de interesse devendo ser formulada por meio de uma pergunta clara e precisa. A área de interesse dessa pesquisa se concentra na tomada de decisão pela alta gestão relacionada à gestão de riscos cibernéticos. Sob forma de pergunta, o problema pode ser assim formulado:

Problema (P1): *O apetite a risco cibernético pode ser medido por meio de um modelo de apoio à tomada*

de decisões e um conjunto de controles já estabelecidos e conhecidos?

Considerando o **Problema** exposto, as hipóteses abaixo foram formuladas;

Hipótese 1 (H1): *Que há um conjunto limitado de critérios que possam traduzir o apetite a risco à cibernético estabelecido pela alta gestão de uma organização.*

Hipótese 2 (H2): *Que há um conjunto finito de controles que possibilitam a medição do apetite a risco cibernético, conectando a declaração de apetite a risco estabelecido pela alta gestão com os aspectos operacionais que deverão ser tratados pelos gestores.*

Hipótese 3 (H3): *Que dado um conjunto de controles que são classificados por importância, baseando-se em critérios e alternativas que representem as declarações de apetite da organização, é possível medir o apetite a risco de forma quantitativa, assim como medir o* ***gap*** *do apetite a risco com as atuais escolhas de controles utilizados.*

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Propor um modelo de mensuração do apetite a riscos cibernéticos de uma organização, a partir de um conjunto de controles voltados para a segurança cibernética, empregando um modelo de apoio à decisão, o AHP, com foco na priorização na aplicação dos controles.

1.2.2 Objetivos Específicos

1. Apresentar os principais frameworks voltados à segurança cibernética citados na literatura;
2. Selecionar e apresentar os controles a serem utilizados pelo modelo proposto;
3. Apresentar os critérios e alternativas dos artigos lidos, utilizados em modelos de apoio à decisão com foco em tecnologia da informação, segurança da informação, segurança cibernética, gerenciamento de riscos e partes interessadas, a partir de artigos que tratam essa abordagem;
4. Apresentar a relação priorizada dos Critérios e Alternativas da Organização;
5. Apresentar os controles que minimizam o Apetite a Risco Cibernético da organização, baseando-se nas prioridades estabelecidas e nas escolhas de controles da Estrutura Básica.

1.3 JUSTIFICATIVA DA PESQUISA

O uso intensivo de tecnologias que apoiam o negócio das organizações tem se demonstrado um caminho sem volta, possibilitando melhorias contínuas dos processos de trabalho, com a consequente diminuição de custos, o surgimento de novos serviços, maiores controles na cadeia de suprimentos, cada vez mais aprimorada por tecnologias cibernéticas. Embora esses elementos elencados se mostrem como positivos, os riscos associados não podem ser ignorados, pois são alvos frequentes de hackers no acesso aos dados relacionados ao negócio da organização [23].

Para Ganin et al. [24], muitos são os desafios relacionados aos sistemas cibernéticos enfrentados por avaliadores e gestores de risco, tendo uma natureza em constante mudança, por vezes causados por avanços tecnológicos, inúmeros domínios físicos e sociocognitivos, assim como estruturas em rede altamente complexas.

Guillet [25] compreende que ferramentas e modelos de apoio à decisão são uma necessidade para gestores, sejam de empresas privadas ou públicas, implicando em diminuição de gastos e um processo decisório mais preciso, atingindo setores estratégicos.

O uso do método multicritério *Analytic Hierarchy Process* (AHP) se dá em diversos campos, permitindo a seleção de alternativas melhores, assim como a boa alocação de recursos e a resolução de conflitos. Trata-se de um método amplamente utilizado, caracterizando-se por regular critérios tangíveis de forma organizada, apresentando soluções simples, permitindo a comparação tanto quantitativa como qualitativa, decompondo um problema complexo em subproblemas [26] .

Para Maček et al. [27], o uso do AHP justifica-se para fins de avaliação em sistemas de TI, estruturando problemas voltados à tomada de decisão, suportando tanto critérios qualitativos quanto quantitativos, permitindo a tomada de decisão em grupo, possibilitando a verificação da consistência das avaliações e classificação de alternativas.

Em Quinn et al. [17] encontramos que o apetite de risco é a interpretação, por parte dos líderes empresariais e organizacionais, como a variação aceitável do desempenho em relação aos objetivos estabelecidos. Há um crescente aumento no interesse, por parte das organizações, nos aspectos relacionados à uma estratégia de segurança cibernética, justificada por uma dependência de tecnologia que percorrem quasse todos os processos organizacionais [28].

A tomada de decisão gerencial torna-se cada vez mais relevante à medida que a complexidade das inovações tecnológicas afetam a segurança da informação, sendo fortemente influenciada por diferentes fatores organizacionais e psicológicos, envolvendo muitas partes interessadas. Fatores como setores de atuação, tipos de pessoas, necessidades da empresa, assim como a própria estrutura organizacional, afetam as escolhas de aquisição de sistemas de segurança da informação [29].

O presente estudo se justifica, dessa maneira, por apresentar uma forma de tradução dos anseios da alta gestão em relação aos gestores operacionais, suportando o apetite de risco que a organização está disposta a aceitar no alcance de sua missão e visão de futuro, devidamente estabelecido pelo nível mais alto da organização, servindo de guia para as decisões com foco na estratégia e na seleção de objetivos [17, 30].

O modelo proposto busca a maximização do uso de controles comuns, o aumento da eficácia de planos

de segurança cibernética, a redução do nível de esforço e das despesas com foco na missão organizacional, buscando, de forma contínua, o aumento da eficiência de ações voltadas à segurança e privacidade, inspirando-se no NIST *Risk Management Framework* (RMF) [6].

Gil [31] defende que uma justificativa poderá incluir fatores que determinaram a escolha do tema, a importância da pesquisa em termos teóricos, metodológicos ou empíricos, e uma possível contribuição para o conhecimento de alguma questão prática ainda não resolvida.

1. Fatores que determinaram a escolha do tema: dentre os fatores, destaca-se a área escolhida para o desenvolvimento da pesquisa dentro do PPEE, Gestão de Riscos em Segurança Cibernética, a formação do autor em Compliance e Governança e Gestão Estratégica em Tecnologia da Informação, assim como 35 anos de prática em desenvolvimento de software corporativo;
2. Em termos teóricos e metodológicos, destaca-se o uso de 105 artigos que abrangeram diversos aspectos relacionados à tomada de decisão em gerenciamento de riscos cibernéticos, buscando trazer os principais elementos tratados pelos autores, utilizando-se de 31 revisões sistemáticas que tratavam esses elementos;
3. Por fim, quanto à questão prática não resolvida, trata-se de uma proposta inovadora, que busca auxiliar na tradução das declarações de apetite ao risco cibernético, formuladas pela alta gestão de uma organização, e, com isso, maximizar as ações e investimentos nesse setor.

1.4 PUBLICAÇÕES RELACIONADAS AO TRABALHO

Publicadas:

1. GEORG, Marcus Aurélio Carvalho et al. Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. Revista Ibérica de Sistemas e Tecnologias de Informação, n. E54, p. 602-616, 2022. (Qualis A4)
2. ALVES, Renato Solimar; GEORG, Marcus Aurélio Carvalho; NUNES, R. R. Judiciário sob ataque hacker: fatores de risco para a segurança do processo decisório em sistemas judiciais eletrônicos. Encontro de Administraçâo da Justiça-ENAJUS, 2022.
3. ALVES, Renato Solimar; GEORG, Marcus Aurélio Carvalho; NUNES, R. R. Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. (Qualis A4)

Em avaliação:

1. GEORG, Marcus Aurélio Carvalho et al. Resumo Expandido. Proposta de Modelo de Medição do Apetite a Risco Cibernético em um Tribunal Superior. ENAJUS 2023;
2. Zottmann, Carlos Eduardo et al. Resumo Expandido. Proposta de Metodologia para Avaliação de Riscos de Privacidade para Órgãos do Poder Judiciário no Brasil. ENAJUS 2023;

3. Classificação de soluções de TI (enviado para a Revista Gestão & Tecnologia) (Qualis A3)

1.5 ORGANIZAÇÃO DA DISSERTAÇÃO

Essa dissertação divide-se em 6 capítulos, contando com a Introdução:

- Capítulo 2 - Revisão da Literatura : realizou-se a revisão da literatura, que abrange os principais conceitos tratados na pesquisa.
- Capítulo 3 - Trabalhos Relacionados: realizou-se a revisão da literatura abrangendo artigos que se correlacionam com a pesquisa, buscando-se o estado da arte no campo de pesquisa.
- Capítulo 4 - Metodologia: fez-se o detalhamento da metodologia utilizada na pesquisa.
- Capítulo 5 - Resultados: fez-se a apresentação dos principais resultados.
- Capítulo 6 - Conclusão: fez-se a apresentação dos limites da pesquisa, conclusões, sugestões de trabalhos futuros e limitações.

1.6 APÊNDICES

Com o levantamento das informações oriundas da Revisão Bibliográfica, da Metodologia e dos Resultados, foram disponibilizadas, na forma de apêndices:

- Apêndice 01 - Desafios e Dificuldades,
- Apêndice 02 - Frameworks Utilizados e Citados,
- Apêndice 03 - Critérios e Alternativas Citados,
- Apêndice 04 - Critérios e Alternativas do Modelo Proposto,
- Apêndice 05 - Controles utilizados no Modelo Proposto,
- Apêndice 06 - Relacionamentos entre os Controles e as Alternativas

2 REVISÃO DA LITERATURA

Yin [32] divide a revisão de literatura em três grupos: incursão inicial, revisão seletiva e revisão abrangente. No primeiro grupo estão os estudos que auxiliam na definição do tema, o método e as evidências visando ao novo estudo, que, para efeitos desse estudo, está disposto neste Capítulo 2.

No segundo grupo encontram-se os estudos que cobrem um terreno próximo ao que se pretende desenvolver com a pesquisa, dispostos, nessa pesquisa, no Capítulo 3.

No terceiro grupo encontram-se estudos que buscam sintetizar sobre o que é conhecido sobre um tema, que, para efeitos desse estudo, foram fonte de informações secundárias relevantes na metodologia proposta. Não é objetivo desse estudo realizar uma síntese a respeito dos temas tratados, mas foram utilizados estudos que buscaram sintetizar o estado da arte nas áreas de conhecimento relacionadas à pesquisa.

Este Capítulo dedica-se a contextualizar o problema por meio de teoria, apresentando o estágio atual acerca das questões tratadas, buscando-se fundamentação à pesquisa, trazendo contribuições de investigações já produzidas e publicadas [31].

2.1 CONCEITOS DE RISCO

O risco está presente nas atividades humanas, e os avanços da humanidade aconteceram, entre outros fatores, em virtude do enfrentamento dos desafios encontrados por pessoas que se dispuseram a assumir riscos. Salienta-se, entretanto, que os riscos não se limitam aos desafios enfrentados, e temas como sustentabilidade, corrupção, fraude, abusos nos incentivos a executivos e a investidores, reputação organizacional e ética, entre outros, trazem riscos às organizações, que necessitam realizar suas ações com foco na obtenção de lucros, criação de valor e na proteção da sua sobrevida [33].

Para Dickinson [34, p. 361], o risco corporativo pode ser traduzido como "a medida em que os resultados da estratégia corporativa de uma empresa podem diferir daqueles especificados em seus objetivos corporativos, ou a medida em que eles falham em atender a esses objetivos". As estratégias selecionadas pelas organizações acabam por incorporar um perfil de risco, impactando nas atividades, processos e recursos escolhidos em suas implementações. Fatores externos (novos entrantes, mudanças nos gostos dos consumidores, mudança na economia, mudanças das condições nos mercados financeiros, entre outros) e fatores internos (erros humanos, fraudes, falhas de sistemas, interrupção na produção) podem impactar no alcance dos objetivos desejados.

A norma ISO 31000 (Gestão de riscos — Diretrizes), publicada pela Associação Brasileira de Normas Técnicas (ABNT), conceituando o risco como o "efeito da incerteza nos objetivos" [35, p. 3].

A Controladoria Geral da União (CGU), órgão de controle interno do Governo Federal do Brasil, em sua Metodologia de Gestão de Riscos [36, p. 9] traz três conceitos relacionados a risco (destaque em negrito feito pelo autor):

- **Risco**: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização;
- **Risco inerente**: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
- **Risco residual**: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco;

Em seu Manual de Gestão de Riscos, o Tribunal de Contas da União (TCU), órgão do controle externo do Governo Federal, traz, em seu Manual de Gestão de Riscos [37, p. 50] três conceitos associados ao risco (destaque em negrito feito pelo autor):

- **Risco**: possibilidade de que um evento afete negativamente o alcance de objetivos.
- **Risco-chave**: risco que, em função do impacto potencial ao TCU, deve ser conhecido pela alta administração.
- **Risco Real**: nível do risco que existe na situação concreta, considerados os controles porventura existentes.

Observa-se que, embora haja uma convergência de que o risco trata-se de possibilidade de um evento que atue sobre o atingimento de objetivos, para o TCU esse atingimento se faz de forma negativa, e para a CGU basta que haja um impacto nele. Observa-se, também, que o TCU traz à tona o conceito de **Risco-Chave**, aquele em que há a necessidade de ciência por parte da alta administração, que compreende a Presidência do Órgão e a Comissão de Coordenação-Geral (CCG).

O Instituto Brasileiro de Governança Corporativa (IBGC) conceitua o risco como "a possibilidade de ocorrência de eventos que afetem a capacidade de uma organização atingir seus objetivos" [33, p. 61], alinhando-se à percepção mais ampla da CGU.

Já o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) [38, p. 133] define o risco como "a possibilidade de que um evento ocorra e afete desfavoravelmente a realização dos objetivos", e risco inerente como "o risco que se apresenta a uma organização na ausência de qualquer medida gerencial que poderia alterar a probabilidade ou impacto de um risco" [38, p. 132].

Em documento mais recente, de 2017, o COSO [39, p. 9] nos traz os conceitos de risco, evento, incerteza e severidade:

- **Risco**: A possibilidade de que eventos ocorram e afetem o alcance da estratégia e dos objetivos do negócio.

- **Evento**: Uma ocorrência ou conjunto de ocorrências.
- **Incerteza**: O estado de não saber como ou se eventos potenciais podem se manifestar.
- **Severidade**: Uma medição de considerações como a probabilidade e o impacto de eventos ou o tempo que leva para se recuperar de eventos.

De forma mais abrangente que o COSO, o Superior Tribunal de Justiça (STJ) [40, p. 6] define risco como "a possibilidade de ocorrência de eventos que afetem positiva ou negativamente a realização de objetivos, processos de trabalho e iniciativas nos níveis estratégico, tático ou operacional". Chama a atenção de que risco (um evento incerto) não pode ser confundido com problema por ser uma situação já existente, podendo ser em decorrência de um risco que se concretizou. Salienta-se que os riscos não ficam limitados às questões estratégicas, abrangendo também as iniciativas táticas e operacionais.

Para o Conselho Nacional de Justiça (CNJ) [41], órgão responsável pela promoção do desenvolvimento do Poder Judiciário brasileiro, os eventos que afetam negativamente são chamados de ameaças, e os que afetam positivamente podem ser considerados como oportunidades, podendo afetar tanto a organização como suas unidades organizacionais. Para o órgão, ambos eventos são considerados riscos.

A entrega antecipada de um projeto [42], por exemplo, é citada como um risco positivo, diferenciando daquele que ocorre por um acaso ou por sorte, não devendo ser considerado como um risco positivo.

Para efeitos dessa pesquisa, o risco será considerado de uma maneira mais ampla, englobando, inclusive, aqueles eventos que podem, de alguma medida, gerar oportunidades de melhoria para a organização.

2.2 GERENCIAMENTO DE RISCOS CORPORATIVOS

O Gerenciamento de Riscos Corporativo não é uma coisa única, seja conceitual ou prática, caracterizando-se como um conjunto de conceitos acrescidos nas organizações desde os anos 1990, devendo estar explicitamente relacionado tanto aos objetivos organizacionais como aos objetivos operacionais. As organizações devem identificar todos os riscos que atinjam seus objetivos, dispondo controles conectados ao apetite ao risco estabelecido, e monitorar todo o processo. Power [43] compara esse modelo a um termostato que possibilita ajustes às alterações no ambiente observando-se a temperatura alvo estabelecida, integrado no nível da organização, com a promessa de um uso mais racional e eficiente do capital tanto da organização como das unidades de negócio que a compõe.

Segundo Dickinson [34, p. 360], o gerenciamento de riscos corporativos emergiu nos meados da década de 1990 como uma função de gerenciamento, traduzindo-se em "uma abordagem sistemática e integrada para o gerenciamento de riscos totais que uma empresa enfrenta". Duas causas principais provocaram seu surgimento: (i) com um número alto de falências de corporações relevantes e com perdas evitáveis, o gerenciamento de risco passou a ser introduzido na governança corporativa, obrigando os diretores a relatarem os riscos em seus controles internos e, (ii) os modelos de valor para acionistas estão cada vez mais inseridos no planejamento estratégico, inspirados na "teoria das finanças, onde o risco sempre desempenhou um papel central". Entretanto os processos de tomada de decisão corporativos já levavam em consideração a gestão de riscos desde o final da década de 1940, destacando-se a prática de transferên-

cia de riscos (catástrofes naturais, acidentes, erro humano ou fraude) por meio de seguros, evoluindo para outros tipos (riscos de crédito, por exemplo) à medida que o mercado de seguros entrou em expansão [34].

Ainda Dickinson [34, pp. 362-363], como os riscos gerais fazem parte da estratégia corporativa, "uma forma de gerenciar esses riscos é por meio da escolha da própria estratégia corporativa", concluindo que o "gerenciamento de riscos corporativos deve ser um processo de cima para baixo". A pesquisa atual leva em consideração essa premissa para a formulação da mensuração do apetite a risco cibernético.

Arruda et al. [44, p. 1] nos informa que o gerenciamento de riscos corporativos, oriundo do termo inglês *Enterprise Risk Management* (ERM), tornou-se fundamental na gestão de negócios, apontando o aumento da complexidade do ambiente de negócios devido "à concorrência global, à desregulamentação, ao downsizing e ao avanço da tecnologia, além das crises financeiras e fraudes em instituições financeiras e não financeiras no âmbito nacional e internacional ocorridas nas últimas décadas", distinguindo da forma tradicional, onde o riscos eram gerenciados separadamente. A quantidade de risco assumido pelas organizações em um cenário de incertezas, acabam por elevar a relevância das abordagens ao apetite e à tolerância ao risco, buscando-se alinhamento às estratégias de negócio.

O COSO [38, p. 4] define o gerenciamento de riscos como:

> O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

Já o IBGC [33, p. 14] nos traz a seguinte definição:

> O gerenciamento de riscos corporativos (GRCorp) pode ser entendido como um sistema intrínseco ao planejamento estratégico de negócios, composto por processos contínuos e estruturados – desenhados para identificar e responder a eventos que possam afetar os objetivos da organização – e por uma estrutura de governança corporativa – responsável por manter esse sistema vivo e em funcionamento. Por meio desses processos, a organização pode mapear oportunidades de ganhos e reduzir a probabilidade e o impacto de perdas. Trata-se, portanto, de um sistema integrado para conduzir o apetite à tomada de riscos no ambiente de negócios, a fim de alcançar os objetivos definidos.

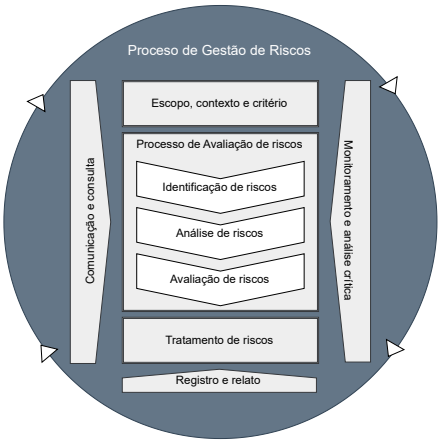
Cabe ao GRCorp se integrar à estratégia organizacional, contribuindo para longevidade e consecução dos objetivos estratégicos. O Conselho de Administração (CA) é responsável por definir os objetivos estratégicos e o perfil de riscos de um empreendimento. A definição do perfil implica apontar o grau de apetite a riscos, as faixas de tolerância a desvios em relação aos níveis estabelecidos de riscos, considerados como aceitáveis. O apetite a risco indica o grau aceitável de exposição na busca do valor, estabelecido pela visão e missão organizacional. O perfil de riscos está associado ao nível de riscos para o alcance de um determinado desempenho, assim como no comportamento organizacional quando da busca de novas oportunidades e na minimização de impactos. A tolerância a riscos concentra-se nos intervalos aceitáveis de

riscos, seus limites [33].A governança do GRCorp se dá por distribuição de funções dentro da organização, permitindo uma gestão compartilhada dos riscos nos diversos níveis, visando à comunicação adequada das informações, permitindo seu uso na tomada de decisão [33].

A Controladoria Geral da União (CGU) [36, p. 9] faz uma distinção entre a gestão de riscos e o gerenciamento de riscos, conceituando a gestão de riscos como “arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente”, e o gerenciamento de riscos como “processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais”.

A ISO 31000 [35, p. 9] define que o processo de gestão de ricos envolve "a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos", sendo sua sistematização ilustrada na fig. 2.1. Para a norma, é salutar que o processo seja parte da gestão e da tomada de decisão, integrando-se na estrutura organizacional, em suas operações e processos organizacionais, podendo ser aplicado nos níveis estratégico, operacional, assim como em programas e projetos.

Figura 2.1: Processo de Gestão de Riscos



Fonte: Adaptada de [35]

Para o TCU [37], a gestão de riscos objetiva o auxílio à tomada de decisão, buscando prover segurança no alcance dos objetivos da instituição focado na missão da organização, e em seu **Referencial Básico de Governança Organizacional** [45, p. 27] utiliza as expressões “gestão de riscos” e “gerenciamento de riscos” como sinônimas, conceituando:

> A gestão de riscos serve para identificar e entender os riscos e manter as instâncias responsáveis informadas, para que as respostas aos riscos sejam apropriadas. Para isso, a organização precisa implantar estrutura de gestão de riscos adequada às suas necessidades, definir o processo de gestão de riscos e integrá-lo à gestão e à tomada de decisão, garantindo a alocação de recursos e a existência dos canais de comunicação necessários.

O CNJ aponta alguns princípios relacionados à gestão de riscos, conforme o seu **Manual de Gestão de Riscos** [41, p. 7] (destaque em negrito feito pelo autor):

1. **Ser alinhada com os objetivos organizacionais estabelecidos**. Só é possível gerenciar riscos se objetivos são claramente estabelecidos e existem indicadores de desempenho que mensurem os resultados alcançados;
2. **Ser adaptável ao contexto organizacional**. Isso significa dizer que a forma do gerenciamento de riscos não é mais importante que o conteúdo e que, por essa razão, gestores e servidores podem evidenciar um gerenciamento de riscos adequado sem necessariamente seguir os modelos padronizados propostos neste manual;
3. **Envolver as partes interessadas**. Para se ter um gerenciamento de riscos adequado é preciso envolver os atores adequados e assim entender as diversas perspectivas dos atores envolvidos no alcance dos resultados pretendidos;
4. **Prover as orientações necessárias para gestores e servidores**. É preciso fornecer as ferramentas adequadas para que servidores e gestores possam gerenciar adequadamente seus riscos;
5. **Prover informações para a tomada de decisão**. Para se tomar boas decisões é preciso ter informações adequadas e o gerenciamento de riscos busca subsidiar os tomadores de decisão com as melhores informações e análises possíveis;
6. **Facilitar o aprimoramento contínuo**. É natural que problemas surjam e é importante que as organizações não cometam o mesmo erro sucessivamente;
7. **Incentivar a cultura de gerenciamento de riscos**. Identificar e avaliar riscos, problemas e oportunidades evidencia uma boa gestão por parte de servidores e gestores e não deve ser visto como expressão de vulnerabilidade pessoal ou da unidade; e
8. **Gerar valor mensurável para a organização**. Gerenciar riscos é buscar garantir o alcance dos objetivos organizacionais, portanto é extremamente importante para mensurar os resultados

Entretanto, apesar dos objetivos do gerenciamento de riscos estarem muito claros, o COSO [38] alerta que, por melhor projetado e operado, o gerenciamento de riscos trará apenas uma **segurança razoável** quanto ao alcance dos objetivos da organização, pois são afetados pelas limitações existentes nos processos administrativos. Um dos fatores que pertencem a essas limitações é a falha de julgamento humano no processo decisório.

Maček et al. [27] apresentam algumas características associadas à Gestão de Riscos:

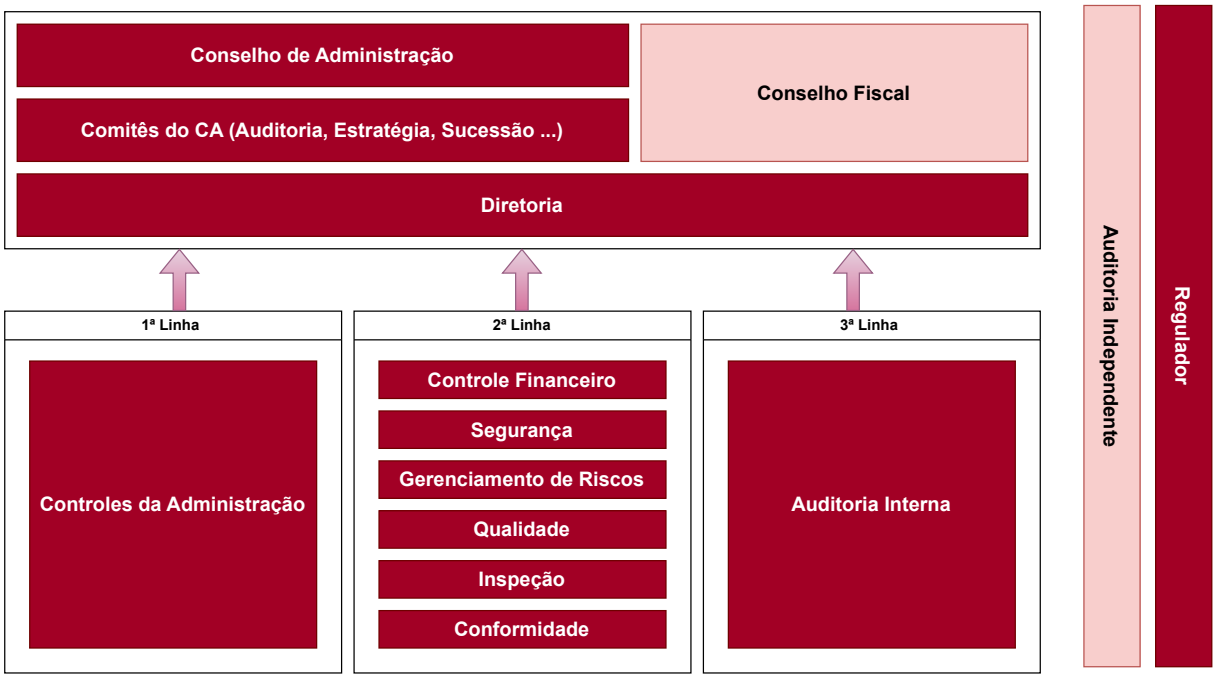
- Processo altamente crítico,
- É composto por um conjunto de atividades relacionadas ao controle e gerenciamento de risco,
- Seu objetivo é reduzir os riscos a um nível aceitável,
- Dependente do apetite ao risco da gestão.

Observando as limitações do gerenciamento de riscos corporativos, Power [43] compreende que deva estar incorporado aos controles internos e aos processos de negócio, embora haja um distanciamento sobre o que isso realmente significa e o que possa envolver. Uma das consequências dessa prática, segundo

Power, é a inclusão nas descrições de cargos onde os gestores de negócio passam as ser designados como proprietários do risco. Entretanto, Power compreende que o gerenciamento de riscos corporativos é incapaz de representar internamente questões de riscos, pois exige uma imaginação mais ampla do que a extensão para o qual foi criado. Como resposta às limitações do gerenciamento de riscos, aponta como possibilidade de complementação o Gerenciamento de Continuidade de Negócios (GCN), responsável por integrar não apenas as unidades internas, como fornecedores e concorrentes. O GCN nasce com a perspectiva de representar a interconexão entre os elementos que compõe a vida comercial, necessitando, entretanto, que as organizações percebam a existência de barreiras e que necessitam ser superadas de forma coletiva, podendo "fornecer uma plataforma de conhecimento mais bem-sucedida para repensar a gestão de riscos" [43, p. 853].

A Figura 2.2 demonstra como se dá a governança, por meio de três linhas: a 1ª por gestores de unidades e responsáveis pelos processos de trabalho, a 2ª por gestores corporativos, de conformidade e de práticas de controle, e a 3ª é formada pela auditora interna.

Figura 2.2: Linhas do Gerenciamento de Risco



Fonte: Adaptada de [33, p. 25]

O gerenciamento de riscos corporativos feito de forma integrada traz alguns benefícios [39]:

- Aumento da gama de oportunidades,
- Aumento de resultados positivos e a redução das surpresas negativas,
- O gerenciamento dos riscos de toda a organização, considerando-se o todo e as suas partes,
- Redução da variabilidade do desempenho,
- Melhoria da distribuição e uso dos recursos

Para efeitos desse trabalho, consideramos o gerenciamento e a gestão de riscos como sinônimos, destacando-se alguns pontos relevantes:

- Trata-se de um processo de trabalho composto por atividades que permeiam toda a organização: não só a organização enfrenta riscos, como as unidades que a compõem;
- É limitado, pois há riscos que vão além da capacidade da organização e da capacidade de julgamento das pessoas que a compõem;
- A sobrevivência e o alcance dos objetivos organizacionais formam o norte do gerenciamento de riscos;
- Os objetivos organizacionais devem levar em consideração os riscos de sobrevivência;
- Deve buscar minimizar os impactos negativos dos eventos de riscos enfrentados no alcance dos objetivos;
- As diversas unidades que compõem uma organização devem buscar sinergia no enfrentamento aos riscos;
- A alta gestão deve comunicar qual o apetite a risco da organização, possibilitando que gestores compreendam os limites a serem enfrentados em suas decisões;
- A tradução das declarações de apetite a risco da alta gestão deve possibilitar uma compreensão ampla, buscando-se evitar os efeitos nocivos de traduções equivocadas;
- O apetite a risco deve ser revisto, sempre que a sobrevivência da organização estiver em jogo, ou que novos objetivos sejam estabelecidos;
- É voltado para a tomada de decisão, envolvendo desde a alta gestão, gestores táticos, gestores operacionais, funcionários e colaboradores;
- É dinâmico, exigindo melhorias contínuas.

2.3 APETITE E TOLERÂNCIA A RISCO

Como podemos observar na Seção 2.2, expressões como perfil a (ou de) risco, tolerância a risco e apetite a risco são usadas com certa frequência, sendo motores do comportamento organizacional, em um nível mais alto de abstração e compreensão. Falar de riscos sem falar de apetite a risco poderia ser considerado um erro crasso, entretanto, como veremos, falar de apetite a risco não traz muita precisão na tomada de decisão, mas se trata de uma ferramenta necessária.

Para Marshall, Ojiako e Chipulu [46], o apetite ao risco é uma metáfora que orienta o gerenciamento de riscos, levando o imaginário do gestor para a generalização e abstração de alto nível podendo reduzir a compreensão de questões complexas. Para os autores, soa estranho dizer que um gerente possua um apetite por um determinado nível de risco, alertando que tal abordagem usada no risco organizacional poderá

trazer resultados fúteis e perversos em relação aos objetivos desejados, e enganosos quanto ao próprio gerenciamento de riscos. Entre as descobertas apontadas pelos autores, destacam-se a falta de confiança na avaliação do risco organizacional e uma cegueira relacionada ao risco comportamental. Entre os pontos ressaltados pelos autores, a corrupção, a imprudência e o encobrimento de ações acabam por aparecerem toda vez que o apetite ao risco é experimentado. Os prazos do gerenciamento de risco serão diferentes do da gestão e da medição do desempenho, sendo que "culturas saudáveis levam tempo para crescer e culturas disfuncionais geralmente levam tempo para mudar" [46, p.].O caminho a ser percorrido, com o uso do apetite a risco quando um conceito comportamental, é longo, mas poderá ser muito valioso.

A metáfora do apetite a risco nos leva ao desejo humano de se expor para saciar a fome, evitando que morra por inanição: à sobrevivência. Entretanto, à medida que o ser humano dominava o seu ambiente, desenvolvia novas formas de enfrentamentos dos problemas apresentados, percebia que novos desafios estavam presentes: o aumento da população, novos inimigos interessados pelos ganhos alcançados, doenças, períodos de tempos sem chuva, frio e calor em excesso. Tecnologias foram sendo introduzidas gradualmente, permitindo desde o arar da terra para o plantio, o desenvolvimento de armas que auxiliavam na defesa de invasores como conquista de novas regiões, a escrita para registrar os fatos da natureza, gerando conhecimento, e, se trouxermos para os dias de hoje, o enfrentamento aos desafios apresentados pela criação de redes sociais, que permitiu uma conexão mundial sem termos uma compreensão dos seus riscos. Esse enfrentamento desejado pelo ser humano, sem muitas análises sobre os resultados futuros, se dá, muitas vezes, pelo desejo da melhoria contínua, pelo apetite humano de buscar sempre mais, mesmo que novos riscos se apresentem.

Assim como os seres humanos, as organizações e empresas modernas mimetizam esses comportamentos, enfrentando os desafios inerentes ao ambiente em que atuam, visando à sua sobrevivência e aos objetivos desejados, sendo algumas mais vorazes em seus comportamentos, se expondo a riscos de diversos tipos (legal, financeiro, saúde, reputacional, entre outros), e outras empresas mais conservadoras, mais controladas, com apetite menor aos riscos. O apetite a risco dentro de uma organização é compartilhado, mesmo que não se tenha ciência de qual é, mas ele existe e todos são impactados.

O apetite a risco "permite comunicar, evidenciar e formalizar o quanto de risco a organização está disposta a incorrer para atingir seus objetivos", podendo ser evidenciado por meio de uma declaração por parte da alta administração na definição dos seus objetivos estratégicos, dando suporte às decisões por parte das áreas de negócio [44, p. 2]. Os autores salientam que, apesar de fazer parte central do gerenciamento de riscos corporativos, a compreensão e o uso adequado do apetite a risco está muito aquém do desejado.

Martens e Rittenberg [47] acreditam que entre a estratégia e o desempenho há um elo crítico, que se traduz no apetite ao risco, e que evoluirá com o tempo, à medida que as estratégias evoluem, identificando pontos que necessitam ser lembrados em relação ao apetite ao risco:

- Não é uma estrutura separada, devendo ser articulado dentro da organização em conjunto com o gerenciamento de risco,
- Não é o mesmo que tolerância ao risco,
- Sua aplicação não se limita à indústria financeira,
- Deve estar no centro das tomadas de decisão,

- É muito mais que uma métrica, embora útil a abordagem, deve-se focar em ações voltadas para o futuro
- Auxilia no aumento da transparência, informando os riscos que a organização deseja assumir, assim como aqueles que deverão ser evitados

Para uma organização buscar a manutenção de sua competitividade tanto a capacidade operacional quanto o comportamento de risco são estratégias essenciais, dentro de uma ambiente complexo e mutável, sendo a medição e o controle de seu comportamento de risco fundamentais [48]. Embora os retornos das instituições sejam o principal foco tanto dos tomadores de decisão como dos acionistas, entre outros fatores, o comportamento dinâmico do risco e indicadores operacionais fazem parte das preocupações, apresentando-se diferentes nos diversos períodos de desenvolvimento das instituições.

Nesse sentido, o COSO [38, p. 20] define o apetite a risco como:

> O apetite a risco é a quantidade de riscos, no sentido mais amplo, que uma organização está disposta a aceitar em sua busca para agregar valor. O apetite a risco reflete toda a filosofia administrativa de uma organização e, por sua vez, influencia a cultura e o estilo operacional desta. Muitas organizações consideram esse apetite de forma qualitativa, categorizando-o como elevado, moderado ou baixo, enquanto outras organizações adotam uma abordagem quantitativa que reflete e equilibra as metas de crescimento, retorno e risco. Uma organização dotada de um maior apetite a risco poderá desejar alocar grande parcela de seu capital para áreas de alto risco como mercados recém-emergentes. Por outro lado, uma organização com um reduzido apetite a risco poderá limitar seu risco de curto prazo investindo apenas em mercados maduros e mais estáveis.

Salienta-se que quando analisamos a definição trazida pelo COSO [38], percebe-se que algumas palavras / expressões sobressaem: (i) disposta a aceitar, (ii) agregar valor, (iii) filosofia administrativa, (iv) cultura e estilo operacional, (v) forma qualitativa e quantitativa, (vi) alocar capital.

A expressão “agregar valor”, está relacionada ao que se produz e aos efeitos que a organização traz às suas ambições e à sociedade. Já a expressão “alocar capital” está relacionada aos investimentos. Essas duas expressões são de compreensão mais fácil que as demais inseridas no conceito. A expressão “disposta a aceitar” nos leva a uma intenção futura que, muitas vezes, representa, assim como cultura e estilo operacional, aos comportamentos humanos, que são, na maioria das vezes, movidos por impulsos quando as oportunidades acontecem: imagine um grupo de humanos que, ao voltar para casa após uma caça, percebe uma nova oportunidade de alimento, e não leva em consideração que já tem o suficiente, e que seus integrantes estão exaustos, observando apenas a possibilidade de mais mantimentos. Qual seria o comportamento dos líderes do grupo nessa situação? Que critérios levariam em consideração para novos desafios? A sobrevida estaria em jogo caso optassem por não buscar mais alimentos?

O IBGC [33, p. 16] define apetite a risco como "nível de risco que a organização está disposta a aceitar na busca e na realização de sua missão", devendo ser estabelecido pelo Conselho de Administração (CA), e como [33, p. 60] “o nível de risco que a organização pode aceitar, conforme estabelecido por sua visão e missão, indicando o grau de exposição aceitável na sua busca de valor”.

Enquanto o COSO [38] fala em “disposta a aceitar”, remetendo a um processo decisório baseado em desejo, a definição do IBGC [33] fala tanto em "disposta a aceitar"e “pode aceitar”, a decisão, neste último caso, baseia-se na capacidade organizacional de enfrentar ou não o risco.

Para o *Institute of Risk Management* (IRM), tanto o apetite quanto a tolerância a risco estão ligados ao desempenho organizacional no decorrer do tempo, sendo que o apetite diz respeito à busca do risco, e a tolerância trata sobre o que pode permitir que a organização trate [49]. Para o IRM, a tolerância ao risco “pode ser expressa em termos absolutos (não desejamos mais do que x% capital exposto a perdas em uma linha de negócios, por exemplo), o apetite a risco trata do que a organização quer fazer e como ela faz” [49, p. 8].

Os seguintes princípios dão sustentação aos trabalhos do IRM [49, p. 6] (negritos por conta do autor):

1. **O apetite ao risco pode ser complexo**. A simplicidade excessiva, embora superficialmente atraente, leva a águas perigosas: muito melhor reconhecer a complexidade e lidar com ela, em vez de ignorá-la.
2. **O apetite ao risco precisa ser mensurável**. Caso contrário, existe o risco de que quaisquer declarações se tornem vazias e inexpressivas. Não estamos promovendo nenhuma abordagem de medição individual, mas fundamentalmente é importante que os diretores entendam como seus direcionadores de desempenho são afetados pelo risco. O valor para o acionista pode ser um ponto de partida apropriado para algumas organizações privadas, o valor para o acionista ou “Valor Econômico Agregado” pode ser apropriado para outras. Também prevemos um maior uso de indicadores-chave de risco e indicadores-chave de controle que devem estar prontamente disponíveis dentro ou fora da organização. Dados relevantes e precisos são vitais para esse processo e instamos os diretores a garantir que haja o mesmo nível de governança de dados sobre esses indicadores que haveria sobre os dados contábeis de rotina.
3. **O apetite ao risco não é um conceito único e fixo**. Haverá uma gama de apetites por riscos diferentes que precisam se alinhar e esses apetites podem variar ao longo do tempo: o aspecto temporal do apetite ao risco é um atributo chave para todo esse desenvolvimento.
4. **O apetite ao risco deve ser desenvolvido no contexto da capacidade de gestão de risco de uma organização, que é uma função da capacidade de risco e da maturidade em gestão de risco**. A gestão de riscos continua sendo uma disciplina emergente e algumas organizações, independentemente do tamanho ou complexidade, fazem isso muito melhor do que outras. Isso se deve em parte à sua cultura de gerenciamento de riscos (um subconjunto da cultura geral), em parte devido a seus sistemas e processos e em parte à natureza de seus negócios. No entanto, até que uma organização tenha uma visão clara de sua capacidade de risco e sua maturidade de gerenciamento de riscos, não pode ser claro qual abordagem funcionaria ou como ela deveria ser implementada.
5. **O apetite ao risco deve levar em conta as diferentes visões nos níveis estratégico, tático e operacional**. Em outras palavras, enquanto o Código de Governança Corporativa

do Reino Unido prevê uma visão estratégica do apetite ao risco, na verdade o apetite ao risco precisa ser abordado em toda a organização para que faça algum sentido prático.

6. **O apetite ao risco deve estar integrado à cultura de controle da organização**. Nossa estrutura explora isso observando tanto a propensão a assumir riscos quanto a propensão a exercer controle. A estrutura promove a ideia de que o nível estratégico é proporcionalmente mais sobre assumir riscos do que exercer controle, enquanto no nível operacional as proporções são amplamente invertidas. Claramente, as proporções relativas dependerão da própria organização, da natureza dos riscos que enfrenta e do ambiente regulatório em que opera.

O *Financial Stability Board* (FSB) [1], que sucedeu em 2009 o *Financial Stability Forum* (FSF) fundado em 1999 pelos Ministros das Finanças e Presidentes do Banco Central do Grupo dos Sete (G7), sendo composto por membros de 24 países de vários continentes, entre eles EUA, Japão, Canadá, Alemanha, França e Brasil, além de órgãos relevantes, como o Fundo Monetário Internacional (FMI), estabeleceu uma série de princípios voltados para uma *Risk Appetite Frameworks* (RAF) - estrutura eficaz a apetite a risco com foco em instituições financeiras [50]. Alguns pontos são relevantes para esse estudo:

- **Elementos-chave**: (i) estrutura de apeite a risco, (ii) declaração de apetite a risco, (iii) limites de risco, e (iv) definição das funções e responsabilidades dentro da organização;
- **RAF Consistente**: A RAF deve permear uma organização como um todo, e se possuir subsidiárias, deverão possuir suas RAF's que deverão estar aderentes a toda a instituição.
- **Alto Nível**: Os Princípios são estabelecidos em alto nível, permitindo que as instituições financeiras desenvolvam sua própria RAF, adaptando-se aos ambientes regulatórios e o tipo de negócio que atua, com foco no gerenciamento de seus riscos.
- **Garantia de cumprimento dos Princípios**: As supervisões devem tomar medidas no sentido de garantir que os Princípios sejam cumpridos.

O apetite a riscos trata-se de uma declaração que a organização faz para definir se um risco é aceitável ou inaceitável, devendo ser compreendidos, sendo instrumentos que habilitam e delimitam a atuação inovadora da organização [42].

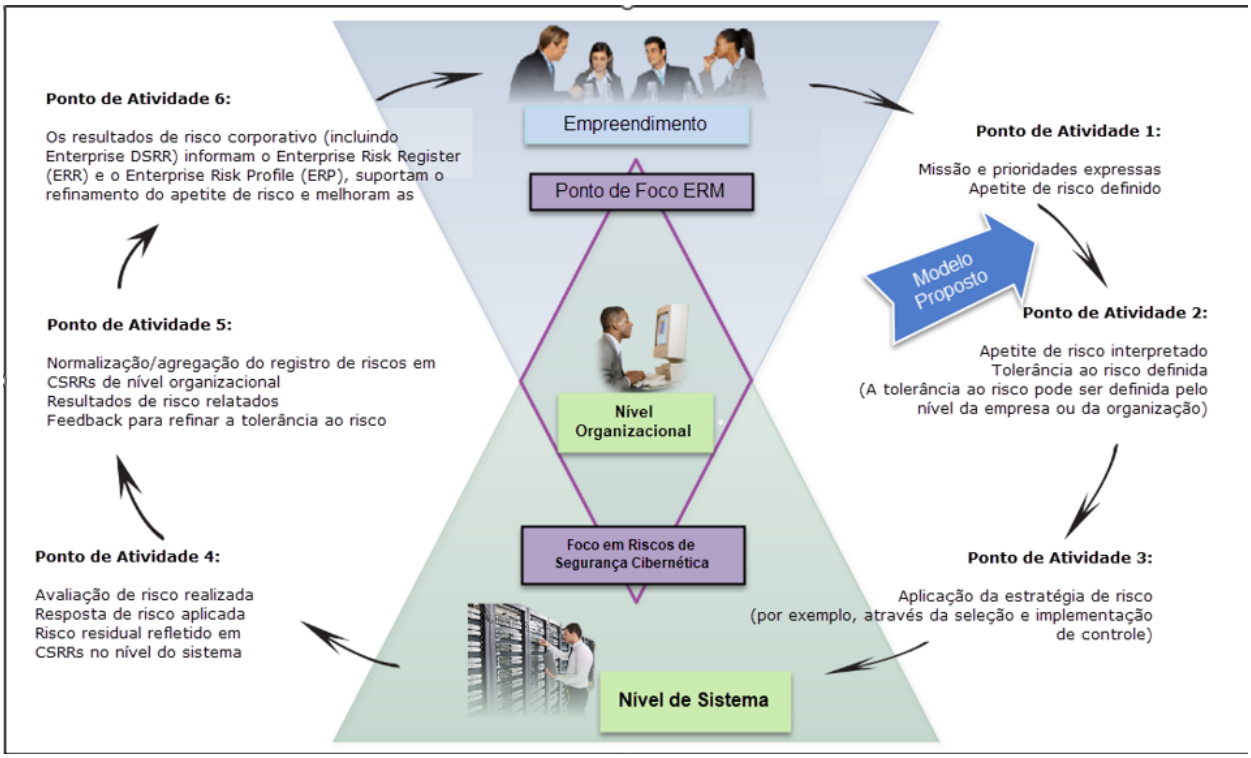
Power [43] chama a atenção que a expressão "apetite a risco"está ligada a uma postulação neoliberal das organizações compostas por indivíduos empreendedores, e que o Gerenciamento de Riscos Corporativos impõem uma normatividade de se assumir riscos, cabendo a seus colaboradores que conheçam seu apetite por riscos. A visão empresarial observa a organização como um ator com inteligência e com intenções, reduzindo-a a uma máquina de ação, em que valores de entrada são tratados por gatilhos com limites e tolerâncias visando ao feedback e às medidas de controle. Salienta, Power, que o COSO, ao definir o apetite a risco, que a alta administração possa determinar de forma racional a quantidade de risco que está disposta a suportar.

[1] <https://www.fsb.org/about/history-of-the-fsb/> acessado em 12/03/2023

Para Power [43, p. 851] se faz necessário conceituar o apetite ao risco como um processo que pode "direcionar melhor a atenção do gerenciamento de risco para onde ele provavelmente tem faltado, ou seja, para a multiplicidade de interações que moldam os limites operacionais e éticos no nível da prática organizacional". A abordagem do COSO, para Power, é limitante na concepção voltada para o capital, devendo-se incluir outros elementos, alinhando-se às preocupações recentes da governança corporativa.

Quinn et al. [17] estabelece um paralelo entre apetite ao risco e tolerância ao risco semelhante à governança e atividades de gestão, sendo que o apetite a risco e a governança são estabelecidas pela alta gestão, e a tolerância ao risco e atividades de gestão estão explicitadas em nível de programas e de objetivos. As declarações de apetite e tolerância ao risco buscam o foco às atividades de gerenciamento de riscos, comunicando as expectativas organizacionais. Na fig. 2.3 vemos um processo cíclico de definição do apetite a risco por parte da alta gestão, sendo compreendido e interpretado, transformando-se em tolerância a risco no nível organizacional. O modelo proposto pela pesquisa busca situar-se nessa transformação.

Figura 2.3: Ilustração de Risco e Coordenação Organizacional



Fonte: Adaptada de [17]

Salienta-se que a abordagem na gestão de riscos não pode ser feita de forma única, dependendo da realidade de cada empresa ou organização, fazendo com que seus apetites e tolerâncias a risco estejam relacionados aos seus ambientes específicos [51]. Stine et al. [30] remetem à necessidade da liderança de alto nível de uma organização de definir o apetite a risco, servindo de orientação para as definições de estratégias e seleção de objetivos.

Para Power [43], deve-se buscar a conceitualização do apetite ao risco como um processo, direcionando a atenção da gestão de risco com foco na multiplicidade de interações tanto operacionais quanto éticos da organização, indo além da visão do COSO, que possui um discurso com foco na medição de capital.

Para efeitos dessa pesquisa, o apetite a risco de uma organização encontra-se manifestado:

1. Declaração de Apetite a Risco feito de forma oficial
2. Normas internas que tratem de que cuidados são necessários na condução de atividades relacionadas ao negócio da organização
3. Nas regras informacionais que impõem comportamentos aos funcionários e colaboradores
4. Normas do setor que impõem controles em suas atividades
5. No exemplo que vem de cima, na forma que os funcionários veem as práticas de sua liderança
6. Nas escolhas estratégicas da instituição, em especial aquelas que implicam na defesa da sobrevivência
7. Na Cultura Organizacional

2.4 CONTROLES

A ISO 31000 [35, p. 2] conceitua controle como a "medida que mantém e/ou modifica o risco".

Vieira e Barreto [52, p. 70] definem controle como processos estruturados que visam à mitigação de riscos com foco no alcance de objetivos da instituição "para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos".

Nunes et al. [53, p. 7] definem os controles como:

> ... são medidas que mantêm ou modificam os riscos. Eles incluem, mas não estão limitados a processos, políticas, dispositivos, práticas, ou quaisquer outras condições, sem, contudo, haver garantia de que eles exercerão, necessariamente, o efeito modificador pretendido no risco.

As instituições expressam as atividades de controle por meio de políticas e procedimentos de controle, devendo ser estabelecidos e aplicados, assegurando a eficácia no tratamento de riscos associados ao cumprimento dos objetivos da organização, classificando-se em três categorias: de processos / operacionais, de registros e de conformidade. Tais atividades buscam assegurar [54, p. 9]:

- os objetivos sejam alcançados;
- as diretrizes administrativas sejam cumpridas;
- as ações necessárias para gerenciar os riscos com vistas à consecução dos objetivos da entidade estejam sendo implementadas.

Encontramos em CGU [36, p. 9], sobre medida de controle:

> ... medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados;
>
> Controle interno da gestão: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

A CGU [36, p. 24] apresenta uma classificação dos controles (negritos por conta do autor):

- **Controles preventivos**: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos / checklist definidos para o processo e capacitação dos servidores envolvidos no processo.
- **Controles de atenuação e recuperação**: controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.
- **Controles detectivos**: controles existentes que atuam na detecção da materialização de um risco ou de sua iminência. Exemplos de controles de detecção: indicadores; termômetros; sensores.

Já o COSO [39, p. 5] nos traz que o gerenciamento de riscos corporativos incorpora conceitos do controle interno, mas que alguns conceitos tratados no risco empresarial extrapolam os tratados pelo controle interno:

> Controle interno é o processo posto em prática por uma entidade para fornecer uma garantia razoável de que os objetivos serão alcançados. O controle interno ajuda a organização a identificar e analisar os riscos para atingir esses objetivos e como gerenciar riscos. Permite que a gestão se mantenha focada nas operações da entidade e na prossecução dos seus objetivos de desempenho, cumprindo as leis e regulamentos relevantes. Observe, no entanto, que alguns conceitos relacionados à gestão de risco empresarial não são considerados dentro do controle interno (por exemplo, conceitos de apetite ao risco, tolerância, estratégia e objetivos são definidos dentro da idade humana de risco da empresa, mas vistos como pré-condições do controle interno).

Ainda nesse sentido, no Manual de Gestão de Riscos do CNJ [41, p. 8], podemos observar o seguinte conceito associado aos controles:

> ... são ações tomadas para prover alguma garantia de que os objetivos estabelecidos serão alcançados. Ocorre que alguns procedimentos são estabelecidos sem que exista uma clara conexão com os objetivos definidos e que o estabelecimento de controles envolve invariavelmente custos administrativos. Percebe-se, portanto, a necessidade de que gestores e servidores

saibam estabelecer controles apropriados e efetivos para evitar gastos desnecessários. Por essa razão é recomendável realizar análises periódicas dos controles estabelecidos pelas unidades, que devem abordar, no mínimo, a efetividade e a relação custo-benefício de tais controles.

Observa-se, assim, a preocupação do CNJ [41] quanto à necessidade de escolhas corretas, com clara conexão com os objetivos, evitando-se gastos desnecessários.

O **Guia de Aperfeiçoamento da Segurança Cibernética** do NIST [55, p. 8], propõe uma Estrutura Básica que "fornece um conjunto de atividades para alcançar resultados específicos de segurança cibernética e faz referência a exemplos de diretrizes para que esses resultados sejam alcançados". Para efeitos desse trabalho, usaremos o conjunto de cento e oito (108) atividades técnicas e/ou de gerenciamento como a fonte dos controles a serem avaliados no modelo proposto.

Sobre controles de privacidade e segurança para sistemas de informações e organizações, o NIST [56] nos traz os seguintes pontos relacionados ao gerenciamento de riscos:

- As organizações devem ser diligentes no gerenciamento de riscos relacionados à segurança da informação e da privacidade;
- Deve estabelecer um programa abrangente de gerenciamento de riscos, categorizando sistemas e implementando controles que atendam às necessidades da missão e do negócio, avaliando a eficácia e monitorando de forma contínua os sistemas;
- A implementação de programas robustos poderá facilitar a conformidade, seja legal, seja do setor em que atua;
- Necessidade de estruturas de gerenciamento de riscos visando ao desenvolvimento, à implementação e à manutenção de medidas protetivas;
- Atendimento às necessidades das partes interessadas e às ameaças a ativos organizacionais, pessoas, organizações e nação;
- Foco na missões essenciais e funções de negócios

2.5 SEGURANÇA CIBERNÉTICA

O WEF publicou a 18ª edição do Relatório de Riscos Globais 2022-2023 [57], onde apresenta uma lista de riscos a serem enfrentados a curto (dois anos) e médio prazos (dez anos), como pode ser observado na Fig. 2.4. A combinação de riscos relacionados a energia, a escassez de matéria-prima e a insegurança cibernética geram impactos na cadeia de suprimentos, trazendo incertezas aos investidores. Os crimes cibernéticos e a insegurança cibernética se encontram entre os dez maiores riscos a serem enfrentados globalmente, tanto a curto, quanto a longo prazo, dando a dimensão do desafio global no seu equacionamento.

As organizações variam de uma para outra, fazendo que não exista uma abordagem de segurança cibernética padronizada, pois acabam por envolver diferenças relevantes entre as partes interessadas, ameaças

cibernéticas, ambientes de informação, dependências entre os negócios praticados, níveis de aceitação ao risco, entre outras [51].

Figura 2.4: Lista dos principais riscos globais

Fonte: Adaptada de [57]

Para Carcary et al. [20], tanto o ritmo da transformação digital como o aparecimento de novas tecnologias têm levado as organizações a um escopo mais amplo e com maior severidade de ataques cibernéticos de segurança. Em um ambiente digital, onde a liderança tem uma maior tolerância e apetite a risco, se faz necessário que se repense as abordagens da gestão de segurança cibernética, devendo-se buscar abordagens holísticas e proativas, que possam evoluir e se adaptar no combate às ameaças, assim como na minimização dos efeitos negativos.

Mastwijk [58] conceitua o ciberespaço como o local onde as atividades cibernéticas são efetuadas por pessoas utilizando-se de sistemas de tecnologia da informação, consistindo de três camadas: técnica, sociotécnica e de governança. A proteção da camada técnica se dá pela segurança de TI, já a proteção da camada sociotécnica, onde há interação entre as pessoas e a tecnologia, é chamada de segurança cibernética, e, por fim, a camada de governança trata dos níveis de risco e conformidade das duas camadas citadas.

Zhao et al. [8] nos lembra que a segurança cibernética envolve tanto a segurança nacional, como a corporativa e a privacidade pessoal, e que a medição dessa segurança se mostra um passo importante para a proteção de redes, cujas ameaças são cada vez mais diversas, com mudanças constantes de estados.

A onipresença dos ataques cibernéticos, o uso de tecnologias avançadas por meio de entidades mal-intencionadas, o aumento de violações de dados impulsionadas "por motivações financeiras, políticas, vingança, espionagem, roubo de identidade e outras, resultando em consequências financeiras de longo prazo, reputação e perda de clientes, perda de vantagem competitiva e outros passivos", perda de ativos valiosos, são elementos que acabaram por elevar a relevância do papel da gestão de riscos cibernéticos, tornando-se um "componente vital do portfólio de gerenciamento de riscos corporativos" [59, p. 4-5].

Para Facchinetti et al. [60, p. 174] o domínio que envolve os riscos cibernéticos "é mais amplo do que o dos ataques cibernéticos, pois também inclui eventos de risco que podem ser causados por pessoas internas ou eventos que podem ser causados sem qualquer intenção de prejudicar", definindo o risco cibernético como "qualquer risco decorrente do uso de TIC que comprometa a confidencialidade, a disponibilidade ou a integridade de dados ou serviços".

A Segurança Cibernética possui algumas características, dentre elas destacam-se a a garantia em [61]:

- **Confidencialidade**: que as informações confidenciais sejam mantidas em sigilo e não sejam acessadas por pessoas não autorizadas;
- **Integridade**: que as informações não sejam modificadas de forma não autorizada ou acidental;
- **Disponibilidade**: que as informações estejam disponíveis quando necessárias e que o sistema esteja em funcionamento contínuo;
- **Autenticidade**: que apenas pessoas autorizadas tenham acesso ao sistema e que a identidade dessas pessoas seja verificada;
- **Confiabilidade**: que o sistema seja confiável e que possa resistir a ciberataques e falhas.

Larsen e Lund [62], revisando a literatura que trata da percepção de riscos na perspectiva da Marinha dos EUA, definem a segurança cibernética como a proteção do espaço onde ela habita, das informações que transitam nesse espaço, daqueles que se utilizam desse espaço, das áreas da tecnologia da informação que suportam o espaço, assim como dos interesses (tangíveis ou não), que estão expostos aos ataques originados no ciberespaço.

Já Herath, Khanna e Ahmed [63], ao realizarem uma revisão sistemática sobre as práticas de usuários em mídias sociais, nos informam que a segurança cibernética trata-se de uma conjunto de técnicas voltadas à proteção dos ambientes cibernéticos, sejam de usuários individuais, sejam organizações.

Desolda et al. [64], revendo a literatura sobre os fatores humanos em ataques de phishing, posicionam a segurança cibernética como o encapsulamento de quaisquer assunto de segurança que se relaciona com a tecnologia da informação e comunicação. O conceito, segundo os autores, concentra-se em salvaguardas, políticas, diretrizes, gerenciamento de risco, ferramentas, boas práticas e tecnologias que focam na proteção do espaço cibernético, da organização e de ativos, devendo ser consideradas, também, práticas que impõem um comportamento online mais seguro.

A segurança cibernética é composta por cinco pilares da TI [65]: programação, rede, interações do ser humano com o computador, banco de dados e sistemas web. Os autores, ao realizarem uma revisão sistemática da literatura com foco em competências-chave em segurança cibernética voltada para infraestrutura crítica, apontam uma série de desafios a serem enfrentados na segurança cibernética, entre eles: infraestrutura envelhecida, a falta de padronização, a conectividade com a internet, processos industriais em tempo real, falta de conscientização de segurança dos atores humanos.

Ganin et al. [24] nos informam que a avaliação e gerenciamento de riscos de segurança cibernética é um problema complexo e desafiador, devido à natureza em constante mudança dos sistemas cibernéticos e à complexidade das abordagens existentes para avaliação de riscos cibernéticos.

Indivíduos, pequenas, médias e grandes organizações encontram-se no uso do espaço cibernético, e o nível de investimento em segurança para cada uma dessas categorias é bem distinto. Se para as grandes corporações já é bastante complexa a tomada de decisão por onde iniciar os investimentos, é de se supor que as pequenas e médias empresas têm um grau de dificuldade ainda maior.

Como pode ser observado, a própria definição sobre a segurança cibernética ainda é bastante difusa, mas há alguns elementos comuns:

- Atua em um espaço específico, conhecido como espaço cibernético ou ciberespaço;
- O espaço cibernético tem sido altamente utilizado pelas organizações para o alcance de seus objetivos estratégicos;
- O fator humano e a cultura de segurança cibernética têm grande relevância;
- A proteção das informações organizacionais faz parte do núcleo protetivo da segurança cibernética;
- Dados pessoais têm sido foco de atenção cada vez maior por parte dos Estados;
- A interconectividade faz com que todos os participantes estejam expostos aos fiscos cibernéticos;
- As ameaças e os resultados obtidos por meio do espaço cibernético têm aumentado significativamente nos últimos anos;
- Deve garantir a proteção contra intrusos que visam às informações e às redes;
- Envolve o Estado, as organizações e os indivíduos;
- Tem exigido novas abordagens do espaço cibernético, em especial quando se trata da resiliência organizacional, protegendo sua própria existência;

2.6 FRAMEWORKS DE MERCADO COM FOCO EM SEGURANÇA

A área de Tecnologia da Informação está repleta de normas que visam à boas práticas. Vários são os órgãos que contribuem na formulação de estruturas voltadas para o gerenciamento de riscos cibernéticos: ISO, NIST, *Central Computer and Telecommunications Agency* (CCTA) com a metodologia CRAMM, *Ministerio de Hacienda y Administraciones Publicas com a metodologia* (MAGERIT) , *Agence nationale de la sécurité des systèmes d'information* (ANSSI) com o método EBIOS .

A ideia central dessa seção é apresentar estudos que tratam de frameworks voltados para o gerenciamento de riscos cibernéticos. Como o modelo proposto pressupõe um conjunto de controles, é salutar que a escolha primária desses controles esteja alinhada com as melhores práticas do mercado.

Srinivas et al. [66, p. 179], analisando a importância dos padrões na defesa cibernética e na arquitetura da estrutura de segurança cibernética, apontam razões para o uso de abordagens voltadas para esse fim:

- Melhorar a eficiência e a eficácia dos principais processos.
- Facilitar a integração e interoperabilidade de sistemas.
- Intitular vários produtos ou métodos, que precisam ser comparados de forma significativa.
- Forneça um meio para os usuários avaliarem novos produtos/serviços.
- Estruturar o método para implantar novas tecnologias/modelos de negócios.
- Simplifique ambientes complexos.
- Promover o crescimento econômico.

Alguns estudos como os de Sulistyowati, Handayani e Suryanto [67], Bashofi e Salman [68], Roy [69] e [70] estabelecem uma comparação entre frameworks que tratam da segurança da informação e cibernética. A Tabela tabela 2.1 apresenta os frameworks tratados nas obras.

Tabela 2.1: Obras que comparam os Frameworks de Segurança

Frameworks	**Obras**				
	[67]	[69]	[71]	[70]	[68]
NIST CSF	✓	✓		✓	✓
ISO 27001		✓	✓		✓
ISO 27002	✓				
COBIT	✓				
PCI DSS	✓				
C2M2	✓				
NIST 800-53			✓		
ISO 27000 série				✓	
CIS Controls					✓

A partir desses estudos, fez-se uma pesquisa nos 102 artigos que contribuíram com a Revisão da Literatura e Trabalhos Correlatos, buscando-se identificar quais *frameworks* foram citados, sendo que em

49 foram encontradas referências às famílias de normas NIST e ISO 27000. A tabela 2.2 apresenta a distribuição dessas duas famílias.

Tabela 2.2: Distribuição de Artigos Relacionados às Normas

Normas citadas	**Qtde**
NIST - Família de Normas	37
ISO - Família de Normas	32
ISO 27001	19
ISO 27005	16
ISO 27002	10
NIST - *Cybersecurity Framework* (CSF)	10
NIST 800-30	10
COBIT	9
ISO 27000	8
NIST 800-53	8
NIST 800-37	3
NIST - *National Institute of Standards and Technology*	2
NIST *National Vulnerability Database*	2
NIST 800-55	2
ISO 27032	1
ISO 27102	1
ISO 27701	1
NIST - *Framework for Improving Critical Infrastructure Cybersecurity*	1
NIST - *Information Security Handbook*	1
NIST 800-100	1
NIST 800-53A	1
NIST 800-57	1
NISTIR 8286A	1

Embora seja inegável a contribuição e o uso das normas ISO em segurança da informação, fez-se a escolha pelo NIST CSF levando-se em consideração alguns pontos:

- Se trata de um ponto inicial, ou seja, outros controles podem ser inseridos no modelo proposto, sem prejuízo da proposta da pesquisa, corroborando com Roy [69] e Sulistyowati, Handayani e Suryanto [67], que apontam a relevância da combinação de estruturas e controles,
- O CSF tem foco em um dos temas do estudo, a segurança cibernética, conforme sugere seu próprio nome, *Cybersecurity Framework*
- O CSF traz uma série de referências baseadas em orientações que apareceram com maior frequência durante o seu processo de desenvolvimento, como: CIS CSC, COBIT, ISO/IEC 27001, ISA 62443-2-1, e NIST 800-53.

- É possível combinar o modelo proposto, que visa ao apetite ao risco, com abordagens voltadas à maturidade [70, 67, 72, 73, 59, 51],
- Mais estruturado, amigável e simplificado em especial para gerenciamento superior ou empresarial [69],
- Moreira [70] traz um estudo realizado em 2017 apontando que 52% das grandes organizações responderam que adotaram alguma parte do NIST CSF
- Tem sido atualizado, devendo receber uma nova versão, NIST CSF 2.0, ainda no ano de 2023 [2]

2.7 TOMADA DE DECISÃO - MÉTODOS MULTICRITÉRIO

Uma das tarefas mais relevantes e desafiadoras no campo da conformidade e segurança da informação se concentra na tomada de decisões pelas partes interessadas, devendo considerar múltiplos aspectos, lidando tanto com os problemas atuais, assim como no planejamento do futuro [26], buscando, com isso, um alinhamento com as expectativas organizacionais.

Para Maček et al. [27], os riscos de segurança da informação têm elevado as preocupações das empresas, sendo que a busca por meios mais eficientes na tomada de decisão no gerenciamento de riscos tem se tornado um objetivo cada vez mais presente.

A tomada de decisão, seja na vida profissional, seja na vida pessoal, implica buscar ajustar os riscos negativos para os resultados desejados e, sempre que possível, observando as oportunidades que possam trazer melhorias. Para Kaplan e Garrick [74] a decisão racional faz parte de um processo que requer uma forma clara e quantitativa em relação aos riscos, custos e benefícios. A conscientização é uma salvaguarda, reduzindo o risco: o fato de se saber que há um buraco ao virar a esquina, por si só, já diminui o risco, sendo, portanto, relativo àqueles que participam do processo de tomada de decisão.

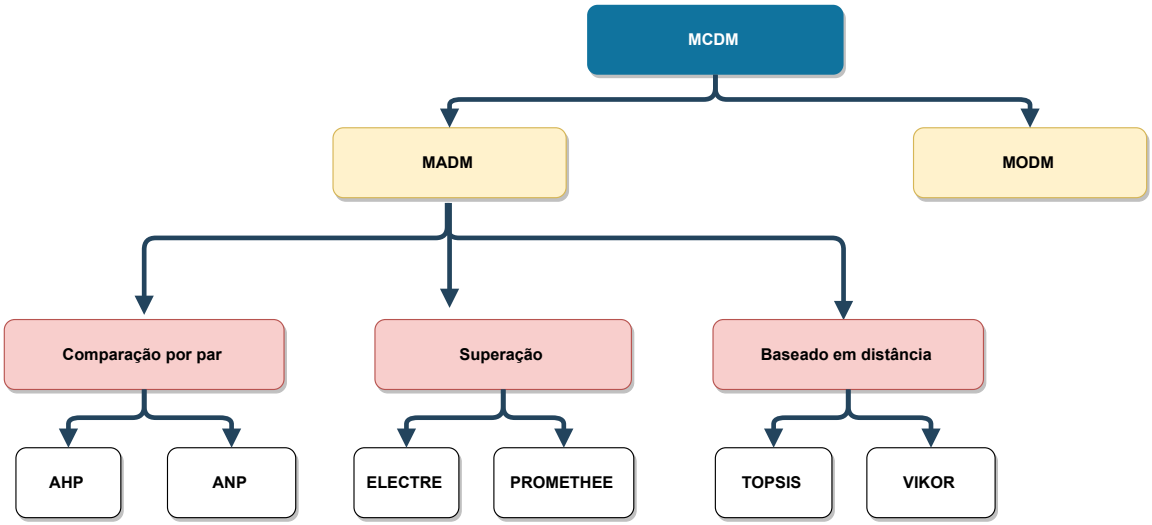
Duas questões se apresentam quando se fala de decisão: o que se entende por decisão e por que se estuda a decisão. Na primeira questão, tem-se como o processo que leva, o decisor, a escolha de pelo menos uma alternativa candidata a resolver determinado problema. Quanto à questão do porquê se estuda, por fazer parte do nosso dia a dia e pela importância dos resultados práticos de uma determinada forma de pensar. A decisão se faz necessária para a resolução de grandes problemas, podendo ser tomada de forma individual, ou por um grupo de indivíduos [75].

A fig. 2.5, adaptada de Azhar, Radzi1 e Ahmad [76], estrutura como os *Multi Criteria Decision Making* (MDCM) estão distribuídos, a partir de um estudo aprofundado de técnicas MCDM, cobrindo vários campos onde a técnica é utilizada, e o AHP encontra-se no espaço dedicado aos métodos que se utilizam de comparações de pares de critérios e alternativas.

Para Bhol, Mohanty e Pattnaik [61], os problemas de tomada de decisão de multicritérios podem auxiliar na construção de métricas, cujo o objetivo, no modelo que propuseram, "é fazer determinados negócios

[2]Disponível em: <https://csrc.nist.gov/publications/detail/white-paper/2023/04/24/discussion-draft-of-the-nist-csf-20-core/draft> acessado em 17/05/2023

Figura 2.5: Visão geral das abordagens MCDM



Fonte: Adaptada [76]

e minimizar os danos aos negócios, prevenindo ou diminuindo o impacto de incidentes cibernéticos", podendo ser "desenvolvida para medir a confiabilidade da segurança cibernética de uma empresa" [61, p. 665]

Mardani et al. [77], na revisão sistemática a respeito do uso de métodos multicritério para tomada de decisão, analisaram 393 artigos que foram publicados entre os anos 2000 e 2014, demonstrando o vigor desses métodos. A Tabela tabela 2.3 traz a classificação dos métodos analisados.

Tabela 2.3: Distribuição de artigos por método MCDM

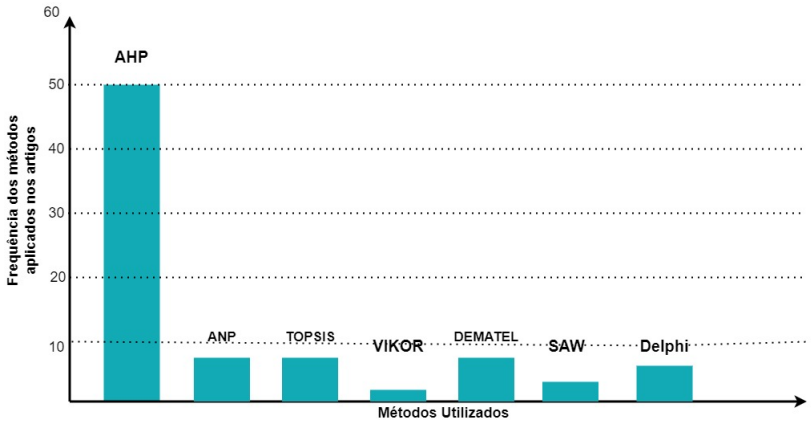
Classe	Método	Nr artigos	%
AHP	128	32,6%	
MCDM Híbrido	64	16,3%	
Métodos DM de agregação	46	11,7%	
TOPSIS	45	11,4%	
ELECTRE	34	8,7%	
ANP	29	7,4%	
PROMETHEE	26	6,6%	
VIKOR	14	3,6%	
DEMATEL	7	1,8%	
Total	**393**	**100,0%**	

Fonte: Adaptada [76]

Em outra revisão sistemática com foco no uso de métodos multicritérios na área de conhecimento de segurança da informação, Maček, Magdalenić e Ređep [78] trazem uma contribuição importante para nossa pesquisa, ao analisar 65 artigos publicados entre os anos de 2012 a 2018. A Figura 2.6 a apresenta como se deu a distribuição de artigos, e pode-se observar, novamente, uma certa preferência no uso do AHP.

Em estudo que demonstra que um plano de risco cibernético pode ser resolvido com o auxílio de métodos multicritério, Moreira et al. [79] nos informam que tais métodos auxiliam os tomadores de decisão

Figura 2.6: Distribuição de artigos usando métodos multicritério em segurança da informação



Fonte: Adaptada de [78]

na classificação, determinação e priorização de diferentes alternativas, apresentando vantagens quando há divergências entre partes interessadas, tornando o problema mais gerenciável, reduzindo a complexidade.

Em seu estudo, Torbacki [80] nos traz alguns pontos relevantes a respeito de métodos multicritérios, entre outros: são utilizados para avaliar, por parte dos especialistas, um conjunto de critérios, possibilitando a classificação de alternativas pelos seus graus de importância, podendo ser tanto quantitativos – esses são independentes de especialistas – como qualitativos, havendo uma grande quantidade de métodos. A possibilidade de se poder utilizar uma gama maior de especialistas é considerada uma fortaleza desses métodos, diminuindo os efeitos de vieses individuais. No que diz respeito à segurança cibernética, por sua complexidade, a tomada de decisão deve buscar métodos que envolvam diferentes especialistas, permitindo a transformação de problemas complexos em formas mais compreensíveis de interpretação.

Em sua revisão sistemática com foco em técnicas MCDM utilizadas para avaliar a qualidade de sites da internet, Rekik et al. [81] informam que as técnicas além de serem muito utilizadas na solução de problemas, seu uso vem crescendo em áreas como matemática, negócios, administração, medicina, ciências sociais e ambientais, economia, entre outras. Os autores destacam que as áreas de engenharia e da ciência da computação têm a parte mais importante no uso dessas técnicas, sendo usados por tomadores de decisão com problemas que apresentam múltiplos critérios conflitantes, sendo suportados por técnicas computacionais, como conjuntos fuzzy, redes neurais e algoritmos genéticos, buscando melhorar a precisão das decisões.

Ao buscar solucionar questões relativas à Lei Geral de Proteção de Dados Pessoais (LGPD), com foco na busca de critérios relacionados à privacidade, Ribeiro e Canedo [82] utilizaram-se da metodologia Multiple Criteria Decision Analysis (MCDA), outra denominação do MCDM, estabelecendo critérios a partir da compreensão do problema, a definição dos critérios e a aplicação do método, propriamente dito. Nível de proteção de dados, riscos de segurança, gravidade do incidente e riscos de privacidade de dados foram os critérios utilizados, sendo o derradeiro, após a aplicação do método, considerado o mais importante. A partir de uma relação por importância de critério, busca-se dar aos tomadores de decisão uma direção sobre as possíveis ações a serem tomadas, baseando-se nas prioridades.

Para Gamper e Turcanu [83], a análise de múltiplos critérios pode ser uma técnica valiosa no apoia-

mento às tomadas de decisões no setor público, em especial em relação a problemas complexos, destacando a necessidade de uma análise cuidadosa dos critérios de avaliação, bme como uma consideração cuidadosa dos resultados apresentados.

A norma ISO 31010:2012 [84, p. 94] traz um conjunto de técnicas voltadas para a gestão de riscos, dentre elas a "Análise de decisão por multicritérios (MCDA)", podendo ser usada para:

- comparar múltiplas opções para uma primeira análise para determinar opções preferenciais e potenciais e as inapropriadas,
- comparar opções onde existam critérios múltiplos e, algumas vezes, conflitantes,
- alcançar um consenso sobre uma decisão onde diferentes partes interessadas têm objetivos ou valores conflitantes.

A análise multicritério tem se demonstrado útil em trabalhos voltados à gestão de riscos cibernéticos, possibilitando a priorização dos riscos em pequenas empresas [85], cadeia de riscos de suprimentos [86], no monitoramento de sistemas de energia [87], na detecção de intrusão [88], em requisitos de segurança [89], em requisitos de qualidade de software [90], nos requisitos de segurança da Indústria 4.0 [80], entre muitos outros exemplos, demonstrando o seu vigor e a sua aplicação prática na tomada de decisão.

Método AHP

Com o avançar da pesquisa, verificou-se que o maior uso entre os estudos voltados para a ciência da computação associado às questões de facilidade, optou-se, para a pesquisa, o uso do AHP quando da seleção de critérios e alternativas que farão parte do modelo proposto.

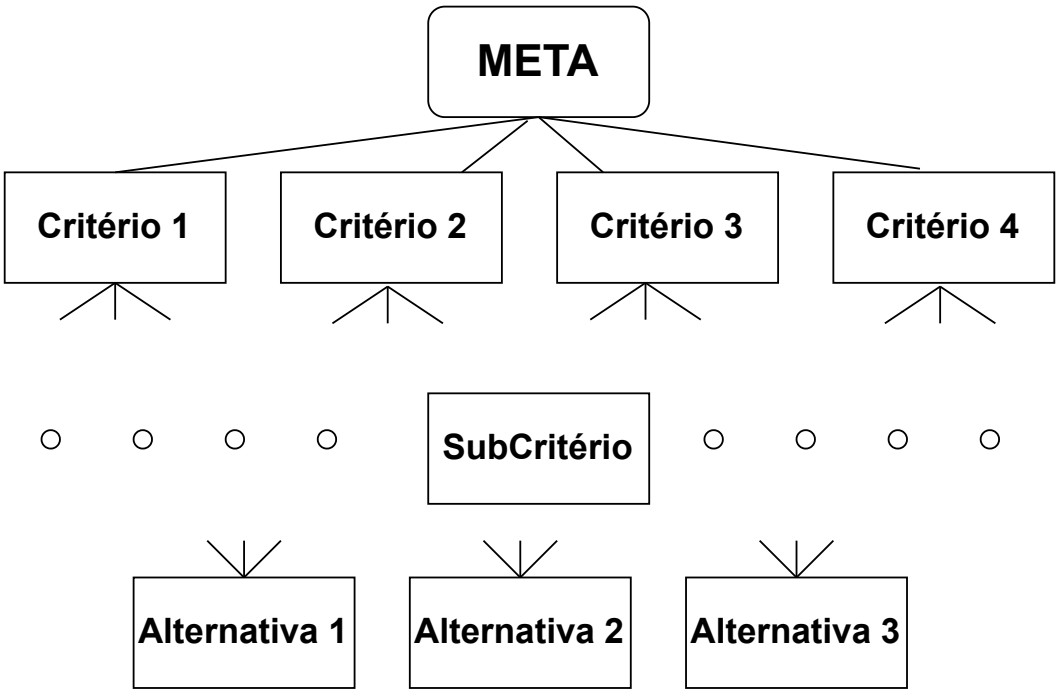
Saaty propôs o modelo em 1980 [91], objetivando auxiliar os tomadores de decisão para alcançar seus objetivos, devendo respeitar as premissas: o problema e as metas devidamente definidos, vários critérios e alternativas devem estar presentes, devendo ser distribuídos hierarquicamente, a exemplo da fig. 2.7. Além disso, os tomadores de decisão deverão realizar um exercício comparativo entre critérios e alternativas, utilizando-se de uma escala de pontuação, conhecida como Escala Saaty: (1) igualmente significativo, (3) ligeiramente significativo, (5) mais significativo, (7) altamente significativo, e, (9) significativamente muito alto, sendo possível utilizar-se 2,4,6 e 8, compreendidos entre os números 1,3,5,7 e 9 [76].

O AHP é uma ferramenta que permite tratar problemas complexos de forma eficaz, estabelecendo prioridades e auxiliando na tomada de decisão, sendo viável tanto o uso de critérios qualitativos e quantitativos, tendo como saída, após sua aplicação, uma lista priorizada de alternativas [61].

Uma das muitas vantagens do método AHP é a sua facilidade de uso, por meio de comparações de pares, possibilitando que os tomadores de decisão as alternativas de forma simples, sendo escalável, o que viabiliza o ajuste ao tamanho do problema, tendo uma desvantagem que é a impossibilidade de comparar pontos fortes e fracos entre alternativas [92].

Para Lakhani et al. [93], o uso do método pelo AHP traz vantagens em circunstâncias onde o estabelecimento de pesos relativos de alternativas é difícil, e envolve as etapas de identificação de critérios e

Figura 2.7: Visão geral da estrutura hierárquica AHP



Fonte: Adaptada de [76, 73]

alternativas, as comparações pareadas, a verificação da consistência das comparações pareadas, e, por fim, a formulação dos pesos de cada alternativa e critério.

A escolha dos critérios e alternativas é um ponto importantíssimo na tomada da decisão, estruturando os elementos em grupos que tenham influências semelhantes, organizados racionalmente. O processo prevê as etapas: (1) estruturação do problema de forma hierárquica; (2) julgamentos que reflitam tanto ideias, como sentimentos; (3) devendo ser traduzidos em números; (4) que devem ser utilizados para estabelecer prioridades; (5) alcance um resultado geral, e, por fim (6) analise a sensibilidade às mudanças de determinados julgamentos [94].

Saaty [94] estabelece um conjunto de passos a serem seguidos, que permitem fazer uma decisão organizada para gerar prioridades:

1. Definir o problema
2. Estruturar a hierarquia de decisão
   (a) Topo – Objetivo a ser alcançado
   (b) Critérios,
   (c) Subcritérios (se houver),
   (d) Alternativas – último nível
3. Construir conjunto de matrizes par a par voltados para critérios e subcritérios.
4. Continuar o processo de ponderação até o nível mais baixo

Tabela 2.4: Escala Fundamental de Saaty

Intensidade	Definição	Explanação
1	Importância igual	Dois fatores contribuem igualmente para o objetivo
3	Um pouco mais importante	A experiência e o julgamento favorecem ligeiramente um em detrimento do outro.
5	Importância essencial ou forte	A experiência e o julgamento favorecem fortemente um sobre o outro.
7	Muito mais importante	A experiência e o julgamento favorecem fortemente um sobre o outro. Sua importância é demonstrada na prática.
9	Absolutamente mais importante	A evidência que favorece um sobre o outro é da maior validade possível.
2,4,6,8	Valores intermediários	Quando se procura uma condição intermediária

Fonte: Adaptada de Saaty [91]

A comparação por pares é feita utilizando-se da escala fundamental Saaty, disposta na tabela 2.4.

Para o propósito desse estudo, o AHP foi utilizado para possibilitar a classificação da importância dos critérios e alternativas relacionados ao apetite a risco corporativo em segurança cibernética, segundo a visão de especialistas.

3 TRABALHOS RELACIONADOS

Quando você pode medir o que está falando e expressar em números, você sabe algo sobre isso; mas quando você não pode expressá-lo em números, seu conhecimento é escasso e insatisfatório; pode ser o começo do conhecimento, mas você dificilmente avançou em seus pensamentos para o estado da ciência.
Lord Kelvin, 1824-1907
Em meus seminários, muitas vezes peço ao público para me desafiar com medições difíceis ou aparentemente impossíveis. Em um caso, um participante ofereceu "mentoria"como algo difícil de medir. Eu disse: "Isso soa como algo que alguém gostaria de medir. Eu poderia dizer que mais mentoria é melhor do que menos mentoria. Posso ver pessoas investindo em maneiras de melhorá-lo, então posso entender por que alguém pode querer medi-lo. Então, o que você quer dizer com 'mentoria'?"A pessoa respondeu quase imediatamente, "Eu acho que não sei", ao que eu disse, "Bem, então talvez seja por isso que você acredita que é difícil de medir. Você não descobriu o que é."
Hubbard [95, p. 26]

Este Capítulo dedica-se à aproximação com o estado da arte da investigação científica que trata dos principais temas da pesquisa: gestão de riscos cibernéticos, o uso de métodos multicritérios para a tomada de decisão por parte dos gestores, o apetite a risco, indicadores de riscos cibernéticos, visão holística do risco cibernético, aspectos humanos relacionados ao risco cibernético.

A partir do problema apresentado para a pesquisa, seção 1.1, buscou-se identificar a literatura que tratasse do uso de métodos multicritérios para o apoio à tomada de decisão e que desse suporte ao uso de um indicador que traduzisse as declarações de apetite a risco cibernético em um índice de apetite a risco. Até o momento da escrita desta dissertação não foram encontrados artigos que trouxessem uma abordagem que buscasse traduzir o apetite a risco cibernético, mesmo fora da área de conhecimento de métodos multicritério. Para esse intento, utilizou-se de bases de dados disponibilizadas pelo Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) [1], por meio da Comunidade Acadêmica Federada (CAFe) [2], destacando-se as bases da Scopus, *Web of Science*, IEEE Xplore, assim como a base de dados do Google Scholar [3].

Após a busca inicial, fez-se pesquisas em bases de dados buscando obter artigos que tratassem de temas

[1] Acessível em <https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php/sobre/quem-somos.html>, acessado em 20/04/2023

[2] Acessível em <https://www-periodicos-capes-gov-br.ez54.periodicos.capes.gov.br/index.php/acesso-cafe.html>, utilizando-se as credenciais de aluno da Universidade de Brasília (UnB), acessado em 20/04/2023

[3] Acessível em <https://scholar.google.com/>, acessado em 20/03/2023

como: o uso de métodos multicritério em segurança da informação, em segurança cibernética, em aspectos humanos voltados para a segurança cibernética, em escolha de frameworks de segurança cibernética, em escolha de ferramentas voltadas para apoiar a segurança cibernética e segurança da informação. Tais estudos contribuíram para a formulação dos critérios e alternativas do modelo proposto, como poderá ser observado no capítulo 5. A literatura pesquisada que trata dos objetivos secundários da pesquisa item 1 e item 3 foram tratadas no capítulo 5, na seção 5.7 e na seção 5.1.

3.1 MEDIÇÃO DO APETITE A RISCO EM SEGURANÇA CIBERNÉTICA

Salienta-se que não foram encontrados artigos que focassem na medição do apetite a risco de forma quantitativa em segurança cibernética. Esse fato fez com que a pesquisa se extendesse a temas correlacionados, buscando-se evitar que o estudo não alcançasse profundidade nos temas tratados.

3.2 TOMADA DE DECISÃO

Os estudos que contribuíram para o modelo proposto foram tratados na seção 5.1, um dos objetivos gerais dessa pesquisa. Optou-se, desta feita, dispô-los como resultado alcançado.

3.3 REVISÕES SISTEMÁTICAS COM MÉTODOS MULTICRITÉRIOS EM SEGURANÇA CIBERNÉTICA

Inicialmente fez-se uma pesquisa com o intuito de obter revisões sistemáticas que abordassem segurança cibernética e métodos multicritério voltados à decisão, e, até o momento da defesa dessa dissertação, não foram encontrados artigos. A ideia era utilizar-se desses estudos que compilam o estado da arte nessas áreas de conhecimento, buscando respostas dos métodos mais utilizados nesse campo da ciência.

3.4 REVISÕES SISTEMÁTICAS COM MÉTODOS MULTICRITÉRIOS EM SEGURANÇA DA INFORMAÇÃO

Após a não identificação de revisões sistemáticas com foco no uso de métodos multicritérios em segurança cibernética, repetiu-se a pesquisa focando em segurança da informação, e dois trabalhos foram avaliados.

No primeiro deles, **Mačekˇ, Magdalenić e Ređep [78]** classificam as técnicas MCDM em quatro categorias: métodos de utilidade de múltiplos atributos (MAUT), onde encontram-se o AHP e o ANP, métodos de superação, onde encontram-se ELECTRE, PROMETHEE e QUALIFLEX, métodos de compromisso, tendo como representantes TOPSIS e VIKOR, e, por fim, outros métodos, exemplificados por SMART,

DEMATEL e SAW. Dentre os métodos MAUT, o AHP é o mais difundido, utilizando-se de uma hierarquia na decomposição do problema, tendo o objetivo a ser alcançado no topo do modelo, seguido pelos critérios (podendo ser seguidos por subcritérios), deixando, no nível inferior, as alternativas. A revisão sistemática envolveu um conjunto de 140 artigos, publicados entre os anos de 2012 a 2018, demonstrando o vigor do modelo nessa área temática, sendo o AHP o mais utilizado para a análise de risco de segurança de TI. Nesse artigo, entretanto, não ficou evidenciado o uso do método multicritério com foco em propor um índice de risco organizacional relacionado.

No segundo artigo que mereceu destaque, **Moreira et al. [79]** elaboraram um estudo com o objetivo de demonstrar que o uso de métodos multicritério pode auxiliar a construção de um plano de risco cibernético. Os autores utilizaram o Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica [55]. Os autores se utilizaram de um método construtivista com foco na tomada de decisão na gestão de riscos cibernéticos em um grande banco brasileiro. O Framework proposto pelo NIST, o *Cyber Security Framework* (CSF), que é composto por 5 Funções, que são divididas em Categorias. No modelo proposto, utilizaram-se da Função Detectar (a terceira do Framework), para verificar quais das três categorias (Anomalias e Incidentes, Monitoramento Contínuo de Segurança, e Processos de Detecção) encontravam-se os principais controles a serem implementados. A pesquisa levou à priorização dos controles relacionados ao Monitoramento Contínuo, sendo aquele que recebeu o maior índice de prioridade. Esse estudo trouxe informações relevantes para o uso do CSF.

3.5 MEDIÇÃO DE RISCO

A pesquisa realizada possibilitou a aproximação de estudos que buscaram a elaboração de índices para a medição dos riscos cibernéticos, destacando-se [11, 12, 15, 19, 59, 60, 96, 97, 98, 99, 100, 101, 102]. Os estudos apresentados não se limitam à medição do risco cibernético, incluindo propostas de outras indústrias, mesmo assim compreende-se que se trata de uma abordagem pouco explorada, com poucos estudos que visam à medição dos riscos, seja de forma financeira, seja de forma a apontar a probabilidade de que ocorram.

Em obra reeditada em abril de 2023, ***How to Measure Anything in Cybersecurity Risk***, **Douglas W. Hubbard e Richard Seiersen [102]** partem do princípio, baseado em artigos publicados por diversos autores, que a matriz de risco tão utilizada se trata de um placebo, e que apesar de aumentar a confiança na tomada de decisões, acaba por prejudicar a qualidade dessas tomadas de decisões. Dentre os pontos que ressaltam o aumento dos riscos sistêmicos relacionados à cibernética, os autores apresentam "pontos fracos potenciais em software amplamente utilizado; acesso de rede interdependente entre empresas, fornecedores e clientes; e a possibilidade de grandes ataques coordenados" **[102, p. 8]**.

Gai e Vause [96], embora não abordem o apetite a risco de uma organização, têm o mérito de propor um índice de apetite a risco do investidor, com foco financeiro, sendo baseado na comparação de probabilidades de retorno com as probabilidades subjetivas correspondentes, e, segundo os autores, a abordagem traz como vantagem a distinção entre o apetite a risco e a aversão a risco.

Já **Belles-Sampera, Guillén e Santolino [15]** compreendem que há uma dicotomia entre o alcance

dos objetivos organizacionais e o controle de riscos, e propuseram uma família de medidas de riscos, que foi denominada GlueVaR, sendo a sua aplicação voltada para múltiplos problemas, abrangendo a saúde, segurança, meio ambiente e riscos catastróficos, incluindo o terrorismo. Os autores estabeleceram a correlação do novo índice com os comumente utilizados em aplicações financeiras e de seguros: *value-at-risk* (VaR) e *tail value-at-risk* (TVaR). Para os autores, o GlueVaR supera as vantagens do VaR e o conservadorismo do TVaR, por ser mais flexível e simples, acomodando um maior número de elementos que compõem a tomada de decisão, permitindo a introdução de informações qualitativas, possibilitando o estabelecimento de dois níveis de tolerância: casos ruins e casos muito ruins. Para os autores, os resultados apresentados são aplicáveis ao setor financeiro, existindo potencial para a aplicação em outrás áreas além da financeira.

Ainda nessa linha de pesquisa, **Ruan [98]** propôs um estudo visando à utilização de métodos já existentes (MicroMort - MM e VaR) voltados à medição de riscos encontrados nas áreas de medicina e finanças. O autor compreende que seu estudo seria o primeiro a propor índices para medir o risco cibernético: o BitMort (BM) e o hekla. O autor utiliza-se da teoria econômica do valor para a avaliação dos ativos digitais, definidos como aqueles que poderão gerar prejuízo econômico à sua proprietária quando comprometidos, (ii) estabelece uma relação entre os fatores de risco médico à modelagem holística relacionada ao risco cibernético (identificando os principais fatores de risco cibernético - Key Cyber Risk Factors - KCFR, semelhantemente como se faz na medicina com os fatores de risco modificáveis e fatores de risco não modificáveis), e, por fim, (iii) realiza a avaliação do controle e a quantificação da perda por meio de uma análise de cenário. O artigo traz alguns resultados, onde se destacam: o *framework Cybernomic*s, unidades de medida para o risco cibernético, e exemplos de cálculo de risco cibernético em diferentes categorias de ativos digitais. **Ruan [98]** conclui que a gestão de riscos cibernéticos é um desafio crítico para as empresas e organizações em todo o mundo, e que a abordagem atual para medir e gerenciar riscos cibernéticos é insuficiente e fragmentada, destacando a importância da integração da gestão de riscos cibernéticos com a economia e a Gestão de Riscos Corporativos, e conclui que a implementação do *framework Cybernomics* requer uma mudança cultural e organizacional significativa nas empresas.

Com os objetivos de identificar as características de perdas relacionadas à cibernética e propor um modelo para a medição do VaR para setores financeiros e não financeiros, **Kim e Song [103]** utilizam-se da abordagem de distribuição de perdas (*loss distribution approach* LDA), do modelo de série temporal, do modelo *Generalized Autoregressive Conditional Heteroskedasticity* (GARCH) e do método *Peaks over threshold* (POT). O artigo acaba por detalhar cada um dos métodos utilizados. Para avaliar as perdas cibernéticas, as análises foram divididas em dois setores(financeiros e não financeiros), sendo que as maiores perdas ficaram associadas ao primeiro grupo.

Ainda na busca de um índice com foco em perdas econômicas, **Moro [19]** elaborou um estudo utilizando-se de dados oriundos de clientes da Symantec de diversos países, abrangendo cerca de 127 mil registros (vírus bloqueados pelo Norton) entre julho de 2016 e dezembro de 2018, e cerca de 128 mil registros gerados pelo sistema de prevenção contra intrusões (*intrusion prevention system* - IPS). **Moro [19]** discute a criação de um índice econômico de perda cibernética baseado em indicadores de segurança de TI, buscando com que as empresas de resseguros aumentem sua apetite por riscos cibernéticos. Para o autor, modelos transparentes e robustos de segurança de TI, com indicadores, parâmetros e métricas bem definidos possibilitarão a criação de apólices de seguros por parte das empresas inseridas nesse setor da economia. O

estudo buscou correlacionar os dados da Symantec com a perda de dados real objetivando estabelecer um índice de perda por meio desses dados, demonstrando que a existência de atividades de pico poderiam ser a base para um índice voltado a medir a perda de dados.

A ausência de dados foi apontado como um fator limitante da aplicação do índice proposto. Nessa linha de estudo, **Zängerle e Schiereck [99]** utilizaram-se de dados históricos para a quantificação do impacto financeiro dos incidentes cibernéticos, examinando os dados de riscos operacionais (banco de dados *Öffentliche Schadenfälle OpRisk* - ÖffSchOR, com eventos de perda divulgados publicamente no setor financeiro europeu), para modelar e prever a probabilidade, assim como a gravidade e a dependência em relação ao tempo de exposição. Os autores se utilizaram de técnicas avançadas de modelagem, sugeridas por outros autores (Shi e Yang - 2018, Eling e Wirfs - 2019 e Fang - 2021), com o objetivo de prever a probabilidade e a exposição a perdas a partir de um incidente cibernético. Entre as conclusões, destacam-se: os riscos cibernéticos diferem dos riscos operacionais, em geral são "em média, menores, menos distorcidos e menos extremos em comparação com os riscos não cibernéticos no conjunto de dados" **[99, p. 21]**, e os resultados forneceram insights quantitativos apontando os impactos financeiros a partir de incidentes cibernéticos por meio de dados históricos. Apesar da importância dos dados históricos, os autores acreditam que devido a dinâmica dos riscos cibernéticos, é provável que tais dados deverão se tornar inúteis com o decorrer do tempo, necessitando o uso de novas bases mais recentes.

Visando superar a ausência de dados disponíveis para a medição de riscos, como apontado em [19], assim como a qualidade dos dados, apontado por **Zängerle e Schiereck [99]**, **Facchinetti, Giudici e Osmetti [60]** propuseram uma metodologia para medir riscos cibernéticos por meio do emprego de dados ordinais coletados em nível mundial. Para os autores, a literatura que trata da medição quantitativa de riscos operacionais com base em dados de perda é bastante vasta, porém quando se trata de riscos cibernéticos há uma limitação, apresentando três artigos que tratam o assunto de forma teórica, e outro que aborda o problema de falta de dados na abordagem de risco cibernético. Com foco em fornecer uma medida de risco cibernético, possibilitando aos tomadores de decisão a priorização das intervenções, foram utilizados medidas propostas em outros setores (acadêmico, qualidade de processo e produto, entre outros).

Em outra linha de estudo, visando à análise da eficácia da auditoria interna de segurança cibernética, **Slapničar et al. [100]** propuseram a criação e uso do Índice de Auditoria de Segurança Cibernética, aplicando o índice em uma pesquisa que contou com um total de 183 pessoas, tanto auditores como executivos de vários países e setores. O objetivo principal do estudo é avaliar a eficácia da auditoria de segurança cibernética (*Cybersecurity Audit* - CSA) na gestão de riscos. Entre outras conclusões do trabalho, destacam-se que (i) a média alcançada no índice foi considerada alta (58 em uma escala de 1 a 100), havendo uma grande variação entre setores, (ii) das três fases da auditoria (planejar, executar e relatar), as duas primeiras estão fortemente correlacionadas, não acontecendo o mesmo com a de relatar.

Por fim, **Pour et al. [101]** elaboraram uma revisão abrangente de artigos que trataram de aspectos de medição de riscos cibernéticos, avaliando trabalhos as abordagens de medição voltadas à segurança cibernética. Compreendem que a avaliação dos elementos que cercam a internet é desafiadora, apresentando número como quase uma centena de milhar de redes autônomas únicas, 5,3 bilhões de usuários (dois terços da população global), com cerca de três vezes a população mundial de dispositivos conectados à internet, e cerca de 15 bilhões de conexões *Machine-to-Machine* (M2M). As aplicações de medição da internet, se-

gundo os autores, podem ser classificas em três grupos: **(i)** as que estudam os protocolos e serviços usados (*Hyper Text Transfer Protocol* - HTTP, *Transport Layer Security* - TLS, *Transmission Control Protocol* - TCP, *Domain Name System* - DNS, *Name System Security Extensions* - DNSSEC, *Remote Desktop Protocol* - RDP, *Virtual Private Networks* - VPN, **(ii)** as que investigam a segurança do ciberespaço (incluindo *Denial of Service* - DoS, *Distributed* DoS - DDoS, *botnets*, *ransomware*, *cryptojacking*, e *phishing*), e, **(iii)** medição para eventos do mundo real com avaliação dos impactos de um sobre o outro (impacto de eventos sociais, políticos e naturais no ecossistema da internet). O estudo utilizou-se de 337 artigos voltados para suas conclusões. Algumas conclusões dos autores a respeito dos resultados da revisão abrangente: **(a)** é necessário medir o sucesso das iniciativas de redução de riscos como das defesas implantadas, **(b)** as abordagens acabam por terem difíceis acessos aos dados, requerendo abordagens individualizadas para obterem precisão, **(c)** compreendem que se trata do primeiro estudo que visou à integração abrangente dessa literatura, e, **(d)** apresentaram uma taxonomia de medição da internet relacionados à segurança cibernética que poderá se tornar em uma ferramenta útil para novos estudos. Sugerem, por fim, uma coleta e análise de dados empíricos em larga escala, que poderia gerar *insights* confiáveis e mais abrangentes, sendo úteis para o enfrentamento dos desafios trazidos pela cibernética.

Conclui-se, a partir das leituras desses artigos, que os desafios relacionados às medidas que apoiam à tomada de decisão em riscos cibernéticos ainda estão muito aquém de uma reposta definitiva. São inegáveis os ganhos alcançados, mas em virtude da complexidade do tema, soma-se ao coro dos estudiosos que apontam um caminho longo e desafiador, em especial pela introdução massiva de novidades nesse setor. Boa parte dos indicadores visaram à medição de perdas econômicas, mesmo assim sem uma resposta razoável.

3.6 PARTES INTERESSADAS E ASPECTOS HUMANOS

As organizações estão cada vez mais focadas na sustentabilidade, tomando medidas que visam à governança interna, identificando as necessidades das partes interessadas como parte da tomada de decisão, buscando objetivos, estratégia e desempenho sejam medidos, avaliados e geridos, com uma preocupação na divulgação de informações baseando-se em suas decisões [104].

Quando observada no olhar do Estado, a gestão das partes interessadas deve buscar o alinhamento de todo o governo, coordenando um planejamento que envolva tanto o setor público quanto o privado, estabelecendo parcerias com as partes interessadas, por meio de estratégias que promovam o engajamento destas [105].

O envolvimento das partes interessadas, na busca de uma segurança cibernética eficaz, deve buscar uma série de resultados por meio de formulação e implementação de políticas, procurando o aumento da conscientização, minimizando as ineficiências dessa implementação [1].

No setor manufatureiro, a desejada sustentabilidade tem sido impactada negativamente com os avanços da tecnologia, em virtude do aumento de preocupações dos conselhos de administração em relação à segurança cibernética, devendo ser necessário o desenvolvimento de princípios de segurança cibernética, tornando-se força motriz na fabricação sustentável [80].

Para **Sharkov [106]**, os objetivos em segurança cibernética devem buscar uma abordagem multissetorial, de forma inclusiva e ativa de todas as partes interessadas, com colaboração de empresas, universidades e órgãos não governamentais, definindo, de forma clara, os papeis mais relevantes em relação a ativos, sistemas, processos de negócio, entre outros.

O trabalho de **Gordon et al. [107]** de 2019, foca na suscetibilidade dos funcionários de saúde dos EUA em relação aos ataques de phishing, o que pode significar um grande risco de segurança cibernética nesse setor. O estudo levou em consideração seis instituições que realizaram simulações de phishing entre os anos de 2011 e 2018, com cerca de 2,9 milhões de e-mails, alcançando a incrível marca média de 16,7 % de cliques por parte dos usuários. Os autores apresentam três estratégias que se demonstraram eficazes no combate aos ataques de phishing: impedir que os e-mails de phishing sejam recebidos, uso de senhas com autenticação multifator, e, a terceira, campanhas de conscientização e treinamento dos funcionários.

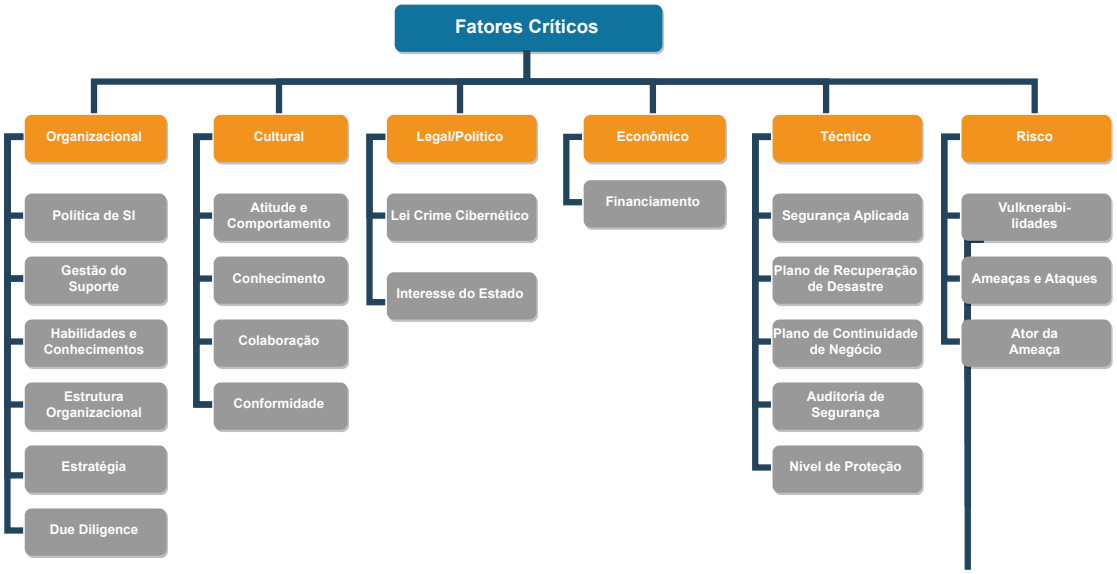
Jeong et al. [108] realizaram uma visão sistemática da literatura com o objetivo de examinar a natureza complexa e subjetiva dos fatores humanos relacionados à segurança cibernética. Os autores sugerem que a segurança cibernética deve ser examinada com uma abordagem multidisciplinar, levando-se em consideração fatores como personalidade, atributos demográficos e o contexto cultural, como principais fatores humanos identificados no estudo. **Jeong et al. [108]** concluem que há um foco predominantemente técnico nos trabalhos, ao avaliarem artigos que propunham perspectivas técnicas, comportamentais e ciências sociais em segurança cibernética, excluindo os fatores humanos, devendo-se à falta de atributos consolidados em relação aos seres humanos.

Na pesquisa realizada por **Kessler et al. [109]**, os autores utilizaram-se do índice de clima organizacional, já consagrado na literatura, e propuseram o *Information Security Climate Index* (ISCI), analisando o comportamento de quatro categorias de profissionais de saúde: auxiliares de enfermagem certificados, dentistas, farmacêuticos e médicos assistentes. Entre os resultados, o índice estava relacionado à motivação de segurança da informação e a comportamentos relacionados a esse tema. O estudo traz elementos importantes sobre as dificuldades entre alta gestão em implantar políticas e procedimentos com foco em segurança da informação, pois a implementação dessas políticas se dá em níveis mais baixos, nem sempre de forma enfática por parte dos supervisores, impactando nos resultados esperados, e, consequentemente, na privacidade e segurança das informações.

AL-Nuaimi [110] elaborou uma revisão sistemática da literatura que explora os fatores humanos e contextuais que influenciam o comportamento de cibersegurança nas organizações, com foco especial em instituições de ensino superior, destacando a importância de uma cultura organizacional forte de cibersegurança para o desenvolvimento sustentável da educação e treinamento em cibersegurança, sendo sua que revisão apresenta uma abordagem abrangente e inovadora, pois a maioria dos estudos anteriores tem investigado apenas fatores relacionados aos ativos de informações, indicadores de chave de desempenho, as ameaças mais comuns, vulnerabilidades, além dos agentes de ameaças à segurança cibernética. O autor revelou, por meio do estudo, que vários temas centrais, incluindo fatores humanos e culturais que afetam a cibersegurança nas organizações, como a conscientização e treinamento em cibersegurança, a percepção de riscos, a motivação e a cultura organizacional. **AL-Nuaimi [110]** destaca a necessidade de estudos futuros que envolvam o design experimental para testar a eficácia dos programas de treinamento em segurança da informação, bem como a classificação de riscos, ameaças e vulnerabilidades de cibersegurança em di-

ferentes domínios de infraestrutura de TI em, concluindo que a cibersegurança é uma questão complexa e multifacetada que envolve fatores humanos e tecnológicos, ressaltando que uma cultura organizacional forte de cibersegurança é essencial para proteger as organizações e seus ativos de TI contra ameaças cibernéticas.

Figura 3.1: Fatores relacionados à estratégia de segurança cibernética



Fonte: Adaptada de [28]

O estudo de **Aman e Shukaili [28]** se propõe a elencar uma lista estruturada de fatores-chave de da estratégia de segurança cibernética (*Cyber Security Strategy* - CSS) no setor público, com foco no negócio e missões críticas, destacando-se os organizacionais, culturais, econômicos, jurídicos e políticos e os de segurança. Para os **Aman e Shukaili [28]** apresentam uma classificação de fatores essenciais para o desenvolvimento e implementação de uma estratégia de segurança cibernética (CSS) em organizações do setor público , destacando a importância de avaliar fatores tecnológicos, culturais, regulatórios, econômicos e outros que podem limitar a eficácia da estratégia. O artigo propõe uma lista completa de fatores que deve ser considerada em qualquer programa de segurança cibernética, e destaca a importância de avaliar e abordar fatores organizacionais, culturais, legais, políticos e econômicos. Os autores apontam uma lista de fatores críticos em um programa de segurança cibernética: conscientização e treinamento, política de segurança, orçamento, auditoria de segurança, responsabilidade de segurança, estrutura organizacional, gerenciamento de mudanças e comunicação e colaboração, sistemas, habilidades, pessoal, estratégia, estilo de liderança e valores compartilhados. Aman e Shukaili [28] destacam a falta de estudos holísticos sobre os fatores críticos que afetam uma CSS e a necessidade de realizar mais pesquisas para aprimorar a compreensão desses fatores. Os fatores foram divididos em seis grandes grupos: (i) organizacionais, (ii) culturais, (iii) legais e políticos, (iv) econômicos, (v) técnicos e (vi) de risco. Este estudo foi muito relevante para a nossa pesquisa, trazendo uma estruturação básica interessante na formulção dos critérios voltados ao apetite a risco cibernético. **Aman e Shukaili [28]** concluem que uma estratégia de segurança cibernética eficaz envolve não apenas controles de segurança baseados em tecnologia, mas também a conscientização e participação de todas as pessoas em todos os níveis da organização. Para os autores, é necessário avaliar e abordar fatores críticos, incluindo fatores tecnológicos, culturais, regulatórios, econômicos e outros, e

envolver todas as pessoas em todos os níveis da organização na segurança cibernética , destacando (i) a importância de uma abordagem holística e integrada para a segurança cibernética, que inclui tanto controles técnicos quanto comportamentais, e a necessidade de uma cultura de segurança cibernética nas organizações do setor público, , (ii) a falta de estudos holísticos sobre os fatores críticos que afetam uma CSS e a necessidade de pesquisas adicionais para aprimorar a compreensão desses fatores e (iii) que a segurança cibernética é uma responsabilidade compartilhada entre organizações do setor público e do setor privado e que é necessário estabelecer parcerias para compartilhar informações e recursos de segurança cibernética.

3.7 APETITE A RISCO, SEGURO E RESSEGURO

Para os fins desse trabalho, alguns estudos foram relevantes na busca de maior proximidade com os aspectos que tratam do apetite a risco na tomada de decisão.

Eling e Schnell [111] apresentam uma visão geral dos principais tópicos de pesquisa nas áreas de risco cibernético e seguro contra riscos cibernéticos, realizando uma revisão da literatura usando um processo padronizado de pesquisa e identificação e criam um banco de dados com 209 artigos. Os autores discutem várias maneiras de superar as limitações de segurabilidade, como requisitos de relatórios obrigatórios, agrupamento de dados ou parcerias público-privadas em que o governo cobre partes do risco. A principais descobertas são extraídas e organizadas em sete grupos: **(i)** definição e categorização dos riscos cibernéticos, **(ii)** custos e efeitos prejudiciais causados pelo risco cibernético, **(iii)** obtenção de dados sobre o risco cibernético, **(iv)** modelagem do risco cibernético, **(v)** organização do gerenciamento do risco cibernético, **(vi)** se o risco cibernético é uma ameaça à economia e à sociedade globais e **(vii)** os desafios da segurabilidade do risco cibernético. **Eling e Schnell [111]** concluem que apesar de sua crescente relevância para as empresas, as pesquisas sobre o risco cibernético são limitadas, apontando as direções futuras de pesquisa, tanto do ponto de vista acadêmico como prático, além de discutirem os desafios de segurar riscos cibernéticos, incluindo a falta de dados, a falta de abordagens de modelagem, o risco de mudança e os riscos incalculáveis de acumulação.

O trabalho proposto por **Feng e Wang [112]** aborda a questão de como o apetite de risco do *Chief Information Officer* (CIO) está associado a incidentes de violação de segurança da informação, buscando explorar a relação entre o apetite de risco do CIO e do CEO da empresa e como isso pode criar sinergias para alcançar objetivos de negócios. Os resultados indicam que CIOs com maior aversão ao risco têm maior probabilidade de adotar uma abordagem conservadora que favorece o *status quo*, o que pode deixar inadvertidamente sua empresa vulnerável a violações de segurança. O estudo mostra que o nível de aversão do CIO ao risco está negativamente associado à probabilidade de incidentes de violação de segurança, apresentando que a associação é mais forte se o CEO da empresa também for avesso ao risco. **Feng e Wang [112]** também sugere que o apetite de risco do CIO deve estar alinhado com os objetivos estratégicos da empresa para alcançar uma gestão eficaz de riscos de TI.

Em um cenário de crescente ameaça de ataques cibernéticos em infraestruturas de transporte e a necessidade de uma maior conscientização e preparação para lidar com esses riscos, **Tonn et al. [113]** utilizam-se de uma abordagem de métodos mistos, incluindo análise de dados de incidentes cibernéticos nos sistemas

de transporte nos EUA e entrevistas com gestores de infraestrutura de transporte e seguradoras. O estudo trouxe alguns resultados: principais tendências e tipos de incidentes, as barreiras para um mercado de seguros cibernéticos robusto e aprimorado, novos insights sobre os riscos cibernéticos específicos para infraestruturas de transporte nos EUA, e a necessidade de medidas de mitigação e resiliência para enfrentar esses riscos. Com foco na perda de receitas, os autores perceberam que tais perdas ocorriam devido a interrupções e falhas, a desfiguração de sites e a extorsão cibernética como os principais riscos enfrentados pela indústria, e também descobriu que os atacantes cibernéticos incluem hackers, organizações criminosas e espiões, hackers patrocinados pelo estado, outras empresas e organizações, *insiders* maliciosos e contratados. Para os autores, tanto a frequência quanto a gravidade dos incidentes cibernéticos estão aumentando na indústria de transporte nos Estados Unidos, elencando os principais tipos de incidentes, como extorsão cibernética e incidentes relacionados à privacidade, e destacam as perdas financeiras associadas a cada tipo de incidente, apontando as principais barreiras para um mercado de seguros cibernéticos robusto e aprimorado, incluindo a falta de dados históricos sobre incidentes cibernéticos em infraestruturas de transporte e a falta de padrões de segurança cibernética.

Aziz, Suhardi e Kurnia [114] apresentam uma revisão sistemática da literatura dos desafios no âmbito do seguro cibernético, fazendo um levantamento dos setores de cobertura ou redução de perda financeira do segurado causada por incidentes cibernéticos e os desafios do seguro cibernético e suas soluções. O estudo paresenta alguns resultados: a revisão sistemática com foco no levantamento dos setores de cobertura ou redução de perda financeira por incidentes cibernéticos, os desafios do seguro cibernéticos e suas soluções, incluindo modelos, frameworks e sugestões de análises, a lista de setores de cobertura e redução de perda financeira do segurado causada por incidentes cibernéticos. Os autores concluem que a falta de dados confiáveis e a falta de conhecimento sobre segurança cibernética estão entre os desafios no seguro cibernético.

Facchinetti, Giudici e Osmetti [60] propõem uma nova metodologia para medir riscos cibernéticos que utiliza dados ordinais em vez de dados quantitativos, que muitas vezes não estão disponíveis, utilizando-se de dados sobre ataques cibernéticos coletados em nível mundial e a medida proposta é encontrada para ser bastante eficaz para classificar tipos de riscos cibernéticos. O método proposto depende da construção de um índice de criticidade, cujas propriedades são discutidas e comparadas com medidas alternativas empregadas na medição de riscos operacionais. Como resultados, o estudo propõe o Índice de Criticidade e apresenta a análise dos dados de ataques cibernéticos coletados em nível mundial. A medida proposta pode ajudar a proteger a privacidade das vítimas de ataques cibernéticos, uma vez que só utiliza dados ordinais, e não os dados reais de perda que podem ser sensíveis e difíceis de serem obtidos. A metodologia proposta pode ser aplicada em outros contextos de risco cibernético e pode ser usada como uma medida simples e efetiva para priorizar riscos cibernéticos. **Facchinetti, Giudici e Osmetti [60]** destacam que os riscos e ameaças cibernéticos são cada vez mais importantes, devido ao avanço tecnológico e à globalização das atividades financeiras, e que são uma preocupação crescente para os formuladores de políticas e as instituições financeiras.

O autor busca verificar se a atividade de TI (número de vírus ou intrusões bloqueados pela Norton em computadores de usuários finais) pode ser usada como índice para coberturas paramétricas propostas pelas empresas de resseguros, ivestigando as correlações da atividade de TI entre diferentes regiões para confirmar a natureza sistêmica dos riscos cibernéticos.

Xu e Hua [115] apresentam um modelo para o risco cibernético em empresas, levando em consideração a propagação de epidemias em redes de computadores. O modelo é baseado em uma abordagem de risco latente de um fator e binomial e usa processos de Markov e não-Markov para modelar a propagação de ataques. Os autores discutem estratégias de simulação e precificação do seguro cibernético, oferecendo insights sobre questões práticas na modelagem do risco cibernético e revisa trabalhos relevantes sobre o tema. O artigo revisa os trabalhos relevantes sobre o tema e oferece *insights* sobre questões práticas na modelagem do risco cibernético, discutindo estratégias de simulação e precificação do seguro cibernético. **Xu e Hua [115]** concluem que o modelo proposto é uma ferramenta útil para avaliar o risco cibernético em empresas e para precificar seguros contra esse risco, levando em consideração a propagação de epidemias em redes de computadores e a dependência entre os riscos cibernéticos. Os autores destacam que a modelagem do risco cibernético apresenta desafios, especialmente na estimativa das correlações entre os riscos.

Com o objetivo de explorar as limitações da abordagem qualitativa na avaliação de riscos de segurança cibernética, considerar como as abordagens quantitativas podem abordar essas limitações e entender como os profissionais de segurança cibernética estão usando e combinando as abordagens qualitativas e quantitativas, **Crotty e Daniel [116]** discutem a crescente importância da segurança cibernética para as organizações, que agora dependem cada vez mais de serviços online e armazenamento de dados digitais para criar valor econômico. Os autores fornecem insights e recomendações para os profissionais de segurança cibernética e tomadores de decisão, demonstrando a importância de adotar abordagens tanto qualitativas quanto quantitativas para avaliação de riscos de segurança cibernética. Os entrevistados enfatizaram a necessidade de adotar abordagens tanto qualitativas quanto quantitativas para avaliação de riscos de segurança cibernética e alertaram contra a dependência exclusiva de abordagens qualitativas. Para **Crotty e Daniel [116]** as organizações devem adotar uma abordagem combinada de avaliação de risco de segurança cibernética que inclua tanto abordagens qualitativas quanto quantitativas para fornecer uma visão mais abrangente dos riscos de segurança cibernética.

Já **Erola et al. [117]** apresentam um sistema para calcular o valor em risco cibernético (CVaR) de uma organização, considerando ameaças e controles de segurança. Os autores destacam a importância de entender o risco residual após a implementação de controles de segurança e planejar estratégias de segurança para alcançar a resiliência da organização. O sistema proposto utiliza um modelo de ameaças e controles, e simula ataques cibernéticos para estimar a perda esperada. O estudo apresenta alguns resultados: **(i)** a proposta de um sistema para calcular o CVaR de uma organização, considerando ameaças e controles de segurança, **(ii)** a aplicação do sistema em um cenário real, mostrando como ele pode ser usado para estimar o risco residual e avaliar a eficácia dos controles de segurança, **(iii)** uma discussão de possíveis melhorias e desenvolvimentos futuros do sistema, como a incorporação de *machine learning* e a utilização de dados de perdas cibernéticas para melhorar a precisão das estimativas de perda, e **(iv)** uma lista de controles de segurança que podem ajudar as organizações a mitigar os riscos e ameaças cibernéticas identificados. Para os autores, o sistema proposto para calcular o valor em risco cibernético (CVaR) é uma ferramenta útil para ajudar as organizações a alcançar esse objetivo. No entanto, o artigo destaca que o sistema tem limitações e que mais pesquisas são necessárias para melhorar sua precisão e relevância. O artigo também destaca a importância de uma abordagem colaborativa para o compartilhamento de dados e boas práticas de segurança entre as organizações, a fim de melhorar a segurança cibernética em geral.

Ainda no setor de seguros, **Kejwang [118]** avalia o efeito das práticas de gerenciamento de risco de segurança cibernética no desempenho no setor, utilizando-se de uma revisão de literatura para identificar referências relevantes e artigos de revistas. O autor apresenta uma revisão teórica e empírica sobre o tema, incluindo a teoria da resiliência proposta por Hollnagel e estudos anteriores sobre o gerenciamento de riscos cibernéticos em empresas de diferentes setores. A pesquisa concluiu que as empresas de seguros devem adotar técnicas de gerenciamento de segurança cibernética para lidar com o problema dos ciberataques. **Kejwang [118]** identificou lacunas no conhecimento e metodologia em estudos anteriores sobre o tema, destacando a necessidade de mais pesquisas para melhorar o entendimento sobre o efeito das práticas de gerenciamento de risco de segurança cibernética no desempenho do setor de seguros.

objetivando explorar a transferência de risco de seguro para a indústria de seguros cibernéticos nos Estados Unidos, com base no conjunto de dados líder da indústria de eventos cibernéticos fornecidos pela Advisen, **Malavasi et al. [18]** abordam duas questões principais: **(i)** quais são os fatores mais significativos que podem explicar a frequência e a gravidade dos eventos de perda cibernética e **(i)** se o risco cibernético é segurável em relação aos prêmios necessários, tamanho do pool de risco e mitigação de seguros. No estudo são discutidos os modelos de distribuição de severidade e aborda a capacidade de ser segurável do risco cibernético, e utiliza um conjunto de dados de eventos cibernéticos fornecido pela Advisen, incluindo modelos de regressão para análise de risco. **Malavasi et al. [18]** indicam que a frequência e a gravidade dos eventos de perda cibernética são influenciadas por vários fatores, incluindo o setor da indústria, o tamanho da empresa, o tipo de dados perdidos e o tipo de ataque cibernético. Os autores concluem que o risco cibernético é segurável, mas os prêmios exigidos podem ser altos e o *pool* de risco necessário pode ser grande, destacando a importância de uma abordagem de gerenciamento de riscos holística para a mitigação do risco cibernético e a necessidade de um gerenciamento de risco mais colaborativo entre seguradoras, empresas e especialistas em cibersegurança.

Em seu estudo, **Kim e Song [103]** tratam da importância da gestão de risco cibernético, que é definido como um risco acidental ou intencional relacionado a ativos de informação e tecnologia, propondo um **(i)** um modelo para medir o risco cibernético por meio da abordagem de distribuição de perda (LDA), **(ii)** um modelo de séries temporais para descrever as perdas cibernéticas dos setores financeiro e não financeiro, e **(iii)** a incorporação do método *Peaks over threshold* (POT) para melhorar a medição do risco. **Kim e Song [103]** concluem que o modelo proposto pode ser útil para gerenciar o risco cibernético em diferentes setores, destacando a importância de medidas preventivas e de preparação para incidentes de segurança cibernética, como a implementação de políticas de segurança, a realização de testes de segurança e a criação de planos de contingência em caso de incidentes. Os resultados mostraram que a distribuição de perda de perda de risco cibernético é mais assimétrica e com cauda pesada do que a distribuição de perda de risco operacional tradicional.

Pour et al. [101] discutem a importância da medição da Internet para a segurança cibernética, dada a crescente vulnerabilidade da sociedade às falhas de segurança cibernética, e sugerem que a coleta e análise de dados empíricos em larga escala usando técnicas de medição da Internet pode gerar insights abrangentes e confiáveis que podem ajudar a enfrentar esses desafios. O artigo explora as várias aplicações da medição da Internet e fornece uma taxonomia dos estudos de medição da Internet relacionados à segurança cibernética em duas dimensões: camadas verticais e componentes do ecossistema da Internet, e funções normais internas vs. o impacto negativo de partes externas na Internet e no mundo físico. O artigo apresenta uma

visão geral das técnicas de medição do DNS, incluindo métodos passivos e ativos, e identifica possíveis ameaças, como mudanças de propriedade de domínio e atividades mal-intencionadas de DNS, classificando as técnicas de medição com base na implantação do caso de uso: medições de acesso à linha fixa, medições de acesso móvel e suporte operacional. Os autores entendem que apesar dos esforços substanciais do setor, do governo e do meio acadêmico para lidar com as vulnerabilidades, os ataques à segurança cibernética continuam a aumentar em intensidade, diversidade e impacto, concluindo com uma relação de obstáculos para a realização de medições eficazes da Internet e possíveis direções futuras de pesquisa.

Examinando a literatura relevante sobre seguro cibernético, **Tsohou et al. [119]** apresentam a paisagem atual e as tendências futuras neste setor. Com a crescente dependência da sociedade em relação à infraestrutura e serviços de TI, o trabalho remoto resultante da pandemia de COVID-19 levou a um aumento nos ataques cibernéticos e, consequentemente, na necessidade de proteção dos sistemas de informação. O seguro cibernético surge como uma importante ferramenta para proteger as organizações contra perdas relacionadas a ataques cibernéticos. Os autores abordam temas como os desafios enfrentados pelas seguradoras, o processo de subscrição, as políticas e contratos de seguro cibernético e as tendências futuras. Para os autores, o seguro cibernético é uma ferramenta importante para proteger as organizações contra perdas relacionadas a ataques cibernéticos, sendo que as políticas e contratos de seguro cibernético são complexos e podem variar amplamente em termos de cobertura e exclusões. **Tsohou et al. [119]** as tendências futuras incluem **(i)** um aumento na demanda por seguro cibernético, **(ii)** uma maior ênfase na avaliação do risco cibernético, **(iii)** uma maior colaboração entre seguradoras e outras partes interessadas e **(iv)** uma maior harmonização das políticas e contratos de seguro cibernético. O artigo conclui com uma discussão sobre as implicações dos resultados e as forças e fraquezas da revisão da literatura.

A indústria de seguros e resseguros tem muito a contribuir com a gestão de riscos cibernéticos, mas também tem muitas carências relacionadas à percepção dos riscos, em especial pelas características evolutivas e mutantes da tecnologia da informação, que são responsáveis por inserções de inúmeros pontos de vulnerabilidades e consequentes riscos associados. Nessa seção buscou-se identificar as principais tendências e preocupações relacionadas à medição de riscos com foco em práticas de seguros. Conclui-se que a busca por indicadores que auxiliem à tomada de decisão ainda é algo almejado, e que o tema, em virtude da complexidade que cerca a segurança cibernética e seu impactos nos objetivos estratégicos e na sobrevivência organizacional, merecerá uma atenção especial por um longo período de tempo.

3.8 CONCLUSÕES DO CAPÍTULO

À medida que a pesquisa evoluía, percebeu-se que a abordagem de apetite a risco associada ao mundo cibernético, à gestão de riscos e à tomada de decisão, traria uma amplitude maior de fatores do que inicialmente se apresentava, levando a uma busca quase que incessante de se alcançar conexões relevantes entre os temas tratados. Este capítulo buscou compartilhar parte dos resultados de estudos que tangenciam a proposta inicial, para que se evidenciasse qual o estado atual de indicadores que colaboram com os tomadores de decisão. A partir desses elementos buscou-se agrupar os fatores que contribuem com o apetite a risco cibernético organizacional, assim como seus elementos formadores, como pretendido inicialmente.

4 METODOLOGIA

Nunca ande pelo caminho traçado, pois ele conduz somente até onde os outros já foram.

Alexander Graham Bell

Com o intuito de elaborar um modelo de mensuração de apetite a riscos cibernéticos com foco ao apoio à tomada de decisão, essa pesquisa classifica-se em Ciências Sociais Aplicadas - Administração envolvendo Engenharia, Tecnologia e Gestão, classificando-se como pesquisa **aplicada** [31, 120]. Quanto aos **métodos utilizados**, a pesquisa classifica-se como **métodos mistos**, empregando tanto o método qualitativo quanto o quantitativo.

Ao buscar os critérios e alternativas que influenciam a tomada de decisão em relação ao apetite a risco cibernético, a pesquisa utilizou-se de **pesquisa bibliográfica** com o objetivo de elucidar tais elementos, permitindo a construção de um modelo que guiasse o processo escolhido (AHP), assim como no levantamento dos principais frameworks de mercado voltado aos controles em segurança cibernética, proporcionando maior familiaridade do problema, dedicando-se à avaliação de hipóteses em relação à tomada de decisão na segurança cibernética, classificando-se como **exploratória** [31, 121], delimitando um campo de trabalho [122].

4.1 LOCAL DA PESQUISA

Para a aplicação do modelo proposto, optou-se por realizar no STJ, local em que o autor da pesquisa é servidor desde maio de 1995, tendo uma visão ampla da atuação dos principais atores, assim como das unidades envolvidas com os temas tratados na pesquisa. A pesquisa ocorreu em duas etapas (seção 4.3.2 e seção 4.3.2, entre os meses de janeiro e fevereiro de 2023.

Quatro servidores do STJ participaram tanto da fase de escolhas de controles quanto da fase de ponderação de pesos utilizados no AHP, tendo os seguintes perfis:

- Área: Assessoria de Gestão Estratégica / Riscos Corporativos, com 19 anos de experiência no Tribunal, com especialização em Gestão do Conhecimento , Gestão de Riscos e de Continuidade de Negócios.
- Área: Coordenadoria de Infraestrutura do Tribunal, com 12 anos de experiência no Tribunal, com especialização em Governança de TIC,
- Área: Coordenadoria de Segurança Cibernética do Tribunal, com 27 anos de experiência na área;
- Área: Coordenadoria de Governança em Tecnologia da Informação, com 10 anos de experiência na área.

4.2 O PASSO A PASSO DA PESQUISA

Alguns passos foram relevantes para o alcance dos objetivos:

1. Pesquisa bibliográfica que permitiu a identificação dos critérios e alternativas utilizados em pesquisas anteriores, assim como dos principais frameworks de mercado em segurança cibernética, servindo de base para formulação de uma proposta de modelo, abordados na seção 4.3.1.
    - Fez-se uma pesquisa em bases de dados da Scopus, Web of Science, IEEE Xplore, assim como a base de dados do Google Scholar.
    - Utilizou-se de termos como: segurança cibernética, segurança da informação, tomada de decisão, métodos de tomada de decisão em segurança da informação e cibernética, *frameworks* de segurança da informação e cibernética, apetite a risco, medidas de apetite a risco, medidas relacionadas a risco, gestão de riscos, gestão de riscos corporativos, gestão de riscos cibernéticos, revisão sistemática.
    - Utilizou-se como base os Critérios e Alternativas utilizados por vinte artigos que tratam do uso de métodos multicritérios nas áreas de conhecimento da pesquisa.
    - Identificação dos frameworks voltados à segurança cibernética e segurança da informação nas pesquisas utilizadas. As características dos frameworks tratadas nos artigos foram levados em conta na escolha do *framework* e do conjunto de controles a serem tratados no modelo proposto.
    - 105 artigos compuseram a base de dados do estudo.
2. Utilização do método AHP para a priorização dos critérios e alternativas prioritários, segundo a visão de profissionais de um Tribunal, na seção 4.3.2.
3. O apontamento realizado por profissionais do Tribunal sobre os controles desejados e a situação atual de implementação utilizando-se da Estrutura Básica de Segurança Cibernética do NIST, na seção 4.3.2.
4. Estabelecimento da correlação dos critérios e alternativas com os controles selecionados por meio de Análise de Conteúdo, na seção 4.3.3.
5. Análise comportamental do modelo, na seção 4.3.4.

4.3 FASE DE PRODUÇÃO DE DADOS PARA ANÁLISE

4.3.1 Seleção de Critérios e Alternativas

Nessa fase fez-se o mapeamento dos Critérios e Alternativas utilizados por vinte estudos que trataram métodos multicritérios em Segurança da Informação e Segurança Cibernética, possibilitando-se um mapeamento inicial para o modelo proposto.

Outros estudos que tratam de gestão de riscos corporativos, gestão de riscos cibernéticos, fatores humanos, partes interessadas, apetite a risco, cadeia de suprimentos cibernéticos e controles foram utilizados para compor o modelo, dando sustentação aos Critérios e Alternativas do modelo proposto.

4.3.2 Estudo de Caso

Utilização do método AHP

Saaty [94] nos informa que a construção de hierarquias se dá por meio de inclusão de detalhes relevantes ao retratar o problema, considerando o ambiente em torno dele, identificando os atributos que contribuem para a solução. A hierarquia vai ser considerada completa quando os itens constantes em um nível são avaliados em termos dos elementos do nível acima. Além de identificar quais fatores deverão compor a hierarquia que irão influenciar o resultado de uma decisão, há a necessidade de se decidir se o os fatores contribuem de forma igual, podendo ser ignorados aqueles que forem considerados de pouca relevância.

Nessa fase, seguiu-se os passos apresentados por Saaty [123]:

1. Definir o problema - relaciona-se ao problema da pesquisa;
2. Estruturar a hierarquia de decisão - a pesquisa bibliográfica foi utilizada para a estruturação da árvore do AHP;
    - Topo – Objetivo a ser alcançado,
    - Critérios,
    - Subcritérios (se houver), e
    - Alternativas – último nível.
3. Construir conjunto de matrizes par a par voltados para critérios e subcritérios;
4. Continuar o processo de ponderação até o nível mais baixo.

Os participantes do estudo de caso, servidores do STJ, contribuíram nas comparações pareadas previstas pelo AHP, tanto nos Critérios como nas Alternativas.

Seleção dos Controles

Após a pesquisa bibliográfica, onde foram considerados os frameworks de mercado voltados para a segurança cibernética, optou-se por utilizar o **Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica** [55], por atender às expectativas quanto a abordar não apenas aspectos relacionados ao operacional da tecnologia da informação, como também controles voltados para a organização (com foco nos objetivos estratégicos), a cadeia de suprimentos cibernéticos e corpo gerencial, funcionários e colaboradores.

Essa etapa foi responsável pelos apontamentos a respeito do interesse dos integrantes da organização sobre o conjunto de controles proposto pelo NIST, dispostos na sua Estrutura Básica, conforme tratado na seção 2.6, identificando quais controles são desejados para serem implementados, e, desses, quais já se encontram implementados.

O Guia [55] tem como foco a orientação das atividades voltadas à segurança cibernética, concentrando-se em indicadores de negócio, considerando que os riscos cibernéticos fazem parte do gerenciamento de riscos corporativos, dividindo-se em três partes: a Estrutura Básica, os Níveis de Implementação e as Avaliações da Estrutura. O Guia não se trata de uma abordagem única no gerenciamento de risco de segurança cibernética, cabendo às organizações apontarem quais são as atividades importantes que permitirão a entrega de serviços críticos, priorizando seus investimentos.

4.3.3 Análise de Conteúdo - Relacionamentos Controles X Alternativas

Essa etapa foi realizada para estabelecer o relacionamento entre as alternativas propostas e os controles previstos no framework selecionado, constantes no **Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica** [55], utilizou-se a análise de conteúdo, que visa à inferência entre o conteúdo de mensagens (medidas de controle do Guia) para um contexto mais objetivo [124, 125], as alternativas do modelo.

Bardin [125, p. 10] define a "Análise de Conteúdo"como:

> O que é a análise de conteúdo actualmente? Um conjunto de instrumentos metodológicos cada vez mais sutis em constante aperfeiçoamento, que se aplicam a «discursos» (conteúdos e continentes) extremamente diversificados. O factor comum destas técnicas múltiplas e multiplicadas — desde o cálculo de frequências que fornece dados cifrados, até à extracção de estruturas traduzíveis em modelos — é uma hermenêutica controlada, baseada na dedução: a inferência. Enquanto esforço de interpretação, a análise de conteúdo oscila entre os dois pólos do rigor da objectividade e da fecundidade da subjectividade. Absolve e cauciona o investigador por esta atracção pelo escondido, o latente, o não–aparente, o potencial de inédito (do não-dito), retido por qualquer mensagem. Tarefa paciente de «desocultação», responde a esta atitude de voyeur de que o analista não ousa confessar-se e justifica a sua preocupação, honesta, de rigor científico. Analisar mensagens por esta dupla leitura onde uma segunda leitura se substitui à leitura «normal» do leigo, é ser agente duplo, detective, espião... Daí a investir-se o instrumento técnico enquanto tal e a adorá-lo como um ídolo capaz de todas as magias, fazer-se dele o pretexto ou o álibi que caucione vãos procedimentos, a transformá-lo em gadget inexpugnável do seu pedestal, vai um passo... que é preferível não transpor.

Já Riffe et al. [126, p. 23] apresenta uma definição de análise quantitativa de conteúdo:

> A análise quantitativa de conteúdo é o exame sistemático e replicável de símbolos de comunicação, aos quais foram atribuídos valores numéricos de acordo com regras de medição válidas, e a análise de relacionamentos envolvendo esses valores usando métodos estatísticos, para des-

crever a comunicação, fazer inferências sobre seu significado ou inferir da comunicação ao seu contexto, tanto de produção como de consumo.

Em sua obra de 1977, Bardin [127] nos informa que a análise de conteúdo organiza-se em torno de três polos cronológicos:

1. Pré-análise - tem três missões:
   (a) Escolha dos documentos a serem analisados, a
   (b) Formulação de hipóteses e objetivos, e a
   (c) Elaboração dos indicadores que irão fundamentar a interpretação final.
2. Exploração do material – consiste de operações de codificação, desconto ou enumeração, respeitando-se as regras estabelecidas.
3. Tratamento dos resultados, inferência e interpretação – possibilitam a construção de quadros de resultados, pondo em evidência as informações fornecidas pela análise.

Para a codificação proposta, seguiu-se os passos indicados por Bardin. Na pré-análise foram utilizados os cento e oito controles previstos no CSF, como fonte documental. As operações de codificações consistiram na identificação da presença ou não presença dos códigos utilizados, as Alternativas do modelo proposto, em cada leitura dos controles. Já a fase final, o tratamento dos resultados, foi utilizada na proposta do modelo, sendo uma fase relevante na medição do risco ao apetite a risco cibernético.

4.3.4 Análise do Comportamento do Modelo

Antes da aplicação prática do modelo, fez-se um estudo comportamental, buscando-se avaliações a respeito dos índices alcançados, variando-se controles e pesos dos critérios e alternativas.

Para o propósito dessa etapa foram estabelecidas duas simulações, objetivando observar os resultados de saída do modelo proposto:

1. Manteve-se os Controles, sendo alterados os pesos de Critérios e Alternativas;
2. Manteve-se os pesos de Critérios e Alternativas, alterando-se a seleção de Controles.

5 RESULTADOS

Neste Capítulo, buscou-se trazer os principais achados da pesquisa, seguindo-se o que ficou estabelecido como Objetivos Específicos e Objetivo Geral.

Após a leitura e o levantamento dos Critérios e Alternativas dos artigos, elaborou-se o modelo esquematizado na fig. 5.1, sendo sua construção tratada na seção 5.1. Muitos desses critérios tiveram influência dos trabalhos analisados. A relação de critérios e alternativas priorizados é tratada na seção 5.2.

Figura 5.1: Árvore Hierárquica AHP

Fonte: feito pelo Autor

5.1 A CONSTRUÇÃO DA ÁRVORE DE CRITÉRIOS E ALTERNATIVAS

"Três princípios orientam a solução de problemas usando o AHP: decomposição, julgamentos comparativos e síntese de prioridades, conforme demonstrado no exemplo anterior." [128, p. 166]

O princípio da decomposição, segundo Saaty [128, p.166]:

> O princípio da decomposição é aplicado por meio da estruturação de um problema simples, com os elementos em um nível sendo independentes dos elementos nos níveis seguintes, trabalhando de forma descendente a partir do foco no nível superior, para os critérios que afetam

o foco no segundo nível, seguidos pelos subcritérios no terceiro nível, e assim por diante, do mais geral (e às vezes incerto) para o mais particular e concreto. Saaty faz uma distinção entre dois tipos de dependência, que ele chama de funcional e estrutural. A primeira é a conhecida dependência contextual dos elementos em relação a outros elementos no desempenho de sua função, enquanto a segunda é a dependência da prioridade dos elementos em relação à prioridade e ao número de outros elementos. A medição absoluta, às vezes chamada de pontuação, é usada quando se deseja ignorar essa dependência estrutural entre os elementos, enquanto a medição relativa é usada em outros casos.

Para alcançarmos o primeiro princípio, o da decomposição, foi realizada uma extensiva pesquisa bibliográfica que contou com cento e cinco artigos, sendo que vinte deles trazem em sua estrutura conjutos de critérios e alternativas que merecem uma atenção especial. A partir desse conjunto foi possível identificar cento e dez critérios e quase três centenas de alternativas. A relação completa de Critérios e Alternativas encontra-se em Apêndice 03 - Critérios e Alternativas Citados.

Outro ponto relevante trazido por Saaty [94] é fazer com que os elementos (critérios e alternativas) deverão ser dispostos em grupos homogêneos de cinco a nove para que possam ser significativamente comparados. Buscou-se, à medida do possível, seguir tais regras estabelecidas pelo autor.

A seguir é feita uma análise dos artigos que foram úteis para a formulação do modelo AHP proposto. Salienta-se que os temas que cercam a pesquisa são diversos e de alta complexidade, mas que nosso método deve almejar o proposto por Saaty [128, p. 163]: "Uma regra geral é que a hierarquia deve ser complexa o suficiente para capturar a situação, mas pequena e ágil o suficiente para ser sensível às mudanças."

Tabela 5.1: Referências utilizadas para formulação de Critérios e Alternativas

Distribuição de Critérios e Alternativas					
Ano	**Seq**	**Referência**	**Tópico Central**	**Critérios**	**Alternativas**
2019	1	[26]	Segurança Cibernética	4	16
	2	[51]	Segurança Cibernética	4	21
	3	[129]	Serviços Digitais	7	18
	4	[8]	Segurança Cibernética	4	11
2020	5	[130]	Saúde	6	
	6	[61]	Segurança Cibernética	4	
	7	[82]	Proteção de Dados Pessoais	4	19
	8	[24]	Gerenciamento de Riscos	3	26
	9	[9]	Gerenciamento de Riscos	5	16
2021	10	[89]	Segurança Cibernética	5	
	11	[131]	Segurança Cibernética	8	
	12	[28]	Segurança Cibernética	6	21
	13	[90]	Qualidade de Software	11	13
	14	[27]	Gerenciamento de Riscos	5	
	15	[80]	Segurança Cibernética	7	20
	16	[73]	Resiliência Cibernética	6	25

Tabela 5.1: Referências utilizadas para formulação de Critérios e Alternativas

Distribuição de Critérios e Alternativas					
2022	17	[88]	Segurança Cibernética	8	
	18	[132]	Segurança Cibernética	2	9
	19	[133]	Gerenciamento de Riscos	6	8
	20	[134]	Partes Interessadas	5	56
			Totais	**110**	**279**

Fonte: feito pelo Autor

A tabela 5.2 apresenta como ficaram distribuídos critérios e artigos por tópico central. Segurança Cibernética e Gerenciamento de Riscos foram os tópicos que mais contribuíram nesse quesito.

Salienta-se, entretanto, que os artigos trazem mais de uma área de conhecimento, como, por exemplo, artigo classificado como **Proteção de Dados Pessoais** também esteja inserido no tópico **Segurança Cibernética**, ou mesmo **Gerenciamento de Riscos**, ou oturo qualquer. Na verdade, muitos textos têm múltiplos tópicos, abrangendo características relevantes para a pesquisa proposta. Como todos os artigos tratam de MMDC, é inevitável que sejam relacionados à **Tomada de Decisão**, um dos tópicos centrais dessa pesquisa.

Tabela 5.2: Distribuição por Tópico Central - Critérios e Alternativas

Distribuição por Tópico Central			
Tópico Central	**Qtde Artigos**	**Critérios**	**Alternativas**
Segurança Cibernética	10	52	98
Gerenciamento de Riscos	4	19	50
Qualidade de Software	1	11	13
Serviços Digitais	1	7	18
Resiliência Cibernética	1	6	25
Saúde	1	6	
Partes Interessadas	1	5	56
Proteção de Dados Pessoais	1	4	19
Totais	**20**	**110**	**279**

Fonte: feito pelo Autor

Segurança Cibernética e **Gerenciamento de Riscos** foram os dois tópicos centrais que mais contribuíram no levantamento de Critérios e Alternativas no uso do AHP. Essa análise inicial dos textos abordados se faz necessária para que pudéssemos posicionar os textos selecionados nos temas tratados pela pesquisa: métodos multicritérios com foco na tomada de decisão em segurnaça cibernética, envolvendo aspectos humanos e partes interessadas.

A maioria dos artigos foram classificados como **Métodos Multicritérios**, e aí se depositam a maioria dos Critérios e Alternativas levantados, podendo ser observado na tabela 5.3,.

Tabela 5.3: Distribuição de artigos pela Classe

Distribuição por Classificação de Artigo		
Classe	**Critérios**	**Alternativas**
Apetite a risco	5	
Aspectos Humanos	6	21
Cadeia de Suprimentos	6	25
Métodos Multicritérios	93	233
Totais	**110**	**279**

Fonte: feito pelo Autor

Na tabela 5.4

Tabela 5.4: Referência cruzada Tópico X Classe - Distribuição de Critérios e Alternativas

Quantidade de Critérios e Alternativas por Tópico Central dos artigos										
Tópico Central	**Totais**		**Métodos**		**Humanos**		**Suprimentos**		**Apetite**	
	C	**A**	**C**	**A**	**C**	**A**	**C**	**A**	**C**	**A**
Segurança Cibernética	**52**	**98**	46	77	6	21				
Gerenciamento de Riscos	**19**	**50**	14	50					5	
Qualidade de Software	**11**	**13**	11	13						
Serviços Digitais	**7**	**18**	7	18						
Resiliência Cibernética	**6**	**25**					6	25		
Saúde	**6**		6							
Partes Interessadas	**5**	**56**	5	56						
Proteção de Dados Pessoais	**4**	**19**	4	19						
Totais	**110**	**279**	**93**	**233**	**6**	**21**	**6**	**25**	**5**	

Fonte: feito pelo Autor

Os vinte trabalhos que influenciaram as escolhas dos critérios e das alternativas do modelo proposto são trazidos para os resultados, buscando-se evidenciar os critérios e alternativas utilizados.

1. Maček et al. [27] após promoverem um estudo detalhado sobre métodos e técnicas de avaliação de risco, assim como métodos multicritério para a tomada de decisão na seleção de sistemas de informação, desenvolveram um modelo multicritério com critérios que consideraram relevantes, com focos em sistemas críticos de uma instituição financeira: **Ameaça**, **Vulnerabilidade**, **Probabilidade**, **Consequência** e **Resiliência**. Os autores concluem que a abordagem sugerida contribuiu em especial por levar em consideração as influências e as dependências entre os critérios avaliados, o que tem sido negligenciado em outras abordagens multicritério.

2. Aman e Shukaili [28] apresentam uma relação de critérios e alternativas bastante abrangente, voltada para uma estratégia de segurança cibernética. Utilizou-se de seis fatores como critérios (**Organizacionais**, **Culturais**, **Econômicos**, **Legais e Políticos**, **Técnicos** e de **Risco**), com 21 alternativas distribuídas

nos critérios. Para os autores, o desenvolvimento e a implementação eficaz da estratégia de segurança cibernética necessita levar em consideração os fatores críticos com foco na sua eficácia, e uma visão holística dos fatores pode fornecer uma base importante nessa etapa. Esse estudo trouxe bons *insights* para o modelo proposto da pesquisa.

3. Uraipan, Praneetpolgrang e Manisri [73] desenvolveram um modelo que possibilitou determinar o nível de maturidade da resiliência cibernética de nove pequenas e médias empresas. Os autores usaram 6 critérios e 25 alternativas: **Identificar** (Gestão de ativos, Ambiente de negócios, Governança, Avaliação de risco, Estratégia de Segurança da Cadeia de Suprimentos, Gestão de Riscos da Cadeia de Suprimentos), **Proteger** (Conscientização e Treinamento, Controle de acesso, Manutenção, Privacidade, Processo e Procedimentos de Proteção de Informações, Tecnologia de proteção), **Detectar** (Anomalias e Eventos, Inteligência Cibernética, Monitoramento Contínuo de Segurança, Processos de detecção), **Responder** (Agilidade da Cadeia de Suprimentos, Análise, Comunicação, Melhorias, Mitigação, Planejamento de resposta), **Recuperar** (Plano de Recuperação, Melhorias, Comunicação) e **Continuar** (Sustentabilidade da Cadeia de Suprimentos, Confiabilidade da Cadeia de Suprimentos, Plano de Continuidade de Negócios e Avaliação de Continuidade de Negócios). Os autores concluem que o modelo permitiu a avaliação do ponto de vista funcional, utilizando-se do *fuzzy* AHP, tendo os fatores relacionaods à **Identificar** os de maior relevância. Esse estudo trouxe bons exemplos para o modelo proposto da pesquisa.

4. Ansari et al. [130] desenvolveram um estudo com foco em engenharia de requisitos de segurança com o objetivo de classificar cinco frameworks (SREP, SQUARE, STORE, MOSRE e SREF) que serviram de alternativas para a tomada de decisão. Os autores utilizaram 7 critérios para obter a classificação por meio do uso do método *fuzzy* TOPSIS: **Objetivo de segurança**, **Requisito de segurança**, **Parte interessada**, **Ativo**, **Ameaça**, **Risco**, **Vulnerabilidade**. A aplicação do método se deu no setor de saúde, sendo a metodologia STORE considerada a abordagem mais eficaz com base nas seleções dos especialistas em segurança. Assim como nos estudos anteriores, houve uma visão mais ampla dos fatores que compõem o espectro da segurança.

5. Torbacki [80] utiliza uma combinação de três métodos (DEMATEL, ANP e PROMETHEE II), objetivando a estabelecer uma classificação de três grupos de medidas (operacional, tecnológica e organizacional), com sete dimensões e vinte critérios: **Serviços de confiança** (Assinatura eletrônica selo eletrônico e carimbo de hora eletrônico, Validação e manutenção de assinaturas e selos eletrônicos, Entrega Eletrônica Registrada), **Criptografia** (Autenticação de portais BB online; Protocolos X09/TLS/SSL, Tecnologia Blockchain), **Segurança de rede** (Segurança técnica adequada de uma rede da empresa, Arquitetura de rede e servidor ideal, Monitoramento e análise de incidentes de segurança), **Segurança do aplicativo** (Segurança do banco de dados, Estabelecimento de um sistema de backup eficiente, Verificação de vulnerabilidades; Análise de código-fonte para procurar fraquezas de software, Atualizações de software), **Segurança do endpoint** (Técnicas apropriadas para proteger estações de trabalho e dispositivos móveis, Antivírus e antimalware, Testes de penetração para encontrar vulnerabilidades), **Controle de acesso** (Estabelecendo uma conexão remota segura VPN com o servidor corporativo, Treinamento regular de funcionários na área de segurança cibernética, Criação de regras para gerenciamento de acesso a dados corporativos, Autenticação de

usuário) e **Ataques cibernéticos** (Sistema de Prevenção de Intrusão e Sistema de Detecção de Intrusão com algoritmos para detectar em tempo real os ataques maliciosos, Firewall Gateway e Proxy). O estudo é voltado para a aplicação nas tecnologias relacionadas à Indústria 4.0, com foco na implementação de fabricação sustentável. Por meio do uso dos métodos, a validação e manutenção de assinaturas e selos eletrônicos foi considerada o critério mais relevante, a segurança de rede é a área mais importante e, por fim, as medidas tecnológicas são o grupo de medidas que requer mais atenção.

6. Alzahrani e Johnson [26] estabelecem um modelo de apoio à decisão, utilizando-se do AHP, com foco em fatores que influenciam a conformidade da política de segurança da informação. Utilizou-se os critérios **Autonomia** , **Competência**, **Intenção comportamental**, **Relacionamento**, combinando com as alternativas **Ataque cibernético**, **Conformidade com as políticas**, **e-mail e Internet** e **Resposta a incidentes**. A pesquisa levou em consideração tomadores de decisão de uma empresa fortune 600. **Intenção comportamental** foi classificado como principal critério, com 52%, seguido por **Autonomia** e **Competência**, cada um com 21%, e **Relacionamento**, com os 6% restantes. Para os autores, os resultados podem ser úteis na formulação de programas de conscientização de segurança cibernética, com foco na conformidade de políticas de segurança.

7. Alshahrani et al. [133] realizaram uma investigação com foco em um modelo de apoio à decisão voltada à priorização de fatores de riscos de TIC, utilizando-se dos critérios **Eficácia**, **Frequência do evento**, **Disponibilidade**, **Consequência**, **Adequação**, **Descoberta**, e das alternativas **Tecnologia**, **Financeiro**, **Pessoas**, **Fornecedores**, **Operacional**, **Política e Procedimentos**, **Meio Ambiente** e **Estratégico**. Para os autores, o uso do método *fuzzy* TOPSIS, o fator de risco mais relevante foi a **Tecnologia**, devendo a segurança de rede ser tratada de forma correta.

8. Belinda et al. [90] desenvolveram um estudo com uso do AHP com o intuito de obter uma relação priorizada de requisitos de qualidade de software. Utilizaram-se de 11 atributos principais, e 13 subatributos, como critérios, seguindo a proposta do modelo utilizado: **Manutenibilidade** (Extensibilidade, Flexibilidade, Suportabilidade), **Usabilidade** (Compreensibilidade), **Confiabilidade** (Robustez, Precisão), **Testabilidade**, **Funcionalidade** (Correção, Interoperabilidade), **Disponibilidade**, **Reutilização**, **Custo**, **Eficiência** (Performance), **Portabilidade**, (Adaptabilidade), **Segurança**, (Confidencialidade, Integridade, Não-repúdio). Na avaliação alcançada pelas partes interessadas, a **Manutenibilidade** foi considerada como o principal critério, seguido por **Testabilidade**, sendo o **Custo** o de menor índice. O estudo é relevante, principalmente quando consideramos que o uso de controles implicará em avaliar ações complementares, em especial para aquelas organizações que possuem, em sua estrutura, desenvolvimento próprio de software.

9. Zhao et al. [8] utilizaram-se do AHP, por meio dos critérios **Detecção** (Métrica de perigo, Mudança de fluxo, Status do host), **Gestão** (Importância do ativo de segurança, Pontuação de custo de prevenção de vulnerabilidade), **Proteção** (Força da Estratégia de proteção, Força protetora), **Resposta** (Índice de integridade do equipamento chave, Índice de tempo de resposta da lista negra, Plano de Recuperação, Tempo de resposta à intrusão). Os autores se basearam no modelo PDR (Proteção, Detecção, Resposta), proposta pela empresa ISS (*American Internet Security System*, agregando funções de gerenciamento buscando otimizar o modelo original. Apesar de compreenderem que

os resulatados alcançados com o uso do AHP foram razoáveis, perceberam que o modelo apresentou limitações, apresentando que a coleta e quantificação indicadores, na segurança de redes, são atividades complexas e difíceis de serem executadas.

10. O trabalho de Shojaeshafiei, Etzkorn e Anderson [9] se propôs desenvolver uma metodologia voltada a quantificar vulnerabilidades em aplicações voltadas para a Web, utilizando-se do método *Goal Question Metrics* (GQM) determinando os fatores e subfatores de segurança de aplicativos no órgão estudado, o Departamento de Transporte. Após a identificação inicial de fatores e subfatores, os autores utilizaram-se do *fuzzy* AHP para ponderar os pesos dos critérios / subcritérios identificados: **Autenticação** (Dois fatores de autenticação, Username / Password), **Autorização e Identificação** (Teste de penetração), **Manutenção** (Alterações de software, Rastreador de dependência), **Segurança do Software** (Código Fonte Seguro, Padrões de Qualidade de Desenvolvimento, Desenvolvimento Seguro), **Segurança em tempo de execução** (Encriptação, HTTP/HTTPS, Outras encriptações, Monitoramento e Log, Teste de penetração, Política de Filtering, XSS, Firewall e Antivirus). Em seus resultados, consideraram a metodologia muito eficiente e flexível para acrescentar novas camadas de fatores, não ficando restrita apenas aos aplicativos Web, mas que apresenta uma limitação à medida que o número de variáveis cresce, tornando o processo mais complexo.

11. A principal contribução de Llansó, McNeil e Noteboom [51], para a nossa pesquisa, é o agrupamento de critérios observados em outros artigos, com foco no engeheiro de segurança: **Organizacional** (Impacto no Negócio, Tolerância ao Risco, Legal e Regulamentar, Restrições Auto-Impostas), **Ativo** (Importância / Valor, Risco Avaliado, Probabilidade de Violação), **Ameaça** (Antecipado, Mais Significativo, Risco Residual), **Controle** (Custo, Compra / Configuração, Dificuldade de Implementação, Custo de Operação, Eficiência / Eficácia / Desempenho / Número de ameaças abordadas, Grau de implementação, Alinhamento com Normas, Disponibilidade, Número de Benefícios, Combinação, Preferência Partes Interessadas). Alguns desses critérios foram observados no modelo proposto da pesquisa.

12. Abushark et al. [89] analisaram seis abordagens distintas voltadas para requisitos de segurança de software (SQUARE, SREF, STORE, MOSRE, SREP e MSRA) , utilizando-se do método híbrido de apoio à decisão AHP-TOPSIS *fuzzy*, com um total de cinco critérios e 12 subcritérios: **Eficiência** (esforço do usuário, economia de tempo), **Efetividade** (operabilidade, escalabilidade, extensibilidade), **Capacidade de aprendizado** (interface do usuário, treinamento, estrutura do sistema), **Satisfação** (conveniência, simpatia), **Produtividade** (resultado útil, custo-benefício). A proposta dos autores focou em priorizar as seis abordagens de requisito de segurança de softawre sob a ótica dos especialistas em segurança. Concluíram que a metodologia STORE se demonstrou consistente e utilizável com foco orientado a ameaças, sendo eficaz e organizada ao elicitar requisitos de segurança no desenvolvimento de software.

13. Alfakeeh et al. [132] estruturaram um modelo a partir da combinação entre o método *Fuzzy Analytic Network Process* (*Fuzzy* ANP) e o método *Fuzzy* TOPSIS, com o objetivo de estimar o impacto da segurança sustentável em software voltados para a saúde. Para a definição do modelo, utilizaram-se de uma árvore hierárquica com dois critérios principais e outros nove sub-critérios: **Segurança** (Disponibilidade, Integridade, Confiabilidade), **Sustentabilidade** (Consumo de Energia, Otimiza-

ção de recursos baseado em software, Durabilidade, Manutenibilidade, Portabilidade). Como um dos achados do estudo, os autores concluem que o desenvolvimento sustentável de software voltado para a indústria da saúde deve, necessariamente, combinar caracterísitcas de segurança da informação, alcançando a conformidade legal, equilibrando com os requisitos de sustentabilidade com foco econômico, ambiental e social, buscando maximizar a satisfação dos clientes.

14. Bhol, Mohanty e Pattnaik [61] comparam o uso de duas abordagens MCDM, AHP e ELECTRE III, com o intuito de avaliar métricas de segurança cibernética. Para realizar as comparações, foram utilizadas informações de três organizações e quatro critérios: **Suscetibilidade**, **Mecanismo de proteção**, **Medição de riscos**, **Resultados do encontro entre a ameaça e os mecanismos de preteção**.

15. Ribeiro e Canedo [82] identificaram e selecionaram um conjunto de critérios de segurança de dados com foco na implantação da Lei Geral de Proteção de Dados Pessoais (LGPD), utilizando-se um método de Análise de Decisão de Múltiplos Critérios (MCDA), o PROMETHEE II, combinado com o AHP, utilizando-se de quatro critérios e dezenove alternativas: **Nível de proteção de dados** (Limitando o acesso apenas aos dados do titular, Anonimização de dados pessoais, Hashing de dados confidenciais, Excluindo dados pessoais, Mantendo dados pessoais armazenados, Classificando a importância dos dados pessoais), **Riscos de segurança** (Definir Agentes de Segurança, Definir uma Política de Segurança de Dados Pessoais, Usar Sistema de Criptografia, Usar Certificado para Acesso a Dados Pessoais, Criar Grupos de Usuários, Usar Firewall), **Gravidade do Incidente** (Mapear Incidentes Potenciais, Desenvolver Plano de Resposta a Incidentes, Avaliar as Melhores Soluções Técnicas de Resolução de Incidentes, Definir Medidas de Mitigação de Incidentes), **Riscos de privacidade de dados** (Verifique a privacidade dos serviços da Web, Crie um grupo restrito de acesso a dados pessoais, Verifique os dados pessoais armazenados por cada um dos sistemas). Após a ponderação dos pesos estabelecidos pelas partes interessadas, os autores concluíram que o critério **Riscos à Privacidade** foi considerado o de maior prioridade quando da implementação da segurança de dados pessoais na instituição estudada.

16. Ganin et al. [24] desenvolveram um modelo com o objetivo de quantificar os critérios estabelecidos (Ameaça, Vulnerabilidade e Consequência) por meio de um conjunto de sub-critérios, buscando avaliar as abordagens atuais em avaliação de riscos cibernéticos (OCTAVE, CIS Security Metrics, Cyber threat metrics, Network Security Risk Model, Information security risk Analysis method, entre outros).Critérios e sub-critérios utilizados: **Ameaça** (Facilidade de Ataque, Informações, Tecnologia à disposição, Opções de entrega, Benefícios, Ganho Financeiro, Ganho Político, Outros Ganhos), **Vulnerabilidade** (Domínio Físico, Facilidade de Acesso Físico, Hardware Obsoleto, Hardware falsificado, Dispositivos Portáteis, Domínio Informações, Facilidade de Acesso Lógico, Software obsoleto, Cobertura antivírus e de varredura, Software falsificado, Domínio Social, Histórico de Pessoal, Conscientização e Treinamento, Controle de Acesso, Lealdade e bem-estar) e **Consequência** (Confidencialidade, Integridade, Disponibilidade). Para os autores, o modelo proposto preencheu uma lacuna na avaliação de risco, assegurando um processo que traz sua estruturação e transparência na seleção de alternativas, fornecendo justificativas racionais na seleção de ações no gerenciamento de riscos.

17. Gonzales et al. [134] elaboraram um estudo com foco nas partes interessadas na área de Educa-

ção 4.0 (EDU4), utilizando-se do método CRITIC-CODAS-SORT, estabelecendo o grau em que os papéis superam as barreiras quando da implementação da EDUC4. Para isso usaram um modelo hierárquico com quatro critérios, representando as partes interessadas, e outros cinquenta e sete subcritérios, representando ações que cada uma das áreas interessadas deve executar: **Educadores** (13 ações), **Governo** (16 ações), **Recursos Humanos** (12 ações) e **Gestão Universitária** (10 ações). Para os autores, a identificação e apriorização das barreiras, em diferentes níveis gerenciais, é fundamental para o enfrentamento dessas barreiras nas instituições de nível superior. No estudo, os autores apresentam doze barreiras para a implementação: Ameaça à segurança cibernética (B1), Dispendioso (B2), Lacuna de competências do capital humano (B3), Partes interessadas apreensivas (B4), Falta de recursos de treinamento (B5), Falta de colaboração (B6), Lacuna de conhecimento para a personalização do design do currículo (B7), Tecnologias disponíveis insuficientes (B8), Problemas de saúde (B9), Restrição de tempo para preparação de material (B10), Complexidade das plataformas de aprendizado (B11), Fundação insuficiente na fundação básica (B12). Como resultado do estudo, as mais relevantes foram B6, B4, B1, B9 e B2. Esse trabalho traz bons *insights* para nossa proposta, principalmente com a possibilidade de se propor algo complementar ao modelo, em estudos futuros. Destaca-se por envolver muitas questões organizacionais, em especial às partes interessadas, além de se utilizar de um modelo multicritério pouco referenciado na literatura, mas que se demonstrou bastante útil para a proposta apresentada.

18. Mustafa e Kar [129] desenvolveram um estudo, com um grupo de usuários na Índia, utilizando-se do método de rede analítica generalizada (GANP), com o objetivo de estabelecer priorização entre sete dimensões do risco: **Risco de Privacidade** (Comprometimento de informações pessoais, Usos de informações pessoais sem o seu conhecimento, Controle da minha conta por hackers), **Risco Financeiro** (Perda de dinheiro, Perda de informações financeiras, Risco financeiro da conta bancária), **Risco Social** (Efeito negativo do pensamento dos outros, Perda social por familiares e amigos), **Risco de Tempo** (Perda de tempos por inconveniência), **Risco Psicológico** (Autoimagem da pessoa, Perda psicológica por causa da adaptação), **Risco Físico** (Ameaça à saúde, Viva por muito tempo, Causa da doença, Exposto por radiação nociva, Risco de dano cerebral) e **Risco de Performance** (Entrega de desempenho conforme prometido, Transação feita pelo provedor de serviços corretamente), O resultado encontrado com a aplicação do método indicou que os riscos de privacidade, de desempenho e financeiro foram elencados como os mais prioritários.

19. Abushark et al. [88] e Alharbi et al. [131] desenvolveram duas pesquisas semelhantes, com o objetivo de avaliar o impacto de atributos relacinados à segurança cibernética em sistemas de detecção de intrusão baseados em aprendizado de máquina. No estudo utilizaram-se do AHP-TOPSIS baseado no *fuzzy* hesitante, tendo oito critérios: **Complexidade de Implementação**, **Detecção de anomalias**, **Detecção de ataques DDoS**, **Detecção de spam**, **Detecção de uso indevido**, **Identificação de malware**, **Identificação de phishing**, **Precisão**. Como alternativas, no primeiro trabalho foram analisados dez sistemas de detecção de intrusão [131], e no segundo trabalho foram analisados seis sistemas de detecção de intrusão Abushark et al. [88], obtendo opiniões de especialistas (não apresenta a quantidade ou perfis desses especialistas) para obter a comparação dos pares. Como o AHP foi criado com a possibilidade de inclusão de sub-categorias, esse estudo pode ser utilizado em análises futuras do método proposto pela nossa pesquisa, podendo ser muito útil na escolha de soluções

com foco na prevenção à intrusão.

Estruturar a Hierarquia da decisão

Os grupos foram compostos de forma homogênea, por elementos correlacionados, seguindo-se a orientação de Saaty [94]. Fez-se processo de agrupamentos, com elementos semelhantes, evitando-se comparar elementos com dimensões muito distintas. Os grupos estão descritos da seguinte forma:

1. **A estrutura organizacional**: missão, objetivos estratégicos, alta gestão, governança, cultura organizacional, aspectos legais, processos de trabalho, investimentos, entre outros;
2. **Tomadores de decisão**: funcionários, colaboradores, gestores (TIC, Processos de Trabalho, Sistemas de Informação, Riscos Corporativos, Recursos Humanos);
3. **Medidas de segurança**: sistemas e aplicativos, de rede, de usuário, física, estações de trabalho;
4. **Ativos da organização a serem protegidos**: dados (CID), resiliência (a capacidade de retornar ao nível adequado após um incidente), privacidade, processos de trabalho, pessoas, hardware e software;
5. **Tecnologias utilizadas**: as ultrapassdas, as múltiplas tecnologias, o uso de nuvem, as novas tecnologias (IoT, Big Data, IA, entre outras) e,
6. **Ameaças**: incidentes ocorridos, as vulnerabilidades, o ambiente externo e o ambiente externo.

Esses vinte estudos deram uma dimensão bastante ampla quando tratamos de critérios e alternativas na tomada de decisão no mundo cibernético. A partir da leitura dos artigos somando-se à orientação dada por Saaty, buscou-se os principais grupos de critérios tratados pelos autores, destacando-se: Organização, Tomadores de Decisão, aspectos de Segurança, Ativos relevantes para a organização, aspectos Tecnológicos e as Ameaças. Todos esses critérios podem ser considerados grupos separados, que possuem suas próprias características, aqui representadas pelas Alternativas. A tabela 5.5 apresenta como se deu a distribuição dos critérios utilizados no modelo proposto nos artigos analisados.

Tabela 5.5: Distribuição dos artigos com os critérios do modelo proposto

Relacionamentos de Artigos com Critérios do Modelo								
Ano	**Artigo**	**Total**	**Org**	**TD**	**Seg**	**Ativ**	**Tec**	**Ame**
2019	Alzahrani e Johnson [26]	**4**	✓	✓	✓	✓		
	Llansó, McNeil e Noteboom [51]	**5**	✓	✓	✓	✓		✓
	Mustafa e Kar [129]	3	✓			✓		✓
	Zhao et al. [8]	1			✓			
2020	Ansari et al. [130]	**5**		✓	✓	✓	✓	S
	Bhol, Mohanty e Pattnaik [61]	2			✓			✓
	Ribeiro e Canedo [82]	3			✓	✓		✓
	Ganin et al. [24]	**5**	✓	✓	✓		✓	✓

Tabela 5.5: Distribuição dos artigos com os critérios do modelo proposto

Relacionamentos de Artigos com Critérios do Modelo								
	Shojaeshafiei, Etzkorn e Anderson [9]	1			✓			
2021	Abushark et al. [89]	2		✓	✓			
	Alharbi et al. [131]	1			✓			
	Aman e Shukaili [28]	**4**	✓	✓	✓			✓
	Belinda et al. [90]	1			✓			
	Maček et al. [27]	1						✓
	Torbacki [80]	2			✓			✓
	Uraipan, Praneetpolgrang e Manisri [73]	**6**	✓	✓	✓	✓	✓	✓
2022	Abushark et al. [88]	2			✓			✓
	Alfakeeh et al. [132]	3	✓	✓	✓			
	Alshahrani et al. [133]	**5**	✓	✓		✓	✓	✓
	Gonzales et al. [134]	**4**	✓	✓	✓	✓		
	Totais	60	10	10	**17**	8	3	**12**

Fonte: feito pelo Autor

(Legenda: Org - Organização, TD - Tomadores de Decisão, Seg - Segurança, Ati - Ativos, Tec - Tecnologias, Ame - Ameaças)

Há de se destacar a quantidade de artigos que contribuem para os aspectos de Segurança (85%) e Ameaças (60%).

5.2 MÉTODO AHP - PRIORIZANDO OS CRITÉRIOS E ALTERNATIVAS

5.2.1 Comparação pareada de Critérios e Alternativas

Para realizar essa etapa, foram convidados quatro profissionais, **??**, do STJ para que estabelecessem as matrizes de comparação, assim como apontassem os controles que compreendiam necessários para o órgão.

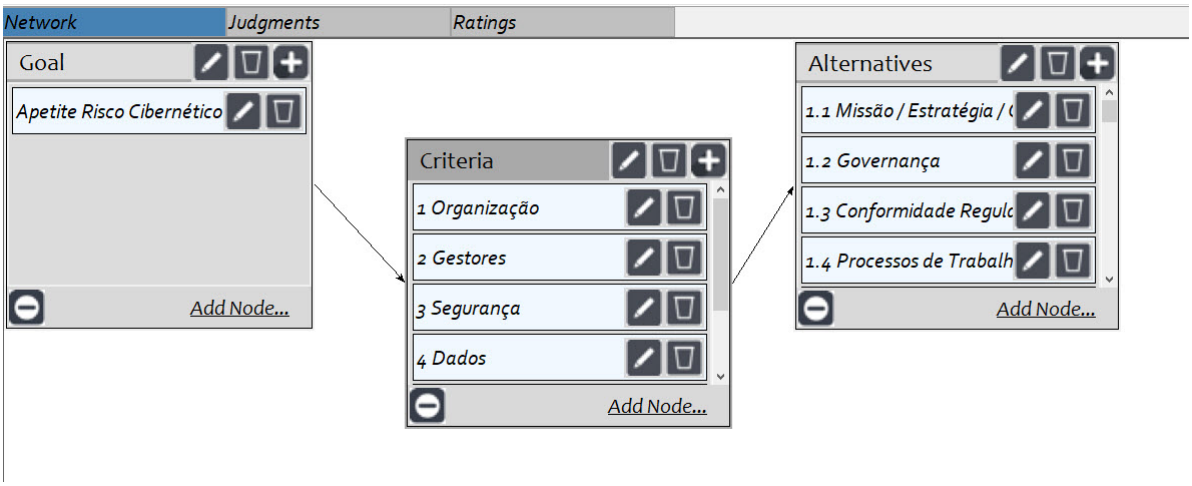
Para isso, utilizou-se o software Super-Decision, criado para comportar o uso do método AHP.

O primeiro passo consistiu na inserção da Meta, dos Critérios e das Alternativas, como pode ser observado na fig. 5.2 apresenta a Meta (Goal), os Critérios (Criteria) e as Alternativas (Alternative).

O passo seguinte dedicou-se a estabelecer os relacionamentos entre a Meta e os Critérios, conforme pode ser observado na fig. 5.3.

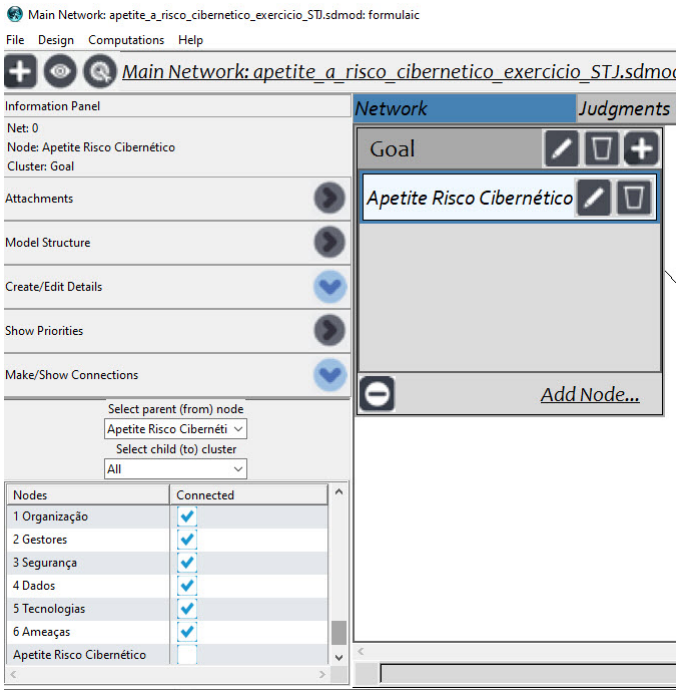
Após Meta e Critérios relacionados, fez-se os relacionamentos entre Critérios e Alternativas, respeitando as regras do modelo estabelecido, como pode ser observado na fig. 5.4.

Figura 5.2: Estrutura Hierárquica no Super-Decisions



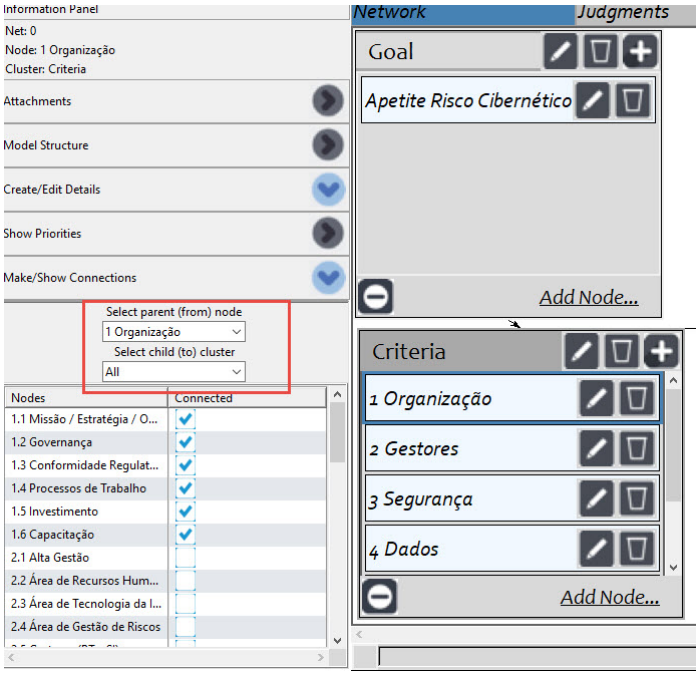
Fonte: do Autor

Figura 5.3: Relacionando Metas e Critérios



Fonte: do Autor

Figura 5.4: Relacionando Critérios e Alternativas

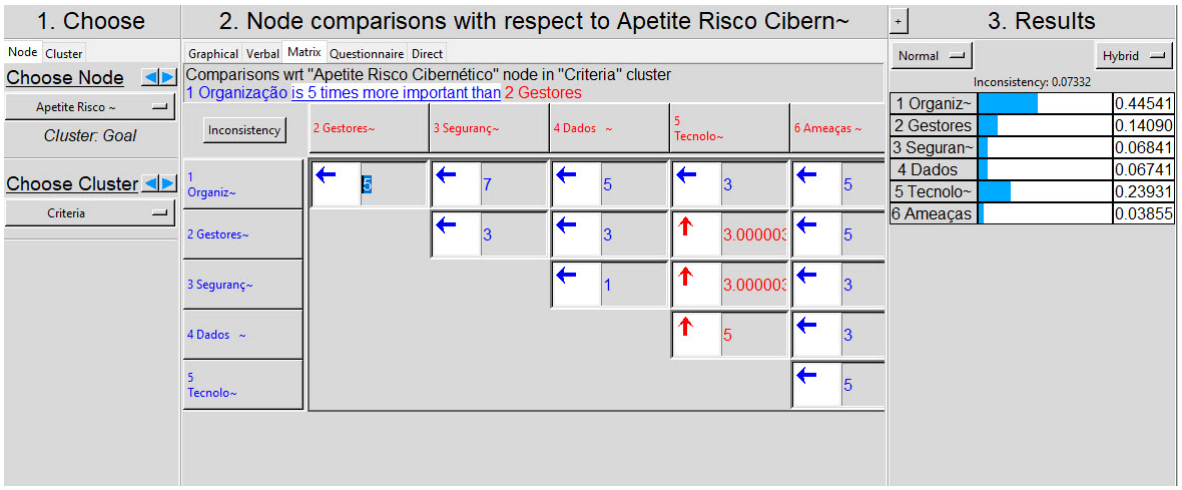


Fonte: do Autor

Comparação Pareada entre Critérios

Após a montagem da árvore hierárquica no software, fez-se a primeira rodada de comparação: os Critérios foram comparados par a par, como pode ser observado na fig. 5.5.

Figura 5.5: Comparação Pareada dos Critérios

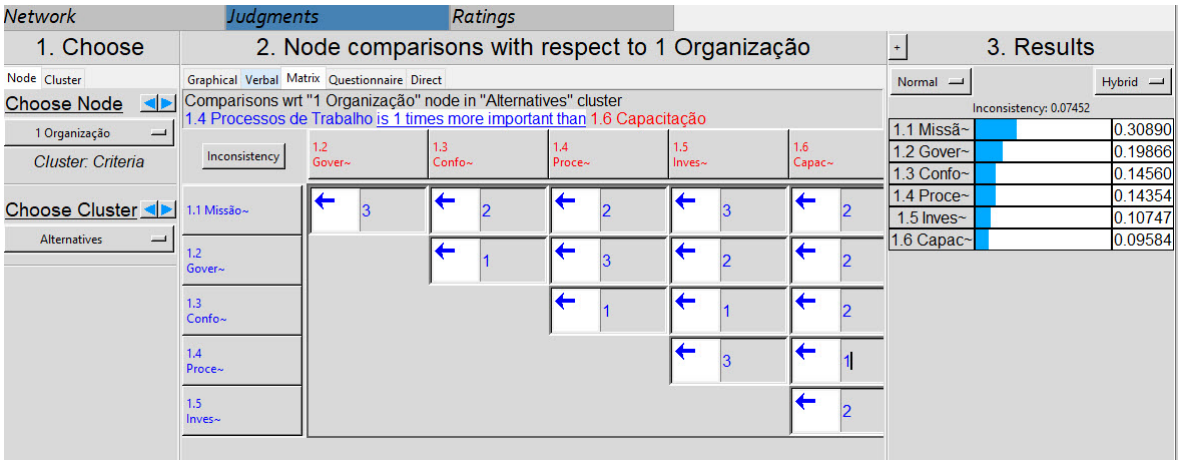


Fonte: do Autor

Comparação Pareada entre Alternativas

O último passo foi realizar as comparações pareadas para cada grupo de Alternativas pertencentes a cada Critério, como pode ser observado o exemplo na fig. 5.6.

Figura 5.6: Comparação Pareada de Alternativas

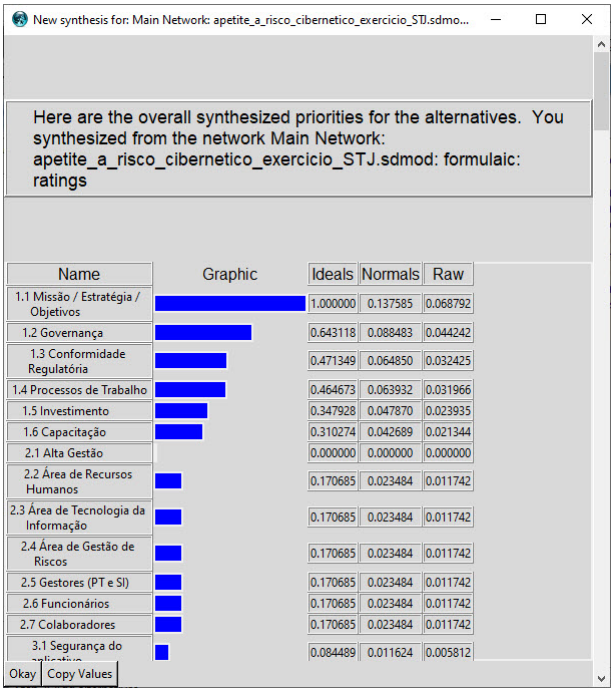


Fonte: do Autor

Executadas todas as comparações pareadas, o processo finalizou com a recuperação dos índices de priorização calculados pelo Super-Decisions, conforme pode ser observado na fig. 5.7.

Após as comparações pareadas, a etapa voltada para o AHP foi finalizada, e os índices gerados foram transferidos para um aplicativo Microsfot Access, feito com o objetivo de centralizar as informações geradas e analisadas na pesquisa.

Figura 5.7: Prioridades para as Alternativas



Fonte: do Autor

5.2.2 Índices alcançados pelos Critérios

Após o exercício de comparação pareada de Critérios e Alternativas, os resultados relativos aos critérios encontram-se na tabela 5.6 e às alternativas encontram-se na tabela 5.7.

Tabela 5.6: Importância dos Critérios

Critério	**%**
1. Organização	35,54%
2. Tomadores de Decisão	23,98%
3. Segurança	16,25%
4. Ativos	9,60%
5. Tecnologias	8,81%
6. Ameaças	5,82%

Para os participantes, o papel da Organização, aí incluído o "Tom que vem de cima", tem o papel mais importante, sendo o principal fator de apetite a risco no que tange à segurança cibernética, seguido pelos Tomadores de Decisão e dos aspectos da Segurança.

5.2.3 Índices alcançados pelas Alternativas

Quando observamos as priorizações relativas às Alternativas, chama-se a atenção o destaque dado às tecnologias ultrapassadas, que se encontra no Critério Tecnologias.

Tabela 5.7: Relação das Alternativas Priorizadas

Alternativa	**%**
1.3 Conformidade Regulatória	19,15%
1.2 Governança	14,22%
5.1 Ultrapassadas	13,58%
1.4 Capacitação	6,36%
5.2 Múltiplas	4,78%
2.3 Gestão de TIC	3,93%
1.5 Investimento	3,76%
5.4 Novas Tecnologias	3,75%
3.2 Rede - LAN e WAN	3,52%
2.5 Gestores (PT e SI)	3,50%
2.1 Funcionários	2,56%
6.1 Incidentes	2,48%
4.2 Resiliência	2,42%
1.1 Missão / Estratégia / Objetivos	2,24%
5.3 Nuvem	1,73%
4.1 Dados - CID	1,68%

Tabela 5.7: Relação das Alternativas Priorizadas

Alternativa	**%**
3.1 Sistema / Aplicativo	1,54%
2.6 Colaboradores	1,45%
4.3 Privacidade	1,34%
3.5 Estação	0,97%
2.4 Gestão de Riscos	0,93%
6.2 Vulnerabilidades	0,72%
2.2 Gestão de Pessoas	0,60%
4.6 Hardware e Software	0,59%
3.3 Usuário	0,56%
4.4 Processos de Trabalho	0,47%
3.4 Física	0,30%
4.5 Pessoas	0,30%
6.3 Ambiente Interno	0,29%
6.4 Ambiente Externo	0,29%
Total	100,00%

5.3 SELEÇÃO DOS CONTROLES DESEJADOS E IMPLEMENTADOS

Os controles utilizados na pesquisa são aqueles dispostos na Estrutura Básica de Segurança Cibernética do NIST [55].

Vide Apêndice 05 - Controles do Modelo Proposto

Estrutura Básica de Segurança Cibernética

A **Estrutura Básica de Segurança Cibernética** (NIST CSF) elaborada pelo NIST [55] é composta por:

- Cinco funções - Identificar (seis categorias), Proteger (seis categorias), Detectar (três categorias), Responder (cinco categorias) e Recuperar (três categorias),
- Vinte e três (23) Categorias, distribuídas nas funções, e
- Cento e oito (108) atividades de controle, distribuídas nas categorias.

Com o propósito de que cada integrante participasse nos apontamentos a respeito dos controles do NIST CSF, fez-se a divisão das cento e oito (108) atividades de controles em quatro grupos: Cadeia de Suprimento, Organização, Infraestrutura e Segurança Cibernética, observado na fig. 5.8. A divisão se deu pela experiência dos participantes ou pela área que atua nesse momento.

Figura 5.8: Distribuição de Controles

Fonte: do Autor

Elaborou-se um aplicativo que permitiu a seleção por parte dos participantes, cabendo a cada um deles, baseando-se nas suas áreas de conhecimento, que apontassem se o controle era desejado pela instituição, assim como se já o possuía em suas práticas, como exemplificado na fig. 5.9.

Figura 5.9: Controles Desejados e Possuídos

		Deseja	Possui	Controle
1	☐	Sim	Não	1.2.1 O papel da organização na cadeia de suprimentos é identificado e comunicado
2	☐	Sim	Não	1.2.2 O lugar da organização na infraestrutura crítica e seu setor industrial é identificadc
3	☐	Sim	Não	1.6.1 Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos sã
4	☐	Sim	Não	1.6.2 Fornecedores e parceiros terceirizados de sistemas de informação, componentes e
5	☐	Sim	Sim	1.6.3 Os contratos com fornecedores e parceiros terceirizados são usados para impleme
6	☐	Sim	Não	1.6.4 Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de
7	☐	Sim	Não	2.2.3 Stakeholders terceirizados entendem suas funções e responsabilidades
8	☐	Sim	Sim	3.2.6 A atividade de provedor de serviços externo é monitorada para detectar possíveis
9	☐	Sim	Não	4.2.1 Os colaboradores conhecem seus papéis e a sequência de operações quando uma
10	☐	Sim	Não	4.2.5 O compartilhamento voluntário de informações ocorre com os stakeholders extern

Fonte: do Autor

Por questões de sigilo, fez-se a opção de não dispor das informações tratadas nessa fase. Salienta-se, contudo, que a equipe que participou dessa fase selecionou cento e seis dos cento e oito controles como desejados, demonstrando um apetite a controle bastante alto por parte da organização.

Na tabela 5.8 estão representados os percentuais de implementação e não implementação dos controles por Categoria do NIST. Observa-se que as prioridades de controles implementados encontram-se nas categorias Proteger (59%), Detectar (78%) e Responder (63%), e onde se concentram a maioria dos controles desejados (71 dos 106 - 67% dos controles).

Tabela 5.8: Resumo Controles Implementados

		Implementado		%	
Categoria	**Total**	**Não**	**Sim**	**Não**	**Sim**
1. Identificar	29	20	9	69%	31%
2. Proteger	37	15	22	41%	59%
3. Detectar	18	4	14	22%	78%
4. Responder	16	6	10	38%	63%
5. Recuperar	6	4	2	67%	33%
Totais	106	49	57	46%	54%

5.4 RELACIONAMENTO ENTRE ALTERNATIVAS E CONTROLES

Exploração do Material

A codificação pretendida, utilizando-se de rótulos e os associando aos textos contidos nas atividades / controles, assim como, uma análise ampla do significado existente na construção da atividade / controle, deve-se à necessidade de tradução dos controles às alternativas, que servirão de rótulos na interpretação pretendida.

Nesse sentido, busca-se a tradução integrativa do que se pretende com o controle respondendo a algumas questões, entre elas:

1. Quem aponta para a necessidade do controle:
   (a) Missão, Visão, Objetivos estratégicos?
   (b) A Governança Institucional?
   (c) Aos Processos de Trabalho / Conformidade Regulatória?
   (d) A Culutura / Capacitação Organizacional?
   (e) Necessidades de Investimentos
2. Quem é o Agente que se utiliza do controle?
   (a) Funcionários?
   (b) A Área de Gestão de Pessoas?
   (c) Gestão de TIC?
   (d) Gestores de Riscos?
   (e) Gestores de Sistemas de Informações / Processos de Trabalho?
   (f) Colaboradores?
3. O controle ou atividade trata de que segurança?
   (a) Aplicativos e Sistemas?
   (b) LAN e WAN?

(c) Usuário?

(d) Da parte Física?

(e) Das Estações de Trabalho?

4. Qual o ativo visado pelo controle?

(a) Dados - CID?

(b) Resiliência

(c) Privacidade

(d) Os Processos de Trabalho?

(e) As Pessoas?

(f) Hardware e Software?

5. Qual tipo de tecnologia é visada?

(a) Ultrapassadas

(b) Múltiplas tecnologias

(c) Nuvem

(d) Novas tecnologias

6. Que Ameaças são visadas?

(a) Incidentes

(b) Vulnerabilidades

(c) Ambiente Interno

(d) Ambiente Externo

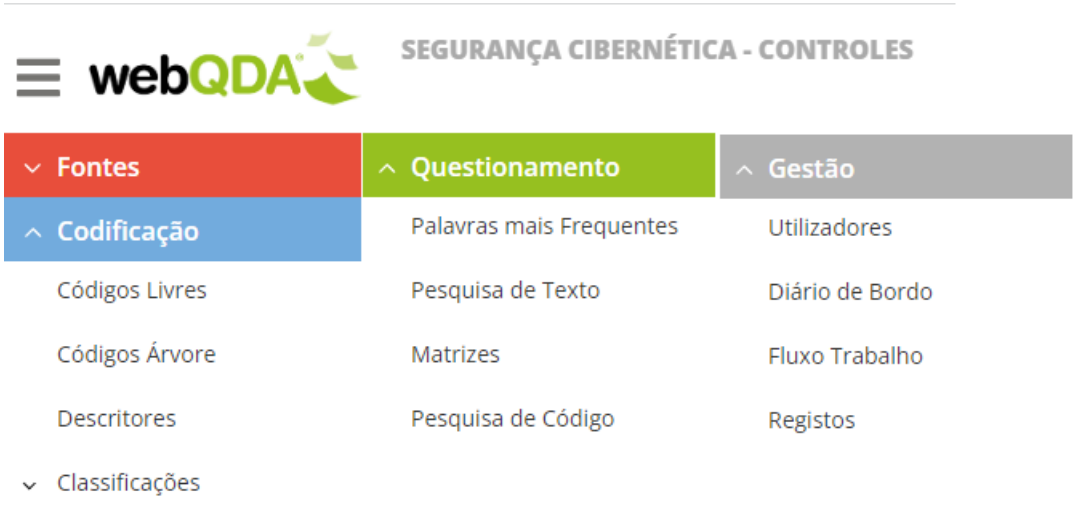
Para realizar a codificação, prevista na análise de conteúdo, utilizou-se do software WebQDA, que disponibiliza uma sistematização do método, com várias funcionalidades e facilidades, conforme a pode ser observado na fig. 5.10.

Elaborou-se a árvore de código, utilizando-se dos Critérios e Alternativas propostos na Macro-Etapa 1, mostrado na fig. 5.11.

Codificar é "um método que permite ao pesquisador organizar e agrupar dados codificados em categorias ou famílias pelo compartilhamento de suas características", mas não se limita apenas em etiquetar o conteúdo, como, também, "conectar o pesquisador dos dados às ideias e das ideias a todos os dados pertencentes a essa ideia" [124, p. 46].

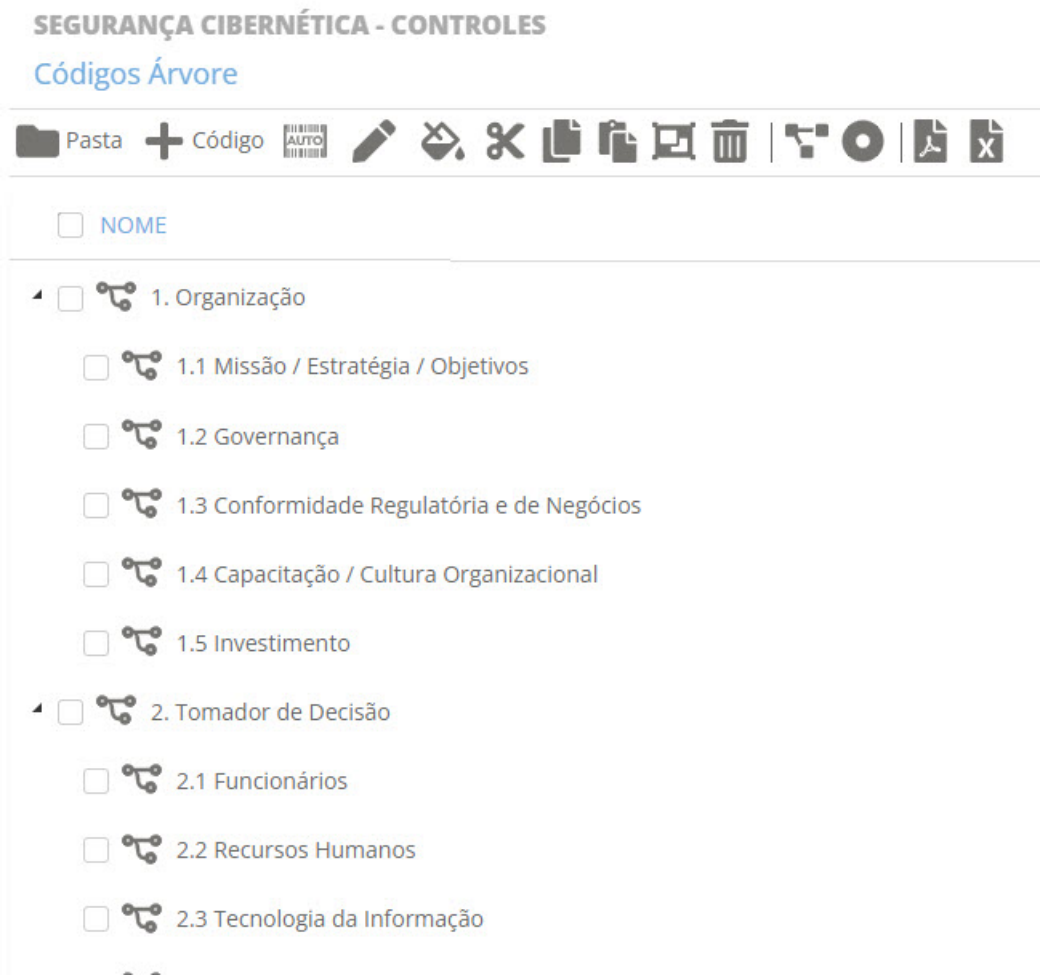
Finalizado o processo de codificação de cada um dos cento e oito controles, as informações foram transportadas para o aplicativo Access, para que pudessem ser usados de forma integrada com os outros dados da pesquisa, podendo ser observado na fig. 5.12.

Figura 5.10: Software WebQDA



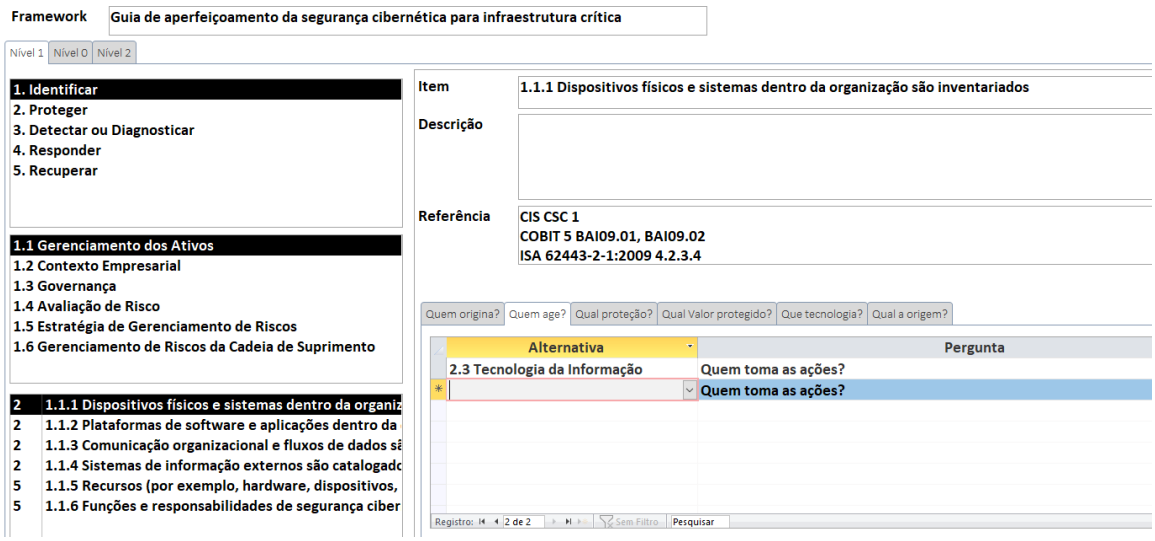
Fonte: Feito pelo Autor

Figura 5.11: Árvore de Códigos no Software WebQDA



Fonte: Feito pelo Autor

Figura 5.12: Migração da Codificação do WebQDA



Fonte: Feito pelo Autor

Tratamento dos Resultados e Interpretação

Os resultados obtidos nessa fase foram utilizados juntamente com a seleção de controles para identificar os percentuais de apetite a risco de cada alternativa presente no modelo. Essas informações serão tratadas nas matrizes que possibilitaram o alcance do índice proposto.

A tabela 5.9 mostra, de forma agrupada por Critérios e Categorias do CSF, como ficaram distribuídas as codificações relativas à fase de Análise de Conteúdo. Organização (146) e Tomadores de Decisão (141) são os dois critérios que mais obtiveram referências, perfazendo 52% das referências, e Proteger (231), Identificar (111) e Detectar (107), foram as três categorias mais referenciadas, perfazendo 81% das referências.

Tabela 5.9: Critérios X Categorias do CSF

Critério	Identificar	Proteger	Detectar	Responder	Recuperar	Totais
Organização	50	43	14	27	12	**146**
Tomadores Decisão	39	44	22	28	8	**141**
Segurança		51	13	4		**68**
Ativos	13	60	15	4	5	**97**
Tecnologias		22	20			**42**
Ameaças	9	11	23	11	6	**60**
Totais	**111**	**231**	**107**	**74**	**31**	**554**

5.5 ANÁLISE COMPORTAMENTAL DO MODELO

Antes da aplicação do modelo AHP, fez-se simulações com o objetivo de avaliar o comportamento do modelo proposto, conforme proposto pela metodologia. Observa-se que o principal foco das simulações consistiu na avaliação do comportamento, independentemente das escolhas tratadas.

Abaixo são apresentados alguns resultados obtidos com variações dos pesos dos Critérios e Alternativas, e com a variação dos Controles selecionados.

5.5.1 Variação dos Pesos dos Critérios e Alternativas

Esse estudo se propôs a analisar o comportamento dos índices alcançados, mantendo-se constante o conjunto de controles de riscos cibernéticos, variando-se os pesos dos critérios e alternativas, sendo criados três modelos de simulação:

Critérios utilizados:

- Quanto aos percentuais do AHP - foram alterados,
- Quanto à seleção dos controles - foram mantidos semelhantes

A hipótese para essa simulação é de que os índices de apetite tenham pequena variação (o apetite está associado à relevância dos controles), mas que as priorizações de alternativas se alterem (organizações diferentes possuem prioridades diferentes). Caso se confirme, entende-se que o método atende à expectativa de se moldar às prioridades estabelecidas pela organização.

5.5.2 Variação do conjunto de controles diferentes

Esse estudo se propôs a analisar o comportamento dos índices alcançados pelo modelo, mantendo-se constantes os pesos dos critérios e alternativas, variando-se as seleções do conjunto de controles de riscos cibernéticos.

Critérios utilizados:

- Quanto aos percentuais do AHP - foram mantidos semelhantes
- Quanto à seleção dos controles - foram alterados

A hipótese para essa simulação é de que os índices de apetite variem em virtude dos controles selecionados, mas as priorizações das alternativas mantenham-se semelhantes. Caso se confirme, entende-se que o método atende à expectativa da relevância dos controles na gestão de riscos cibernéticos.

5.5.3 Conclusão da Análise

Após as simulações, concluiu-se que o modelo comportou-se segundo as hipóteses estabelecidas, sendo relevante anotar que a medida de apetite a risco cibernético está altamente correlacionada com os controles selecionados, podendo ter uma variação alta, quando selecionamos um conjunto de controles distintos. Por outro lado, quando desejamos identificar as priorizações, motivo pelo qual o AHP se faz presente, a variação de prioridades se demonstra alinhada com a variação dos pesos de Critérios e Alternativas.

5.6 A MEDIDA DE APETITE A RISCO CIBERNÉTICO

Essa seção destina-se à apresentação da proposta do modelo de mensuração do apetite a riscos cibernéticos de uma organização, a partir de um conjunto de controles voltados para a segurança cibernética, empregando um modelo de apoio à decisão, o AHP, com foco na priorização na aplicação dos controles.

5.6.1 Passo a Passo para chegar na Medida de Apetite a Risco Cibernético - MARC

Para a realização dos cálculos até a obtenção do índice almejado, Medida de Apetite ao Risco Cibernético (MARC), foram utilizadas as seguintes matrizes:

1. **Matriz de Alternativas (Al)**
   Contém as 30 alternativas
   Coluna **Al** da tabela 5.10

2. **Matriz de Controles (Cn)**
   Contém os 108 controles.
   Vide Apêndice 05 - Controles do Modelo Proposto

3. **Matriz de Priorização das Alternativas (Pr)**
   Contém o percentual alcançado no AHP das 30 alternativas
   Coluna **Pr** da tabela 5.10

4. **Matriz de Relacionamentos entre as Alternativas e os Controles (Rac)**
   Contém 30 X 108 relacionamentos.
   Quando $\boldsymbol{Rac}_{i,j}$ for 0 ou nulo, isso significa que não há relacionamento entre a Alternativa a_i e o Controle c_j, e se for 1, há o relacionamento.
   Vide Apêndice 06 - Lista dos Relacionamentos entre Controles e Alternativas

5. **Matriz Somatório de Controles Referenciados da Alternativa (Sra)**
   Contém a quantidade de controles que foram referenciados por Alternativa.
   Coluna **Sra** da tabela 5.10

6. **Matriz de Controles Desejados (Ds)**
   Contém a informação se o Controle foi ou não selecionado como desejado.
   Quando d_j for 0 ou nulo, isso significa que o Controle não é desejado, e se for 1 ele é desejado.
   Essa informação não foi disponibilizada por questões de sigilo.

7. **Matriz de Controles Possuídos (*Ps*)**
   Contém a informação se o Controle foi ou não selecionado como possuído.
   Quando p_j for 0 ou nulo, isso significa que o Controle não é desejado, e se for 1 ele consta como implementado no órgão.
   Essa informação não foi disponibilizada por questões de sigilo.

8. **Matriz Somatório de Controles Desejados da Alternativa (*Scd*)**
   Contém a quantidade de controles desejados de cada Alternativa.
   Resultante da multiplicação de $\boldsymbol{Rac}$ X $\boldsymbol{Ds}$.
   Coluna **Scd** da tabela 5.10

9. **Matriz Somatório de Controles Possuídos da Alternativa (*Sps)***
   Contém a quantidade de controles desejados de cada Alternativa.
   Resultante da multiplicação de $\boldsymbol{Rac}$ X $\boldsymbol{Ps}$.
   Coluna **Sps** da tabela 5.10

Matriz $\boldsymbol{Rac}$ - Relacionamento Alternativas X Controles

Essa matriz foi criada por meio da Análise de Conteúdo, conforme a metodologia proposta. Cada elemento $r_{i,j}$ representa o relacionamento entre a Alternativa a_i com o Controle c_j, podendo ser 1 quando houver a referência, e nulo quando não houver. A soma de todos os r_{ij} de uma determinada **linha** *i* indicará o total de controles que uma determinada alternativa foi referenciada. A soma de todos os r_{ij} de uma determinada **coluna** *j* indicará o total de alternativas que um determinado controle foi referenciado.

$$Rac = \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} & r_{1,4} & \cdots & r_{1,108} \\ r_{2,1} & r_{2,2} & r_{2,3} & r_{2,4} & \cdots & r_{2,108} \\ r_{3,1} & r_{3,2} & r_{3,3} & r_{3,4} & \cdots & r_{3,108} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{30,1} & r_{30,2} & r_{30,3} & r_{30,4} & \cdots & r_{30,108} \end{bmatrix}$$

Matriz $\boldsymbol{Ds}$ - Deseja o Controle

Essa matriz corresponde a seleção feita pelos profissionais que participaram da pesquisa, quando da identificação se o controle era desejado ou não. Cada elemento d_i representa o desejo por determinado controle c_i, podendo ser 1 quando houver o desejo, e 0 quando não houver.

$$\boldsymbol{Ds} = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_{108} \end{bmatrix}$$

Matriz $\boldsymbol{Ps}$ - Possui o Controle

Essa matriz corresponde a seleção feita pelos profissionais que participaram da pesquisa, quando da identificação se o controle estava implementado ou não. Cada elemento p_i representa se a organização possui o controle c_i, implementado, podendo ser 1 quando possui, e 0 quando não estiver implementado.

$$\boldsymbol{Ps} = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_{108} \end{bmatrix}$$

Matriz $\boldsymbol{Sra}$ - Somatório de Controles da Alternativa

Essa matriz representa a quantidade de controles que fazem referência a cada uma das alternativas. A soma de todos os r_{ij} de $\boldsymbol{Rac}$ de uma determinada linha i indicará o total de controles da alternativa a_i.

$$\boldsymbol{Sra} = \begin{bmatrix} 24 & 36 & 70 & 12 & \cdots & 17 \end{bmatrix}$$

Matriz $\boldsymbol{Scd}$ - Somatório de Controles Desejados da Alternativa

Essa matriz representa a quantidade de controles que fazem referência a cada uma das alternativas e que foram apontados como desejados pelos profissionais envolvidos.

$$\boldsymbol{Scd} = \begin{bmatrix} 24 & 36 & 70 & 12 & \cdots & 17 \end{bmatrix}$$

Matriz $\boldsymbol{Sps}$ - Somatório de Controles Possuídos da Alternativa

Essa matriz representa a quantidade de controles que fazem referência a cada uma das alternativas e que foram apontados como integrantes das práticas atuais pelos profissionais envolvidos.

$$\boldsymbol{Sps} = \begin{bmatrix} 8 & 12 & 38 & 4 & \cdots & 12 \end{bmatrix}$$

Matrizes $\boldsymbol{Snd}$, $\boldsymbol{Snp}$ e $\boldsymbol{Srs}$

A matriz $\boldsymbol{Snd}$ é resultado da subtração de $\boldsymbol{Sra}$ e $\boldsymbol{Scd}$, ou seja, informa a quantidade de referências dos controles que não foram considerados como desejados. Essa informação é relevante à medida que o seu valor seja expressivo, uma vez que significará que uma quantidade alta de controles não são desejados. Quanto menor for o somatório de referências não desejadas, mais apetite a controles essa organização demonstra ter. Deve-se salientar, entretanto, que não se pode inferir que um número alto significará que aumenta o apetite a risco, mas apenas significa que tais controles não foram considerados relevantes para a realidade da empresa, conforme observado na Estrutura Básica de Segurança Cibernética do NIST [55].

Semelhante à matriz $\boldsymbol{Snd}$, a $\boldsymbol{Snp}$ é resultado da subtração de $\boldsymbol{Sra}$ e $\boldsymbol{Sps}$, ou seja, informa a quantidade de referências aos controles que não foram considerados como implementados.

A matriz $\boldsymbol{Srs}$ é a mais relevante para a medida de apetite a risco cibernético, pois indica a diferença

entre a quantidade de referências a controles que são desejados (matriz $\boldsymbol{Scd}$) e que foram implementados (matriz $\boldsymbol{Sps}$), que consideraremos como o gap do apetite a risco cibernético.

A matriz $\boldsymbol{Gap}$ é a resultante entre a divisão da $\boldsymbol{Srs}$ e $\boldsymbol{Scd}$, demonstrando, percentualmente, o que falta ser atendido em relação aos controles desejados e não possuídos.

Para se obter o índice MARC, representado pela matriz $\boldsymbol{MARC}$, utilizou-se o peso relativo da alternativa constante na matriz $\boldsymbol{Pr}$ pelo gap encontrado em cada uma das alternativas, representado pela matriz $\boldsymbol{Gap}$. Para o caso em estudo, o MARC do STJ poderá ser observado na última linha da tabela 5.10, com valor de 41,1%.

Tabela 5.10: Distribuição das Matrizes

Alternativa	**Pr**	**Sra**	**Scd**	**Sps**	**Srs**	**Gap**	**MARC**	**Snd**	**Snp**
1.1 Missão/Estratégia/Objetivos	2,2%	24	24	8	16	66,7%	1,5%		16
1.2 Governança	14,2%	36	36	12	24	66,7%	9,5%		24
1.3 Conform. Regul. e Negócios	19,2%	70	70	38	32	45,7%	8,8%		32
1.4 Capacitação/Cultura Organ.	6,4%	12	12	4	8	66,7%	4,2%		8
1.5 Investimento	3,8%	4	4	2	2	50,0%	1,9%		2
2.1 Funcionários	2,6%	4	4	1	3	75,0%	1,9%		3
2.2 Recursos Humanos	0,6%	1	1		1	100,0%	0,6%		1
2.3 Tecnologia da Informação	3,9%	92	90	54	36	40,0%	1,6%	2	38
2.4 Gestão de Riscos	0,9%	29	29	11	18	62,1%	0,6%		18
2.5 Gestores (PT e SI)	3,5%	2	2	2	0	0,0%	0,0%		
2.6 Colaboradores	1,4%	13	13	4	9	69,2%	1,0%		9
3.1 Sistema / Aplicativo	1,5%	20	20	15	5	25,0%	0,4%		5
3.2 Rede - LAN e WAN	3,5%	15	15	12	3	20,0%	0,7%		3
3.3 Usuário	0,6%	10	10	8	2	20,0%	0,1%		2
3.4 Física	0,3%	10	10	9	1	10,0%	0,0%		1
3.5 Estação	1,0%	13	13	10	3	23,1%	0,2%		3
4.1 Dados - CID	1,7%	20	19	14	5	26,3%	0,4%	1	6
4.2 Resiliência	2,4%	12	12	6	6	50,0%	1,2%		6
4.3 Privacidade	1,3%	8	8	6	2	25,0%	0,3%		2
4.4 Processos de Trabalho	0,5%	22	22	9	13	59,1%	0,3%		13
4.5 Pessoas	0,3%	9	9	5	4	44,4%	0,1%		4
4.6 Hardware e Software	0,6%	26	24	17	7	29,2%	0,2%	2	9
5.1 Ultrapassadas	13,6%	13	13	10	3	23,1%	3,1%		3
5.2 Múltiplas	4,8%	5	5	5	0	0,0%	0,0%		
5.3 Nuvem	1,7%	12	12	10	2	16,7%	0,3%		2
5.4 Novas Tecnologias	3,8%	12	12	9	3	25,0%	0,9%		3
6.1 Incidentes	2,5%	21	21	14	7	33,3%	0,8%		7
6.2 Vulnerabilidades	0,7%	6	6	4	2	33,3%	0,2%		2
6.3 Ambiente Interno	0,3%	16	16	11	5	31,3%	0,1%		5
6.4 Ambiente Externo	0,3%	17	17	12	5	29,4%	0,1%		5
		554	**549**	**322**	**227**	**41,3%**	**41,1%**	**5**	**232**

Tabela 5.11: Prioridades: AHP X MARC

Prioridades AHP		**Prioridades MARC**		
Alternativa	**AHP**	**MARC**	**MARCr**	**Alternativa**
1.3 Conform. Regul. de Negócios	19,2%	9,5%	23,0%	1.2 Governança
1.2 Governança	14,2%	8,8%	21,3%	1.3 Conform. Regul. de Negócios
5.1 Ultrapassadas	13,6%	4,2%	10,3%	1.4 Capacitação/Cultura Organiz.
1.4 Capacitação/Cultura Organiz.	6,4%	3,1%	7,6%	5.1 Ultrapassadas
5.2 Múltiplas	4,8%	1,9%	4,7%	2.1 Funcionários
2.3 Tecnologia da Informação	3,9%	1,9%	4,6%	1.5 Investimento
1.5 Investimento	3,8%	1,6%	3,8%	2.3 Tecnologia da Informação
5.4 Novas Tecnologias	3,8%	1,5%	3,6%	1.1 Missão/Estratégia/Objetivos
3.2 Rede - LAN e WAN	3,5%	1,2%	2,9%	4.2 Resiliência
2.5 Gestores (PT e SI)	3,5%	1,0%	2,4%	2.6 Colaboradores
2.1 Funcionários	2,6%	0,9%	2,3%	5.4 Novas Tecnologias
6.1 Incidentes	2,5%	0,8%	2,0%	6.1 Incidentes
4.2 Resiliência	2,4%	0,7%	1,7%	3.2 Rede - LAN e WAN
1.1 Missão/Estratégia/Objetivos	2,2%	0,6%	1,5%	2.2 Recursos Humanos
5.3 Nuvem	1,7%	0,6%	1,4%	2.4 Gestão de Riscos
4.1 Dados - CID	1,7%	0,4%	1,1%	4.1 Dados - CID
3.1 Sistema / Aplicativo	1,5%	0,4%	0,9%	3.1 Sistema / Aplicativo
2.6 Colaboradores	1,4%	0,3%	0,8%	4.3 Privacidade
4.3 Privacidade	1,3%	0,3%	0,7%	5.3 Nuvem
3.5 Estação	1,0%	0,3%	0,7%	4.4 Processos de Trabalho
2.4 Gestão de Riscos	0,9%	0,2%	0,6%	6.2 Vulnerabilidades
6.2 Vulnerabilidades	0,7%	0,2%	0,5%	3.5 Estação
2.2 Recursos Humanos	0,6%	0,2%	0,4%	4.6 Hardware e Software
4.6 Hardware e Software	0,6%	0,1%	0,3%	4.5 Pessoas
3.3 Usuário	0,6%	0,1%	0,3%	3.3 Usuário
4.4 Processos de Trabalho	0,5%	0,1%	0,2%	6.3 Ambiente Interno
3.4 Física	0,3%	0,1%	0,2%	6.4 Ambiente Externo
4.5 Pessoas	0,3%	0,0%	0,1%	3.4 Física
6.3 Ambiente Interno	0,3%	0,0%	0,0%	2.5 Gestores (PT e SI)
6.4 Ambiente Externo	0,3%	0,0%	0,0%	5.2 Múltiplas
	100,0%	41,1%	100,0%	

5.6.2 Diferenças das Prioridades AHP e MARC

Após a aplicação do modelo proposto, é possível ver que a lista de prioridades sofre alguns ajustes, em boa parte em função da existência / inexistência de controles implementados. O MARC reforça a necessidade de se implantar novos controles, apontando às Alternativas que encontram-se carentes. Na tabela 5.11 podemos observar essa mudança. A coluna MARCr representa o peso relativo do MARC da alternativa em relação ao MARC organizacional (41,1%). A título de exemplo, o MARC da Governança é de 9,5% e seu MARCr é de 23,0%, representando quase um quarto do apetite a risco cibernético medido, de 41,1%.

5.7 PRINCIPAIS FRAMEWORKS VOLTADOS À SEGURANÇA CIBERNÉTICA

No **Apêndice 02 - Frameworks Utilizados e Citados** encontram-se dispostos os *frameworks* citados pelos artigos avaliados.

A seguir são enumerados os principais *frameworks* referenciados nos artigos que serviram de base para a pesquisa. Os *frameworks* estão dispostos em ordem alfabética, sendo colocado entre parênteses a quantidade de documentos que foram referenciados.

1. **BYOD (3) -** ***Bring Your Own Device***
   Política popular no local de trabalho que permite que os funcionários usem seus dispositivos pessoais, como *smartphones*, *tablets* e *laptops*, para fins de trabalho.

2. **COBIT (9) -** ***Control Objectives for Information Technologies***
   Fornece uma estrutura abrangente para governança e gerenciamento de TI em organizações.

3. **CORAS (4) -** ***Conceptual Modelling for Risk Analysis and Security***
   É uma estrutura para análise e mitigação de riscos usada em vários setores, incluindo tecnologia da informação, aeroespacial e defesa. A estrutura foi projetada para ajudar as organizações a identificar, avaliar e mitigar os riscos associados a suas operações, projetos e sistemas.

4. **COSO (2) -** ***The Comitee of Sponsoring Organizations***
   Estrutura amplamente reconhecida para controle interno, gerenciamento de riscos corporativos e prevenção de fraudes. COSO é a sigla para *Committee of Sponsoring Organizations of the Treadway Commission* (Comitê de Organizações Patrocinadoras da Comissão Treadway), uma iniciativa conjunta de cinco organizações do setor privado que foi criada nos Estados Unidos.

5. **CRAMM (2) - CCTA** ***Risk Analysis and Management Method***
   Estrutura de avaliação e gerenciamento de riscos desenvolvida pela *Central Computer and Telecommunications Agency* (CCTA) do governo do Reino Unido. Ele foi projetado para ajudar as organizações a avaliar os riscos associados aos seus sistemas de TI e fornecer uma abordagem estruturada para gerenciar esses riscos.

6. **CVSS (5) -** ***Common Vulnerability Scoring System***
   Estrutura usada para avaliar e comunicar a gravidade das vulnerabilidades em sistemas e redes de computadores. Ela foi projetada para fornecer um método padronizado e objetivo para avaliar o impacto das vulnerabilidades de segurança.

7. **FAIR (6) -** ***Factor Analysis of Information Risk***
   Metodologia de quantificação de riscos criada para ajudar as empresas a avaliar os riscos da informação. O FAIR é a única estrutura de modelo quantitativo padrão internacional que oferece risco operacional e segurança da informação.

8. **ICS (4) -** ***Industrial Control Systems security***
   Sistemas controlados por computador que gerenciam processos industriais, como fabricação, produ-

ção de energia e transporte. Devido à natureza crítica desses sistemas, garantir sua segurança é de extrema importância.

9. **ISMS (2) - *Information Security Management System***
   Estrutura de políticas e controles que gerenciam a segurança e os riscos de forma sistemática e em toda a empresa - segurança da informação.

10. **ISO 27000 (8)**
    Conjunto de certificações de segurança da informação e proteção de dados para empresas e órgãos públicos

11. **ISO 27001 (19)**
    Padrão e a referência Internacional para a gestão da Segurança da informação

12. **ISO 27002 (10)**
    Norma internacional que estabelece as diretrizes e boas práticas para a gestão da segurança da informação em uma organização

13. **ISO 27005 (16)**
    Descreve um processo de gerenciamento de riscos que as organizações podem usar para identificar e avaliar os riscos à segurança da informação

14. **ISO 31000 (9)**
    Fornece um conjunto de princípios, estrutura e processos para a gestão de riscos eficaz em qualquer organização.

15. **ISO 31010 (5)**
    Guia internacional que estabelece princípios e diretrizes para a gestão de riscos, fornecendo uma estrutura para a avaliação de riscos em diversos setores e contextos.

16. **ISRM (3)** - *Information security risk management*
    Processo de identificação, avaliação e controle dos riscos associados aos sistemas de informação

17. **KRI (6)** - *Key Risk Indicators*
    Um documento ou um conjunto de documentos que incluem seções para histórico e projeto, identificação, gerenciamento de limites ou gatilhos, monitoramento, uso e relatórios, eficácia e governança do programa.

18. **MAGERIT (2)** - *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*
    Metodologia de gerenciamento de riscos desenvolvida pelo *Centro Criptológico Nacional* (CCN) da Espanha para ajudar as organizações a avaliar e gerenciar os riscos de segurança da informação.

19. **NICE (2)** - *National Initiative for Cybersecurity Education*
    Tem como objetivo fornecer uma linguagem e um padrão comuns para a educação, o treinamento e o desenvolvimento da força de trabalho em segurança cibernética.

20. **NIST 800-30 (10)**
    Projetado para ajudar as organizações a identificar, avaliar e gerenciar os riscos para suas informações e sistemas de informação.

21. **NIST 800-37 (3)**
    Fornece orientação e diretrizes para a gestão de riscos de segurança da informação em organizações governamentais e não governamentais.

22. **NIST 800-53 (8)**
    Fornece um conjunto abrangente de controles de segurança para sistemas e organizações de informações federais.

23. **NIST 800-55 (2)**
    Fornece orientação sobre como uma organização pode usar métricas para identificar a adequação de controles, políticas e procedimentos de segurança no local.

24. **NIST CSF (10)**
    Estrutura voluntária que fornece às organizações orientações sobre como gerenciar e reduzir os riscos de segurança cibernética. A estrutura foi criada em resposta à Ordem Executiva 13636, que solicitou o desenvolvimento de uma estrutura para melhorar a segurança cibernética da infraestrutura crítica.

25. **NIST *National Vulnerability Database* (2)**
    É um banco de dados abrangente de vulnerabilidades e exposições de segurança. Ele é mantido pelo NIST e é um repositório de informações sobre vulnerabilidades de segurança de várias fontes, incluindo pesquisadores de segurança, fornecedores e outras organizações.

26. **OWASP (3) - *Open Web Application Security Project***
    Fornece aos desenvolvedores de software uma lista de melhores práticas e ferramentas para garantir a segurança dos aplicativos web.

27. **SABSA (3) - *Sherwood Applied Business Security Architecture***
    Fornece uma estrutura para a arquitetura de segurança que possa ser adaptada às necessidades específicas de uma organização.

28. **SQUARE (3) - *Security Quality Requirements Engineering***
    Ajuda as organizações a desenvolver e manter sistemas de software seguros, fornecendo orientações e práticas recomendadas.

29. **SRE (2) - *Site reliability engineering***
    Busca garantir a confiabilidade, resiliência e segurança dos sistemas de software, por meio da aplicação de práticas e processos de segurança em todas as etapas do ciclo de vida do desenvolvimento de software.

30. **SSM (2) - *Systems Manager***
    Conjunto de serviços da AWS que permite gerenciar e automatizar tarefas operacionais nos seus recursos da AWS. A segurança é um aspecto fundamental da estrutura do SSM, e a AWS oferece vários recursos e práticas recomendadas para ajudá-lo a garantir a segurança dos recursos gerenciados pelo SSM.

31. **STORE (5) - *Security, Trust, and Oversight for Research and Engagement***
    Conjunto de princípios e práticas criados para promover o uso responsável de dados em atividades

de pesquisa e engajamento. Quando se trata de segurança, a estrutura enfatiza vários princípios fundamentais.

32. **TARA (2) - *Trustworthy and Resilient Authorization***
    Projetado para aprimorar a segurança dos sistemas de autorização em sistemas distribuídos. Seu objetivo é enfrentar os desafios associados ao gerenciamento e à segurança das políticas de controle de acesso, especialmente em ambientes complexos e dinâmicos.

5.8 RELAÇÃO DOS CONTROLES QUE MINIMIZAM O APETITE A RISCO CIBERNÉTICO

A identificação dos Controles que minimizam o Apetite a Risco se deu seguindo-se os seguintes passos:

1. **Criação do Índice Unitário da Alternativa (IUA)**
   Consiste em dividir o percentual alcançado pela Alternativa (constantes na matriz $\boldsymbol{Pr}$) pela quantidade de controles desejados na Alternativa (constantes na matriz $\boldsymbol{Scd}$) multiplicando o valor alcançado por 1.000 (mil). A multiplicação por 1.000 se deu para termos números mais expressivos.
   O resultado pode ser observado na tabela 5.12

2. **Distribuição do IUA nos Controles**
   Consiste em distribuir em cada controle desejado os IUA, gerando um somatório para cada controle, chamado de Índice de Participação do Controle (IPC).
   O IPC traz o grau de relevância do Controle na diminuição do MARC.
   O resultado pode ser observado na tabela 5.13
   As linhas em destaque representam os Controles que precisam ser implementados por ordem de relevância na construção da Medida de Apetite a Risco Cibernético. São os controles que mais contribuirão para a diminuição do MARC.

Tabela 5.12: Índice Unitário da Alternativa

Al	Pr	Scd	IUA
1.1 Missão / Estratégia / Objetivos	2,2%	24	0,93
1.2 Governança	14,2%	36	3,95
1.3 Conformidade Regulatória e de Negócios	19,2%	70	2,74
1.4 Capacitação / Cultura Organizacional	6,4%	12	5,30
1.5 Investimento	3,8%	4	9,40
2.1 Funcionários	2,6%	4	6,40
2.2 Recursos Humanos	0,6%	1	6,03
2.3 Tecnologia da Informação	3,9%	90	0,44
2.4 Gestão de Riscos	0,9%	29	0,32
2.5 Gestores (PT e SI)	3,5%	2	17,50

Tabela 5.12: Índice Unitário da Alternativa

Al	Pr	Scd	IUA
2.6 Colaboradores	1,4%	13	1,11
3.1 Sistema / Aplicativo	1,5%	20	0,77
3.2 Rede - LAN e WAN	3,5%	15	2,35
3.3 Usuário	0,6%	10	0,56
3.4 Física	0,3%	10	0,30
3.5 Estação	1,0%	13	0,74
4.1 Dados - CID	1,7%	19	0,88
4.2 Resiliência	2,4%	12	2,02
4.3 Privacidade	1,3%	8	1,68
4.4 Processos de Trabalho	0,5%	22	0,21
4.5 Pessoas	0,3%	9	0,33
4.6 Hardware e Software	0,6%	24	0,25
5.1 Ultrapassadas	13,6%	13	10,45
5.2 Múltiplas	4,8%	5	9,55
5.3 Nuvem	1,7%	12	1,44
5.4 Novas Tecnologias (IA, Big Data, 5G, IoT)	3,8%	12	3,13
6.1 Incidentes	2,5%	21	1,18
6.2 Vulnerabilidades	0,7%	6	1,20
6.3 Ambiente Interno	0,3%	16	0,18
6.4 Ambiente Externo	0,3%	17	0,17

A tabela 5.13 além de estabelecer uma ordem de priorização da implantação dos controles visando à diminuição do MARC, é possível observar se a implementação dos Controles está sendo feita de forma adequada, levando-se em consideração aos pesos dados às alternativas. O ideal é que os Controles que mais têm pesos já estejam implementados, demonstrando o alinhamento da área operacional com as expectativas estratégicas.

Tabela 5.13: Exemplificação da relação de Controles Priorizados pelo Modelo Proposto

Controle	IPC	Possui?
2.5.1 Manutenção e reparo de ativos organizacionais ...	37,57	✓
2.6.5 Alguns mecanismos são implementados para ...	30,69	✓
5.3.3 As atividades de recuperação são comunicadas ...	28,77	✓
2.5.2 A manutenção remota de ativos organizacionais ...	28,32	✓
3.3.3 Os processos de detecção são testados	27,95	✓
3.2.1 A rede é monitorada para detectar potenciais inc...	27,09	✓
2.6.1 Os registros de auditoria/registro são determ ...	**25,69**	
2.6.2 As mídias removíveis são protegidas e seu uso ...	**23,32**	
3.3.5 Processos de detecção são continuamente aperfei „	22,35	✓
2.1.1 Identidades e credenciais são emitidas, gerenciad ...	22,02	✓

Tabela 5.13: Exemplificação da relação de Controles Priorizados pelo Modelo Proposto

Controle	IPC	Possui?
2.6.3 O princípio de menor funcionalidade é incorpo ...	**20,05**	
3.3.4 Informações de detecção de incidente são comunic...	19,36	✓
2.6.4 Redes de comunicação e controle são protegidas	18,00	✓
3.2.5 Código móvel não autorizado é detectado	**17,73**	
3.2.4 Código malicioso é detectado	17,73	✓
...		
...		
1.1.2 Plataformas de software e aplicações dentro ...	**0,68**	

6 CONCLUSÃO

O atual estudo exigiu que se buscasse uma visão holística e integrada dos elementos que cercam o apetite a risco cibernético, devendo-se levar em consideração as expectativas organizacionais com o uso do espaço cibernético, os objetivos organizacionais, a sua cultura, o papel do conselho administrativo, as relações com fornecedores que estão entrelaçados na cadeia de suprimento, os tomadores de decisão que fazem parte do corpo técnico e gerencial, dos colaboradores, das proteções advindas de investimentos, dos ativos organizacionais, sem deixar de lado as ameaças, sejam internas ou externas, assim como os aspectos de segurança praticados na instituição com seus controles, práticas e soluções, sejam de hardware, software ou físicas. A segurança cibernética trata-se de uma responsabilidade exercida de forma distribuída, tanto interna como externamente à área de TI, sendo, muitas vezes, necessário que se priorize o compartilhamento de informações a seu respeito.

A Gestão de Riscos tradicional, embora sendo tratada, muitas vezes, como inadequada para o mundo cibernético (autores acabam por destacar as limitações das matrizes de risco tradicionais, propondo alternativas mais abrangentes e eficazes), ela se demonstra uma ferramenta organizacional extremamente importante, em especial quando integrada à Gestão de Riscos Cibernéticos. O aumento dos desafios relacionados à Gestão de Riscos Cibernéticos têm levado as Nações ao fomento de iniciativas que visam ao compartilhamento tanto de informações como de iniciativas: sabe-se da relevância que o ambiente cibernético e das novas tecnologias na competitividade internacional e nas melhorias dos serviços prestados à sociedade, mas essa relevância traz consigo inúmeros riscos à infraestrutura crítica que necessitam ser observados e tratados. A Gestão de Riscos Cibernéticos, como como pode ser observada em muitos artigos, deve ser tratada de forma multidisciplinar, um processo cognitivo que variará de população para população, de organização para organização, e até mesmo de profissões. A Gestão de Riscos necessita ter uma abordagem que possa lidar com diferentes tipos de requisitos regulatórios, incluindo obrigações, proibições e condições extintas. Elementos humanos e comportamentais foram identificados como críticos na gestão de risco cibernético nas cadeias de suprimentos, sendo necessária uma maior atenção a esses fatores. Pode-se perceber, com o estudo, que a Gestão de Riscos Cibernéticos carece de avanços e que tal carência tem uma relação intrínseca à sua própria natureza: a mutabilidade imposta por introdução de inúmeras e novas tecnologias acabam por impedir uma visão concreta dos problemas e desafios enfrentados. Os elementos comportamentais dentro dos riscos de segurança cibernética são considerados críticos, mas têm recebido pouca atenção, sendo necessária a elevação da conscientização sobre os riscos, políticas padronizadas, estratégias colaborativas e modelos empíricos para criar uma cultura de segurança cibernética. Tanto a governança institucional quanto à de TI são requisitos relevantes no tratamento da segurança cibernética, devendo existir uma participação efetiva dos *stakeholders* no processo de formulação de políticas de gestão de riscos complexos, incertos e ambíguos.

A tomada de decisão por parte dos envolvidos acaba influenciando a segurança cibernética. O uso de novos métodos de tomada de decisão, onde se destacam os métodos multicritérios de apoio à decisão assim como a inteligência artificial deverão se popularizar: a simplificação de problemas complexos em modelos que dão transparência e envolvam as partes interessadas é um dos fatores que mais contribuirão

para esse fato, sendo necessário avaliar e abordar fatores críticos, incluindo fatores tecnológicos, culturais, regulatórios, econômicos e outros, o que torna a cibersegurança uma questão cada vez mais complexa e multifacetada. Os tomadores de decisão, e aí estão inseridos todos dentro de uma cadeia integrada de informações, necessitarão ser conscientizados, participar da criação e consolidação de uma cultura cibernética e serem treinados em segurança cibernética, fatores cruciais para a construção e manutenção de uma cultura organizacional resiliente em segurança cibernética. A falta de conhecimento, de recursos, e de consciência, as normas associadas à complacência são fatores relacionados aos seres humanos que não podem ser negligenciados. Muitos estudos acabam por apontar um foco excessivo em aspectos técnicos excluindo os fatores humanos, muitas vezes devendo-se à falta de atributos que se relacionam aos seres humanos. Quanto ao método utilizado na pesquisa, o AHP, demonstrou-se bastante útil aos integrantes, sem grandes dificuldades na sua utilização, embora levando a um tempo extenso e acalorado, nas defesas das pontuações de seus critérios e alternativas. Somando-se aos tomadores de decisão, o tom que vem de cima representado pela liderança estratégica é fundamental para garantir a cibersegurança efetiva, buscando-se o alcance dos objetivos estratégicos nesse sentido, exigindo a identificação de estruturas que possam responder aos requisitos operacionais estabelecidos pelo ambiente, devendo ser traduzida em uma liderança clara e eficaz. Destaca-se a importância de uma abordagem de gerenciamento de riscos holística para a mitigação do risco cibernético e a necessidade de um gerenciamento de risco mais colaborativo entre seguradoras, empresas e especialistas em cibersegurança.

Muitas são as ameaças cibernéticas existentes, tais como perda de produtividade, *cyberbullying*, *cyberstalking*, roubo de identidade, sobrecarga de informações sociais, *branding* pessoal inconsistente, danos à reputação pessoal, violação de dados, software malicioso, interrupções de serviço, invasões e acesso não autorizado a contas de mídias sociais, o que acabam por impor a necessidade de se ter um nível apropriado de conscientização sobre segurança cibernética ao usar a Internet. Notou-se, com as leituras e os apontamentos, que há lacunas na literatura a respeito de práticas de segurança cibernética sob o ponto de vista daquele que se utiliza dos serviços, o usuário. A falta de dados confiáveis que registram os incidentes cibernéticos associada às novas formas de ataques, tornando rapidamente obsoletas as coletas existentes, e a falta de conhecimento sobre a segurança cibernética têm sido consideradas grandes desafios para o aproveitamento do espaço cibernético, o que leva à necessidade de uma ação conjunta de âmbito mundial: explorar a oportunidade da criação de um banco de dados internacional que venha conter fatos relevantes a respeito de incidentes cibernéticos. Salienta-se, entretanto, que o fato de não explorar de forma econômica esse espaço não é uma garantia de segurança, como apontado pelo estudo de Feng e Wang [112], onde mostra que o nível de aversão do CIO ao risco está negativamente associado à probabilidade de incidentes de violação de segurança, apresentndo que a associação é mais forte se o CEO da empresa também for avesso ao risco, sugerindo que o apetite de risco do CIO deve estar alinhado com os objetivos estratégicos da empresa para alcançar uma gestão eficaz de riscos de TI.

Os *frameworks* voltados à segurança cibernética podem ser aplicados em organizações para avaliar e melhorar sua maturidade em resiliência de cibersegurança, possibilitando a priorização de controles mais adequados à instituição, observando-se o contexto em que ela se encontra. Pode-se observar que são muitos os *frameworks*, o que, por um lado, possa dar uma certa liberdade nas escolhas, por outro pode significar que sejam feitas escolhas menos adequadas. Um dos pontos que ficou bem latente é que é possível escolher controles de diferentes *frameworks*, podendo ser traduzido como algo saudável para a

organização. O estudo acabou por trazer um conjunto expressivo de *frameworks*, o que demonstra que o setor de tecnologia encontra-se em uma fase de construção da sua segurança, em especial aos seus aspectos cibernéticos.

O setor de seguros e resseguros demonstrou-se rico na busca por indicadores que possam traduzir os prêmios baseados nos custos financeiros, destacando-se que em muitos trabalhos não há referências às boas práticas preconizadas pelos *frameworks* de segurança cibernética. Por outro lado, percebe-se que os estudos voltados para a segurança cibernética *stricto sensu* também mantém um distanciamento com as visões desse setor da economia. Há uma necessidade de que se faça uma aproximação entre essas duas abordagens, garantindo, com isso, a possibilidade de criação de modelos mais abrangentes. O mercado de seguro cibernético está evoluindo e amadurecendo, mas ainda enfrenta desafios significativos em relação à avaliação do risco cibernético, à complexidade do processo de subscrição e à falta de harmonização nas políticas e contratos de seguro cibernético, e a adoção de uma abordagem combinada de avaliação de risco de segurança cibernética, incluindo abordagens qualitativas e quantitativas, poderá ampliar a visão, tornando-a mais abrangente a respeito dos riscos. Uma das preocupações apresentadas, nessa busca por indicadores voltados para o setor de seguros, foi a necessidade da proteção dos investimentos que a Indústria 4.0 tem envidado para que a cadeia de suprimentos cibernéticos possa existir sem grandes percalços. Nesse sentido, percebeu-se que artigos a respeito da cadeia de suprimentos cibernéticos são raros, devendo merecer maior atenção por parte de futuros estudos.

Nesse cenário quase caótico, a pesquisa teve como objetivo a elaboração de proposta de medição de apetite a risco cibernético de uma organização, utilizando-se de um método multicritério de apoio à tomada de decisão, o AHP, e a Estrutura Básica de Segurança Cibernética, o NIST. Estabeleceu-se três hipóteses que se demonstraram verdadeiras no decorrer da pesquisa, o que possibilitou o alcance do objetivo central da pesquisa: uma metodologia que possibilitou medir o apetite a risco cibernético de uma organização.

A Hipótese **H1**, que trata de um conjunto limitado de critérios que possa traduzir o apetite a risco cibernético, demonstrou-se verdadeira, e que a escolha por buscar na literatura esse conjunto acabou por trazer fatores relevantes. Entretanto, à medida que os estudos avançavam, percebeu-se que outro caminho poderia ser encontrar tais fatores nos prórios *frameworks*, que se demonstraram uma fonte rica de critérios e alternativas relacionadas ao tema. Alguns ajustes realizados nos critérios e alternativas estabelecidos se deram em função dessa aproximação com os *frameworks*.

Quanto a Hipótese **H2**, que trata de um conjunto limitado de controles, salienta-se que a escolha do *framework* CSF se demonstrou satisfatória, em especial por trazer em sua construção elementos que compõem outras estruturas que são bastante utilizadas, como a família de normas ISO 27000, assim como o CIS *Controls* V8.

Já na Hipótese **H3**, que trata da possibilidade de se medir o apetite a risco cibernético de forma quantitativa a partir de escolhas de controles associados às suas priorizações, também se demonstrou verdadeira, e a pesquisa trouxe, como bônus, pois não havia essa expectativa inicialmente, uma pontuação de cada controle que, embora desejado, a ser priorizado pela instituição, podendo estabelecer uma lista ordenada como observada nos resultados alcançados.

Para alcançar esse objetivo, assim como os objetivos secundários, foi elaborada uma pesquisa bibliográfica para evidenciar os fatores que contribuem na tomada de decisão em segurança cibernética, sendo

criado um modelo de critérios e alternativas a partir desse levantamento. Em um segundo momento, fez-se uma dinâmica com profissionais do STJ para que identificassem os controles desejados, assim como os controles que já se encontravam implementados no Tribunal, e participassem do processo de priorização de critérios e alternativas preconizados por Saaty [91]. Fez-se uma análise de conteúdo dos controles preconizados pelo NIST [55] utilizando-se as alternativas como elementos de codificação.

A pesquisa buscou identificar fatores que pudessem traduzir a relevância do apetite a risco cibernético dentro de uma organização e no cenário em que ela se encontra. Essa identificação acabou por apontar, conforme orientado por Saaty, seis grandes grupos, os critérios, e trinta alternativas distribuídas nos critérios. A opção por buscar tais critérios e alternativas acabou se demonstrando bastante relevante, embora compreenda-se, após o estudo, que essa busca poderá ser feita, em estudos futuros, nos próprios *frameworks* que tratam de segurança cibernética.

6.1 LIMITAÇÕES

Percebe-se que esse estudo pode ter avanços significativos com a combinação de métodos, uso de critérios e alternativas que difiram dos propostos, assim como um conjunto de controles que possam abranger mais aspectos.

A aplicação do gerenciamento de riscos associados ao apetite ao risco cibernético, assim como a própria segurança cibernética, são temas muito relevantes, mas são, por sua natureza tão nova, ainda merecedoras de avanços e novas formas de abordagens.

Outra limitação desse estudo é que ele assume que uma organização possua, de forma clara, uma declaração de apetite de risco cibernético com elementos que possam ser traduzidos facilmente como requisitos para a seleção de controles. É muito comum que as organizações partam de uma declaração do tipo: ameaças médias e altas devem ser tratadas em nossa organização. Nesses casos, a tradução poderá se dar de forma equivocada, já que foge da proposta do modelo. Em declarações onde a organização estabelece critérios objetivos a serem alcançados, por exemplo, em relação à disponibilidade dos serviços, à privacidade do cliente, à precisão das informações, aspectos relevantes à conformidade regulatória, são mais úteis no uso do modelo proposto.

Vê-se que apenas o apontamento de que se possui um determinado controle (ou controles associados ao proposto pelo NIST), não é o sufcitente para assumir que haverá uma supressão de 100% dos riscos, e seria necessário avaliar como calcular essa supressão. Muitas vezes há inúmeras práticas relacionadas com um determinado controle, sendo que algumas são mais eficientes na mitigação do risco em relação às outras. Um avanço apontando que soluções e como elas influenciam a mitigação do risco, e, consequentemente o impacto no apetite a risco, deve ser fruto de estudos futuros.

Outra limitação do estudo está nas questões financeiras relacionadas aos controles, devendo ser fruto de análise futura, o que pode ser outro elemento de tomada de decisão, para que dê elementos às partes interessadas sobre que escolhas devam ser feitas levando-se em consideração as limitações financeiras da organização.

6.2 TRABALHOS FUTUROS

Um dos pontos que chamaram a atenção na pesquisa bibliográfica é o fato de haver um número satisfatório de artigos que tratam de métodos multicritérios para a tomada de decisão em segurança cibernética, mas não foi encontrado artigo de revisão sistemática nesse tópico. Acredita-se que uma revisão sistemática da literatura, que aborde esse tema, irá favorecer e ampliar novas linhas de pesquisa nesse tema.

A combinação do índice proposto com modelos de maturidade, preconizados por Mbanaso, Abrahams e Apene [59], Sulistyowati, Handayani e Suryanto [67], Uraipan, Praneetpolgrang e Manisri [73] e Bashofi e Salman [68] poderá trazer bons frutos, dando uma amplitude maior na sua aplicação em organizações.

REFERÊNCIAS BIBLIOGRÁFICAS

1 SHAPIRA, N.; AYALON, O.; OSTFELD, A.; FARBER, Y.; HOUSH, M. Cybersecurity in Water Sector: Stakeholders Perspective. *Journal of Water Resources Planning and Management*, 2021. Disponível em: <https://orcid.org>.

2 JAKOBSON, G. Mission cyber security situation assessment using impact dependency graphs. In: *14th International Conference on Information Fusion (FUSION)*. [s.n.], 2011. p. 1–8. Disponível em: <https://ieeexplore-ieee-org.ez54.periodicos.capes.gov.br/document/5977648>.

3 MUSMAN, S.; TEMIN, A.; TANNER, M.; FOX, D.; PRIDEMORE, B. *Evaluating the Impact of Cyber Attacks on Missions*. [S.l.], 2010.

4 BAHŞI, H.; UDOKWU, C. J.; TATAR, U.; NORTA, A. Impact assessment of cyber actions on missions or business processes: A systematic literature review. In: *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*. [s.n.], 2018. v. 2018-March, p. 11–20. ISBN 9781911218746. Disponível em: <https://www.researchgate.net/publication/321874448>.

5 WEF. *The Global Risks Report 2022 17th Edition*. [S.l.], 2022. 1–117 p. Disponível em: <https://www.zurich.com.br/-/media/project/zwp/brazil/docs/the-global-risks-report-2022.pdf?rev=6fc9924616fe4ae295e9d9aec1418c22>.

6 NIST. *NIST SP 800-37 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. [S.l.], 2018. 1–183 p. Disponível em: <https://doi.org/10.6028/NIST.SP.800-37r2>.

7 ULVEN, J. B.; WANGEN, G. A systematic review of cybersecurity risks in higher education. *Future Internet*, Multidisciplinary Digital Publishing Institute, v. 13, n. 2, p. 1–40, 2 2021. ISSN 19995903. Disponível em: <https://www.mdpi.com/1999-5903/13/2/39/htmhttps://www.mdpi.com/1999-5903/13/2/39>.

8 ZHAO, X.; ZHAO, J.; JIANG, X.; ZHANG, X.; ZHANG, W. Construction and Security Measurement of Cybersecurity Metrics Framework Based on Network Behavior. *Journal of Physics: Conference Series*, v. 1302, n. 2, 2019. ISSN 17426596.

9 SHOJAESHAFIEI, M.; ETZKORN, L.; ANDERSON, M. Analytic hierarchy process-based fuzzy measurement to quantify vulnerabilities of web applications. *International Journal of Computer Networks and Communications*, v. 12, n. 4, p. 105–123, 2020. ISSN 09749322.

10 GHADGE, A.; WEISS, M.; CALDWELL, N. D.; WILDING, R. Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management*, Emerald Group Holdings Ltd., v. 25, n. 2, p. 223–240, 2 2020. ISSN 13598546.

11 ALLODI, L.; MASSACCI, F. Security Events and Vulnerability Data for Cybersecurity Risk Estimation. *Risk Analysis*, John Wiley & Sons, Ltd, v. 37, n. 8, p. 1606–1627, 8 2017. ISSN 1539-6924. Disponível em: <https://onlinelibrary-wiley.ez54.periodicos.capes.gov.br/doi/full/10.1111/risa.12864https://onlinelibrary-wiley.ez54.periodicos.capes.gov.br/doi/abs/10.1111/risa.12864https://onlinelibrary-wiley.ez54.periodicos.capes.gov.br/doi/10.1111/risa.12864>.

12 POLLMEIER, S.; BONGIOVANNI, I.; SLAPNIČAR, S. Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science*, Elsevier, v. 159, p. 106022, 3 2023. ISSN 0925-7535.

13 MISHINA, R.; TANIMOTO, S.; GOROMARU, H.; SATO, H.; KANAI, A. Risk Management of Silent Cyber Risks in Consideration of Emerging Risks. In: *10th International Congress on Advanced Applied Informatics (IIAI-AAI)*. [S.l.]: IEEE, 2021. p. xxviii. ISBN 9781665424202.

14 LAU, P.; WANG, L.; WEI, W.; LIU, Z.; TEN, C. W. A Novel Mutual Insurance Model for Hedging Against Cyber Risks in Power Systems Deploying Smart Technologies. *IEEE Transactions on Power Systems*, IEEE, v. 38, n. 1, p. 630–642, 2023. ISSN 15580679.

15 BELLES-SAMPERA, J.; GUILLÉN, M.; SANTOLINO, M. Beyond Value-at-Risk: GlueVaR Distortion Risk Measures. *Risk Analysis*, John Wiley & Sons, Ltd, v. 34, n. 1, p. 121–134, 1 2014. ISSN 1539-6924. Disponível em: <https://onlinelibrary-wiley.ez54.periodicos.capes.gov.br/doi/full/10.1111/risa.12080https://onlinelibrary-wiley.ez54.periodicos.capes.gov.br/doi/abs/10.1111/risa.12080https://onlinelibrary-wiley.ez54.periodicos.capes.gov.br/doi/10.1111/risa.12080>.

16 CARFORA, M. F.; ORLANDO, A. Quantile based risk measures in cyber security. *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019*, IEEE, p. 1–4, 2019.

17 QUINN, S.; IVY, N.; BARRETT, M.; WITTE, G.; GARDNER, R. *NISTIR 8286A - Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*. [S.l.], 2021. 1–52 p.

18 MALAVASI, M.; PETERS, G. W.; SHEVCHENKO, P. V.; TRÜCK, S.; JANG, J.; SOFRONOV, G. Cyber risk frequency, severity and insurance viability. *Insurance: Mathematics and Economics*, North-Holland, v. 106, p. 90–114, 9 2022. ISSN 0167-6687.

19 MORO, E. D. Towards an Economic Cyber Loss Index for Parametric Cover Based on IT Security Indicator: A Preliminary Analysis. *Risks 2020, Vol. 8, Page 45*, Multidisciplinary Digital Publishing Institute, v. 8, n. 2, p. 45, 5 2020. ISSN 2227-9091. Disponível em: <https://www.mdpi.com/2227-9091/8/2/45/htmhttps://www.mdpi.com/2227-9091/8/2/45>.

20 CARCARY, M.; DOHERTY, E.; CONWAY, G.; IE, M. C. A Framework for Managing Cybersecurity Effectiveness in the Digital Context. In: *European Conference on Cyber Warfare and Security*. [S.l.: s.n.], 2019.

21 LAVILLE, C.; Jean Dionne. *A Construção do Saber - Manual de Metodologia da Pesquisa em Ciências Humanas*. São Paulo: artmed, 2008. 326 p. ISBN 2894610254.

22 MATIAS-PEREIRA, J. *Manual de Metodologia da Pesquisa Científica*. São Paulo: Editora Atlas S.A., 2010. 158 p.

23 CREAZZA, A.; COLICCHIA, C.; SPIEZIA, S.; DALLARI, F. Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management*, Emerald Group Holdings Ltd., v. 27, n. 1, p. 30–53, 1 2022. ISSN 13598546.

24 GANIN, A. A.; QUACH, P.; PANWAR, M.; COLLIER, Z. A.; KEISLER, J. M.; MARCHESE, D.; LINKOV, I. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, v. 40, n. 1, 2020.

25 GUILLET, V. M. M. *Análise de fornecedores de um setor público empregando o método Fuzzy-TOPSIS com auxílio do método AHP*. 92 p. Tese (Doutorado) — Uniiversidade Federal de Santa Maria, 2019. Disponível em: <https://repositorio.ufsm.br/handle/1/17035>.

26 ALZAHRANI, A.; JOHNSON, C. AHP-based Security decision making: How intention and intrinsic motivation affect policy compliance. *International Journal of Advanced Computer Science and Applications*, v. 10, n. 6, p. 1–8, 2019. ISSN 21565570.

27 MAČEK, D.; MAGDALENI´C, I. M.; BEGIČEVI´, N.; RE, B.; FRANCISCO, A.; HIERRO, R. L. D. A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment. *Mathematics 2021, Vol. 9, Page 1045*, Multidisciplinary Digital Publishing Institute, v. 9, n. 9, p. 1045, 5 2021. ISSN 2227-7390. Disponível em: <https://www.mdpi.com/2227-7390/9/9/1045/htmhttps://www.mdpi.com/2227-7390/9/9/1045>.

28 AMAN, W.; SHUKAILI, J. A. A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations. *International Journal of Advanced Computer Science and Applications*, The Science and Information (SAI) Organization Limited, v. 12, n. 8, p. 169–176, 2021. ISSN 2156-5570. Disponível em: <www.ijacsa.thesai.org>.

29 DOR, D.; ELOVICI, Y. A model of the information security investment decision-making process. *Computers & Security*, Elsevier Advanced Technology, v. 63, p. 1–13, 11 2016. ISSN 0167-4048.

30 STINE, K.; QUINN, S.; WITTE, G.; GARDNER, R. K. *NISTIR 8286 - Integrating Cybersecurity and Enterprise Risk Management (ERM)*. [S.l.], 2020. 76 p. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286-draft.pdf%0Ahttps://doi.org/10.6028/NIST.IR.8286-draft2>.

31 GIL, A. C. *Como Elaborar Projetos de Pesquisa*. Rio de Janeiro: Rio de Janeiro: Atlas, 2022. 353 p.

32 YIN, R. K. *Pesquisa Qualitativa do Início ao Fim (do Kindle)*. Porto Alegre: [s.n.], 2016.

33 IBGC. *Gerenciamento de riscos corporativos: evolução em governança e estratégia*. São Paulio: IBGC, 2017. 1–66 p. ISBN 9788599645505.

34 DICKINSON, G. Enterprise risk management: its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance – Issues and Practice*, v. 26, n. 3, p. 360–366, 2001.

35 ABNT. *ABNT ISO 31000*. [S.l.]: ABNT, 2018. 1–23 p.

36 CGU. *Metodologia de Gestão d Riscos:*. [S.l.: s.n.], 2020. v. 6. 46–54 p.

37 TCU. *Manual de Gestão de Riscos do TCU - Um passo para a eficiência*. TCU, 2020. 53 p. Disponível em: <www.tcu.gov.br>.

38 COSO. *COSO Gerenciamento de Riscos Corporativos*. [s.n.], 2007. v. 1. 01–141 p. ISSN 0014-2956. ISBN 9788599645505. Disponível em: <www.cpa2biz.com.>

39 COSO. *Enterprise Risk Management Integrating with Strategy and Performance*. [S.l.: s.n.], 2017.

40 STJ. *Gestão de Riscos*. Brasília: STJ, 2022. 1–45 p. Disponível em: <http://bdjur.stj.jus.br>.

41 CNJ. *Manual de Gestão de Riscos*. [S.l.: s.n.], 2019.

42 ENAP. *Governança de TIC no contexto da transformação digital - Módulo 4 - Gestão de Riscos*. [S.l.]: ENAP, 2021.

43 POWER, M. The risk management of nothing. *Accounting, Organizations and Society*, Elsevier Ltd, v. 34, n. 6-7, p. 849–855, 2009. ISSN 03613682. Disponível em: <http://dx.doi.org/10.1016/j.aos.2009.06.001>.

44 ARRUDA, C. L.; RUSSO, P. T.; SOUZA, R. P.; FERNANDES, F. C. A Influência do Apetite a Riscos no Processo de Gestão de Riscos Corporativos: um estudo de caso. In: *Congresso Internacional AECA*. [s.n.], 2018. v. 20, p. 1–19. Disponível em: <https://xxcongreso.aeca.es/wp-content/uploads/2019/09/127d.pdf>.

45 TCU. *Referencial Básico de Governança Organizacional: para organizações públicas e outros entes jurisdicionados ao TCU*. Brasília: TCU, 2020. v. 37. 95 p. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799>.

46 MARSHALL, A.; OJIAKO, U.; CHIPULU, M. A futility, perversity and jeopardy critique of "risk appetite". *International Journal of Organizational Analysis*, Emerald Group Holdings Ltd., v. 27, n. 1, p. 51–73, 3 2019. ISSN 19348835.

47 MARTENS, F.; RITTENBERG, L. *Using Risk Appetite to Thrive in a Changing World*. COSO, 2020. 1–40 p. Disponível em: <https://www.coso.org/SharedDocuments/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf>.

48 GU, R.; ZHANG, Q.; ZHOU, W. Judging the True Health of Finance Institutions Based on Risk Behavior and Operation Performance. *Mathematical Problems in Engineering*, Hindawi Limited, v. 2022, 2022. ISSN 15635147.

49 IRM. *Risk Guidance Paper Appetite & Tolerance*. [S.l.: s.n.], 2011. 1–42 p.

50 FSB. *Principles for An Effective Risk Appetite Framework*. [S.l.], 2013.

51 LLANSÓ, T.; MCNEIL, M.; NOTEBOOM, C. Multi-Criteria Selection of Capability-Based Cybersecurity Solutions. In: *Proceedings of the 52nd Hawaii International Conference on System Sciences*. [s.n.], 2019. p. 9. ISBN 9780998133126. Disponível em: <https://hdl.handle.net/10125/60169>.

52 VIEIRA, J. B.; BARRETO, R. T. d. S. Governança, gestão de riscos e integridade. *Escola Nacional de Administração Pública*, 2019. Disponível em: <https://repositorio.enap.gov.br/handle/1/4281>.

53 NUNES, R. R.; PERINI, M. T. B. S.; PINTO, I. E. M. M. A Gestão de Riscos como Instrumento para a Aplicação Efetiva do Princípio Constitucional da Eficiência. *Revista Brasileira de Políticas Públicas*, v. 11, n. 3, p. 260–281, 2021.

54 ENAP. *Implementando a Gestão de Riscos no Setor Público*. [S.l.]: ENAP, 2018. 14 p.

55 NIST. *Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica*. [S.l.], 2018. 68 p.

56 NIST. *NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations*. [S.l.], 2020. Disponível em: <https://doi.org/10.6028/NIST.SP.800-53r5>.

57 Global Risk Report. *The Global Risks Report 2023 - 18th Edition*. [S.l.], 2023. 1–98 p. Disponível em: <www.weforum.orghttps://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf>.

58 MASTWIJK, K. *Dealing with uncertainty : cybersecurity risk assessment approaches A qualitative research on cyber risk assessment practices in organizations*. Tese (Doutorado) — Universiteit Leiden, 2020.

59 MBANASO, U. M.; ABRAHAMS, L.; APENE, O. Z. Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework. *The African Journal of Information and Communication*, Authors, v. 23, n. 23, p. 1–26, 6 2019. ISSN 2077-7213. Disponível em: <http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2077-72132019000100002&lng=en&nrm=iso&tlng=enhttp://www.scielo.org.za/scielo.php?script=sci_abstract&pid=S2077-72132019000100002&lng=en&nrm=iso&tlng=en>.

60 FACCHINETTI, S.; GIUDICI, P.; OSMETTI, S. A. Cyber risk measurement with ordinal data. *Statistical Methods and Applications*, Springer, v. 29, n. 1, p. 173–185, 3 2020. ISSN 1613981X. Disponível em: <https://link-springer-com.ez54.periodicos.capes.gov.br/article/10.1007/s10260-019-00470-0>.

61 BHOL, S. G.; MOHANTY, J. R.; PATTNAIK, P. K. *Cyber Security Metrics Evaluation Using Multi-criteria Decision-Making Approach*. Springer Singapore, 2020. v. 160. 665–675 p. ISSN 21903026. ISBN 9789813296893. Disponível em: <http://dx.doi.org/10.1007/978-981-32-9690-9_71>.

62 LARSEN, M. H.; LUND, M. S. Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 9, p. 144895–144905, 2021. ISSN 2169-3536. Disponível em: <https://ieeexplore.ieee.org/document/9585112/>.

63 HERATH, T. B. G.; KHANNA, P.; AHMED, M. Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy 2022, Vol. 2, Pages 1-18*, Multidisciplinary Digital Publishing Institute, v. 2, n. 1, p. 1–18, 1 2022. ISSN 2624-800X. Disponível em: <https://www.mdpi.com/2624-800X/2/1/1/htmhttps://www.mdpi.com/2624-800X/2/1/1>.

64 DESOLDA, G.; FERRO, L. S.; MARRELLA, A.; CATARCI, T.; COSTABILE, M. F. Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, v. 54, n. 8, 2022. ISSN 15577341. Disponível em: <https://doi.org/10.1145/3469886>.

65 CHOWDHURY, N.; GKIOULOS, V. Key competencies for critical infrastructure cyber-security: a systematic literature review. *Information and Computer Security*, Emerald Group Holdings Ltd., v. 29, n. 5, p. 697–723, 11 2021. ISSN 2056497X.

66 SRINIVAS, J.; DAS, A. K.; KUMAR, N. Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, Elsevier B.V., v. 92, p. 178–188, 2019. ISSN 0167739X. Disponível em: <https://doi.org/10.1016/j.future.2018.09.063>.

67 SULISTYOWATI, D.; HANDAYANI, F.; SURYANTO, Y. Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *International Journal on Informatics Visualization*, Politeknik Negeri Padang, v. 4, n. 4, p. 225–230, 2020. ISSN 25499904.

68 BASHOFI, I.; SALMAN, M. Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. *Proceedings - 2022 IEEE International Conference on Cybernetics and Computational Intelligence, CyberneticsCom 2022*, Institute of Electrical and Electronics Engineers Inc., p. 58–62, 2022.

69 ROY, P. P. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020*, Institute of Electrical and Electronics Engineers Inc., 2 2020. Disponível em: <https://ieeexplore-ieee-org.ez54.periodicos.capes.gov.br/document/9119914>.

70 MOREIRA, F. R. *Uma proposta para priorização de controles de segurança cibernética com o uso de um método multicritério*. Tese (Doutorado) — Universidade de Brasília, 2022.

71 KURII, Y.; OPIRSKYY, I. Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. *NIST Special Publication 800*, v. 53, n. 10, p. 21–32, 2022.

72 REA-GUAMAN, A. M.; SANCHEZ-GARCIA, I. D.; FELIU, T. S.; CALVO-MANZANO, J. A. Modelos de Madurez en Ciberseguridad: una revisión sistemática. In: *Iberian Conference on Information Systems and Technologies, CISTI*. [S.l.]: IEEE Computer Society, 2017. ISBN 9789899843479. ISSN 21660735.

73 URAIPAN, N.; PRANEETPOLGRANG, P.; MANISRI, T. *Application of a fuzzy analytic hierarchy process to select the level of a cyber resilient capability maturity model in digital supply chain systems*. 2021. 198–207 p.

74 KAPLAN, S.; GARRICK, B. J. On The Quantitative Definition of Risk. *Risk Analysis*, I , No. I, 1981.

75 GOMES, L. F. A. M. *Teoria da Decisão (livro eletrônico)*. São Paulo: [s.n.], 2020. 127 p. ISBN 9786555582024.

76 AZHAR, N. A.; RADZI1, N. A. M.; AHMAD, W. S. H. M. W. Multi-criteria Decision Making: A Systematic Review. *(Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*, v. 14, n. 8, p. 779–801, 2021. ISSN 23520965.

77 MARDANI, A.; JUSOH, A.; NOR, K. M.; KHALIFAH, Z.; ZAKWAN, N.; VALIPOUR, A. Multiple criteria decision-making techniques and their applications - A review of the literature from 2000 to 2014. *Economic Research-Ekonomska Istrazivanja*, v. 28, n. 1, p. 516–571, 2015. ISSN 1331677X. Disponível em: <http://www.tandfonline.com/action/journalInformation?journalCode=rero20>.

78 MAČEK, D.; MAGDALENIĆ, I.; REđEP, N. B. A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. *International Journal of Safety and Security Engineering*, v. 10, n. 2, p. 161–174, 2020. ISSN 2041904X.

79 MOREIRA, F. R.; FILHO, D. A. D. S.; NZE, G. D. A.; JUNIOR, R. T. D. S.; NUNES, R. R. Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 9, p. 129605–129618, 2021.

80 TORBACKI, W. A hybrid mcdm model combining danp and promethee ii methods for the assessment of cybersecurity in industry 4.0. *Sustainability (Switzerland)*, v. 13, n. 16, 2021. ISSN 20711050.

81 REKIK, R.; KALLEL, I.; CASILLAS, J.; ALIMI, A. M. Using Multiple Criteria Decision Making Approaches to Assess the Quality of Web Sites. *International Journal of Computer Science and Information Security*, v. 14, n. 7, p. 747, 2016.

82 RIBEIRO, R. C.; CANEDO, E. D. Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security. *ACM International Conference Proceeding Series*, p. 175–184, 2020.

83 GAMPER, C. D.; TURCANU, C. On the governmental use of multi-criteria analysis. 2007. Disponível em: <www.legge109-94.it/leges/DPR554-1999.doc>.

84 Associação Brasileira de Normas Técnicas. *Gestão de riscos — Técnicas para o processo de avaliação de riscos (ABNT ISO/IEC 31010)*. 1ª. ed. [S.l.], 2012. 1–110 p. Disponível em: <www.abnt.org.br>.

85 SUKUMAR, A.; MAHDIRAJI, H. A.; JAFARI-SADEGHI, V. Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*, John Wiley & Sons, Ltd, 2023. ISSN 1539-6924. Disponível em: <https://onlinelibrary.wiley.com/doi/full/10.1111/risa.14092https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.14092https://onlinelibrary.wiley.com/doi/10.1111/risa.14092>.

86 ALTUBAISHE, B.; DESAI, S. Multicriteria Decision Making in Supply Chain Management Using FMEA and Hybrid AHP-PROMETHEE Algorithms. *Sensors 2023, Vol. 23, Page 4041*, Multidisciplinary Digital Publishing Institute, v. 23, n. 8, p. 4041, 4 2023. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/23/8/4041/htmhttps://www.mdpi.com/1424-8220/23/8/4041>.

87 ALGHASSAB, M. Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector. *Energies*, v. 15, n. 1, 2022. ISSN 19961073. Disponível em: <https://www.mdpi.com/1996-1073/15/1/218>.

88 ABUSHARK, Y. B.; KHAN, A. I.; ALSOLAMI, F.; ALMALAWI, A.; ALAM, M. M.; AGRAWAL, A.; KUMAR, R.; KHAN, R. A. Cyber Security Analysis and Evaluation for Intrusion Detection Systems. *Computers, Materials and Continua*, v. 72, n. 1, p. 1765–1783, 2022. ISSN 15462226.

89 ABUSHARK, Y. B.; KHAN, A. I.; ALSOLAMI, F. J.; ALMALAWI, A.; ALAM, M. M.; AGRAWAL, A.; KUMAR, R.; KHAN, R. A. Usability Evaluation through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective. *Computers, Materials and Continua*, v. 68, n. 1, p. 1203–1218, 2021. ISSN 15462226.

90 BELINDA, B. I.; EMMANUEL, A. A.; SOLOMON, N.; KAYODE, A. B. Evaluating Software Quality Attributes using Analytic Hierarchy Process (AHP). *International Journal of Advanced Computer Science and Applications*, v. 12, n. 3, p. 165–173, 2021. ISSN 21565570.

91 SAATY, T. L. The Analytic Hierarchy Process. 1980.

92 YEE, J.; YAP, L.; HO, C. C.; TING, C.-Y. A systematic review of the applications of multi-criteria decision-making methods in site selection problems. *Built Environment Project and Asset Management*, 2018. Disponível em: <www.emeraldinsight.com/2044-124X.htm>.

93 LAKHANI, A.; ZEEMAN, H.; WRIGHT, C. J.; WATLING, D. P.; SMITH, D.; ISLAM, R. Stakeholder priorities for inclusive accessible housing: A systematic review and multicriteria decision analysis. *Journal of Multi-Criteria Decision Analysis*, v. 27, n. 1-2, p. 5–19, 2020. ISSN 10991360.

94 SAATY, T. L. *Fundamentals of Decision Making and Priority Theory With the Analytic Hierarchy Process - Ebook Edition*. Piyyidburgh - USA: RWS Publications, 2013.

95 HUBBARD, D. W. *How to Measure Anything: Finding the Value of Intangibles in Business*. Kindle. Kindle, 2009. Disponível em: <https://www.amazon.com.br/How-Measure-Anything-Intangibles-Business-ebook/dp/B00INUYS2U/ref=sr_1_1?__mk_pt_BR=ÃĚMÃĚÅ¡ÃŢÃŚ&keywords=Hubbard%2C+Douglas+W.&qid=1681996910&s=digital-text&sr=1-1>.

96 GAI, P.; VAUSE, N. Measuring Investors' Risk Appetite. *SSRN Electronic Journal*, 2005. ISSN 1368-5562. Disponível em: <www.bankofengland.co.uk/publications/workingpapers/index.htm.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=872695>.

97 PETER, A. S. Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, Elsevier, v. 17, p. 49–59, 6 2017. ISSN 1874-5482.

98 RUAN, K. Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, Elsevier Advanced Technology, v. 65, p. 77–89, 3 2017. ISSN 0167-4048.

99 ZÄNGERLE, D.; SCHIERECK, D. Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, Palgrave Macmillan, p. 1–29, 12 2022. ISSN 14680440. Disponível em: <https://link.springer.com/article/10.1057/s41288-022-00282-6>.

100 SLAPNIČAR, S.; VUKO, T.; ČULAR, M.; DRAŠČEK, M. Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, Pergamon, v. 44, p. 100548, 3 2022. ISSN 1467-0895.

101 POUR, M. S.; NADER, C.; FRIDAY, K.; BOU-HARB, E. A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security. *Computers & Security*, Elsevier Advanced Technology, v. 128, p. 103123, 5 2023. ISSN 0167-4048.

102 Douglas W. Hubbard; Richard Seiersen. *How to Measure Anything in Cybersecurity Risk*. 5. ed. [s.n.], 2023. Disponível em: <https://www.amazon.com.br/Measure-Anything-Cybersecurity-Risk-English-ebook/dp/B0C1RJ9SR1/ref=sr_1_5?__mk_pt_BR=ÃĚMÃĚÅ¡ÃŢÃŚ&keywords=Hubbard%2C+Douglas+W.&qid=1681996910&s=digital-text&sr=1-5>.

103 KIM, S.; SONG, S. Cyber risk measurement via loss distribution approach and GARCH model. *Communications for Statistical Applications and Methods*, Korean Statistical Society, v. 30, n. 1, p. 75–94, 1 2023. ISSN 2287-7843. Disponível em: <http://www.csam.or.kr/journal/view.html?doi=10.29220/CSAM.2023.30.1.075>.

104 AccountAbility. *Princípios da 2018 accountability*. [S.l.], 2018. 1–40 p.

105 GCAZA, N.; SOLMS, R. von. A strategy for a cybersecurity culture: A South African perspective. *Electronic Journal of Information Systems in Developing Countries*, v. 80, n. 1, p. 1–17, 2017. ISSN 16814835.

106 SHARKOV, G. From Cybersecurity to Collaborative Resiliency. *ACM Digital Library*, 2016. Disponível em: <http://dx.doi.org/10.1145/2994475.2994484>.

107 GORDON, W. J.; WRIGHT, A.; AIYAGARI, R.; CORBO, L.; GLYNN, R. J.; KADAKIA, J.; KUFAHL, J.; MAZZONE, C.; NOGA, J.; PARKULO, M.; SANFORD, B.; SCHEIB, P.; LANDMAN, A. B. Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open*, American Medical Association, v. 2, n. 3, p. e190393–e190393, 3 2019. ISSN 25743805. Disponível em: <https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270>.

108 JEONG, J.; MIHELCIC, J.; OLIVER, G.; RUDOLPH, C. Towards an improved understanding of human factors in cybersecurity. *Proceedings - 2019 IEEE 5th International Conference on Collaboration and Internet Computing, CIC 2019*, Institute of Electrical and Electronics Engineers Inc., p. 338–345, 12 2019.

109 KESSLER, S. R.; PINDEK, S.; KLEINMAN, G.; ANDEL, S. A.; SPECTOR, P. E. Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal*, SAGE Publications Ltd, v. 26, n. 1, p. 461–473, 3 2020. ISSN 17412811. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/1460458219832048>.

110 AL-NUAIMI, M. N. Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review. *Global Knowledge, Memory and Communication*, Emerald Group Holdings Ltd., ahead-of-p, n. ahead-of-print, 2022. ISSN 25149350.

111 ELING, M.; SCHNELL, W. What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, Emerald Group Publishing Ltd., v. 17, n. 5, p. 474–491, 2016. ISSN 09657967. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/JRF-09-2016-0122/full/html>.

112 FENG, C. Q.; WANG, T. Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*, Pergamon, v. 32, p. 59–75, 3 2019. ISSN 1467-0895.

113 TONN, G.; KESAN, J. P.; ZHANG, L.; CZAJKOWSKI, J. Cyber risk and insurance for transportation infrastructure. *Transport Policy*, Pergamon, v. 79, p. 103–114, 7 2019. ISSN 0967-070X.

114 AZIZ, B.; Suhardi; Kurnia. A systematic literature review of cyber insurance challenges. *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., p. 357–363, 10 2020.

115 XU, M.; HUA, L. Cybersecurity Insurance: Modeling and Pricing. *https://doi.org/10.1080/10920277.2019.1566076*, Routledge, v. 23, n. 2, p. 220–249, 4 2019. ISSN 10920277. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/10920277.2019.1566076>.

116 CROTTY, J.; DANIEL, E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*, Emerald Publishing, ahead-of-p, n. ahead-of-print, 2022. ISSN 22108327.

117 EROLA, A.; AGRAFIOTIS, I.; NURSE, J. R.; AXON, L.; GOLDSMITH, M.; CREESE, S. A system to calculate Cyber Value-at-Risk. *Computers & Security*, Elsevier Advanced Technology, v. 113, p. 102545, 2 2022. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404821003692>.

118 KEJWANG, B. Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. *International Journal of Research in Business and Social Science (2147-4478)*, v. 11, n. 6, p. 334–340, 2022.

119 TSOHOU, A.; DIAMANTOPOULOU, V.; GRITZALIS, S.; LAMBRINOUDAKIS, C. Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, Springer Science and Business Media Deutschland GmbH, p. 1–12, 1 2023. ISSN 16155270. Disponível em: <https://link-springer-com.ez54.periodicos.capes.gov.br/article/10.1007/s10207-023-00660-8>.

120 DEMO, P. *Pesquisa e informação qualitativa: Aportes Metodológicos (Edição do Kindle)*. Campinas: [s.n.], 2017.

121 MARCONI, M. d. A.; LAKATOS, E. M. *Metodologia do trabalho científico: projetos de pesquisa, pesquisa bibliográfica, teses de doutorado, dissertações de mestrado, trabalhos de conclusão de curso*. 9º. ed. São Paulo: [s.n.], 2022. ISBN 978-85-97-02654-2.

122 SEVERINO, A. J. *Metodologia do trabalho científico [livro eletrônico]*. 2ª. ed. São Paulo: [s.n.], 2017. 274 p. ISBN 9788524920813. Disponível em: <https://www.ufrb.edu.br/ccaab/images/AEPE/DivulgaÃğÃčo/LIVROS/Metodologia_do_Trabalho_CientÃ■fico_-_1Âł_EdiÃğÃčo_-_Antonio_Joaquim_Severino_-_2014.pdf>.

123 SAATY, T. L. Decision making with the Analytic Hierarchy Process. *Scientia Iranica*, v. 9, n. 3, p. 215–229, 2008. ISSN 10263098.

124 SAMPAIO, R. C.; LYCARIÃO, D. *Análise de conteúdo categorial: manual de aplicação*. [s.n.], 2021. 155 p. ISBN 9786587791180. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/6542/1/Analise_de_conteudo_categorial_final.pdfConsultadoem24jul2022,14:39>.

125 BARDIN, L. *Análise de Conteúdo*. [S.l.: s.n.], 2020.

126 RIFFE, D.; LACY, S.; FICO, F.; WATSON, B. *Analyzing Media Messages: Using Quantitative Content Analysis in Research - eBook Kindle*. 4ª. ed. [S.l.: s.n.], 2019.

127 BARDIN, L. *Análise de Conteúdo*. [s.n.], 1977. v. 22. 225 p. ISSN 1098-6596. ISBN 972-44-0020-4. Disponível em: <http://books.google.com/books?id=AFpxPgAACAAJ%5Cnhttp://cliente.argo.com.br/~mgos/analise_de_conteudo_moraes.html#_ftn1>.

128 SAATY, R. W. The analytic hierarchy process-what it is and how it is used. *Mathematical Modelling*, v. 9, n. 3-5, p. 161–176, 1987. ISSN 02700255.

129 MUSTAFA, S. Z.; KAR, A. K. Prioritization of multi-dimensional risk for digital services using the generalized analytic network process. *Digital Policy, Regulation and Governance*, Emerald Group Holdings Ltd., v. 21, n. 2, p. 146–163, 3 2019. ISSN 23985038.

130 ANSARI, M. T. J.; AL-ZAHRANI, F. A.; PANDEY, D.; AGRAWAL, A. A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Medical Informatics and Decision Making*, BioMed Central Ltd, v. 20, n. 1, p. 1–13, 9 2020. ISSN 14726947. Disponível em: <https://bmcmedinformdecismak-biomedcentral-com.ez54.periodicos.capes.gov.br/articles/10.1186/s12911-020-01209-8>.

131 ALHARBI, A.; SEH, A. H.; ALOSAIMI, W.; ALYAMI, H.; AGRAWAL, A.; KUMAR, R.; KHAN, R. A. Analyzing the impact of cyber security related attributes for intrusion detection systems. *Sustainability (Switzerland)*, v. 13, n. 22, p. 1–19, 2021. ISSN 20711050.

132 ALFAKEEH, A. S.; ALMALAWI, A.; ALSOLAMI, F. J.; ABUSHARK, Y. B.; KHAN, A. I.; BAHADDAD, A. A. S.; ALAM, M. M.; AGRAWAL, A.; KUMAR, R.; KHAN, R. A. Sustainable-Security Assessment Through a Multi Perspective Benchmarking Framework. *Computers, Materials and Continua*, v. 71, n. 2, p. 6011–6037, 2022. ISSN 15462226. Disponível em: <https://www.techscience.com/cmc/v71n3/46564/html>.

133 ALSHAHRANI, H. M.; ALOTAIBI, S. S.; ANSARI, M. T. J.; ASIRI, M. M.; AGRAWAL, A.; KHAN, R. A.; MOHSEN, H.; HILAL, A. M. Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach. *Applied Sciences 2022, Vol. 12, Page 5911*, Multidisciplinary Digital Publishing Institute, v. 12, n. 12, p. 5911, 6 2022. ISSN 2076-3417. Disponível em: <https://www.mdpi.com/2076-3417/12/12/5911/htmhttps://www.mdpi.com/2076-3417/12/12/5911>.

134 GONZALES, R.; ALMACEN, R. M.; GONZALES, G.; COSTAN, F.; SULADAY, D.; ENRIQUEZ, L.; COSTAN, E.; ATIBING, N. M.; ARO, J. L.; EVANGELISTA, S. S.; MATURAN, F.; SELERIO, E.; OCAMPO, L. Priority Roles of Stakeholders for Overcoming the Barriers to Implementing Education 4.0: An Integrated Fermatean Fuzzy Entropy-Based CRITIC-CODAS-SORT Approach. *Complexity*, Hindawi Limited, v. 2022, 2022. ISSN 10990526. Disponível em: <https://www.hindawi.com/journals/complexity/2022/7436256/>.

135 INSUA, D. R.; COUCE-VIEIRA, A.; RUBIO, J. A.; PIETERS, W.; LABUNETS, K.; RASINES, D. G. An Adversarial Risk Analysis Framework for Cybersecurity. *Risk Analysis*, v. 41, n. 1, p. 2021, 2021.

136 COLICCHIA, C.; CREAZZA, A.; NOÉ, C.; STROZZI, F. Information Sharing in Supply Chains: a review of risks and opportunities using the Systematic Literature Network Analysis (SLNA). 2019. Disponível em: <https://www.elsevier.com/en->.

137 CREMER, F.; SHEEHAN, B.; FORTMANN, M.; KIA, A. N.; MULLINS, M.; MURPHY, F.; MATERNE, S. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice 2022 47:3*, Palgrave, v. 47, n. 3, p. 698–736, 2 2022. ISSN 1468-0440. Disponível em: <https://link.springer.com/article/10.1057/s41288-022-00266-6>.

138 JOSHI, C.; SINGH, U. K. Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, Elsevier Ltd, v. 35, p. 128–137, 2017. ISSN 22142126. Disponível em: <http://dx.doi.org/10.1016/j.jisa.2017.06.006>.

139 SOKRI, A. Cyber Security Risk Modelling and Assessment: A Quantitative Approach. In: *European Conference on Cyber Warfare and Security*. [S.l.: s.n.], 2019. p. 466–474.

140 TAYLOR, S.; SURRIDGE, M.; PICKERING, B. Regulatory Compliance Modelling Using Risk Management Techniques. In: *2021 IEEE World AI IoT Congress (AIIoT)*. [S.l.]: Institute of Electrical and Electronics Engineers (IEEE), 2021. p. 0474–0481.

141 KITSIOS, F.; CHATZIDIMITRIOU, E.; KAMARIOTOU, M. Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability*, v. 14, n. 3, p. 1269, 2022. ISSN 20711050. Disponível em: <https://www.mdpi.com/2071-1050/14/3/1269/htm>.

142 COLICCHIA, C.; CREAZZA, A.; MENACHOF, D. Managing Cyber and Information Risks in Supply Chains: insights from an Exploratory Analysis. *SUPPLY CHAIN MANAGEMENT-AN INTERNATIONAL JOURNAL*, p. 1–53, 2019.

143 REZAEI, J. A Systematic Review of Multi-criteria Decision-making Applications in Reverse Logistics. *Transportation Research Procedia*, Elsevier, v. 10, p. 766–776, 1 2015. ISSN 2352-1465.

144 SOLTANI, A.; HEWAGE, K.; REZA, B.; SADIQ, R. Multiple stakeholders in multi-criteria decision-making in the context of Municipal Solid Waste Management: A review. *Waste Management*, Pergamon, v. 35, p. 318–328, 1 2015. ISSN 0956-053X.

145 NIFAKOS, S.; CHANDRAMOULI, K.; NIKOLAOU, C. K.; PAPACHRISTOU, P.; KOCH, S.; PANAOUSIS, E.; BONACINA, S. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors 2021, Vol. 21, Page 5119*, Multidisciplinary Digital Publishing Institute, v. 21, n. 15, p. 5119, 7 2021. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/21/15/5119/htmhttps://www.mdpi.com/1424-8220/21/15/5119>.

146 JIANG, L.; JAYATILAKA, A.; NASIM, M.; GROBLER, M.; ZAHEDI, M.; BABAR, M. A. Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access*, Institute of Electrical and Electronics Engineers (IEEE), v. 10, p. 57525–57554, 5 2022.

147 POOL, J.; AKHLAGHPOUR, S.; FATEHI, F. Towards a contextual theory of Mobile Health Data Protection (MHDP): A realist perspective. *International Journal of Medical Informatics*, Elsevier, v. 141, p. 104229, 9 2020. ISSN 1386-5056.

148 XU, P.; GAO, X.; AGE, P. Management Solutions for Cyber-Physical Security in Smart Built Environment. In: *Construction Research Congress 2022*. [S.l.: s.n.], 2022. p. 1024–1032.

149 WAXLER, J. Prioritizing Security Controls Using Multiple Criteria Decision Making for Home Users. *The George Washington University*, n. December 2009, 2018.

150 AL-SARTAWI, A. Information Technology Governance: The Role of Board of Directors in Cybersecurity Oversight. In: *European Conference on Cyber Warfare and Security*. [S.l.: s.n.], 2019.

151 ZABURKO, J.; SZULZYK-CIEPLAK, J. Information security risk assessment using the AHP method. *IOP Conference Series: Materials Science and Engineering*, v. 710, n. 1, 2019. ISSN 1757899X.

152 PETROVA, V. A Decision Hierarchical Model of Cyber Security Risk Assessment. p. 2021, 2021.

153 MITRE. *CROWN JEWELS ANALYSIS*. 2018. Disponível em: <https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis#>.

154 CAMILLO, M. Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, Informa UK Limited, v. 2, n. 1, p. 53–63, 1 2017. ISSN 2373-8871. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1296878>.

155 FRANKE, U. The cyber insurance market in Sweden. *Computers & Security*, Elsevier Advanced Technology, v. 68, p. 130–144, 7 2017. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404817300883>.

156 ALABOOL, H.; KAMIL, A.; ARSHAD, N.; ALARABIAT, D. Cloud service evaluation method-based Multi-Criteria Decision-Making: A systematic literature review. *Journal of Systems and Software*, Elsevier, v. 139, p. 161–188, 5 2018. ISSN 0164-1212. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0164121218300244>.

157 KISSOON, S. T. Optimum spending on cybersecurity measures. *Emerald Publishing Limited*, 2020. Disponível em: <https://www.emerald.com/insight/1750-6166.htm>.

158 KISSOON, S. T. Optimum Spending on Cybersecurity Measures: Part II. *Journal of Information Security*, v. 12, p. 137–161, 2021. Disponível em: <https://doi.org/10.4236/jis.2021.121007>.

159 AL-TURKISTANI, H. F.; ALDOBAIAN, S.; LATIF, R. Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review. *IEEE Explore*, 2021. Disponível em: <https://ieeexplore-ieee-org.ez54.periodicos.capes.gov.br/document/9425343/keywords#keywords>.

Apêndice 01 - Desafios e Dificuldades

Desafios e Dificuldades apontados pelos autores dos artigos avaliados.
Os textos estão distribuídos pelo Tópico principal do artigo (MCDM, Segurança Cibernética, Segurança da Informação, Seguros, por exemplo e por ano de publicação

APETITE A RISCO

2021

1. ***Maček et al. [27] - A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment***

    - A falta de dados necessários.
    - Limitações de tempo.
    - Limitações de recursos.
    - A seleção do método de tomada de decisão multicritério mais adequado.
    - A falta de elementos de avaliação de risco específicos para sistemas críticos de TI em instituições financeiras.

ASPECTOS HUMANOS

2021

1. ***Aman e Shukaili [28] - A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations***

    - A falta de estudos holísticos sobre os fatores críticos que afetam uma CSS.
    - Necessidade de avaliar e abordar fatores culturais, regulatórios, econômicos e outros, fatores técnicos.
    - Importância de conscientizar e envolver todas as pessoas em todos os níveis da organização na segurança cibernética.

CADEIA DE SUPRIMENTOS

2021

1. ***Uraipan, Praneetpolgrang e Manisri [73] - Application of a fuzzy analytic hierarchy process to select the level of a cyber resilient capability maturity model in digital supply chain systems***

    - A avaliação da resiliência cibernética em cadeias de suprimentos digitais pode ser complexa devido à interconexão digital e a possibilidade de ataques cibernéticos.
    - O maior desafio encontra-se na própria escolha dos critérios importantes para para avaliar a resiliência cibernética.

SEGURANÇA CIBERNÉTICA

2017

1. ***Allodi e Massacci [11] - Security Events and Vulnerability Data for Cybersecurity Risk Estimation***

    - A falta de dados confiáveis de "ground truth"que são tipicamente ausentes ou muito limitados na natureza.
    - Lidar com as constantes mudanças na paisagem de ameaças cibernéticas e a necessidade de manter a metodologia atualizada para garantir a eficácia contínua da avaliação de risco.
    - A necessidade de educar os tomadores de decisão sobre a importância de uma abordagem quantitativa de avaliação de risco em segurança cibernética, já que as avaliações qualitativas tradicionais ainda são amplamente utilizadas.

2019

1. ***Mbanaso, Abrahams e Apene [59] - Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework***

    - A imprevisibilidade de eventos de cibersegurança.
    - A necessidade de monitoramento contínuo, a falibilidade humana inerente ao elemento humano da cibersegurança.
    - A necessidade de avaliar a eficácia e consistência dos processos corporativos, aplicativos e dados.
    - A avaliação da infraestrutura física e técnica necessária para apoiar as medidas de cibersegurança.
    - Incorporar uma abordagem ágil na estratégia de design do framework e a incorporação de componentes relevantes de frameworks e padrões de cibersegurança existentes.
    - A implementação do CRMM framework exigirá a coleta sistemática de dados quantitativos relevantes, o que pode ser um desafio para algumas organizações.

2021

1. ***Insua et al. [135] - An Adversarial Risk Analysis Framework for Cybersecurity***

    - Falta de dados históricos confiáveis sobre incidentes de segurança cibernética, o que dificulta a construção de modelos precisos de risco em cibersegurança.
    - Desafios metodológicos envolvidos na análise de risco em cibersegurança, incluindo a modelagem de influência de múltiplos agentes.
    - A avaliação de risco em um ambiente incerto e dinâmico.

SEGURO E RESSEGURO

2005

1. ***Gai e Vause [96] - Measuring Investors' Risk Appetite***

    - O artigo não apresenta desafios ou dificuldades na implementação da abordagem proposta para medir o apetite por risco dos investidores.

2014

1. ***Belles-Sampera, Guillén e Santolino [15] - Beyond Value-at-Risk: GlueVaR Distortion Risk Measures***

    - Os autores apontam para a necessidade dos gestores de risco em encontrar um equilíbrio entre duas demandas opostas: por um lado, eles querem que as unidades de negócios alcancem ou superem os objetivos fixados pelo comitê executivo da empresa e, por outro lado, eles preferem minimizar o nível de reservas de capital exigidas pelas regulamentações de solvência, pois devem lidar com muitas restrições sobre como esse capital pode ser investido e, como tal, o retorno sobre suas reservas de capital geralmente é menor do que o fornecido por outras oportunidades.

2016

1. ***Eling e Schnell [111] - What do we know about cyber risk and cyber risk insurance?***

    - A falta de dados.
    - A falta de abordagens de modelagem.
    - O risco de mudança.
    - Os riscos incalculáveis de acumulação em segurar riscos cibernéticos.
    - A falta de pesquisa sobre risco cibernético no campo da economia e dos negócios.

2017

1. ***Ruan [98] - Introducing cybernomics: A unifying economic framework for measuring cyber risk***

    - A falta de dados históricos confiáveis sobre riscos cibernéticos, o que dificulta a modelagem estatística e a análise de risco.
    - A necessidade de integrar a gestão de riscos cibernéticos com a economia e a Gestão de Riscos Corporativos, o que requer uma mudança cultural e organizacional significativa nas empresas.
    - A falta de padrões e metodologias comuns para medir e gerenciar riscos cibernéticos, o que dificulta a comparação entre organizações e setores.
    - Desenvolvimento de novas métricas e indicadores de desempenho da gestão de riscos cibernéticos e sua contribuição de valor nas empresas.

2019

1. ***Tonn et al. [113] - Cyber risk and insurance for transportation infrastructure***

    - Falta de dados históricos sobre incidentes cibernéticos em infraestruturas de transporte.
    - Dificuldade na avaliação dos riscos de segurança cibernética nas empresas de infraestrutura de transporte.
    - Incerteza na avaliação dos riscos de segurança cibernética.
    - A falta de um quadro legal e de padrões cibernéticos.
    - Incerteza na responsabilidade.
    - A falta de compreensão dos riscos cibernéticos.
    - A falta de cobertura do seguro cibernético.
    - A novidade do mercado, que significa que as seguradoras têm dados limitados para definir prêmios.
    - A falta de padrões e condições padronizadas no mercado de seguro cibernético.

2020

1. ***Aziz, Suhardi e Kurnia [114] - A systematic literature review of cyber insurance challenges***

    - A falta de dados confiáveis e a falta de conhecimento sobre segurança cibernética estão entre os desafios no seguro cibernético.
    - A falta de conhecimento sobre segurança cibernética estão entre os desafios no seguro cibernético.
    - Dificuldade na definição do escopo do risco cibernético.
    - Dificuldade na avaiação do valor do ativo.
    - Falta de padronização nas apólices de seguro cibernético.

- Falta de transparência.
- Falta de cooperação entre seguradoras e empresas de segurança cibernética.
- Dificuldade na avaiação da eficácia da cobertura de seguro cibernético.

2. ***Facchinetti, Giudici e Osmetti [60] - Cyber risk measurement with ordinal data***

    - A falta de dados quantitativos sobre perdas em ataques cibernéticos, que muitas vezes não estão disponíveis por serem sensíveis e difíceis de serem obtidos.
    - A necessidade de coletar e classificar dados sobre diferentes tipos de ataques cibernéticos e as técnicas utilizadas nesses ataques.

3. ***Moro [19] - Towards an Economic Cyber Loss Index for Parametric Cover Based on IT Security Indicator: A Preliminary Analysis***

    - A ausência de limitações geográficas para os riscos cibernéticos e a natureza sistêmica desse risco são confirmadas por meio da análise da atividade de TI em diferentes países.
    - A falta de dados ainda limita a aplicabilidade do modelo proposto.
    - A falta de dados confiáveis sobre riscos cibernéticos.
    - A complexidade na identificação de perdas e fontes de perdas.
    - A falta de modelos de precificação confiáveis para produtos de seguros cibernéticos.
    - A falta de apetite ao risco por parte das seguradoras e resseguradoras devido à acumulação potencial de perdas.
    - O número crescente de crimes na Internet e o total anual de perdas seguradas por catástrofes cibernéticas, que podem chegar a 14 bilhões de dólares
    - O risco de mudança .
    - Riscos de acumulação incalculáveis.
    - Relutância das organizações em divulgar informações sobre suas vulnerabilidades de segurança.
    - A duração incerta dos eventos de risco cibernético torna difícil identificar a fonte e a extensão das perdas, o que pode dificultar a avaliação de riscos e a criação de modelos de precificação confiáveis.
    - A complexidade para modelar o risco cibernético, o que dificulta a criação de produtos de resseguro para cobrir esses riscos.

2021

1. ***Xu e Hua [115] - Cybersecurity Insurance: Modeling and Pricing***

    - Os dados sobre riscos cibernéticos podem ser escassos, o que dificulta a modelagem precisa do risco.

- A complexidade da propagação de ataques em redes de computadores, que pode ser difícil de modelar com precisão.
- A dificuldade em estimar as correlações entre os riscos cibernéticos, que são necessárias para avaliar a dependência entre eles.

2022

1. ***Crotty e Daniel [116] - Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment***

    - A falta de dados numéricos adequados para conduzir análises quantitativas de risco.
    - A abordagem qualitativa de avaliação de risco é amplamente utilizada, mas é questionada por sua falta de precisão e dificuldade na compreensão dos usuários.
    - A falta de especialização e dados também é um grande desafio para os esforços de avaliação de risco de segurança cibernética.

2. ***Erola et al. [117] - A system to calculate Cyber Value-at-Risk***

    - A subjetividade na atribuição de valores de eficácia dos controles de segurança.
    - A falta de dados históricos sobre perdas cibernéticas para validar as estimativas do sistema.
    - A necessidade de incorporar machine learning e outros métodos para melhorar a precisão das estimativas de perda.
    - A dificuldade em obter dados de outras organizações para comparar o desempenho de segurança e avaliar o risco residual.
    - A complexidade do modelo de ameaças e controles de segurança, que pode tornar difícil para as organizações implementarem todas as medidas recomendadas.

3. ***Kejwang [118] - Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature***

    - Alguns estudos anteriores destacados no artigo apresentaram lacunas no conhecimento e metodologia, evidenciando a dificuldade em compreender completamente o efeito das práticas de gerenciamento de risco de segurança cibernética no desempenho do setor de seguros.

4. ***Malavasi et al. [18] - Cyber risk frequency, severity and insurance viability***

    - Malavasi et al. [18] informam que a natureza complexa e heterogênea do risco cibernético torna difícil distinguir atributos estatísticos importantes para diferentes tipos de risco cibernético, como comportamento de cauda.
    - A a falta de dados históricos confiáveis e a natureza em constante evolução das ameaças cibernéticas tornam difícil a previsão precisa do risco cibernético.
    - Necessidade de um gerenciamento de risco mais colaborativo entre seguradoras, empresas e especialistas em cibersegurança.

2023

1. ***Kim e Song [103] - Cyber risk measurement via loss distribution approach and GARCH model***

    - O risco cibernético é um tipo de risco operacional que apresenta características diferentes das perdas operacionais tradicionais, o que pode dificultar a modelagem do risco cibernético.
    - Para a área de seguros, um dos grandes desafios encontra-se na escassez doe dados para a análise, podendo afetar a precisão do modelo.

2. ***Pour et al. [101] - A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security***

    - A complexidade da internet e sua inter-relação com o mundo físico.
    - A necessidade de coleta e análise de dados empíricos em larga escala.
    - O desenvolvimento de novas metodologias para garantir precisão e integridade.
    - A diversidade excessiva de dispositivos IoT.
    - Escassez de dados.

3. ***Tsohou et al. [119] - Cyber insurance: state of the art, trends and future directions***

    - Os desafios enfrentados pelas seguradoras incluem a complexidade do processo de subscrição, a falta de dados históricos e a dificuldade de quantificar o risco cibernético.
    - As políticas e contratos de seguro cibernético são complexos e podem variar amplamente em termos de cobertura e exclusões.
    - A falta de clareza e consistência nas políticas e contratos de seguro cibernético.
    - A dificuldade em avaliar o valor das perdas relacionadas a ataques cibernéticos.
    - A falta de harmonização da linguagem e terminologia usadas entre as partes interessadas no mercado de seguro cibernético.
    - A correlação de riscos e a dispersão geográfica do risco.

TOMADA DE DECISÃO

2019

1. ***Llansó, McNeil e Noteboom [51] - Multi-Criteria Selection of Capability-Based Cybersecurity Solutions***

    - Seleção de soluções de mitigação que atendam aos critérios conflitantes organizacionais.
    - Dificuldade de adapatação de abordagem a diferentes ambientes organizacionais (diferentes ameaças, orçamentos e tolerância a risco).

- A avaliação das soluções defensivas recomendadas devido a ambientes-alvo com cenários distintos.

2. ***Mustafa e Kar [129] - Prioritization of multi-dimensional risk for digital services using the generalized analytic network process***

    - Dentre os deafios e dificuldades tratados no artigo, destaca-se: a relutância dos usuários em fornecer informações pessoais, e o tamanho da amostra que se demonstrou pequena, limitando a generalização dos resultados.

3. ***Zhao et al. [8] - Construction and Security Measurement of Cybersecurity Metrics Framework Based on Network Behavior***

    - Embora não trate de forma direta os desafios, observa-se que a criação do modelo exige um esforço maior na seleção dos indicadores quantitificáveis que possam fornecer informações relevantes e precisas a respeito da situação da rede.
    - A implementação em grandes redes complexas exigirá uma coleta de grande volume de dados, assim como uso de ferramentas avançadas para a análise desses dados.

2020

1. ***Ansari et al. [130] - A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development***

    - A identificação das ameaças ao sistema de software.
    - A seleção de critérios de segurança apropriados.
    - A avaliação de riscos.
    - A garantia da conformidade com as normas de segurança.
    - A escolha do método de SRE mais adequado para o ambiente em que será utilizado.
    - A necessidade de melhorar os métodos de SRE existentes.
    - A importância de considerar a evolução constante das necessidades do mercado.
    - O ambiente de saúde requer atenção especial no desenvolvimento de software.

2. ***Bhol, Mohanty e Pattnaik [61] - Cyber Security Metrics Evaluation Using Multi-criteria Decision-Making Approach***

    - O artigo não apresenta desafios ou dificuldades em relação à avaliação das métricas de segurança cibernética

3. ***Ribeiro e Canedo [82] - Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security***

    - Adaptação da proteção de dados pessoais da UnB aos padrões da LGPD.

- Identificação e seleção dos critérios de segurança de dados pessoais mais relevantes para a implementação da LGPD na UnB.
- Definição de alternativas para cada um dos critérios de segurança de dados pessoais selecionados.
- Redução da ocorrência de eventos inesperados durante a implementação dos critérios de segurança de dados pessoais.

4. ***Ganin et al. [24] - Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management***

    - A complexidade e a natureza em constante mudança dos sistemas cibernéticos tornam difícil quantificar ameaças e vulnerabilidades de forma precisa e abrangente.
    - A falta de dados disponíveis e a incerteza em relação às consequências dos riscos cibernéticos tornam a avaliação mais desafiadora.
    - A complexidade das abordagens existentes para avaliação de riscos cibernéticos pode tornar o problema ainda mais difícil de resolver.
    - A metodologia apresentada no artigo pode ser desafiadora para ser implementada em grande escala
    - A metodologia pode exigir recursos consideráveis, como especialistas em análise de decisão e ferramentas de análise de riscos cibernéticos, que podem não estar disponíveis em todas as organizações.
    - A distribuição dos sistemas cibernéticos em diferentes domínios (físico, informacional e social) e suas complexas estruturas de rede aumentam a complexidade da avaliação de riscos.
    - As limitações das abordagens atuais para avaliação de riscos cibernéticos em abranger todos os componentes de riscos e integrar vários domínios de sistemas cibernéticos

5. ***Shojaeshafiei, Etzkorn e Anderson [9] - Analytic hierarchy process-based fuzzy measurement to quantify vulnerabilities of web applications***

    - A determinação de fatores e subfatores de segurança para aplicações web é uma tarefa árdua e complexa, pois esses fatores devem representar os componentes essenciais da qualidade de segurança das aplicações e cobrir múltiplos aspectos da segurança em aplicações web.
    - A construção de regras de lógica fuzzy para lidar com dados imprecisos e incertos pode aumentar significativamente dependendo do número de variáveis.
    - A falta de pesquisas sobre a quantificação de vulnerabilidades em aplicações web torna difícil avaliar a eficácia e a precisão da metodologia proposta em comparação com outras abordagens existentes
    - A falta de uma metodologia para quantificar vulnerabilidades em aplicações web pode tornar difícil avaliar a eficácia das medidas de segurança implementadas e aprimorar a segurança das aplicações

- A construção de regras de lógica fuzzy pode se tornar muito complexa e aumentar significativamente dependendo do número de variáveis, o que pode dificultar a aplicação da abordagem em aplicações web com muitos fatores de segurança
- A lógica fuzzy pode se tornar muito complexa.

2021

1. ***Abushark et al. [89] - Usability Evaluation through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective***

    - A complexidade e natureza dinâmica da usabilidade do método multicritério proposto.
    - A identificação e priorização dos requisitos de segurança devido sua natureza multifacetada.
    - A constante evolução das ameaças e vulnerabilidades.

2. ***Alharbi et al. [131] - Analyzing the impact of cyber security related attributes for intrusion detection systems***

    - A falta de uma metodologia reconhecida que apoie o processo de tomada de decisão na escolha dos métodos e meios corretos de cibersegurança é um obstáculo significativo para o desenvolvimento da fabricação sustentável.
    - Aumento da quantidade de interfaces entre as soluções de TI das empresas, o que pode levantar preocupações de segurança.
    - Dificuldades na interoperabilidade de componentes, produtos e sistemas.
    - Dificuldades na contratação de trabalhadores tecnicamente qualificados para empresas cada vez mais digitalizadas.
    - Dificuldades na medição da sustentabilidade e métodos para sua mensuração.

3. ***Belinda et al. [90] - Evaluating Software Quality Attributes using Analytic Hierarchy Process (AHP)***

    - A seleção dos atributos de qualidade de software se demonstrou um grande desafio em virtude de muitos modelos disponíveis.
    - O uso do AHP pode requerer habilidades e conhecimentos específicos, podendo representar dificuldades na sua aplicação.

4. ***Torbacki [80] - A hybrid mcdm model combining danp and promethee ii methods for the assessment of cybersecurity in industry 4.0***

    - Aumento da quantidade de interfaces entre as soluções de TI das empresas, o que pode levantar preocupações de segurança.
    - Falta de uma metodologia reconhecida que apoie o processo de tomada de decisão na escolha dos métodos e meios corretos de cibersegurança.

- Dificuldades na interoperabilidade de componentes, produtos e sistemas.
- Dificuldades na contratação de trabalhadores tecnicamente qualificados para empresas cada vez mais digitalizadas.
- Dificuldades na medição da sustentabilidade e métodos para sua mensuração.

2022

1. ***Abushark et al. [88] - Cyber Security Analysis and Evaluation for Intrusion Detection Systems***

    - Aumento no número de violações de segurança.
    - A necessidade de detectar e responder rapidamente às violações.
    - Complexidade de identificar ameaças cibernéticas sofisticadas.
    - Dificuldade em lidar com incertezas e imprecisões na avaliação de sistemas de segurança cibernética.
    - Necessidade de métodos eficazes de avaliação em situações em que a informação é incompleta ou ambígua.

2. ***Alfakeeh et al. [132] - Sustainable-Security Assessment Through a Multi Perspective Benchmarking Framework***

    - A limitação dos dados para sistemas de software de informações de saúde, que foram coletados de uma amostra pequena de pessoas.
    - O número de elementos que influenciam o efeito de segurança sustentável pode variar.

3. ***Alghassab [87] - Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector***

    - A falta de:
    - (i) Regulamentação e de padrões de segurança cibernética específicos para sistemas de controle industrial,
    - (ii) Acesso a conjuntos de dados imparciais e em tempo real para avaliar a segurança cibernética desses sistemas,
    - (iii) Conscientização sobre os riscos de segurança cibernética em sistemas de controle industrial,
    - (iv) Avaliações de segurança cibernética específicas para sistemas de controle industrial, que geralmente são voltadas para sistemas de tecnologia da informação, e,
    - (v) Autenticação e acesso regulamentado nos sistemas de controle industrial.

4. ***Alshahrani et al. [133] - Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach***

    - A natureza dinâmica dos riscos de ativos de TI.

- A falta de liderança nos projetos de TI.
- A falta de consideração aos aspectos humanos no layout e integração do sistema.
- A falta de investimento em soluções de segurança de TI.
- A importância de abordagens adequadas para avaliação e gerenciamento de riscos de TI.
- A necessidade de uma cultura de segurança de TI nas organizações.

5. ***Gonzales et al. [134] - Priority Roles of Stakeholders for Overcoming the Barriers to Implementing Education 4.0: An Integrated Fermatean Fuzzy Entropy-Based CRITIC-CODAS-SORT Approach***

    - Falta de colaboração.
    - Ameaças de cibersegurança.
    - Preocupações com a saúde.
    - Necessidade de identificar papéis específicos de stakeholders para superar as barreiras na implementação da EDUC4.
    - Complexidade do processo de tomada de decisão em instituições de ensino superior em países em desenvolvimento.

2023

1. ***Altubaishe e Desai [86] - Multicriteria Decision Making in Supply Chain Management Using FMEA and Hybrid AHP-PROMETHEE Algorithms***

    - A coleta de dados precisos e confiáveis de fornecedores, a identificação e avaliação de riscos potenciais, a comunicação eficaz com fornecedores e a mitigação de riscos.
    - O uso generealizado de sensores IoT em diferentes níveis da cadeia de suprimentos implica em riscos que exigem implementação de metodologia na seleção de fornecedores.

2. ***Sukumar, Mahdiraji e Jafari-Sadeghi [85] - Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors***

    - A falta de dados confiáveis e completos sobre riscos cibernéticos em pequenas empresas de e-commerce.
    - Orçamentos limitados para investir em medidas de segurança cibernética.
    - Falta de conhecimento e conscientização sobre riscos cibernéticos entre os proprietários e funcionários dessas empresas.

Apêndice 02 - Frameworks Utilizados e Citados

Frameworks de mercado voltados para a segurança da informação e segurança cibernética que foram citados ou utilizados pelos autores dos artigos avaliados.
Os textos estão distribuídos pelo Tópico principal do artigo (MCDM, Segurança Cibernética, Segurança da Informação, Seguros, por exemplo e por ano de publicação

APETITE A RISCO

2021

1. ***Maček et al. [27] - A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética
    - CORAS
    - CRAMM
    - ISO - Família de Normas
    - ISO 27005
    - ISO 31010
    - NIST - Família de Normas
    - NIST 800-30
    - NIST 800-37
    - OCTAVE
    - OWASP
    - STORE

ASPECTOS HUMANOS

2021

1. ***Aman e Shukaili [28] - A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética
    - ENISA

CADEIA DE SUPRIMENTOS

2021

1. ***Uraipan, Praneetpolgrang e Manisri [73] - Application of a fuzzy analytic hierarchy process to select the level of a cyber resilient capability maturity model in digital supply chain systems***

    - CIS CSC
    - COBIT
    - ISA 62443-2-1:2009
    - ISA 62443-3-3:2013
    - ISO 22301
    - ISO 27001
    - ISO 27002
    - ISO 27005
    - ISO 27032
    - ISO 28000
    - ISO 31000
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas
    - NIST 800-53

CADEIA DE SUPRIMENTOS CIBERNÉTICOS

2022

1. ***Creazza et al. [23] - Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era***

    - *Cyber Supply Chain Risk Management* (CSCRM)
    - *General Data Protection Regulation* (GDPR)

COMPARTILHAMENTO DE INFORMAÇÕES

2019

1. ***Colicchia et al. [136] - Information Sharing in Supply Chains: a review of risks and opportunities using the Systematic Literature Network Analysis (SLNA)***

- FC
- MPC
- Secure Multi-Party Computation

COMPETÊNCIAS CHAVE

2021

1. ***Chowdhury e Gkioulos [65] - Key competencies for critical infrastructure cyber-security: a systematic literature review***

    - ICS
    - KSA
    - NICE
    - NIST - Família de Normas
    - NISTIR

DISPONIBILIDADE DE DADOS

2022

1. ***Cremer et al. [137] - Cyber risk and cybersecurity: a systematic review of data availability***

    - FAIR
    - FC
    - GDPR
    - KRI

GEO-ESPACIAL

2019

1. ***Yee et al. [92] - A systematic review of the applications of multi-criteria decision-making methods in site selection problems***

    - CC

GERENCIAMENTO DE RISCOS

2017

1. ***Joshi e Singh [138] - Information security risks management framework – A step towards mitigating security risks in university network***

    - *Common Vulner- ability Scoring System* (CVSS)
    - *Threat Agent Risk Assessment* (TARA)
    - FAIR
    - NIST - Família de Normas
    - NIST RMF
    - OCTAVE

2019

1. ***Sokri [139] - Cyber Security Risk Modelling and Assessment: A Quantitative Approach***

    - CC
    - ISO - Família de Normas
    - ISO 27001
    - KRI
    - NIST - Família de Normas
    - NIST 800-100
    - NIST 800-55
    - Simulação de Monte Carlo

2020

1. ***Ghadge et al. [10] - Managing cyber risk in supply chains: A review and research agenda***

    - ISO - Família de Normas
    - ISO 9001

2. ***Maček, Magdalenić e Ređep [78] - A systematic literature review on the application of multicriteria decision making methods for information security risk assessment***

    - CC
    - COBIT
    - CORAS

- COSO
- ENISA
- FAIR
- FC
- ISO - Família de Normas
- ISO 27001
- ISO 27005
- ISO 31010
- ISRM
- MAGERIT
- NIST - Família de Normas
- NIST 800-30
- NIST 800-53
- OCTAVE
- OWASP
- TARA

2021

1. ***Larsen e Lund [62] - Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review***

    - ENISA

2. ***Quinn et al. [17] - NISTIR 8286A - Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management***

    - ISO 31000
    - ISO 31010
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas
    - NIST 800-30
    - NIST 800-53
    - NIST 800-53A
    - NISTIR 8286A

3. ***Taylor, Surridge e Pickering [140] - Regulatory Compliance Modelling Using Risk Management Techniques***

- *Cyber Security, Decision Support*
- BPMN
- GDPR
- ISO - Família de Normas
- ISO 27000
- ISO 27002
- ISO 27005
- SSM
- Trust Builder

2022

1. ***Kitsios, Chatzidimitriou e Kamariotou [141] - Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry***

    - *Information Security Management System* (ISMS)
    - ISO - Família de Normas
    - ISO 17799
    - ISO 27000
    - ISO 27001
    - ISO 27002
    - ISO 27005
    - ISO 31000
    - NIST - Família de Normas
    - NIST 800-30

GESTÃO DE RISCOS CIBERNÉTICOS E INFORMACIONAIS

2019

1. ***Colicchia, Creazza e Menachof [142] - Managing Cyber and Information Risks in Supply Chains: insights from an Exploratory Analysis***

    - CSCRM
    - ISO - Família de Normas
    - ISO 27000

- ISO 31000
- ISO 31010
- NIST - Família de Normas

LOGÍSTICA REVERSA

2015

1. ***Rezaei [143] - A Systematic Review of Multi-criteria Decision-making Applications in Reverse Logistics***

    - CC

PARTES INTERESSADAS

2015

1. ***Soltani et al. [144] - Multiple stakeholders in multi-criteria decision-making in the context of Municipal Solid Waste Management: A review***

    - KRI
    - STORE

2019

1. ***Gordon et al. [107] - Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions***

    - CC
    - FAIR
    - ICS
    - NIST - Família de Normas
    - NISTIR

2020

1. ***Kessler et al. [109] - Information security climate and the assessment of information security risk among healthcare employees***

    - HIPAA

2021

1. ***Desolda et al. [64] - Human Factors in Phishing Attacks: A Systematic Literature Review***
    - CC
    - KRI
2. ***Nifakos et al. [145] - Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review***
    - 104-191
    - 27799
    - 80001
    - BYOD
    - ENISA
    - ISO - Família de Normas
    - ISO 27000
    - ISO 27001
    - ISO 27002
    - NIST - Família de Normas
    - NIST 800-53
    - Regulamento (UE) 2016/679

2022

1. ***AL-Nuaimi [110] - Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review***
    - BYOD
    - Estrutura de Segurança Cibernética
    - GDPR
    - NIST - *National Institute of Standards and Technology*
    - NIST - Família de Normas
    - SQUARE

PARTES INTERESSADAS - CONSCIÊNCIA CIBERNÉTICA

2022

1. ***Jiang et al. [146] - Systematic Literature Review on Cyber Situational Awareness Visualizations***
    - CC

PROTEÇÃO DE DADOS PESSOAIS MHEALTH

2020

1. ***Pool, Akhlaghpour e Fatehi [147] - Towards a contextual theory of Mobile Health Data Protection (MHDP): A realist perspective***

    - GDPR
    - HIPAA

RISCO CIBERNÉTICO

2017

1. ***Allodi e Massacci [11] - Security Events and Vulnerability Data for Cybersecurity Risk Estimation***

    - COBIT
    - COSO
    - CVSS
    - ISO - Família de Normas
    - ISO 27001
    - ISO 27005
    - ISO 31000
    - ISRM
    - NIST - Família de Normas
    - NIST 800-30
    - SABSA

2. ***Ruan [98] - Introducing cybernomics: A unifying economic framework for measuring cyber risk***

    - ISO - Família de Normas
    - ISO 27000
    - ISO 27002
    - ISO 27005
    - ISO 31000
    - NICE
    - NIST - Família de Normas
    - NIST 800-37
    - NIST 800-53

SEGURANÇA CIBER FÍSICA

2022

1. ***Xu, Gao e Age [148] - Management Solutions for Cyber-Physical Security in Smart Built Environment***

    - *security-oriented cyber-physical contingency analysis* (SOCCA)
    - KRI
    - NIST - Família de Normas

SEGURANÇA CIBERNÉTICA

2016

1. ***Sharkov [106] - From Cybersecurity to Collaborative Resiliency***

    - CC
    - ENISA
    - STIX
    - TAXII

2017

1. ***Allodi e Massacci [11] - Security Events and Vulnerability Data for Cybersecurity Risk Estimation***

    - *Security Operation Center* (SOC)
    - COBIT
    - COSO *Enterprise Risk Management*
    - CVSS
    - EU 2013/0027 NIS—Network and Information Security
    - ISO - Família de Normas
    - ISO 27001
    - ISO 27005
    - ISO 31000
    - ISRM
    - NIST - *Information Security Handbook*
    - NIST - *National Institute of Standards and Technology*

- NIST - Família de Normas
- NIST 800-30
- PCI-DSS
- SABSA

2. ***Gcaza e Solms [105] - A strategy for a cybersecurity culture: A South African perspective***

    - Estrutura de Segurança Cibernética

3. ***Rea-Guaman et al. [72] - Modelos de Madurez en Ciberseguridad: una revisión sistemática***

    - COBIT

2018

1. ***Waxler [149] - Prioritizing Security Controls Using Multiple Criteria Decision Making for Home Users***

    - Estrutura de Segurança Cibernética
    - FC
    - FIPS 199
    - ISO - Família de Normas
    - ISO 27001
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas
    - NIST 800-37
    - NIST 800-53

2019

1. ***Al-Sartawi [150] - Information Technology Governance: The Role of Board of Directors in Cybersecurity Oversight***

    - Estrutura de Segurança Cibernética

2. ***Carcary et al. [20] - A Framework for Managing Cybersecurity Effectiveness in the Digital Context***

    - CC
    - COBIT
    - Estrutura de Segurança Cibernética

- ISO - Família de Normas
- ISO 27001
- ISO 27002
- ISO 31000

3. ***Mbanaso, Abrahams e Apene [59] - Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework***

    - *Centre for Internet Security* (CIS) *Security Controls*
    - *Critical Information Infrastructure* (CII)
    - *Cybersecurity Resilience Maturity Measurement* (CRMM)
    - *Cybersecurity Resilience Quadrants* (CRQs)
    - COBIT
    - ENISA
    - Estrutura de Segurança Cibernética
    - ISO - Família de Normas
    - ISO 15504
    - ISO 27000
    - ISO 27005
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas
    - NISTIR
    - SoGP for IS

4. ***Zaburko e Szulzyk-Cieplak [151] - Information security risk assessment using the AHP method***

    - GDPR
    - ISO - Família de Normas
    - ISO 27001

2020

1. ***Ulven e Wangen [7] - A Systematic Review of Cybersecurity Risks in Higher Education***

    - BYOD
    - GDPR
    - ISO - Família de Normas
    - ISO 27001
    - ISO 27002
    - ISO 27005
    - KPI

2021

1. ***Insua et al. [135] - An Adversarial Risk Analysis Framework for Cybersecurity***

    - *Agence Nationale de la Scurit des Systems d'Information* (ANSSI)
    - *Central Communication and Telecommunication Agency* (CCTA)
    - *Cloud Security Alliance* (CSA)
    - *Common Criteria Recognition Agreement Members* (CCRA)
    - CC
    - CORAS
    - CRAMM
    - EBIOS
    - ISF
    - ISO - Família de Normas
    - ISO 27001
    - ISO 27005
    - MAGERIT
    - NIST - Família de Normas
    - NIST 800-30

2. ***Moreira et al. [79] - Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology***

    - Estrutura de Segurança Cibernética
    - NIST - Família de Normas

3. ***Petrova [152] - A Decision Hierarchical Model of Cyber Security Risk Assessment***

    - ISO - Família de Normas
    - ISO 27005
    - NIST - Família de Normas
    - NIST 800-30

SEGURANÇA DA INFORMAÇÃO

2018

1. ***MITRE [153] - CROWN JEWELS ANALYSIS***

    - DoDM 3020.45
    - HSPD-7
    - NIPP

SEGURO E RESSEGURO

2005

1. ***Gai e Vause [96] - Measuring Investors' Risk Appetite***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2014

1. ***Belles-Sampera, Guillén e Santolino [15] - Beyond Value-at-Risk: GlueVaR Distortion Risk Measures***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2016

1. ***Eling e Schnell [111] - What do we know about cyber risk and cyber risk insurance?***

    - *Bundesamt für Sicherheit in der Informationstechnik* (BSI)
    - *Cambridge Center for Risk Studies* (CCRS)
    - *Cyber Security Best Practices*
    - *National Association of Insurance Commissioners* (NAIC)
    - *National Vulnerability Database* do NIST
    - *Risk Management Solutions* (RMS)
    - ISO - Família de Normas
    - ISO 27005
    - NIST - Família de Normas
    - NIST *National vulnerability database*

2017

1. ***Camillo [154] - Cyber risk and the changing role of insurance***

    - GDPR
    - ISO - Família de Normas
    - ISO 27001

2. ***Franke [155] - The cyber insurance market in Sweden***

- ENISA

3. ***Peter [97] - Cyber resilience preparedness of Africa's top-12 emerging economies***

    - ISO - Família de Normas
    - ISO 27001

4. ***Ruan [98] - Introducing cybernomics: A unifying economic framework for measuring cyber risk***

    - BSI Guide- RuSecure- Based on BS7799 Standard
    - Business Process: Information Risk Management (BPIRM)
    - Central computer and Telecommunication Agency Risk Analysis and Management Method (CRAMM)
    - Construct a platform for Risk Analysis of Security Critical Systems (CORAS)
    - Consultative, Objective and Bi-functional Risk Analysis (COBRA)
    - Control Objectives for Information and Related Technology (COBIT)
    - Cost-Of-Risk Analysis (CORA)
    - Information Security Forum (ISF)
    - Information Security Risk Analysis Method (ISRAM)
    - ISO - Família de Normas
    - ISO 27000
    - ISO 27002
    - ISO 27005
    - ISO 31000
    - IT Infrastructure Library (ITIL)
    - NICE
    - NIST - Família de Normas
    - NIST 800-37
    - NIST 800-53
    - NIST 800-57
    - Operational Critical Threat and Vulnerability Evaluation (OCTAVE)
    - Simple to Apply Risk Analysis (SARA)
    - Simplified Process for Risk Identification (SPRINT)

2019

1. ***Feng e Wang [112] - Does CIO risk appetite matter? Evidence from information security breach incidents***

    - ISO - Família de Normas
    - ISO 27001
    - KRI

2. ***Tonn et al. [113] - Cyber risk and insurance for transportation infrastructure***

    - FAIR
    - FC
    - GDPR
    - HIPAA
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas

2020

1. ***Aziz, Suhardi e Kurnia [114] - A systematic literature review of cyber insurance challenges***

    - *Cyber Risk Assessment and Mitigation* (CRAM)
    - ISO - Família de Normas
    - ISO 27102

2. ***Facchinetti, Giudici e Osmetti [60] - Cyber risk measurement with ordinal data***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética
    - ICS

3. ***Moro [19] - Towards an Economic Cyber Loss Index for Parametric Cover Based on IT Security Indicator: A Preliminary Analysis***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2021

1. ***Xu e Hua [115] - Cybersecurity Insurance: Modeling and Pricing***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2022

1. ***Crotty e Daniel [116] - Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment***

    - FAIR
    - GDPR
    - ISO - Família de Normas
    - ISO 27005
    - ISO 31000
    - ISO 31010
    - NIST - Família de Normas
    - NIST 800-30

2. ***Erola et al. [117] - A system to calculate Cyber Value-at-Risk***

    - *Critical Security Controls* (SANS)
    - ISO - Família de Normas
    - ISO 27001
    - Modelo de distribuição de Poison
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas
    - Simulações de Monte Carlo

3. ***Kejwang [118] - Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature***

    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas

4. ***Malavasi et al. [18] - Cyber risk frequency, severity and insurance viability***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2023

1. ***Kim e Song [103] - Cyber risk measurement via loss distribution approach and GARCH model***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2. ***Pour et al. [101] - A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

3. ***Tsohou et al. [119] - Cyber insurance: state of the art, trends and future directions***

    - *European Union Agency for Cybersecurity* (ENISA)
    - *Information Security Management System* (ISMS)
    - *International Standardization Organization* (ISO)
    - COBIT
    - ENISA
    - ISO - Família de Normas
    - ISO 27001
    - ISO 27002
    - ISO 27005
    - NIST - Família de Normas

SERVIÇO DE NUVEM

2018

1. ***Alabool et al. [156] - Cloud service evaluation method-based Multi-Criteria Decision-Making: A systematic literature review***

    - CC
    - SSM

TOMADA DE DECISÃO

2007

1. ***Gamper e Turcanu [83] - On the governmental use of multi-criteria analysis***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2019

1. ***Alzahrani e Johnson [26] - AHP-based Security decision making: How intention and intrinsic motivation affect policy compliance***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2. ***Llansó, McNeil e Noteboom [51] - Multi-Criteria Selection of Capability-Based Cybersecurity Solutions***

    - CVSS
    - NIST - Família de Normas
    - NIST *National Vulnerability Database*

3. ***Mustafa e Kar [129] - Prioritization of multi-dimensional risk for digital services using the generalized analytic network process***

    - CC
    - CCM
    - SQUARE

4. ***Zhao et al. [8] - Construction and Security Measurement of Cybersecurity Metrics Framework Based on Network Behavior***

    - Modelagem OODA (Observar, Orientar, Decidir, Agir)
    - CC
    - CCTCEC
    - CEI- PDRM (Characteristic, Efficiency, Impact-Protection, Detection, Response, Management)
    - Common Criteria for Information Security Technology Evaluation was
    - CVSS
    - FC
    - IATF is a guidance document formulated by the National Security Agency (NSA) to describe its information security
    - ISS (American Internet Security System)
    - ITSEC
    - Metric Framework Model of Cyber Security Measurement
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas
    - OODA Circle Based on Network Behavior

- OSI security architecture
- PDR
- PDR Model (Protection Detection Response)
- PDRM
- PDRM Framework
- PDRR (Protection Detection Reaction Recovery) model
- PPDR
- TCSEC
- WPDRRC
- WPDRRC (Warning Protection Detection Reaction Recovery Counterattack)

2020

1. ***Ansari et al. [130] - A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development***

    - HIPAA
    - ISO - Família de Normas
    - ISO 27002
    - ISO 27005
    - MOSRE
    - SQUARE
    - SRE
    - SREF
    - SREP
    - STORE

2. ***Bhol, Mohanty e Pattnaik [61] - Cyber Security Metrics Evaluation Using Multi-criteria Decision-Making Approach***

    - NIST - Família de Normas
    - NIST 800-55

3. ***Ribeiro e Canedo [82] - Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security***

    - *Data Protection Impact Assessment* (DPIA)
    - GDPR
    - ISO - Família de Normas

- ISO 27001
- ISO 27002
- ISO 27701
- LGPD

4. ***Ganin et al. [24] - Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management***

    - *Common Vulnerability Scoring System*
    - *Cyber threat metrics*
    - *Information security risk analysis method* (ISRAM)
    - *Network Security Risk Model* (NSRM)
    - *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE Allegro)
    - *The CIS Security Metrics*
    - 15408
    - CC
    - CVSS
    - Estrutura de Segurança Cibernética
    - ISO - Família de Normas
    - ISO 27000
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - *Framework for Improving Critical Infrastructure Cybersecurity*
    - NIST - Família de Normas
    - OCTAVE

5. ***Shojaeshafiei, Etzkorn e Anderson [9] - Analytic hierarchy process-based fuzzy measurement to quantify vulnerabilities of web applications***

    - *Cybersecurity Framework Requirements to Quantify Vulnerabilities Based on GQM*
    - *Cybersecurity Framework* (CSF)
    - ISO - Família de Normas
    - ISO 27001
    - NIST - Família de Normas
    - NIST 800-53
    - OWASP
    - WAVES

2021

1. ***Abushark et al. [89] - Usability Evaluation through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética
    - SDLC
    - SRE
    - STORE

2. ***Alharbi et al. [131] - Analyzing the impact of cyber security related attributes for intrusion detection systems***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

3. ***Belinda et al. [90] - Evaluating Software Quality Attributes using Analytic Hierarchy Process (AHP)***

    - Modelos de qualidade de software: McCall, Boehm, Dromey, Shackel, FURPS, Nielson, SUMI, ISO 9242-11, ISO 9126, QUIM

4. ***Kissoon [157] - Optimum spending on cybersecurity measures***

    - Estrutura de Segurança Cibernética

5. ***Kissoon [158] - Optimum spending on cybersecurity measures: Part II***

    - Estrutura de Segurança Cibernética
    - NIST - *Cybersecurity Framework* (CSF)
    - NIST - Família de Normas
    - TARA

6. ***Torbacki [80] - A hybrid mcdm model combining danp and promethee ii methods for the assessment of cybersecurity in industry 4.0***

    - 62443
    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética
    - ANNSI
    - estrutura de cibersegurança
    - Estrutura de Segurança Cibernética

- ICS
- ISO - Família de Normas
- ISO 27000
- NIST - Família de Normas
- NIST 800-53

2022

1. ***Abushark et al. [88] - Cyber Security Analysis and Evaluation for Intrusion Detection Systems***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2. ***Alfakeeh et al. [132] - Sustainable-Security Assessment Through a Multi Perspective Benchmarking Framework***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

3. ***Alghassab [87] - Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

4. ***Alshahrani et al. [133] - Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach***

    - CORAS
    - NIST - Família de Normas
    - STORE

5. ***Gonzales et al. [134] - Priority Roles of Stakeholders for Overcoming the Barriers to Implementing Education 4.0: An Integrated Fermatean Fuzzy Entropy-Based CRITIC-CODAS-SORT Approach***

    - Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2023

1. ***Altubaishe e Desai [86] - Multicriteria Decision Making in Supply Chain Management Using FMEA and Hybrid AHP-PROMETHEE Algorithms***

- Além dos métodos apresentados, não foram identificados frameworks voltados para segurança cibernética

2. ***Sukumar, Mahdiraji e Jafari-Sadeghi [85] - Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors***

    - *Core unified risk framework* (CURF)
    - *Factor Analysis of Information Risk* (FAIR)
    - *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE)
    - *security risk assessment* (ISRA)
    - NIST - Família de Normas
    - NIST 800-30

VISÃO HOLÍSTICA

2021

1. ***Al-Turkistani, Aldobaian e Latif [159] - Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review***

    - COBIT
    - DoDAF
    - Federal Enterprise Architecture
    - ISO - Família de Normas
    - MoDAF
    - NIST - Família de Normas
    - SABSA
    - TOGAF
    - Zachman

Apêndice 03 - Critérios e Alternativas Citados

Critérios e Alternativas que foram utilizados pelos autores dos artigos avaliados.
Os textos estão distribuídos pelo Tópico principal do artigo (MCDM, Segurança Cibernética, Segurança da Informação, Seguros, por exemplo e por ano de publicação

APETITE A RISCO

2021

1. ***Maček et al. [27] - A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment***

    - ***1. Ameaça***

        –

    - ***2. Vulnerabilidade***

        –

    - ***3. Probabilidade***

        –

    - ***4. Consequência***

        –

    - ***5. Resiliência***

        –

ASPECTOS HUMANOS

2021

1. ***Aman e Shukaili [28] - A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations***

    - ***1. Fatores organizacionais***

        Fatores organizacionais: Como pode ser visto na Tabela III, Tamanho Organizacional, Valores Compartilhados e Posturas de Risco foram considerados como não críticos. A maioria dos participantes concorda que o tamanho da organização não afeta o desenvolvimento e a execução do CSS desde que haja uma estrutura clara, diretrizes

- 1.01 Política de Segurança da Informação
- 1.02 Suporte à Gestão
- 1.03 Habilidades e perícia
- 1.04 Estrutura de organização
- 1.05 Estratégia
- 1.06 Due diligence

- ***2. Fatores culturais***

  Fatores culturais: de todas as entrevistas realizadas, como evidenciado na Tabela IV, concluiu-se que a maioria dos participantes, com base em suas experiências, acredita que a atitude positiva, o conhecimento e a colaboração dos funcionários são fundamentais para concluir as tarefas em um trabalho em equipe. A conformidade

  - 2.01 Atitude e Comportamento
  - 2.02 Conhecimento
  - 2.03 Colaboração
  - 2.04 Conformidade

- ***3. Fatores legais e políticos***

  Fatores legais e políticos: As entrevistas foram realizadas antes de abril de 2021, quando não havia impostos e taxas de juros introduzidos em Omã. Eles não eram aplicáveis e, portanto, não eram importantes, conforme refletido na Tabela V. Mesmo com sua introdução como aplicação, ainda é uma preocupação nominal para

  - 3.01 Lei de crimes cibernéticos
  - 3.02 Interesse do governo

- ***4. Fatores econômicos***

  Fatores econômicos: Baseados principalmente no financiamento do governo, todos os participantes concordam que é fundamental. Quanto ao custo e orçamento, a maioria acredita que, embora o custo seja um fator importante para investir na eficácia do CSS, não tem sido um problema fundamental para o setor público. Esses

  - 4.01 Financiamento

- ***5. Fatores técnicos***

  Fatores técnicos: Conforme refletido na Tabela VII, todos os participantes acreditam fortemente que os aspectos técnicos do CSS são de extrema importância. Essa percepção é verdadeira principalmente porque parte substancial das operações e processos são suportados por sistemas baseados em TI nos quais os fatores

  - 5.01 Segurança do aplicativo
  - 5.02 Planejamento de recuperação de desastres
  - 5.03 Planejamento de Continuação de Negócios
  - 5.04 Auditoria de segurança
  - 5.05 Nível de proteção

- ***6. Fatores de risco***

  Fatores de risco: O consenso comum sobre os fatores de risco foi que todos eles são de grande importância, pois todos precisam ser monitorados, analisados e gerenciados com seriedade, não apenas no contexto de um CSS eficaz, mas também no que diz respeito à sensibilidade das informações públicas com as quais estão

  - 6.01 Vulnerabilidades
  - 6.02 Ameaças e Ataques
  - 6.03 Ator da Ameaça

CADEIA DE SUPRIMENTOS

2021

1. ***Uraipan, Praneetpolgrang e Manisri [73] - Application of an Analytic Hierarchy Process to Select the Level of a Cyber Resilient Capability Maturity Model in Digital Supply Chain Systems***

   - ***1. Identificar***

     Identifica e compreende os diversos contextos de gestão de riscos cibernéticos da cadeia de suprimentos, que adicionou uma nova categoria, estratégia de segurança

     - 1.01 Gestão de ativos
     - 1.02 Ambiente de negócios
     - 1.03 Governança
     - 1.04 Avaliação de risco
     - 1.05 Estratégia de Segurança da Cadeia de Suprimentos
     - 1.06 Gestão de Riscos da Cadeia de Suprimentos

   - ***2. Proteger***

     Define padrões e controles para proteger os sistemas da organização contra o risco cibernético da cadeia de suprimentos digital, que adicionou uma nova categoria,

     - 2.01 Conscientização e Treinamento
     - 2.02 Controle de acesso
     - 2.03 Manutenção
     - 2.04 Privacidade
     - 2.05 Processo e Procedimentos de Proteção de Informações
     - 2.06 Tecnologia de proteção

   - ***3. Detectar***

     Define procedimentos e processos para detectar situações anormais, o que adicionou uma nova categoria de inteligência cibernética, baseada na ISO 27001, ISO 27002

     - 3.01 Anomalias e Eventos

  - 3.02 Inteligência Cibernética
  - 3.03 Monitoramento Contínuo de Segurança
  - 3.04 Processos de detecção
- ***4. Responder*** Descreve métodos e processos para lidar com situações inusitadas que ocorrem, o que acrescentou uma nova categoria, a agilidade da cadeia de suprimentos [39].
  - 4.01 Agilidade da Cadeia de Suprimentos
  - 4.02 Análise
  - 4.03 Comunicação
  - 4.04 Melhorias
  - 4.05 Mitigação
  - 4.06 Planejamento de resposta
- ***5. Recuperar***

  Determina as etapas e processos para restaurar o sistema ao normal, o que acrescentou uma nova categoria, estratégia robusta [39].
  - 5.01 Plano de Recuperação
  - 5.02 Melhorias
  - 5.03 Comunicação
- ***6. Continuar***

  Implementa as várias etapas e procedimentos para permitir que o negócio continue, que é uma nova função baseada na ISO 22301, incluindo 4 categorias:
  - 6.01 Sustentabilidade da cadeia de suprimentos
  - 6.02 Confiabilidade da cadeia de suprimentos
  - 6.03 Plano de continuidade de negócios
  - 6.04 valiação de continuidade de negócios

MÉTODOS MULTICRITÉRIOS

2019

1. ***Alzahrani e Johnson [26] - AHP-based Security decision making: How intention and intrinsic motivation affect policy compliance***

   - ***1. Autonomia***
     - 1.1 Ataque cibernético
     - 1.2 Conformidade com as políticas
     - 1.3 e-mail e Internet
     - 1.4 Resposta a incidentes

- ***2. Competência***
  - 2.1 Ataque cibernético
  - 2.2 Conformidade com as políticas
  - 2.3 e-mail e Internet
  - 2.4 Resposta a incidentes
- ***3. Intenção comportamental***
  - 3.1 Ataque cibernético
  - 3.2 Conformidade com as políticas
  - 3.3 e-mail e Internet
  - 3.4 Resposta a incidentes
- ***4. Relacionamento***
  - 4.1 Ataque cibernético
  - 4.2 Conformidade com as políticas
  - 4.3 e-mail e Internet
  - 4.4 Resposta a incidentes

2. ***Zhao et al. [8] - Construction and Security Measurement of Cybersecurity Metrics Framework Based on Network Behavior***
   - ***1. Detecção***
     - 1.01 Métrica de perigo
     - 1.02 Mudança de fluxo
     - 1.03 Status do host
   - ***2. Gestão***
     - 2.01 Importância do ativo de segurança
     - 2.02 Pontuação de custo de prevenção de vulnerabilidade
   - ***3. Proteção***
     - 3.01 Força da Estratégia de proteção
     - 3.02 Força protetora
   - ***4. Resposta***
     - 4.01 Índice de integridade do equipamento chave
     - 4.02 Índice de tempo de resposta da lista negra
     - 4.03 Plano de Recuperação
     - 4.04 Tempo de resposta à intrusão

3. ***Llansó, McNeil e Noteboom [51] - Multi-Criteria Selection of Capability-Based Cybersecurity Solutions***

- ***1. Organizacional***
  - 1.01 Impacto no Negócio
  - 1.02 Tolerância ao Risco
  - 1.03 Legal e Regulamentar
  - 1.04 Restrições Auto-Impostas
- ***2. Ativo***
  - 2.01 Importância / Valor
  - 2.02 Risco Avaliado
- ***3. Ameaça***
  - 3.01 Antecipado
  - 3.02 Mais Significativo
  - 3.03 Risco Residual
- ***4. Controle***
  - 4.01 Custo
  - 4.02 Compra / Configuração
  - 4.03 Dificuldade de Implementação
  - 4.04 Custo de Operação
  - 4.05 Eficiência, Eficácia, Desempenho, Número de ameaças abordadas
  - 4.06 Grau de implementação
  - 4.07 Alinhamento com Normas
  - 4.08 Disponibilidade
  - 4.09 Número de Benefícios
  - 4.10 Combinação
  - 4.11 Preferência Partes Interessadas

4. ***Mustafa e Kar [129] - Prioritization of multi-dimensional risk for digital services using the generalized analytic network process***

   - ***1. Risco de Privacidade***
     - 1.01 Comprometimento de informações pessoais
     - 1.02 Usos de informações pessoais sem o seu conhecimento
     - 1.03 Controle da minha conta por hackers
   - ***2. Risco Financeiro***
     - 2.01 Perda de dinheiro
     - 2.02 Perda de informações financeiras
     - 2.03 Risco financeiro da conta bancária
   - ***3. Risco Social***

  - 3.01 Efeito negativo do pensamento dos outros
  - 3.02 Perda social por familiares e amigos
- ***4. Risco de Tempo***
  - 4.01 Perda de tempos por inconveniência
- ***5. Risco Psicológico***
  - 5.01 Autoimagem da pessoa
  - 5.02 Perda psicológica por causa da adaptação
- ***6. Risco Físico***
  - 6.01 Ameaça à saúde
  - 6.02 Viva por muito tempo
  - 6.03 Causa da doença
  - 6.04 Exposto por radiação nociva
  - 6.05 Risco de dano cerebral
- ***7. Risco de Performance***
  - 7.01 Entrega de desempenho conforme prometido
  - 7.02 Transação feita pelo provedor de serviços corretamente

2020

1. ***Ansari et al. [130] - A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development***

   - ***1. Ativo***

     Ativo de software seria qualquer processo/serviço que uma corporação utiliza como parte das operações econômicas. Para as empresas, monitorar e gerenciar esses

     –

   - ***2. Objetivo de segurança***

     As metas de segurança indicam claramente o que o sistema de software deve evitar e não como essas medidas preventivas devem ser realizadas

     –

   - ***3. Parte interessada***

     Um stakeholder é uma pessoa, uma organização ou uma comunidade com interesse no sistema de software em desenvolvimento. A perspectiva de uma parte

     –

   - ***4. Requisito de segurança***

     Os requisitos de segurança são implicações de ameaças ao sistema de software que podem ser obtidas apenas a partir do processo de design. Os requisitos de

–

- ***5. Risco***

  O risco é uma previsão de falha; um possível problema que pode ou não surgir no futuro. Geralmente é limitado por falta de informação, regulamentação ou tempo. É a

  –

- ***6. Vulnerabilidade***

  A vulnerabilidade pode ser considerada como defeito do sistema de software que pode considerar deixá-lo aberto à manipulação. A vulnerabilidade também pode corresponder a qualquer tipo de deficiência em um sistema de software por si só, em um conjunto de processos, ou mesmo qualquer coisa que coloque em risco a

  –

2. ***Shojaeshafiei, Etzkorn e Anderson [9] - Analytic hierarchy process-based fuzzy measurement to quantify vulnerabilities of web applications***

   - ***1. Autenticação***

     Com que frequência o DOT exige/lembra aos usuários regulares de aplicativos da Web que tenham autenticação de dois fatores para fazer login no sistema?

     – 1.01 Dois fatores de autenticação
     – 1.02 Username / Password

   - ***2. Autorização e Identificação***

     Com que frequência o DOT controla as políticas de restrição de autorização para usuários/funcionários que interagem com os aplicativos web da empresa?

     – 2.01 Teste de penetração 2

   - ***3. Manutenção***

     Com que frequência o DOT usa qualquer rastreador/mapa de dependência para seu aplicativo da web?

     – 3.01 Alterações de software
     – 3.01 Rastreador de dependência

   - ***4. Segurança do Software***

     Com que frequência o DOT tem controles para garantir que os padrões de qualidade sejam atendidos para todo o desenvolvimento de software?

     – 4.01 Código Fonte Seguro
     – 4.01 Padrões de Qualidade de Desenvolvimento
     – 4.02 Desenvolvimento Seguro

   - ***5. Segurança em tempo de execução***

     Como o firewall baseado em software (Windows ou de terceiros etc.) está sendo executado em computadores DOTs para proteger contra a disseminação interna de

- 5.01 Encriptação
  5.01.01 Outras encriptações
  5.01.01 HTTP/HTTPS
- 5.02 Monitoramento e Log
  5.02.04 Firewall e Antivirus
  5.02.03 XSS 5.02.02 Política de Filtering
  5.02.01 Teste de penetração 1

3. ***Bhol, Mohanty e Pattnaik [61] - Cyber Security Metrics Evaluation Using Multi-criteria Decision-Making Approach***

   - ***1. Suscetibilidade***
     –
   - ***2. Mecanismo de proteção***
     –
   - ***3. Medição de riscos***
     –
   - ***4. Resultados do encontro***
     –

4. ***Ganin et al. [24] - Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management***

   - ***1. Ameaças***

     Definimos ameaça como "uma pessoa ou organização que pretende causar danos" seguindo a abordagem dos Laboratórios Sandia

     - 1.1 Facilidade de Ataque
       1.1.1 Informações
       1.1.2 Tecnologia à disposição 1.1.3 Opções de entrega
     - 1.2 Benefícios
       1.2.3 Outros Ganhos 1.2.2 Ganho Político
       1.2.1 Ganho Financeiro
   - ***2. Vulnerabilidades***

     DiMase et al. 53 destacou a importância de abordar o risco de segurança física cibernética em sistemas complexos em quatro domínios, descritos na doutrina de Comando e Controle do Exército dos EUA. 54 Esses domínios são o físico, o informativo, o cognitivo e o social. Neste trabalho, propomos fundir os domínios social e

     - 2.1 Domínio Físico
       2.1.3 Hardware falsificado
       2.1.1 Facilidade de Acesso Físico 2.1.4 Dispositivos Portáteis
       2.1.2 Hardware Obsoleto

- 2.2 Domínio Informações
  2.2.1 Facilidade de Acesso Lógico
  2.2.2 Software obsoleto 2.2.3 Cobertura antivírus e de varredura
  2.2.3 Software falsificado
- 2.3 Domínio Social
  2.3.3 Controle de Acesso .
  2.3.2 Conscientização e Treinamento 2.3.4 Lealdade e bem-estar
  2.3.1 Histórico de Pessoal

- ***3. Consequências***

  Na grande maioria das abordagens de análise de risco, as consequências associadas aos cenários de risco cibernético são caracterizadas usando a tríade clássica

  - 3.1 Confidencialidade
  - 3.2 Integridade
  - 3.3 Disponibilidade

5. ***Ribeiro e Canedo [82] - Using MCDA for Selecting Criteria of LGPD Compliant Personal Data Security***

   - ***1. Nível de proteção de dados*** A LGPD assume que o Brasil só poderá transferir dados para países que forneçam à LGPD um nível adequado de proteção de dados pessoais. A LGPD determina que a autoridade nacional deve dispor de normas e técnicas para garantir a proteção dos dados.

     - 1.1. Limitando o acesso apenas aos dados do titular
     - 1.2. Anonimização de dados pessoais
     - 1.3. Hashing de dados confidenciais
     - 1.4. Excluindo dados pessoais
     - 1.5. Mantendo dados pessoais armazenados
     - 1.6. Classificando a importância dos dados pessoais

   - ***2. Riscos de segurança***

     A LGPD menciona que órgãos do governo federal e empresas privadas devem ter os riscos relacionados aos dados pessoais identificados, bem como quais ações devem ser tomadas para mitigar esses riscos.

     - 2.1. Definir Agentes de Segurança
     - 2.2. Definir uma Política de Segurança de Dados Pessoais
     - 2.3. Usar Sistema de Criptografia
     - 2.4. Usar Certificado para Acesso a Dados Pessoais
     - 2.5. Criar Grupos de Usuários
     - 2.6. Usar Firewall

- ***3. Gravidade do Incidente***

  Dependendo da gravidade do incidente, a LGPD determina que medidas devem ser tomadas para informar os titulares dos dados sobre os danos causados e medidas devem ser tomadas para reverter ou mitigar os efeitos do incidente.

  - 3.1 Mapear Incidentes Potenciais
  - 3.2 Desenvolver Plano de Resposta a Incidentes
  - 3.3 Avaliar as Melhores Soluções Técnicas de Resolução de Incidentes
  - 3.4 Definir Medidas de Mitigação de Incidentes

- ***4. Riscos de privacidade de dados***

  A LGPD aconselha que os riscos de privacidade de dados sejam registrados e medidas apropriadas sejam tomadas para mitigar esses riscos. de acordo com a LGPD [9], um programa de governança deve ser estabelecido para garantir a privacidade dos dados pessoais. É necessário verificar os possíveis

  - 4.1 Verifique a privacidade dos serviços da Web
  - 4.2 Crie um grupo restrito de acesso a dados pessoais
  - 4.3 Verifique os dados pessoais armazenados por cada um dos sistemas

2021

1. ***Torbacki [80] - A hybrid mcdm model combining danp and promethee ii methods for the assessment of cybersecurity in industry 4.0***

   - ***1 - Serviços de confiança***

     Os serviços fiduciários incluem assinatura eletrônica, selo eletrônico, carimbo de hora eletrônico e entrega eletrônica registrada [69, 70, 71, 72]. Essas soluções aumentam a segurança e a credibilidade de documentos eletrônicos (por exemplo, pedidos de empreiteiros, pedidos de componentes para produção, listas de materiais, pedidos de produção, comprovantes de coleta de materiais, comprovantes de transferência do produto para o depósito, planilhas, cartões de instruções, certificados de segurança do produto, documentos de garantia, guias, faturas e contratos.), especialmente no caso do trabalho remoto, que tem se tornado cada vez mais comum. No contexto da sustentabilidade, estas soluções caracterizam-se pela interoperabilidade informática garantindo a sua operação em múltiplas plataformas e em diversos sistemas operativos, bem como suporte no acesso via Internet e em plataformas móveis. Além disso, Isso contribui para a filosofia da empresa sem papel e reduz o espaço de arquivamento desses documentos e os custos de manutenção, o que reduz os custos diretos do negócio juntamente com o consumo e desperdício de papel e tem um impacto positivo na conservação dos recursos naturais.

     - 1.11 - Assinatura eletrônica, selo eletrônico e carimbo de hora eletrônico
     - 1.12 - Validação e manutenção de assinaturas e selos eletrônicos
     - 1.13 - Entrega Eletrônica Registrada

- ***2 - Criptografia***

  A autenticação dos portais web business to business (B2B) das empresas participantes dos processos da cadeia produtiva é realizada por meio do certificado X.509. Essa técnica de criptografia também é usada para estabelecer conexões VPN seguras entre contratados. O X.509 é uma solução extremamente eficaz e, ao mesmo tempo, não degrada a eficiência do ambiente de TI da empresa sem aumentar a pegada de carbono. Outra solução tecnológica que permite a criptografia de dados

  – 2.21 - Autenticação de portais B2B online; Protocolos X.509/TLS/SSL
  – 2.22 - Tecnologia Blockchain

- ***3 - Segurança de rede***

  A área de produção é particularmente vulnerável a ataques devido à natureza fechada dos sistemas de controle, muitas vezes utilizando tecnologias de TI desatualizadas. Combiná-los com os modernos sistemas de gerenciamento ERP/MRP abertos os abre para ataques cibernéticos de rede. A conectividade de rede abriu as fronteiras dos sistemas industriais que normalmente eram fechados, tornando necessário o controle da operação dos canais de comunicação industrial e das informações que circulam pela rede, principalmente nas extensões sem fio da arquitetura industrial de TI. Como resultado, inesperadamente, a implementação de tecnologias modernas da Indústria 4.0 acelera diretamente a degradação técnica de um parque de máquinas. No contexto da sustentabilidade, o desenvolvimento constante de melhorias de software para algoritmos de captura de ameaças amplia o tempo de uso de máquinas mais antigas nas empresas de manufatura e introduz a filosofia de reutilização da economia circular na área de equipamentos de TI e máquinas de produção, bem como

  – 3.31 - Segurança técnica adequada de uma rede da empresa
  – 3.32 - Arquitetura de rede e servidor ideal
  – 3.33 - Monitoramento e análise de incidentes de segurança

- ***4 - Segurança do aplicativo***

  Para garantir o funcionamento estável dos sistemas de TI nas empresas de produção e a segurança dos dados corporativos, é necessário implementar um sistema de backups e atualizações de software eficazes. Esses problemas têm um impacto direto no aumento da pegada de carbono de uma empresa por meio do aumento da demanda por poder de computação e, portanto, do aumento do consumo de energia pelos servidores. A eficiência do trabalho também diminui como resultado de atividades extraordinárias realizadas pelos funcionários. As cópias de segurança são feitas online em tempo real ou periodicamente: diariamente, semanalmente e mensalmente. Na prática, esse processo significa o lançamento simultâneo de vários servidores que aumentam o consumo de energia, que, juntamente com infraestrutura adicional, estão entre os dispositivos técnicos que mais consomem energia. O servidor mestre de trabalho primário transmite dados para o servidor escravo de backup, que em salas de servidores modernas replica os dados para outro servidor de backup escravo. Deve ser lembrado que a operação de cada servidor é suportada por sistemas de backup de energia adicionais constantemente ativos. Tal solução permite que as empresas manufatureiras sejam resistentes a algumas ameaças cibernéticas, mas ao mesmo tempo causa um aumento na demanda por poder de computação, que está

intrinsecamente ligado ao aumento do consumo de energia. Além de armazenar os dados nos discos dos servidores interconectados, as cópias de backup são armazenadas simultaneamente em mídia externa durável em salas com temperatura e umidade adequadas. A manutenção dessa infraestrutura também aumenta a pegada de carbono de uma empresa.

  - 4.41 - Segurança do banco de dados
  - 4.42 - Estabelecimento de um sistema de backup eficiente
  - 4.43 - Verificação de vulnerabilidades; Análise de código-fonte para procurar fraquezas de software
  - 4.44 - Atualizações de software

- ***5 - Segurança do endpoint***

  Garantir a segurança cibernética do usuário final tem um impacto direto na esfera de sustentabilidade das empresas de manufatura. Com o trabalho remoto em massa dos funcionários da empresa de produção, os dispositivos de TI que eles usam podem ser uma fonte de incidentes cibernéticos. Após infectar o ambiente interno de TI, os sistemas de controle podem, neste caso, desligar as linhas de produção, causando paradas não planejadas, reduzindo a eficiência dos funcionários, aumentando o desperdício de produção, o consumo de água e energia, a pegada de carbono de uma empresa como resultado de startups de controle pré-planejadas. A questão da segurança dos dispositivos dos funcionários era frequentemente marginalizada, pois os equipamentos de TI eram protegidos pelas soluções de segurança de rede corporativa (dimensão D3) e de aplicativos (dimensão D4). No entanto, juntamente com a aceleração paralela da implementação de soluções de trabalho remoto e

  - 5.51 - Técnicas apropriadas para proteger estações de trabalho e dispositivos móveis
  - 5.52 - Antivírus e antimalware
  - 5.53 - Testes de penetração para encontrar vulnerabilidades

- ***6 - Controle de acesso***

  O fator humano é uma das causas mais importantes que ameaçam a segurança do ambiente de TI em empresas manufatureiras. No contexto da sustentabilidade, isso significa que a conscientização sobre as ameaças, a educação e o esquema de treinamento tanto para os funcionários da produção quanto para os departamentos de TI estão se tornando características importantes do uso eficaz de pessoas, processos e tecnologias na área de segurança de sistemas industriais. Particular ênfase

  - 6.61 - Estabelecendo uma conexão remota segura VPN com o servidor corporativo
  - 6.62 - Treinamento regular de funcionários na área de segurança cibernética
  - 6.63 - Criação de regras para gerenciamento de acesso a dados corporativos; Autenticação de usuário

- ***7 - Ataques cibernéticos***

  As empresas manufatureiras que já aplicaram os princípios da sustentabilidade em suas operações também podem aplicá-los no mundo digital. Nessa abordagem, arquivos digitais e bancos de dados coletados pelas empresas criam ambientes de dados digitais com seus equivalentes no

ambiente natural. No caso dos ciberataques, ocorre o vazamento de dados, que, assim como no mundo real, causa contaminação do ambiente de TI, ou seja, a divulgação de dados sensíveis da

- 7.71 - Sistema de Prevenção de Intrusão e Sistema de Detecção de Intrusão com algoritmos para detectar em tempo real os ataques maliciosos
- 7.72 - Firewall, Gateway e Proxy

2. ***Alharbi et al. [131] - Analyzing the impact of cyber security related attributes for intrusion detection systems***

   - ***1. Complexidade de Implementação***

     Como o nome indica, especifica todas aquelas complicações que são consideradas durante todo o processo de implementação de um sistema. Aqui, ele define todos os parâmetros de complexidade que são considerados por pesquisadores, cientistas e outros acionistas para construir um sistema de detecção de intrusão baseado em

     –

   - ***2. Detecção de anomalias***

     A identificação ou detecção de ataques de dia zero (ataques desconhecidos) é uma questão desafiadora e uma das características importantes abordadas pelas abordagens baseadas em ML. O comportamento dos tipos de ataque de dia zero não é registrado no banco de dados de suporte do modelo. Um modelo inteligente

     –

   - ***3. Detecção de ataques DDoS***

     Detecção de ataques DDoS: Os três principais componentes de segurança ou cibersegurança são confidencialidade, integridade e disponibilidade (CIA). Estes são comumente conhecidos como tríade CIA e são considerados os componentes básicos para a segurança de qualquer sistema ou rede. Entre os três, um dos componentes vitais é a disponibilidade. Disponibilidade define literalmente o caráter que deve ser usado ou obtido, mas em segurança da informação, garante que,

     –

   - ***4. Detecção de spam***

     A detecção de spam é um recurso significativo dos sistemas de detecção de intrusão baseados em ML usados para identificar spams. Spam, como termo técnico, está principalmente relacionado a e-mails e é conhecido por alguns outros nomes, como lixo eletrônico ou correio em massa não solicitado. É um conteúdo digital indesejado e

     –

   - ***5. Detecção de uso indevido***

     A detecção de uso indevido é uma característica significativa dos sistemas de detecção de intrusão baseados em ML. A detecção de uso indevido garante a identificação dos ataques de segurança cibernética que são familiares a um sistema de detecção de intrusão [27]. O sistema de detecção de intrusão já conhece a

–

- ***6. Detecção de malware***

  Malware, como um conjunto coletivo de vários softwares maliciosos, principalmente, compromete vírus, spyware, keyloggers e ransomware. Malware é um código desenvolvido por ciberataques com a intenção de causar danos graves no sistema da vítima ou adquirir acesso ilegítimo à rede. Geralmente, é um arquivo codificado

  –

- ***7. Identificação de phishing***

  As invasões cibernéticas são muito comuns atualmente e houve um aumento desenfreado em sua ocorrência. O phishing é um dos ataques de engenharia social comuns e interessantes usados por invasores para roubar dados confidenciais. Os dados direcionados geralmente incluem detalhes do cartão de crédito e credenciais

  –

- ***8. Precisão***

  Isso define a medida do grau de correção e precisão de qualquer computação ou processo correspondente ao padrão correto. É uma das características mais notáveis dos algoritmos de ML. No aprendizado de máquina, a precisão é determinada pela forma como os modelos baseados em ML propostos geram os resultados

  –

3. ***Belinda et al. [90] - Evaluating Software Quality Attributes using Analytic Hierarchy Process (AHP)***

   - ***01. Manutenibilidade***
     - 01.01 Extensibilidade
     - 01.02 Flexibilidade
     - 01.03 Suportabilidade
   - ***02. Usabilidade***
     - 02.01 Compreensibilidade
   - ***03. Confiabilidade***
     - 03.01 Robustez
     - 03.02 Precisão
   - ***04. Testabilidade***

     –
   - ***05. Funcionalidade***
     - 05.01 Correção
     - 05.02 Interoperabilidade

- ***06. Disponibilidade***
  - –
- ***07. Reutilização***
  - –
- ***08. Custo***
  - –
- ***09. Eficiência***
  - 09.01 Performance
- ***10. Portabilidade***
  - 10.01 Adaptabilidade
- ***11. Segurança***
  - 11.01 Confidencialidade
  - 11.02 Integridade
  - 11.03 Não-repúdio

4. ***Abushark et al. [89] - Usability Evaluation through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective***

   - ***1. Eficiência***

     Uma vez que os participantes tenham entendido sobre a interface, com que facilidade eles podem executar a tarefa dada?

     - 1.01 Esforço do usuário
     - 1.02 Economia de tempo
   - ***2. Efetividade***

     Quando os usuários mudam para o protótipo depois de um tempo sem utilizá-lo, com que rapidez eles podem recuperar suas habilidades?

     - 2.01 Operabilidade
     - 2.02 Escalabilidade
     - 2.03 Extensibilidade
   - ***3. Capacidade de aprendizado***

     Quão simples é para os indivíduos completarem tarefas básicas na primeira vez que experimentam uma abordagem SRE?

     - 3.01 Interface do usuário
     - 3.02 Treinamento
     - 3.03 Estrutura do sistema
   - ***4. Satisfação***

     Quão bom é utilizar a abordagem SRE?

  - 4.01 Conveniência
  - 4.02 Simpatia
- ***5. Produtividade*** Quão bom é utilizar a abordagem SRE?
  - 5.01 Resultado útil
  - 5.02 Custo-benefício

2022

1. ***Alshahrani et al. [133] - Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach***
   - ***1 - Eficácia***
     –
   - ***2 - Frequência do evento***
     –
   - ***3 - Disponibilidade***
     –
   - ***4 - Consequência***
     –
   - ***5 - Adequação***
     –
   - ***6 - Descoberta***
     –
   - ***Fatores***
     – De Meio Ambiente
     – Estratégico
     – Financeiro
     – Fornecedores
     – Operacional
     – Pessoas
     – Política e Procedimentos
     – Tecnologia
2. ***Abushark et al. [88] - Cyber Security Analysis and Evaluation for Intrusion Detection Systems***
   - ***1. Complexidade de Implementação***
     Como o nome indica, enumera todas as complexidades que devem ser consideradas durante todo o processo de implementação de um sistema. Ele define todos os parâmetros de complexidade que pesquisadores, cientistas e outros acionistas levam em consideração ao desenvolver um sistema de detecção de intrusão baseado

–

- ***2. Detecção de anomalias***

  A detecção ou identificação de ataques de dia zero (ataques desconhecidos) é um problema difícil e uma das principais características abordadas pelas táticas baseadas em aprendizado de máquina. O banco de dados de suporte da estrutura não registra o comportamento dos tipos de ataque de dia zero. Com base em sua

  –

- ***3. Detecção de ataques DDoS***

  Confidencialidade, Integridade e Disponibilidade (CID) são os três componentes essenciais de segurança ou cibersegurança. A tríade CID é um conjunto de três componentes considerados essenciais para a segurança de qualquer sistema ou rede. Um dos aspectos mais importantes de todos os três é a disponibilidade. Disponibilidade refere-se literalmente ao caráter que deve ser empregado ou adquirido, mas no contexto da segurança da informação, garante que usuários autênticos

  –

- ***4. Detecção de spam***

  a detecção de spam é um aspecto fundamental dos sistemas de detecção de intrusão baseados em aprendizado de máquina, que são empregados para detectar spam. Spam é um termo técnico para e-mail em massa não solicitado que está amplamente conectado a mensagens eletrônicas. Também é conhecido por outros nomes, como

  –

- ***5. Detecção de uso indevido***

  a detecção de uso indevido é um recurso importante dos sistemas de detecção de intrusão baseados em aprendizado de máquina. A detecção de uso indevido garante que os ataques de segurança cibernética conhecidos por um sistema de detecção de intrusão sejam identificados [17]. O sistema de detecção de intrusão já está

  –

- ***6. Detecção de malware***

  Malware, como um conjunto coletivo de vários softwares maliciosos, principalmente, compromete vírus, spyware, keyloggers e ransomware. Malware é um código desenvolvido por ciberataques com a intenção de causar danos graves no sistema da vítima ou adquirir acesso ilegítimo à rede. Geralmente, é um arquivo codificado

  –

- ***7. Identificação de phishing***

  as invasões cibernéticas são bastante comuns nos dias de hoje e sua prevalência aumentou drasticamente. Os invasores utilizam o phishing como um dos ataques de engenharia social mais populares e fascinantes para roubar dados pessoais. Números de cartão de crédito e credenciais de login são frequentemente incluídos nos

–

- ***8. Precisão***

  Esta é a métrica para determinar o grau de correção e precisão de qualquer cálculo ou processo quando comparado ao padrão apropriado. É uma das características mais notáveis dos algoritmos de aprendizado de máquina. A precisão dos frameworks baseados em aprendizado de máquina propostos no aprendizado de máquina é

  –

3. ***Gonzales et al. [134] - Priority Roles of Stakeholders for Overcoming the Barriers to Implementing Education 4.0: An Integrated Fermatean Fuzzy Entropy-Based CRITIC-CODAS-SORT Approach***

   - ***E. Educadores***

     Para a função de recursos humanos, a formação periódica dos recursos humanos sobre as competências (ou seja, especialmente a prontidão digital e personalização do desenho curricular) adequadas às demandas atuais do EDUC4 surge como um papel de alta prioridade (H34). Os gerentes de IES e seus conselhos administrativos podem trabalhar juntos para examinar as políticas e diretrizes existentes na contratação de pessoal docente e não docente para incluir as habilidades relevantes para EDUC4 como parte dos critérios de seleção. Por outro lado, o pessoal incumbente poderia ser submetido a treinamentos rigorosos e seminários para transformar a força de trabalho em preparação para o EDUC4. Dessa forma, as IES poderiam abordar efetivamente a lacuna de habilidades da barreira do capital humano, particularmente aquelas relacionadas à falta de habilidades (B3) e recursos de treinamento (B5). Para tornar os treinamentos e seminários relevantes e baseados nas necessidades,

     – E.01 Envolver-se em iniciativas de aprendizado contínuo
     – E.02 Integrando a conscientização das leis aplicáveis ao cyberbullying no ensino em sala de aula (virtual)
     – E.03 Conceber estratégias alternativas de ensino com boa relação custo-benefício
     – E.04 Iniciar esforços de colaboração com outros educadores
     – E.05 Participar de esforços inclusivos
     – E.06 Participar dos esforços para demonstrar a necessidade e relevância do EDUC4 para as partes interessadas (ou seja, pais, investidores, governos locais e comunidade imediata)
     – E.07 Envolvimento nos esforços de planejamento, seleção e manutenção de tecnologias para apoiar o ensino-aprendizagem em um ambiente EDUC4
     – E.08 Estabelecer iniciativas holísticas para ligação e colaboração com universidades estrangeiras, indústria, organizações não governamentais, escritórios governamentais e organizações internacionais
     – E.09 Participação em esforços para aumentar a visibilidade em fóruns e plataformas online para possivelmente estabelecer colaboração
     – E.10 Participar do projeto, desenvolvimento e aprimoramento de currículos inovadores alinhados ao EDUC4

- E.11 Integrando padrões de saúde, incluindo a saúde mental dos alunos, ao projetar seus resultados de aprendizagem pretendidos consistentes com o EDUC4
- E.12 Promover formas de preparar eficientemente materiais de aprendizagem, incluindo o uso de TICs avançadas
- E.13 Participar de iniciativas de desenvolvimento de habilidades destinadas a equipar os educadores com as capacidades para lidar com diferentes plataformas de aprendizagem complexas

- ***G. Governo***

  O uso do FF CODAS-SORT revela os papéis de alta prioridade das partes interessadas na superação das barreiras de implementação do EDUC4. Para o governo, esses papéis incluem a inclusão da conscientização sobre segurança cibernética no currículo da educação básica (G3), alocando mais recursos para apoiar as atividades inclusivas necessárias na implementação da EDUC4 (G4), projetando os currículos de acordo com a implementação e sustentação de EDUC4 (G11), e racionalização das iniciativas de alinhamento da agenda da educação básica (por exemplo, recursos humanos e currículos) ao EDUC4 (G16). Conforme apontado na
  - G1.01 Investir na proteção de endpoints contra ataques de segurança cibernética (por exemplo, malware, phishing e trojans, entre outros)
  - G1.02 Fornecer treinamento atualizado de recursos humanos (por exemplo, educadores) sobre ameaças à segurança cibernética
  - G1.03 Inclusão da conscientização sobre segurança cibernética no currículo da educação básica
  - G1.04 Alocar mais fundos para apoiar as atividades inclusivas necessárias na implementação do EDUC4
  - G1.05 Implementação de iniciativas para direcionar as ligações entre as partes interessadas em diferentes áreas de cooperação (por exemplo, indústria-CHED e organizações internacionais)
  - G1.06 Atualização das ofertas curriculares com base nos sinais do mercado de trabalho colocados pelo I4.0
  - G1.07 Forjar uma maior disseminação de informações sobre EDUC4 para todas as partes interessadas
  - G1.08 Projetar uma agenda política geral, incluindo mapeamento de estradas, na implementação do EDUC4
  - G1.09 Posicionando a implementação do EDUC4 dentro dos Objetivos de Desenvolvimento Sustentável da ONU
  - G1.10 Promover a colaboração multifuncional que envolve diferentes conhecimentos funcionais em vários escritórios governamentais relevantes
  - G1.11 Projetar os currículos de acordo com a implementação e sustentação do EDUC4
  - G1.12 Projetar medidas apropriadas para o surgimento de novas tecnologias que afetam o aprendizado (por exemplo, vício em jogos e mídia social)
  - G1.13 Promoção e criação de iniciativas que produzam benefícios sociais e psicológicos para promover comportamentos saudáveis

- G1.14 Criação de infraestrutura de rede para diminuir a complexidade das plataformas de aprendizado
- G1.15 Promovendo oportunidades para o surgimento de atividades auto-organizadas e dinâmicas com Ias
- G1.16 Simplificação das iniciativas de alinhamento da agenda da educação básica (por exemplo, recursos humanos e currículos) à EDUC4

- ***H. Recursos Humanos***

  Para a função de recursos humanos, a formação periódica dos recursos humanos sobre as competências (ou seja, especialmente a prontidão digital e personalização do desenho curricular) adequadas às demandas atuais do EDUC4 surge como um papel de alta prioridade (H34). Os gerentes de IES e seus conselhos administrativos podem trabalhar juntos para examinar as políticas e diretrizes existentes na contratação de pessoal docente e não docente para incluir as habilidades relevantes para

  - H.01 Incorporando privacidade de dados e orientação de proteção durante a contratação de pessoal
  - H.02 Restringir o acesso de qualquer informação e sites apenas a seus usuários confiáveis ou partes conhecidas
  - H.03 Conceber medidas não ambíguas para a proteção do recurso humano contra ameaças internas, que podem expor conteúdos potencialmente prejudiciais
  - H.04 Implementação de informações para funcionários e outras partes interessadas sobre como se proteger contra phishing, engenharia social (por exemplo, adquirir credenciais de login) e outros ataques de segurança cibernética
  - H.05 Projetar iniciativas que encorajem a cultura de segurança cibernética entre os educadores universitários
  - H.06 Participar ativamente dos esforços de toda a universidade para iniciativas econômicas na construção das capacidades humanas necessárias na implementação do EDUC4
  - H.07 Formação periódica dos recursos humanos nas competências (ou seja, especialmente a prontidão digital e a personalização do desenho curricular) adequadas às atuais exigências do EDUC4
  - H.08 Projetar políticas para contratação de pessoal, mérito e sistema de promoções (ou seja, incluindo colaboração como um indicador) relevantes para EDUC4 para garantir que os funcionários mais competentes e qualificados sejam contratados e retidos
  - H.09 Iniciando fóruns entre as partes interessadas (por exemplo, educadores, pais e governos locais) para discutir a necessidade premente de adoção do EDUC4
  - H.10 Estabelecer programas para treinar ou apoiar os funcionários que procuram adquirir subsídios de treinamento externo e colaboração
  - H.11 Projetar um sistema de reconhecimento que reconheça e reconheça os esforços colaborativos dos educadores e funcionários
  - H.12 Integrar questões de saúde como parte integrante dos esforços de desenvolvimento de pessoal (por exemplo, monitoramento periódico de saúde e benefícios de saúde) da universidade

- ***T. Função de TIC***

  Os investimentos em tecnologias eficientes geralmente abordariam as barreiras relacionadas ao custo (B2), falta de tecnologias disponíveis (B8) e complexidade das plataformas de aprendizagem (B11). Essa função pode ser direta, pois a implementação do EDUC4 está associada a ambientes com uso intensivo de tecnologia. Investir nessas tecnologias eficientes pode integrar as atividades necessárias para o ensino e aprendizagem totalmente automatizados, resultando em maior produtividade

  - T.01 Investir em esforços de colaboração com especialistas em TI capazes de lidar com ameaças de segurança cibernética
  - T.02 Projetando infraestrutura robusta contra ameaças de segurança cibernética
  - T.03 Iniciar programas inclusivos (por exemplo, disseminação de informações, treinamento, workshops e aprendizado contínuo) que encorajem uma cultura de TI entre as partes interessadas da universidade
  - T.04 Direcionar as necessidades de infraestrutura de TI da universidade, incluindo manutenção de equipamentos, que dariam suporte à implementação do EDUC4
  - T.05 Forjando colaboração constante com especialistas em TI para buscar soluções de TI eficientes e eficazes para as necessidades EDUC4

- ***U. Gestão universitária***

  Para os gestores universitários, os papéis de alta prioridade incluem investir em tecnologias eficientes (por exemplo, salas de aula virtuais, capacitação ou auditoria de processos, ferramentas analíticas para planejamento estratégico e o processo híbrido ou totalmente automatizado de gerenciamento de projetos), que são conhecidos por reduzir a custos e melhorar a experiência das partes interessadas da universidade (U19) e forjar ampla colaboração com várias partes interessadas (por exemplo, formuladores de políticas, especialistas acadêmicos, redes universitárias, educadores, líderes educacionais, alunos e parceiros do setor) para fornecer espaço e

  - U.01 Envolver-se em iniciativas para promover a conscientização sobre segurança cibernética entre os membros da universidade (ou seja, educadores, alunos e funcionários)
  - U.02 Projetar medidas que levem em conta a segurança
  - U.03 Investir em tecnologias eficientes
  - U.04 Treinamento constante e atualização de capacidades de educadores
  - U.05 Promover o apoio transformacional e a estrutura ambiental e institucional
  - U.06 Envolver as partes interessadas
  - U.07 Explorando a tradução da estrutura EDUC4 em pedagogia, avaliação e design de um sistema instrucional
  - U.08 Forjar ampla colaboração com várias partes interessadas
  - U.09 Benchmarking de práticas estabelecidas e favoráveis à implementação do EDUC4
  - U.10 Estabeleceu políticas intensificadas de requisitos de entrada na faculdade

4. ***Alfakeeh et al. [132] - Sustainable-Security Assessment Through a Multi Perspective Benchmarking Framework***

- ***1. Segurança***
  - 1.01 Disponibilidade
  - 1.02 Integridade
  - 1.03 Confiabilidade
- ***2. Sustentabilidade***
  - 2.01 Consumo de Energia
  - 2.02 Otimização de recursos baseado em software
  - 2.03 Durabilidade

    2.03.01 Manutenibilidade

    2.03.02 Portabilidade

Apêndice 04 - Critérios e Alternativas do Modelo Proposto

São apresentados os Critérios e Alternativas do Modelo Proposto

1. ORGANIZAÇÃO

1.1 Missão / Estratégia / Objetivos

1.2 Governança

1.3 Conformidade Regulatória e de Negócios

1.4 Capacitação / Cultura Organizacional

1.5 Investimento

2. TOMADORES DECISÃO

2.1 Funcionários

2.2 Recursos Humanos

2.3 Tecnologia da Informação

2.4 Gestão de Riscos

2.5 Gestores (PT e SI)

2.6 Colaboradores

3. SEGURANÇA

3.1 Sistema / Aplicativo

3.2 Rede - LAN e WAN

3.3 Usuário

3.4 Física

3.5 Estação

4. ATIVOS

4.1 Dados - CID

4.2 Resiliência

4.3 Privacidade

4.4 Processos de Trabalho

4.5 Pessoas

4.6 Hardware e Software

5. TECNOLOGIAS

5.1 Ultrapassadas

5.2 Múltiplas

5.3 Nuvem

5.4 Novas Tecnologias (IA, Big Data, 5G, IoT)

6. AMEAÇAS

6.1 Incidentes

6.2 Vulnerabilidades

6.3 Ambiente Interno

6.4 Ambiente Externo

Apêndice 05 - Controles do Modelo Proposto

São apresentados os Controles que foram utilizados no modelo proposto [55]

GUIA DE APERFEIÇOAMENTO DA SEGURANÇA CIBERNÉTICA PARA INFRAESTRUTURA CRÍTICA

1. Identificar

1.1 Gerenciamento dos Ativos

- 1.1.1 Dispositivos físicos e sistemas dentro da organização são inventariados
- 1.1.2 Plataformas de software e aplicações dentro da organização são inventariadas
- 1.1.3 Comunicação organizacional e fluxos de dados são mapeados
- 1.1.4 Sistemas de informação externos são catalogados
- 1.1.5 Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios
- 1.1.6 Funções e responsabilidades de segurança cibernética para toda a força laboral e stakeholders de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos

1.2 Contexto Empresarial

- 1.2.1 O papel da organização na cadeia de suprimentos é identificado e comunicado
- 1.2.2 O lugar da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado
- 1.2.3 Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas
- 1.2.4 Dependências e funções críticas para a entrega de serviços críticos são estabelecidas
- 1.2.5 Requisitos de resiliência

1.3 Governança

- 1.3.1 A política organizacional de segurança cibernética é estabelecida e comunicada
- 1.3.2 As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos

- 1.3.3 Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados
- 1.3.4 Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética

1.4 Avaliação de Risco

- 1.4.1 As vulnerabilidades dos ativos são identificadas e documentadas
- 1.4.2 Informações sobre ameaças cibernéticas são recebidas de fóruns e fontes de compartilhamento de informações
- 1.4.3 Ameaças internas e externas são identificadas e documentadas
- 1.4.4 Potenciais impactos no negócio e probabilidades são identificados na organização
- 1.4.5 Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos
- 1.4.6 As respostas ao risco são identificadas e priorizadas

1.5 Estratégia de Gerenciamento de Riscos

- 1.5.1 Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos stakeholders organizacionais
- 1.5.2 Tolerância ao risco organizacional é determinada e claramente expressa
- 1.5.3 A determinação de tolerância ao risco da organização é permeada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor

1.6 Gerenciamento de Riscos da Cadeia de Suprimento

- 1.6.1 Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders da organização.
- 1.6.2 Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos
- 1.6.3 Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização
- 1.6.4 Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais
- 1.6.5 O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados

2. Proteger

2.1 Gerenciamento de identidade e controle de acesso

- 2.1.1 Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados
- 2.1.2 O acesso físico aos ativos é gerenciado e protegido
- 2.1.3 O acesso remoto é gerenciado
- 2.1.4 Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas
- 2.1.5 A integridade da rede é protegida
- 2.1.6 As identidades são revisadas, vinculadas a credenciais e confirmadas em interações
- 2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

2.2 Conscientização e Treinamento

- 2.2.1 Todos os utilizadores são informados a respeito e treinados
- 2.2.2 Os usuários privilegiados compreendem suas funções e responsabilidades
- 2.2.3 Stakeholders terceirizados entendem suas funções e responsabilidades
- 2.2.4 Executivos seniores compreendem suas funções e responsabilidades
- 2.2.5 Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades

2.3 Segurança de Dados

- 2.3.1 Os dados em repouso são protegidos
- 2.3.2 Os dados em trânsito são protegidos
- 2.3.3 Ativos são formalmente gerenciados durante a remoção, transferências e disposição
- 2.3.4 A capacidade adequada para garantir a disponibilidade é mantida
- 2.3.5 As proteções contra vazamentos de dados são implementadas
- 2.3.6 Os mecanismos de verificação de integridade são usados para verificar o software, o firmware e a integridade das informações
- 2.3.7 O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção
- 2.3.8 Mecanismos de verificação de integridade são usados para verificar a integridade do hardware

2.4 Processos e Procedimentos de Proteção da Informação

- 2.4.01 Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança
- 2.4.02 Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado
- 2.4.03 Processos de controle de mudança de configuração estão em funcionamento
- 2.4.04 Os Backups de informações são realizados, conservados e testados
- 2.4.05 As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos
- 2.4.06 Os dados são destruídos de acordo com a política
- 2.4.07 Os processos de proteção são aperfeiçoados
- 2.4.08 A eficácia das tecnologias de proteção é compartilhada
- 2.4.09 Planos de resposta e planos de recuperação estão em vigor e gerenciados
- 2.4.10 Planos de recuperação e resposta são testados
- 2.4.11 A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desaprovisionamento, triagem de pessoal)
- 2.4.12 Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado

2.5 Manutenção

- 2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas
- 2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6 Tecnologia Protetora

- 2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política
- 2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política
- 2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais
- 2.6.4 Redes de comunicação e controle são protegidas
- 2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

3. Detectar ou Diagnosticar

3.1 Anomalias e Incidentes

- 3.1.1 Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada
- 3.1.2 Os eventos detectados são analisados para compreender os alvos e métodos de ataque
- 3.1.3 Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores
- 3.1.4 O impacto dos eventos é determinado
- 3.1.5 Os limites de alerta de incidentes são estabelecidos

3.2 Monitoramento Contínuo de Segurança

- 3.2.1 A rede é monitorada para detectar potenciais incidentes de segurança cibernética
- 3.2.2 O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética
- 3.2.3 A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética
- 3.2.4 Código malicioso é detectado
- 3.2.5 Código móvel não autorizado é detectado
- 3.2.6 A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética
- 3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado
- 3.2.8 Há realização de varreduras de vulnerabilidade

3.3 Processos de Detecção

- 3.3.1 Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas
- 3.3.2 As atividades de detecção cumprem todos os requisitos aplicáveis
- 3.3.3 Os processos de detecção são testados
- 3.3.4 Informações de detecção de incidente são comunicadas
- 3.3.5 Processos de detecção são continuamente aperfeiçoados

4. Responder

4.1 Planejamento de Resposta

- 4.1.1 Plano de resposta é executado durante ou depois de um incidente

4.2 Comunicações

- 4.2.1 Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária
- 4.2.2 Os incidentes são informados de acordo com os critérios estabelecidos
- 4.2.3 As informações são compartilhadas de acordo com os planos de resposta
- 4.2.4 A coordenação com os stakeholders ocorre de acordo com os planos de resposta
- 4.2.5 O compartilhamento voluntário de informações ocorre com os stakeholders externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética

4.3 Análise

- 4.3.1 As notificações dos sistemas de detecção são analisadas
- 4.3.2 O impacto do incidente é compreendido
- 4.3.3 Há realização de investigações
- 4.3.4 Os incidentes são categorizados de forma consistente com os planos de resposta
- 4.3.5 Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas

4.4 Mitigação

- 4.4.1 Os incidentes são contidos
- 4.4.2 Os incidentes são mitigados
- 4.4.3 As vulnerabilidades identificadas recentemente são mitigadas ou documentadas como riscos aceitos

4.5 Aperfeiçoamentos

- 4.5.1 Os planos de resposta incorporam as lições aprendidas
- 4.5.2 As estratégias de resposta são atualizadas

5. Recuperar

5.1 Planejamento de Recuperação

- 5.1.1 O Plano de recuperação é executado durante ou após um incidente de segurança cibernética

5.2 Aperfeiçoamentos

- 5.2.1 Planos de recuperação incorporam as lições aprendidas
- 5.2.2 As estratégias de recuperação são atualizadas

5.3 Comunicações

- 5.3.1 As relações públicas são gerenciadas
- 5.3.2 A reputação é reparada após um incidente
- 5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

Apêndice 06 - Lista dos Relacionamentos entre Controles e Alternativas

São apresentados os Relacionamentos entre os Controles e Alternativas obtidos pela Análise de Conteúdo

1. ORGANIZAÇÃO

1.1 Missão / Estratégia / Objetivos

1. Identificar

1.1.5 Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios

1.2.1 O papel da organização na cadeia de suprimentos é identificado e comunicado

1.2.2 O lugar da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado

1.2.3 Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas

1.2.4 Dependências e funções críticas para a entrega de serviços críticos são estabelecidas

1.2.5 Requisitos de resiliência

1.4.4 Potenciais impactos no negócio e probabilidades são identificados na organização

1.4.6 As respostas ao risco são identificadas e priorizadas

1.5.1 Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos stakeholders organizacionais

1.5.2 Tolerância ao risco organizacional é determinada e claramente expressa

1.5.3 A determinação de tolerância ao risco da organização é permeada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor

1.6.1 Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders da organização.

1.6.2 Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos

1.6.3 Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização

2. Proteger

2.2.4 Executivos seniores compreendem suas funções e responsabilidades

2.3.4 A capacidade adequada para garantir a disponibilidade é mantida

2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

3. Detectar ou Diagnosticar

3.1.4 O impacto dos eventos é determinado

4. Responder

4.2.4 A coordenação com os stakeholders ocorre de acordo com os planos de resposta

4.2.5 O compartilhamento voluntário de informações ocorre com os stakeholders externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética

4.3.2 O impacto do incidente é compreendido

5. Recuperar

5.3.1 As relações públicas são gerenciadas

5.3.2 A reputação é reparada após um incidente

5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

1.2 Governança

1. Identificar

1.2.1 O papel da organização na cadeia de suprimentos é identificado e comunicado

1.2.2 O lugar da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado

1.2.3 Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas

1.2.4 Dependências e funções críticas para a entrega de serviços críticos são estabelecidas

1.2.5 Requisitos de resiliência

1.3.1 A política organizacional de segurança cibernética é estabelecida e comunicada

1.3.2 As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos

1.3.4 Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética

1.4.2 Informações sobre ameaças cibernéticas são recebidas de fóruns e fontes de compartilhamento de informações

1.5.1 Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos stakeholders organizacionais

1.5.2 Tolerância ao risco organizacional é determinada e claramente expressa

1.6.1 Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders da organização.

1.6.5 O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados

2. Proteger

2.4.05 As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos

2.4.06 Os dados são destruídos de acordo com a política

2.4.09 Planos de resposta e planos de recuperação estão em vigor e gerenciados

2.4.10 Planos de recuperação e resposta são testados

2.4.11 A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desaprovisionamento, triagem de pessoal)

2.4.12 Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política

3. Detectar ou Diagnosticar

3.3.1 Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas

3.3.5 Processos de detecção são continuamente aperfeiçoados

4. Responder

4.1.1 Plano de resposta é executado durante ou depois de um incidente

4.2.3 As informações são compartilhadas de acordo com os planos de resposta

4.2.4 A coordenação com os stakeholders ocorre de acordo com os planos de resposta

4.2.5 O compartilhamento voluntário de informações ocorre com os stakeholders externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética

4.3.3 Há realização de investigações

4.3.4 Os incidentes são categorizados de forma consistente com os planos de resposta

4.3.5 Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas

4.5.1 Os planos de resposta incorporam as lições aprendidas

4.5.2 As estratégias de resposta são atualizadas

5. Recuperar

5.1.1 O Plano de recuperação é executado durante ou após um incidente de segurança cibernética

5.2.1 Planos de recuperação incorporam as lições aprendidas

5.2.2 As estratégias de recuperação são atualizadas

5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

1.3 Conformidade Regulatória e de Negócios

1. Identificar

1.1.3 Comunicação organizacional e fluxos de dados são mapeados

1.1.6 Funções e responsabilidades de segurança cibernética para toda a força laboral e stakeholders de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos

1.2.3 Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas

1.2.4 Dependências e funções críticas para a entrega de serviços críticos são estabelecidas

1.3.1 A política organizacional de segurança cibernética é estabelecida e comunicada

1.3.2 As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos

1.3.3 Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados

1.3.4 Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética

1.4.2 Informações sobre ameaças cibernéticas são recebidas de fóruns e fontes de compartilhamento de informações

1.5.1 Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos stakeholders organizacionais

1.6.1 Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders da organização.

1.6.2 Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos

1.6.4 Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais

1.6.5 O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados

2. Proteger

2.1.1 Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados

2.1.2 O acesso físico aos ativos é gerenciado e protegido

2.1.3 O acesso remoto é gerenciado

2.1.4 Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas

2.1.6 As identidades são revisadas, vinculadas a credenciais e confirmadas em interações

2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

2.2.2 Os usuários privilegiados compreendem suas funções e responsabilidades

2.2.3 Stakeholders terceirizados entendem suas funções e responsabilidades

2.2.4 Executivos seniores compreendem suas funções e responsabilidades

2.2.5 Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades

2.3.3 Ativos são formalmente gerenciados durante a remoção, transferências e disposição

2.3.4 A capacidade adequada para garantir a disponibilidade é mantida

2.3.5 As proteções contra vazamentos de dados são implementadas

2.4.01 Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança

2.4.02 Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado

2.4.03 Processos de controle de mudança de configuração estão em funcionamento

2.4.04 Os Backups de informações são realizados, conservados e testados

2.4.05 As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos

2.4.06 Os dados são destruídos de acordo com a política

2.4.07 Os processos de proteção são aperfeiçoados

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política

2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais

2.6.4 Redes de comunicação e controle são protegidas

2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

3. Detectar ou Diagnosticar

3.1.1 Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada

3.1.5 Os limites de alerta de incidentes são estabelecidos

3.2.2 O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética

3.2.3 A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética

3.2.6 A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.3.1 Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas

3.3.2 As atividades de detecção cumprem todos os requisitos aplicáveis

3.3.3 Os processos de detecção são testados

3.3.4 Informações de detecção de incidente são comunicadas

3.3.5 Processos de detecção são continuamente aperfeiçoados

4. Responder

4.1.1 Plano de resposta é executado durante ou depois de um incidente

4.2.1 Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária

4.2.2 Os incidentes são informados de acordo com os critérios estabelecidos

4.2.3 As informações são compartilhadas de acordo com os planos de resposta

4.2.4 A coordenação com os stakeholders ocorre de acordo com os planos de resposta

4.2.5 O compartilhamento voluntário de informações ocorre com os stakeholders externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética

4.3.3 Há realização de investigações

4.3.4 Os incidentes são categorizados de forma consistente com os planos de resposta

4.3.5 Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas

4.4.1 Os incidentes são contidos

4.4.2 Os incidentes são mitigados

4.4.3 As vulnerabilidades identificadas recentemente são mitigadas ou documentadas como riscos aceitos

4.5.1 Os planos de resposta incorporam as lições aprendidas

4.5.2 As estratégias de resposta são atualizadas

5. Recuperar

5.1.1 O Plano de recuperação é executado durante ou após um incidente de segurança cibernética

5.2.1 Planos de recuperação incorporam as lições aprendidas

5.2.2 As estratégias de recuperação são atualizadas

5.3.2 A reputação é reparada após um incidente

5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

1.4 Capacitação / Cultura Organizacional

1. Identificar

1.2.1 O papel da organização na cadeia de suprimentos é identificado e comunicado

1.2.2 O lugar da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado

1.2.3 Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas

1.3.1 A política organizacional de segurança cibernética é estabelecida e comunicada

1.3.2 As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos

1.3.3 Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados

1.5.2 Tolerância ao risco organizacional é determinada e claramente expressa

2. Proteger

2.2.1 Todos os utilizadores são informados a respeito e treinados

2.2.2 Os usuários privilegiados compreendem suas funções e responsabilidades

2.2.4 Executivos seniores compreendem suas funções e responsabilidades

2.2.5 Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades

4. Responder

4.2.1 Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária

1.5 Investimento

1. Identificar

1.6.3 Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização

1.6.4 Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais

2. Proteger

2.2.3 Stakeholders terceirizados entendem suas funções e responsabilidades

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2. TOMADORES DECISÃO

2.1 Funcionários

1. Identificar

1.1.6 Funções e responsabilidades de segurança cibernética para toda a força laboral e stakeholders de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos

2. Proteger

2.2.1 Todos os utilizadores são informados a respeito e treinados

2.2.2 Os usuários privilegiados compreendem suas funções e responsabilidades

2.2.5 Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades

2.2 Recursos Humanos

2. Proteger

2.4.11 A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desaprovisionamento, triagem de pessoal)

2.3 Tecnologia da Informação

1. Identificar

1.1.1 Dispositivos físicos e sistemas dentro da organização são inventariados

1.1.2 Plataformas de software e aplicações dentro da organização são inventariadas

1.1.4 Sistemas de informação externos são catalogados

1.1.5 Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios

1.1.6 Funções e responsabilidades de segurança cibernética para toda a força laboral e stakeholders de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos

1.2.5 Requisitos de resiliência

1.3.1 A política organizacional de segurança cibernética é estabelecida e comunicada

1.3.2 As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos

1.3.3 Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados

1.3.4 Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética

1.4.1 As vulnerabilidades dos ativos são identificadas e documentadas

1.4.2 Informações sobre ameaças cibernéticas são recebidas de fóruns e fontes de compartilhamento de informações

1.4.3 Ameaças internas e externas são identificadas e documentadas

1.4.4 Potenciais impactos no negócio e probabilidades são identificados na organização

1.4.5 Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos

1.4.6 As respostas ao risco são identificadas e priorizadas

1.6.2 Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos

1.6.3 Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização

1.6.4 Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais

1.6.5 O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados

2. Proteger

2.1.1 Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados

2.1.2 O acesso físico aos ativos é gerenciado e protegido

2.1.3 O acesso remoto é gerenciado

2.1.4 Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas

2.1.5 A integridade da rede é protegida

2.1.6 As identidades são revisadas, vinculadas a credenciais e confirmadas em interações

2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

2.2.3 Stakeholders terceirizados entendem suas funções e responsabilidades

2.2.5 Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades

2.3.1 Os dados em repouso são protegidos

2.3.2 Os dados em trânsito são protegidos

2.3.3 Ativos são formalmente gerenciados durante a remoção, transferências e disposição

2.3.4 A capacidade adequada para garantir a disponibilidade é mantida

2.3.5 As proteções contra vazamentos de dados são implementadas

2.3.6 Os mecanismos de verificação de integridade são usados para verificar o software, o firmware e a integridade das informações

2.3.7 O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção

2.3.8 Mecanismos de verificação de integridade são usados para verificar a integridade do hardware

2.4.01 Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança

2.4.02 Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado

2.4.03 Processos de controle de mudança de configuração estão em funcionamento

2.4.04 Os Backups de informações são realizados, conservados e testados

2.4.05 As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos

2.4.06 Os dados são destruídos de acordo com a política

2.4.07 Os processos de proteção são aperfeiçoados

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.4.09 Planos de resposta e planos de recuperação estão em vigor e gerenciados

2.4.10 Planos de recuperação e resposta são testados

2.4.12 Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política

2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais

2.6.4 Redes de comunicação e controle são protegidas

2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

3. Detectar ou Diagnosticar

3.1.1 Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada

3.1.2 Os eventos detectados são analisados para compreender os alvos e métodos de ataque

3.1.3 Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores

3.1.4 O impacto dos eventos é determinado

3.1.5 Os limites de alerta de incidentes são estabelecidos

3.2.1 A rede é monitorada para detectar potenciais incidentes de segurança cibernética

3.2.2 O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética

3.2.3 A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética

3.2.4 Código malicioso é detectado

3.2.5 Código móvel não autorizado é detectado

3.2.6 A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.2.8 Há realização de varreduras de vulnerabilidade

3.3.1 Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas

3.3.2 As atividades de detecção cumprem todos os requisitos aplicáveis

3.3.3 Os processos de detecção são testados

3.3.4 Informações de detecção de incidente são comunicadas

3.3.5 Processos de detecção são continuamente aperfeiçoados

4. Responder

4.1.1 Plano de resposta é executado durante ou depois de um incidente

4.2.2 Os incidentes são informados de acordo com os critérios estabelecidos

4.2.3 As informações são compartilhadas de acordo com os planos de resposta

4.2.4 A coordenação com os stakeholders ocorre de acordo com os planos de resposta

4.2.5 O compartilhamento voluntário de informações ocorre com os stakeholders externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética

4.3.1 As notificações dos sistemas de detecção são analisadas

4.3.2 O impacto do incidente é compreendido

4.3.3 Há realização de investigações

4.3.4 Os incidentes são categorizados de forma consistente com os planos de resposta

4.3.5 Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas

4.4.1 Os incidentes são contidos

4.4.2 Os incidentes são mitigados

4.4.3 As vulnerabilidades identificadas recentemente são mitigadas ou documentadas como riscos aceitos

4.5.1 Os planos de resposta incorporam as lições aprendidas

4.5.2 As estratégias de resposta são atualizadas

5. Recuperar

5.1.1 O Plano de recuperação é executado durante ou após um incidente de segurança cibernética

5.2.1 Planos de recuperação incorporam as lições aprendidas

5.2.2 As estratégias de recuperação são atualizadas

5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

2.4 Gestão de Riscos

1. Identificar

1.1.3 Comunicação organizacional e fluxos de dados são mapeados

1.3.1 A política organizacional de segurança cibernética é estabelecida e comunicada

1.3.3 Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados

1.3.4 Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética

1.4.4 Potenciais impactos no negócio e probabilidades são identificados na organização

1.4.5 Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos

1.4.6 As respostas ao risco são identificadas e priorizadas

1.5.1 Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos stakeholders organizacionais

1.5.3 A determinação de tolerância ao risco da organização é permeada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor

1.6.1 Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos stakeholders da organização.

1.6.2 Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos

1.6.3 Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização

1.6.4 Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais

2. Proteger

2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

3. Detectar ou Diagnosticar

3.1.4 O impacto dos eventos é determinado

4. Responder

4.1.1 Plano de resposta é executado durante ou depois de um incidente

4.2.3 As informações são compartilhadas de acordo com os planos de resposta

4.2.4 A coordenação com os stakeholders ocorre de acordo com os planos de resposta

4.2.5 O compartilhamento voluntário de informações ocorre com os stakeholders externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética

4.3.1 As notificações dos sistemas de detecção são analisadas

4.3.2 O impacto do incidente é compreendido

4.3.3 Há realização de investigações

4.3.5 Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas

4.4.1 Os incidentes são contidos

4.4.2 Os incidentes são mitigados

4.4.3 As vulnerabilidades identificadas recentemente são mitigadas ou documentadas como riscos aceitos

5. Recuperar

5.3.1 As relações públicas são gerenciadas

5.3.2 A reputação é reparada após um incidente

5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

2.5 Gestores (PT e SI)

2. Proteger

2.1.1 Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados

5. Recuperar

5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

2.6 Colaboradores

1. Identificar

1.1.6 Funções e responsabilidades de segurança cibernética para toda a força laboral e stakeholders de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos

1.3.2 As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos

1.6.2 Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos

1.6.4 Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais

1.6.5 O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados

2. Proteger

2.2.1 Todos os utilizadores são informados a respeito e treinados

2.2.2 Os usuários privilegiados compreendem suas funções e responsabilidades

2.2.3 Stakeholders terceirizados entendem suas funções e responsabilidades

3. Detectar ou Diagnosticar

3.2.3 A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética

3.2.6 A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

4. Responder

4.2.1 Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária

4.2.5 O compartilhamento voluntário de informações ocorre com os stakeholders externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética

3. SEGURANÇA

3.1 Sistema / Aplicativo

2. Proteger

2.1.3 O acesso remoto é gerenciado

2.1.4 Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas

2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

2.3.1 Os dados em repouso são protegidos

2.3.2 Os dados em trânsito são protegidos

2.3.5 As proteções contra vazamentos de dados são implementadas

2.3.7 O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção

2.4.01 Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança

2.4.02 Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado

2.4.03 Processos de controle de mudança de configuração estão em funcionamento

2.4.07 Os processos de proteção são aperfeiçoados

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais

3. Detectar ou Diagnosticar

3.1.1 Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada

3.2.4 Código malicioso é detectado

3.2.5 Código móvel não autorizado é detectado

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.2.8 Há realização de varreduras de vulnerabilidade

4. Responder

4.3.1 As notificações dos sistemas de detecção são analisadas

3.2 Rede - LAN e WAN

2. Proteger

2.1.3 O acesso remoto é gerenciado

2.1.5 A integridade da rede é protegida

2.3.1 Os dados em repouso são protegidos

2.3.2 Os dados em trânsito são protegidos

2.3.5 As proteções contra vazamentos de dados são implementadas

2.4.05 As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos

2.4.07 Os processos de proteção são aperfeiçoados

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.4 Redes de comunicação e controle são protegidas

3. Detectar ou Diagnosticar

3.2.1 A rede é monitorada para detectar potenciais incidentes de segurança cibernética

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.2.8 Há realização de varreduras de vulnerabilidade

4. Responder

4.3.1 As notificações dos sistemas de detecção são analisadas

3.3 Usuário

2. Proteger

2.1.1 Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados

2.1.3 O acesso remoto é gerenciado

2.1.6 As identidades são revisadas, vinculadas a credenciais e confirmadas em interações

2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

2.3.5 As proteções contra vazamentos de dados são implementadas

2.4.07 Os processos de proteção são aperfeiçoados

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

3. Detectar ou Diagnosticar

3.1.1 Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada

4. Responder

4.2.1 Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária

3.4 Física

2. Proteger

2.1.2 O acesso físico aos ativos é gerenciado e protegido

2.3.1 Os dados em repouso são protegidos

2.3.2 Os dados em trânsito são protegidos

2.3.5 As proteções contra vazamentos de dados são implementadas

2.4.05 As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos

2.4.07 Os processos de proteção são aperfeiçoados

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política

3. Detectar ou Diagnosticar

3.2.2 O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.5 Estação

2. Proteger

2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

2.3.1 Os dados em repouso são protegidos

2.3.2 Os dados em trânsito são protegidos

2.3.5 As proteções contra vazamentos de dados são implementadas

2.4.03 Processos de controle de mudança de configuração estão em funcionamento

2.4.04 Os Backups de informações são realizados, conservados e testados

2.4.05 As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos

2.4.07 Os processos de proteção são aperfeiçoados

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

3. Detectar ou Diagnosticar

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.2.8 Há realização de varreduras de vulnerabilidade

4. Responder

4.3.1 As notificações dos sistemas de detecção são analisadas

4. ATIVOS

4.1 Dados - CID

1. Identificar

1.2.4 Dependências e funções críticas para a entrega de serviços críticos são estabelecidas

2. Proteger

2.1.3 O acesso remoto é gerenciado

2.1.6 As identidades são revisadas, vinculadas a credenciais e confirmadas em interações

2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

2.3.1 Os dados em repouso são protegidos

2.3.2 Os dados em trânsito são protegidos

2.3.3 Ativos são formalmente gerenciados durante a remoção, transferências e disposição

2.3.5 As proteções contra vazamentos de dados são implementadas

2.3.6 Os mecanismos de verificação de integridade são usados para verificar o software, o firmware e a integridade das informações

2.3.7 O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção

2.4.04 Os Backups de informações são realizados, conservados e testados

2.4.06 Os dados são destruídos de acordo com a política

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política

2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais

3. Detectar ou Diagnosticar

3.1.2 Os eventos detectados são analisados para compreender os alvos e métodos de ataque

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.2.8 Há realização de varreduras de vulnerabilidade

5. Recuperar

5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

4.2 Resiliência

1. Identificar

1.2.4 Dependências e funções críticas para a entrega de serviços críticos são estabelecidas

1.2.5 Requisitos de resiliência

2. Proteger

2.3.4 A capacidade adequada para garantir a disponibilidade é mantida

2.4.04 Os Backups de informações são realizados, conservados e testados

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.4.09 Planos de resposta e planos de recuperação estão em vigor e gerenciados

2.4.10 Planos de recuperação e resposta são testados

2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

4. Responder

4.5.2 As estratégias de resposta são atualizadas

5. Recuperar

5.1.1 O Plano de recuperação é executado durante ou após um incidente de segurança cibernética

5.2.2 As estratégias de recuperação são atualizadas

5.3.3 As atividades de recuperação são comunicadas aos stakeholders internos e externos, bem como às equipes executivas e de gestão.

4.3 Privacidade

1. Identificar

1.3.3 Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados

2. Proteger

2.1.7 Usuários, dispositivos e outros recursos são autenticados de acordo com o risco da transação

2.3.3 Ativos são formalmente gerenciados durante a remoção, transferências e disposição

2.3.5 As proteções contra vazamentos de dados são implementadas

2.3.7 O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção

2.4.08 A eficácia das tecnologias de proteção é compartilhada

3. Detectar ou Diagnosticar

3.1.2 Os eventos detectados são analisados para compreender os alvos e métodos de ataque

3.2.8 Há realização de varreduras de vulnerabilidade

4.4 Processos de Trabalho

1. Identificar

1.1.5 Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios

1.1.6 Funções e responsabilidades de segurança cibernética para toda a força laboral e stakeholders de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidos

1.2.4 Dependências e funções críticas para a entrega de serviços críticos são estabelecidas

2. Proteger

2.1.1 Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados

2.1.4 Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas

2.2.1 Todos os utilizadores são informados a respeito e treinados

2.2.2 Os usuários privilegiados compreendem suas funções e responsabilidades

2.2.3 Stakeholders terceirizados entendem suas funções e responsabilidades

2.2.4 Executivos seniores compreendem suas funções e responsabilidades

2.2.5 Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades

2.3.7 O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção

2.4.01 Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança

2.4.03 Processos de controle de mudança de configuração estão em funcionamento

2.4.07 Os processos de proteção são aperfeiçoados

2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais

3. Detectar ou Diagnosticar

3.3.1 Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas

3.3.2 As atividades de detecção cumprem todos os requisitos aplicáveis

3.3.3 Os processos de detecção são testados

3.3.5 Processos de detecção são continuamente aperfeiçoados

4. Responder

4.2.1 Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária

4.5.1 Os planos de resposta incorporam as lições aprendidas

5. Recuperar

5.2.1 Planos de recuperação incorporam as lições aprendidas

4.5 Pessoas

1. Identificar

1.1.5 Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios

2. Proteger

2.1.1 Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados

2.1.6 As identidades são revisadas, vinculadas a credenciais e confirmadas em interações

2.2.1 Todos os utilizadores são informados a respeito e treinados

2.3.4 A capacidade adequada para garantir a disponibilidade é mantida

2.4.11 A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desaprovisionamento, triagem de pessoal)

3. Detectar ou Diagnosticar

3.1.1 Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada

3.2.4 Código malicioso é detectado

3.2.5 Código móvel não autorizado é detectado

4.6 Hardware e Software

1. Identificar

1.1.1 Dispositivos físicos e sistemas dentro da organização são inventariados

1.1.2 Plataformas de software e aplicações dentro da organização são inventariadas

1.1.4 Sistemas de informação externos são catalogados

1.1.5 Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em suas classificações, criticidade e valor para os negócios

1.4.1 As vulnerabilidades dos ativos são identificadas e documentadas

2. Proteger

2.1.1 Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados

2.1.2 O acesso físico aos ativos é gerenciado e protegido

2.1.3 O acesso remoto é gerenciado

2.1.5 A integridade da rede é protegida

2.3.3 Ativos são formalmente gerenciados durante a remoção, transferências e disposição

2.3.4 A capacidade adequada para garantir a disponibilidade é mantida

2.3.6 Os mecanismos de verificação de integridade são usados para verificar o software, o firmware e a integridade das informações

2.3.8 Mecanismos de verificação de integridade são usados para verificar a integridade do hardware

2.4.02 Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado

2.4.04 Os Backups de informações são realizados, conservados e testados

2.4.05 As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos

2.4.08 A eficácia das tecnologias de proteção é compartilhada

2.4.12 Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.4 Redes de comunicação e controle são protegidas

3. Detectar ou Diagnosticar

3.1.1 Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada

3.1.2 Os eventos detectados são analisados para compreender os alvos e métodos de ataque

3.2.8 Há realização de varreduras de vulnerabilidade

4. Responder

4.3.1 As notificações dos sistemas de detecção são analisadas

5. TECNOLOGIAS

5.1 Ultrapassadas

2. Proteger

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política

2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais

2.6.4 Redes de comunicação e controle são protegidas

2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

3. Detectar ou Diagnosticar

3.2.1 A rede é monitorada para detectar potenciais incidentes de segurança cibernética

3.2.4 Código malicioso é detectado

3.2.5 Código móvel não autorizado é detectado

3.3.3 Os processos de detecção são testados

3.3.4 Informações de detecção de incidente são comunicadas

3.3.5 Processos de detecção são continuamente aperfeiçoados

5.2 Múltiplas

2. Proteger

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

3. Detectar ou Diagnosticar

3.2.1 A rede é monitorada para detectar potenciais incidentes de segurança cibernética

3.3.3 Os processos de detecção são testados

5.3 Nuvem

2. Proteger

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política

2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais

2.6.4 Redes de comunicação e controle são protegidas

2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

3. Detectar ou Diagnosticar

3.2.4 Código malicioso é detectado

3.2.5 Código móvel não autorizado é detectado

3.2.6 A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética

3.3.3 Os processos de detecção são testados

3.3.4 Informações de detecção de incidente são comunicadas

3.3.5 Processos de detecção são continuamente aperfeiçoados

5.4 Novas Tecnologias (IA, Big Data, 5G, IoT)

2. Proteger

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6.1 Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política

2.6.2 As mídias removíveis são protegidas e seu uso é restrito de acordo com a política

2.6.3 O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais

2.6.5 Alguns mecanismos são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas

3. Detectar ou Diagnosticar

3.2.1 A rede é monitorada para detectar potenciais incidentes de segurança cibernética

3.2.4 Código malicioso é detectado

3.2.5 Código móvel não autorizado é detectado

3.3.3 Os processos de detecção são testados

3.3.4 Informações de detecção de incidente são comunicadas

3.3.5 Processos de detecção são continuamente aperfeiçoados

6. AMEAÇAS

6.1 Incidentes

1. Identificar

1.2.5 Requisitos de resiliência

3. Detectar ou Diagnosticar

3.1.2 Os eventos detectados são analisados para compreender os alvos e métodos de ataque

3.1.3 Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores

3.1.4 O impacto dos eventos é determinado

3.1.5 Os limites de alerta de incidentes são estabelecidos

3.2.1 A rede é monitorada para detectar potenciais incidentes de segurança cibernética

3.2.2 O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética

3.2.3 A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética

3.2.4 Código malicioso é detectado

3.2.5 Código móvel não autorizado é detectado

3.2.6 A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética

3.3.4 Informações de detecção de incidente são comunicadas

4. Responder

4.1.1 Plano de resposta é executado durante ou depois de um incidente

4.2.2 Os incidentes são informados de acordo com os critérios estabelecidos

4.3.1 As notificações dos sistemas de detecção são analisadas

4.3.2 O impacto do incidente é compreendido

4.3.4 Os incidentes são categorizados de forma consistente com os planos de resposta

4.4.1 Os incidentes são contidos

4.4.2 Os incidentes são mitigados

5. Recuperar

5.1.1 O Plano de recuperação é executado durante ou após um incidente de segurança cibernética

5.3.2 A reputação é reparada após um incidente

6.2 Vulnerabilidades

1. Identificar

1.2.5 Requisitos de resiliência

1.4.1 As vulnerabilidades dos ativos são identificadas e documentadas

2. Proteger

2.4.12 Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado

3. Detectar ou Diagnosticar

3.2.8 Há realização de varreduras de vulnerabilidade

4. Responder

4.3.5 Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas

4.4.3 As vulnerabilidades identificadas recentemente são mitigadas ou documentadas como riscos aceitos

6.3 Ambiente Interno

1. Identificar

1.2.5 Requisitos de resiliência

1.4.3 Ameaças internas e externas são identificadas e documentadas

1.4.5 Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos

2. Proteger

2.1.2 O acesso físico aos ativos é gerenciado e protegido

2.1.5 A integridade da rede é protegida

2.3.5 As proteções contra vazamentos de dados são implementadas

2.5.1 Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas

2.6.4 Redes de comunicação e controle são protegidas

3. Detectar ou Diagnosticar

3.1.2 Os eventos detectados são analisados para compreender os alvos e métodos de ataque

3.1.4 O impacto dos eventos é determinado

3.2.3 A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.2.8 Há realização de varreduras de vulnerabilidade

4. Responder

4.3.1 As notificações dos sistemas de detecção são analisadas

5. Recuperar

5.1.1 O Plano de recuperação é executado durante ou após um incidente de segurança cibernética

5.3.2 A reputação é reparada após um incidente

6.4 Ambiente Externo

1. Identificar

1.2.5 Requisitos de resiliência

1.4.3 Ameaças internas e externas são identificadas e documentadas

1.4.5 Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos

2. Proteger

2.1.3 O acesso remoto é gerenciado

2.1.5 A integridade da rede é protegida

2.3.5 As proteções contra vazamentos de dados são implementadas

2.5.2 A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado

2.6.4 Redes de comunicação e controle são protegidas

3. Detectar ou Diagnosticar

3.1.2 Os eventos detectados são analisados para compreender os alvos e métodos de ataque

3.1.4 O impacto dos eventos é determinado

3.2.3 A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética

3.2.6 A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética

3.2.7 O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado

3.2.8 Há realização de varreduras de vulnerabilidade

4. Responder

4.3.1 As notificações dos sistemas de detecção são analisadas

5. Recuperar

5.1.1 O Plano de recuperação é executado durante ou após um incidente de segurança cibernética

5.3.2 A reputação é reparada após um incidente