CAIO DE BONIS ROSSETTI

PROPOSTA DE MODELO DE PRIORIZAÇÃO DE CIBERSEGURANÇA PARA UMA EMPRESA MÉDIA COM BASE NA ANÁLISE DE RISCO DE AMEAÇAS

São Paulo

2022

CAIO DE BONIS ROSSETTI

PROPOSTA DE MODELO DE PRIORIZAÇÃO DE CIBERSEGURANÇA PARA UMA EMPRESA MÉDIA COM BASE NA ANÁLISE DE RISCO DE AMEAÇAS

Trabalho de Formatura apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do diploma de Engenheira de Produção

Orientador: Fausto Leopoldo Mascia

São Paulo

2022

Catalogação-na-publicação

Rossetti, Caio
Proposta de modelo de priorização de Cibersegurança para uma empresa média com base na Análise de Risco de Ameaças/
C. Rossetti – São Paulo, 2022.
98 p.

Trabalho de Formatura - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Produção.

1. Cibersegurança. 2. Segurança da Informação. 3. Modelo de análise de risco. 4. Modelo de priorização. 5. FTA. 6. Análise de Falhas. 7.Teoria de Fuzzy. 8.Empresa em crescimento | Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Produção.

AGRADECIMENTOS

Dedico esse trabalho ao meu irmão, que é minha maior referência e que os passos eu sigo desde criança. Exemplo de resiliência e inteligência, encarou desafios que poucos teriam coragem e me inspirou a buscar mais.

Aos meus pais, que foram o alicerce de tudo isso. Sem eles, nunca teria chegado aonde cheguei. Desde sempre com dedicação, carinho e integridade, me apoiaram nessa e em muitas outras jornadas pela vida.

À Escola Politécnica, deixo meu sentimento de respeito, seus ensinamentos são muito mais do que acadêmicos e vão me acompanhar por toda minha vida.

“The greater danger for most of us lies not in setting our aim too high and falling short; but in setting our aim too low, and achieving our mark.”

(Michelangelo Buonarroti)

RESUMO

O presente trabalho buscou uma maneira de auxiliar empresas médias em crescimento acelerado a priorizarem os seus investimentos em CS, alavancando-se na entrada que o autor tinha no mercado de *venture capital/private equity* para entender as maiores dores no processo de tomada de decisão na frente de CS das companhias. Entrevistou-se uma série de empresas e players do setor de CS e se constatou que havia uma grande desestruturação do modelo de tomada de decisão de companhias médias. As maiores dificuldades identificadas foram (i) a falta de um método estruturado de analisar quantitativamente os investimentos de CS de uma companhia e (ii) a susceptibilidade do tomador de decisão a influências externas na hora de optar por uma solução. Observou-se também, nas entrevistas, que parte das companhias não dava a importância necessária para o segmento de CS, despriorizando-o frente outros investimentos.

Como objeto de estudo desse trabalho, elegeu-se a *Empresa A*, uma *fintech* de porte médio em crescimento acelerado com a qual o autor tinha proximidade e foi capaz de estudar com mais detalhes a estruturação da CS dessa companhia. Foi proposta a aplicação de um modelo de priorização que utiliza Árvore de Análise de Falhas (FTA) e teoria de Fuzzy para fazer a avaliação de CS da companhia por apresentar algumas características interessantes para endereçar os problemas de médias empresas: (i) uma ponte estruturada entre a análise qualitativa e quantitativa e (ii) um método quantitativo para lidar com incertezas da análise.

Em seguida, aplicou-se de maneira demonstrativa o modelo proposto para três diferentes alternativas de investimento em CS. Elegeu-se como critérios para serem analisados as (i) perdas financeiras e o (ii) tempo de recuperação do sistema pós ataque cibernético. Sugeriu-se também a utilização do programa *AIDMS2* para auxiliar nos cálculos. Assim, chegou-se ao resultado de priorização do investimento na alternativa referente ao *gateway de pagamentos* da *Empresa A*. Vale ressaltar que, para a aplicação em um caso real, seria necessário um expert para realizar as análises subjetivas de impacto. O trabalho sugere que há um ganho operacional e estratégico a ser feito ao utilizar o modelo proposto de priorização de investimento em CS em companhias médias.

Palavras-chave: Cibersegurança. Segurança da Informação. Modelo de análise de risco. Modelo de priorização. FTA. Análise de Falhas. Teoria de Fuzzy. Empresa em crescimento.

ABSTRACT

This paper sought a way to help fast-growing mid-sized companies prioritize their CS investments, leveraging on the author's network in the venture capital/private equity market to understand the biggest pains in the decision-making process on the companies' CS front. A number of companies and players in the CS industry were interviewed and it was found that mid-sized companies were lacking on a structured decision-making model for CS investments. The major difficulties identified were (i) the lack of a structured method to quantitatively analyze a company's CS investments and (ii) the susceptibility of the decision maker to external influences when choosing a solution. It was also observed in the interviews that part of the companies did not give the necessary importance to the CS segment, de-prioritizing it in face of other investments.

As the object of study of this work, Company A was chosen, a mid-sized fintech in accelerated growth with which the author had proximity and was able to study in more detail the CS structuring of this company. It`s been proposed the application of a prioritization model that uses Fault Tree Analysis (FTA) and Fuzzy Theory to do the CS evaluation of the company due to some interesting characteristics to address the problems of mid-sized companies: (i) a structured bridge between qualitative and quantitative analysis and (ii) a quantitative method to deal with the uncertainties of the analysis.

Next, the proposed model was applied demonstratively to three different CS investment alternatives. It was elected as criteria to be analyzed (i) financial losses and (ii) system recovery time after a cyber-attack. It was also suggested the use of the AIDMS2 program to assist in the calculations. Thus, the result was the prioritization of investment in the alternative referring to the payment gateway of *Company A*. It is worth pointing out that, for application in a real case, an expert would be needed to perform the subjective impact analysis. This work suggests that there is an operational and strategic gain to be made when using the proposed model for prioritizing investments in CS in medium-sized companies.

Keywords: Cybersecurity. Information security. Risk analysis model. Prioritization model. Fault tree analysis. Fuzzy theory. Growing companies.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo são apresentadas as considerações iniciais a respeito do tópico de cibersegurança, uma contextualização do assunto como um todo, uma breve descrição da empresa em que o trabalho foi desenvolvido, as motivações e importância do trabalho, a definição do problema que está sendo abordado, o objetivo do Trabalho e, por fim, descreve-se como está estruturado o trabalho.

1.1 Considerações iniciais e contextualização do assunto

1.1.1 Panorama Atual

Desde a última década, uma das maiores ameaças que a sociedade enfrenta junto do aquecimento global é o aumento da incidência de crimes cibernéticos (PERLROTH, 2021). Isso se dá por uma série de tendência globais que implicam no aumento da relevância dos contextos digitais, do aumento impacto das interações humanas nesses ambientes e das próprias características intrínsecas do contexto cibernético. A associação dessas tendências cria um panorama adverso para a segurança cibernética (cibersegurança) e favorável para que crimes ocorram. Dentre essas tendências temos:

(i) **digitalização dos serviços** (i.e., adoção generalizada do e-commerce que já começa a substituir parte do varejo físico, serviços financeiros rompendo a barreira física e passando a ter maior parte das suas interações de maneira digital (BABANINA, TKACHENKO, *et al.*, 2021);

(ii) **democratização do acesso à internet**, diretamente ligado o aumento da capilaridade de smartphones atrelados ao aumento da rede de cobertura (i.e. 3G, 4G) de acesso à internet e da banda-larga (i.e. 5G) (STATISTA, 2021);

(iii) ***Internet-of-Things*** (IoT, Internet das coisas), na qual houve um aumento considerável na quantidade de dispositivos interconectados e interagindo (HASAN, 2022);

(iv) **aumento da superfície digital** das entidades (pessoas, empresas, governos, etc.), cada vez mais o contexto digital ganha relevância e o perímetro de contato de cada entidade fica maior. Isso ocorre com a expansão da quantidade de aplicações utilizadas, redes sociais, serviços digitais, dispositivos conectados à internet.

Todos esses fatores implicam numa maior face de interação com as redes públicas e outras entidades (MEYER, 2017);

(v) **criação de redes descentralizadas (Web 3.0)**, através das quais, de maneira bem simplificada, é possível descentralizar os processos decisórios, geralmente atribuídos a uma grande companhia/governo e distribuí-los para para a comunidade que faz parte dessa rede de maneira escalável. Uma das aplicações mais almejadas é a possibilidade de utilizar essas redes de *block-chain* como moeda, as chamadas criptomoedas. Dentre suas diversas características, temos a possibilidade de realizar transações não rastreáveis. Fator bastante relevante para a cadeia de funcionamento dos crimes cibernéticos (REDDY e MINNAAR, 2021);

(vi) **mudanças estruturais da engenharia de software das empresas**, ao redor do mundo, é cada dia mais comum a transição da hospedagem de sistemas de companhias e entidades governamentais de instalações físicas para a nuvem, mudança de *on-premise* para *clou* (GALOV, 2022). Isso expande ainda mais a superfícies de contato digital dessas entidades e torna inevitável a conexão direta com a internet.

(vii) **tendência de aumento regulatório no Brasil e no mundo**, em paralelo a todos esses fatores há uma pressão por parte do governo para o aumento das regulações voltadas para a segurança da informação cibernética e de serviços de alta importância. Isto pode ser observado em regulações voltadas para empresas num contexto geral, como a ISO 9001 (INMETRO, 2022), LGPD (Lei Geral de Proteção de Dados) (PRESIDÊNCIA DA REPÚBLICA SECRETARIA GERAL, 2018), GDPR (*General Data Protection Regulation*) (EU, 2022); e também em setores específicos, como a criação SCS 9001 (*supply chain security standart*) pela *Telecommunitactions Industry Association* (TIA) (TIA, 2022);

(viii) **dinamismo do contexto digital,** onde há uma rápida evolução das soluções e da sofisticação dos cibercriminosos, que são capazes de explorar *gaps* (brechas) entre a estrutura de cibersegurança desenvolvida e os pontos expostos passíveis de ciber-ataques (BABANINA, TKACHENKO, *et al.*, 2021);

(ix) **assimetria de risco, impacto e custos entre atacante e vítima**, panorama global onde os cibercriminosos são capazes de realizar grandes quantidades de ataques, com baixo custo e baixo risco de sofrerem alguma consequência (REDDY e MINNAAR, 2021). Em contrapartida, do lado da vítima do ciber-ataque (governo, empresa, pessoa), há um grande impacto que pode ser causado por um ciber-

ataque, possivelmente repercutindo nas operações, nos resultados financeiros, na reputação ou no quesito legal da entidade. Além disso, basta uma brecha para que o atacante possa impactar o sistema. De forma que, seja necessário grande investimento por parte da companhia para garantir a integridade do seu setor de segurança.

(x) **desinformação dos tomadores de decisão a respeito do contexto de cibersegurança**, por ser um tópico que ganhou grande relevância recentemente, os tomadores de decisão das instituições ainda não possuem grande conhecimento a respeito do assunto. Isto criou uma sensação de urgência que leva instituições a tomarem decisões de investimento em cibersegurança pouco embasadas e que não otimiza a redução de riscos (MCKINSEY, 2019)

(xi) **falta de especialistas no mercado**, justamente pelo surgimento de toda essa urgência, os especialistas desse setor disponíveis no mercado estão sujeitos a grande assédio por diversas instituições, que buscam oferecer benefícios cada vez mais expressivos para atrair seus conhecimentos. Ligado a isso, vemos uma falta de profissionais no mercado, gerando uma diferença expressiva entre o número de pessoas com formação no setor e a demanda por parte das entidades, que se sentem vulneráveis (BUSINESS WIRE, 2022).

Todos esses fatores criam um cenário global onde a segurança digital é cada vez mais importante. Ao mesmo tempo que a cibersegurança possui características intrínsecas que dificultam uma abordagem unificada entre todas as entidades. Variando de acordo com setor de atuação, tamanho da entidade, superfície de contato digital, grau de maturidade digital, cadeia de valor, dependência do contato humano, entre outros.

1.1.2 Casos Emblemáticos de ciberataques

São diversos os casos de ciber-ataques que causaram impactos de todas as dimensões em Governos e empresas. A seguir lista-se alguns dos mais recentes com diferentes causas, dimensões e áreas afetadas:

(i) **Série de ataques da Rússia à Ucrânia** (2015, 2016 e 2017, pré-guerra), logo após anexar a península da Criméia (2014), a Rússia realizou uma série de ataques

às infraestruturas de instituições Ucranianas, culminando em 27 de junho de 2017. Quando a Rússia lançou um ataque cibernético de proporções nunca antes vistas. O incidente impactou: (i) as redes dos serviços financeiros, impossibilitando saque em caixa eletrônicos e pagamentos no cartão de crédito; (ii) os serviços de acesso a internet, como enviar e receber e-mails; (iii) serviços que permitiam o trabalho remoto de empresas, fazendo com que boa parte das empresas que tivessem trabalhadores remotos fosse impactada em algum nível - a Pfizer e a Merck, empresas farmacêuticas, a Maersk, empresa de transporte, e a FedEx, empresa de logística, tiveram suas redes internas altamente impactadas; (iv) até mesmo os sistemas que monitoravam a radiação da usina de Chernobyl foram impactados. Como se não bastasse, este ataque repercutiu fora da Ucrânia, afetando a (v) Tasmania e até mesmo (vi) empresas Russas. As consequências desse incidente foram estimadas em mais de $ 10 bilhões de dólares (PERLROTH, 2021).

(ii) **Ataques da Ucrânia vs Rússia** (2022), em plena guerra entre os países, os ucranianos têm utilizado ataques cibernéticos como forma de contra-ataque aos ataques militares Russos e para criar obstáculos para a vida da população Russa. A Ucrânia tem orquestrado uma sequência de ciberataques para desestabilizar os sistemas russos, por meio de uma equipe composta de profissionais do ramo e civis, que se alto denomina "IT Army" (WIRED, 2022)

(iii) **Ataque contra o Governo da Costa Rica** (2022), o grupo de cibercriminosos russo que se autointitula Conti conseguiu acessar 20 instituições do governo da Costa Rica e, em seguida, bloquear acesso às plataformas, exigindo, em troca das chaves de desbloqueio um pagamento de $ 20 milhões de dólares em criptomoeda. Esse tipo de sequestro de sistema é chamado de *Ransomware* e é um dos ataques mais temidos pelas instituições. Nele, se não há um *back-up* do sistema, a entidade é obrigada a pagar um resgate, caso contrário, pode perder acesso a todos os dados que ali estavam guardados (BBC NEWS, 2022)

(iv) **Ataque às Lojas Americanas** (2022), a empresa de varejo brasileira foi alvo de um ataque cibernético que derrubou todos os sites do conglomerado do ar, que incluiu Lojas Americanas, Shoptime, Submarino, Supermercado Now e Sou Barato. Os prejuízos provenientes do ataque reportados nos balanços da empresa ao final do trimestre totalizaram mais de 900 milhões de reais. (AMERICANAS SA, 2022)

(v) **Ataque ao jogo Axie Infinity** (2022), Axie Infity é um jogo no qual o jogador ganha criptomoedas quanto joga mais na plataforma. Esta empresa sofreu um ciber-ataque no começo de 2022 que levou à perda de $ 625 milhões de dólares em criptomoedas (Ethereum e USDC[1]) (CNN, 2022)

(vi) **Ataque aos clientes da SolarWinds** (2020), um dos serviços que a companhia vendia, chamada Orion, teve seu código alterado. Isso permitiu que os cibercriminosos pudessem instalar uma sequência de *malwares*[2] nos servidores dos clientes que deram acesso a informações internas de diversas empresas multinacionais membras da Fortune 500 [3] (BUSINESS INSIDER, 2021)

(vii) **Ataque à Kaseya** (2021), uma organização criminosa chamada REvil foi capaz de penetrar as barreiras de segurança da Kaseya, uma empresa que fornece infraestrutura de acesso remoto comumente utilizada por MSSPs[4]. Após adentrar a rede interna da Kaseya, o grupo criminoso instalou um *malware* e encriptou os dados, exigindo um resgate de $ 70 milhões de dólares. Empresas em 17 países foram afetadas nesse ataque. (DW, 2021). Esse ataque só ressalta como até empresas fortemente ligadas ao setor de cibersegurança, como a Kaseya, também apresentam vulnerabilidades e são alvos de ataques.

(viii) **Ataque ao partido democrata durante eleições dos Estados Unidos** (2016), durante as dispostas presidenciais desse ano um série de conversas internas do partidos, emails e documentos secretos foram vazados através do site WikiLeaks. Esses atos podem ter afetado de alguma forma os resultados ao disseminar em conjunto aos documentos "verdadeiros", informações falsas (*fake news).* Possivelmente repercutindo na reputação e imagem do partido frente ao eleitorado. (TENCH e YEOMANS, 2014)

Esses são apenas alguns exemplos para demonstrar alguns pontos a respeito dos ciber-ataques: (i) o aumento da quantidade nos últimos anos; (ii) o aumento do impacto causado;

[1] USDC é uma criptomoeda cujo valor está atrelado com o do dólar, sendo chamada de *stable-coin* (moeda estável) justamente por ter ser menos volátil menor do que outras criptomoedas

[2] *Malware* é o termo usado para se referir a qualquer software malicioso projetado para entrar em redes sem ser detectado

[3] Lista publicada pela revista Fortune com as 500 empresas com maior receita naquele ano nos Estados Unidos. Comumente utilizada como referência para um dos grupos com as empresas mais influentes do planeta.

[4] MSSP – *Managed Security Services Provider* é uma empresa que fornece serviço de cibersegurança para outras instituições.

(iii) a diversidade de motivações para esses crimes; (iv) a vulnerabilidade de todo tipo de entidade, seja pessoa, empresa ou governo (BABANINA, TKACHENKO, *et al.*, 2021).

1.2 Contextualização da empresa em que o trabalho foi desenvolvido

Este trabalho de formatura foi desenvolvido em uma empresa de serviços financeiros - (*fintech*) que será endereçada nesse trabalho como *Empresa A*. Esta empresa foi fundada no final de 2018, com o objetivo de oferecer serviços facilitadores de pagamentos para empresas. Funcionando em um modelo B2B (*Business-to-Business)*[5], hoje contam com mais de 25 mil clientes ativos contando todos os seus produtos financeiros. Em questões de porte, hoje em sua totalidade, a empresa conta com mais de 100 funcionários e com um faturamento anualizado de aproximadamente R$ 50 milhões.

Para alcançar tal proporção em tão pouco tempo, a *Empresa A* recebeu aportes de diversos fundos de *venture capital* e *private equity* que permitiram acelerar o crescimento de suas operações sem se preocupar em rentabilizar a companhia no curto prazo. Essa forma de expansão de startups é um modelo bastante comum praticado no mercado afim. Onde buscam-se investimentos diretamente do mercado de capitais fechados (fundos que investem em companhias privadas) para ganhar escala e provar seu modelo de negócio. De forma que, estabeleça-se uma barreira de entrada para que novos *players* não capitalizados operem nesse nicho de mercado.

Junto deste crescimento acelerado, vem a necessidade de expandir a companhia e sua estrutura rapidamente para suportar o aumento do volume de operações. Disso surgem "dores do crescimento" que estão diretamente relacionadas a expansão da oferta, dos times, dos custos e da complexidade das operações. Exigindo um alto grau de sofisticação dos empreendedores para construir a companhia de maneira equilibrada e não criar nenhuma grande lacuna na estrutura. Esse impasse também se reflete na questão da arquitetura de software da companhia e da sua cibersegurança.

Por se tratar de uma empresa atuando no setor financeiro, desde o início, questões a respeito da segurança da informação e dos processos da companhia são de suma importância. Assim, mesmo que seja uma companhia relativamente nova, sendo fundada há apenas 4 anos, exige-se, por questões regulatórias, um sistema de cibersegurança (CS[6]) bastante robusto.

[5] B2B: são as empresas que vendem produtos ou prestam serviços para outras empresas, pessoas jurídicas
[6] CS: Cibersegurança, denotação que será utilizada no decorrer do trabalho

Por questões de segurança da própria companhia, não são expostos os detalhes das operações de CS na companhia. Apenas uma breve descrição de como essa frente está estruturada. A *Empresa A* conta com 10-15 funcionários dedicados para garantira segurança da informação e dos processos de toda companhia. Estes estão divididos entre *Blue Team, Red Team, Yellow Team* e *White Team.* O primeiro cuida da segurança defensiva, fazendo o monitoramento de incidentes e condução da resposta ao incidente, responsável por cuidar de vazamentos, fraudes, comprometimentos da infraestrutura, entre outros. O segundo cuida justamente do oposto, a segurança ofensiva, fazendo diversos testes de penetração no sistema de segurança e simulações de ataques. O *Yellow Team* por sua vez é o responsável pela arquitetura do software, tanto de nuvem quanto de tecnologias, garantindo também as boas práticas no setor. Por fim, o White Team está ligado aos passos de governança da segurança da informação, propondo políticas, procedimentos e processos. Dessa forma, garantindo uma concordância com as métricas legais e de *compliance*[7]. Esses 4 times juntos compõem a equipe de CS da *Empresa A* trabalhando muitas vezes entre si para garantir a conformidade e ressonância no desenvolvimento da companhia.

1.3 Motivação e importância do trabalho

Nesse contexto de rápido crescimento das startups, muito motivado pelas grandes rodadas de capitalização para empresas dos mais diversos setores de 2021 e início de 2022 (TERRA, 2022), são claras as lacunas operacionais e estruturais que surgem desse fenômeno.

Isso ficou evidente durante meu estágio em uma gestora de fundos de investimento em mercados fechados. Essa gestora se propõe a investir em companhia de diferentes maturidades: menos maduras, mais associado a um fundo de *venture capital*, e mais maduras, mais associada às atividades de um fundo de *private equity*. Contudo, em ambos os casos se buscavam empresas em crescimento acentuado +50% de crescimento ano a ano. Dessa forma, companhias demonstravam problemas decorrentes do crescimento independente do estado de maturidade.

Em meio a esse estágio, foi possível perceber a dificuldade e importância de lidar com esses problemas decorrentes do crescimento de maneira estruturada, estratégica e planejada. Sendo vital que as companhias sejam capazes de priorizar diferentes frentes de acordo com

[7] *Compliance* representa as ações que as empresas executam para guiar suas atividades com base em regras e procedimentos legais

(i) o estágio de maturidade das suas operações, (ii) o setor de atuação de cada companhia e (iii) o impacto que a priorização desse projeto traria para a companhia.

Em paralelo a isso, a crescente necessidade de estruturação de um sistema de CS robusto se tornou assunto de todos os conselhos administrativos das empresas que acompanhávamos dentro da gestora, independentemente do setor. Associado a isso, vem um enorme hiato de informação a respeito da segurança da informação e dos processos.

1.4 Definição do problema e objetivo do trabalho

Ao combinarmos os pontos (i) a dificuldade de priorização de diferentes projetos dentro de companhias, e (ii) a crescente ameaça e necessidade de um sistema de CS robusto, define-se o tema deste trabalho: propor um modelo para que empresas sejam capazes de mapear e priorizar o desenvolvimento da CS dentro de seus *roadmaps*[8].

Para tal, tem-se como base a *Empresa A*. A qual, mesmo com disponibilidade de capital e com time dedicado para a estruturação de políticas e estruturas de CS, existe uma dificuldade em definir que em que frente alocar capital e desenvolver. Muito dessa decisão é tomada em aspectos 100% qualitativos e pouco embasados no real impacto que podem causar.

Dessa forma, esse trabalho de se propõem a estudar os modelos e métodos de estruturação e priorização praticados no mercado hoje e já explorados pela literatura. Em seguida, fazer uma análise crítica a respeito dos bônus e ônus dos principais casos e sugerir um modelo específico que se encaixe na realidade da *Empresa A* (exemplo significativo para o mercado atual de empresas médias em crescimento).

Além disso, o trabalho também busca fazer um estudo do setor e das principais questões que devem ser abordadas em um programa de estruturação da CS de uma companhia e também contextualizar os empreendedores frente a um tema tão pouco difundido.

[8] *Roadmap* é o plano de desenvolvimento de processos e produtos de uma companhia. Sendo essencial do ponto de vista estratégico.

1.5 Estrutura do trabalho

O presente trabalho está dividido em 6 partes: **Introdução**, **Revisão Bibliográfica**, **Metodologia**, **Resultados e Discussões**, **Conclusões,** e **Referências Bibliográficas**.

A **Introdução** é o presente capítulo onde discorreu-se sobre o contexto atual da cibersegurança no mundo, apresentou-se a companhia que serve de base para esse trabalho, informou-se as motivações e a importância da realização de tal trabalho, definiu-se o problema os objetivos do trabalho.

A **Revisão Bibliográfica** busca contar a história de evolução da cibersegurança, as principais características desse setor, seus atores, ameaças comuns e principais domínios dentro de uma empresa. Em seguida, compara-se diferentes necessidades de empresas na CS de acordo com o setor e nível de maturidade. E por fim, faz-se uma revisão da literatura existente para diferentes certificações e modelos de priorização da CS em companhias. Buscando encontrar um que se encaixe nas realidades da *Empresa A*.

A **Metodologia** descreve como o trabalho foi desenvolvido com a ajuda de entrevistas com *players* do setor.

Em **Resultados e Discussões**, temos a aplicação da metodologia e análise dos resultados das entrevistas, assim como uma discussão a respeito da escolha do modelo eleito como que mais se enquadra nas necessidades da *Empresa* A e dos seus métodos implícitos. Também se explora as limitações das certificações para suprir a necessidade destas empresas.

Nas **Conclusões**, temos um resumo dos principais pontos abordados neste trabalho e uma análise do autor a respeito de limitações e espaços que podem serem explorados em estudos futuros deste mesmo assunto.

Por fim, temos as **Referências Bibliográficas** com toda a literatura, publicações, livros, notícias, sites e entrevistas realizadas que foram utilizados para formulação do presente trabalho.

2 REVISÃO BIBLIOGRÁFICA

2.1 História da cibersegurança

A história da cibersegurança evolui em paralelo com o desenvolvimento da tecnologia, especialmente dos computadores pessoais e dos pró crime cibernético. A respeito da história do desenvolvimento dos computadores, essa ganha tração após a segunda guerra em 1946 quando inicia-se a produção de computadores comerciais. Nessa época, não existia internet e os crimes cibernéticos estavam associados a intervenções diretas no *hardware*[9] dos computadores e tinham sem impacto limitado justamente a aquelas ligações físicas entre computadores. (DOVGAN, 2018)

A partir da década de 60-70, após a invenção dos transistores e dos circuitos integrados (chips), iniciou-se a produção em massa de computadores comerciais tanto para companhias, como computadores pessoais. Durante este período os crimes cibernéticos estavam relacionados a máquinas utilizadas para realizar investimentos financeiros e só começaram a se espalhar para outras frentes com a dispersão do uso da internet (DOVHAN e TKACHUK, 2018). Em 1995, estima-se que existiam 16 milhões de usuários da internet. Este número aumentou para 580 milhões em 2002 (YAR, 2015). Em janeiro de 2022 esse número se aproxima da marca de 5 bilhões de usuários (DATAREPORTAL, 2022).

Um subsegmento extremamente relevante dos cibercriminosos são os *hackers*. Um *hacker* é alguém com grande especialização em Tecnologia da Informação (TI) e que entende os detalhes intrínsecos de estruturas computacionais e softwares. Eles podem ser *black-hat hackers*, cibercriminosos, e *White-hat hackers*, que se refere a outros profissionais de segurança da informação que não quebram a lei (como exemplos profissionais de empresa que trabalham com segurança da informação) (MOISEEV, 2016). No decorrer dos anos esses *players* foram interagindo e desenvolvendo novas ferramentas de ataque e, consequentemente, de defesa das operações e informações digitais.

Na figura a seguir temos uma linha do tempo com um resumo das principais teorias e tecnologias de cibersegurança desenvolvidas de acordo com os avanços principalmente nos computadores e nos servidores utilizados (LE VPN, 2021):

[9] Hardware é a parte física do computador, ou seja, o conjunto de aparatos eletrônicos, peças e equipamentos que fazem o computador funcionar.

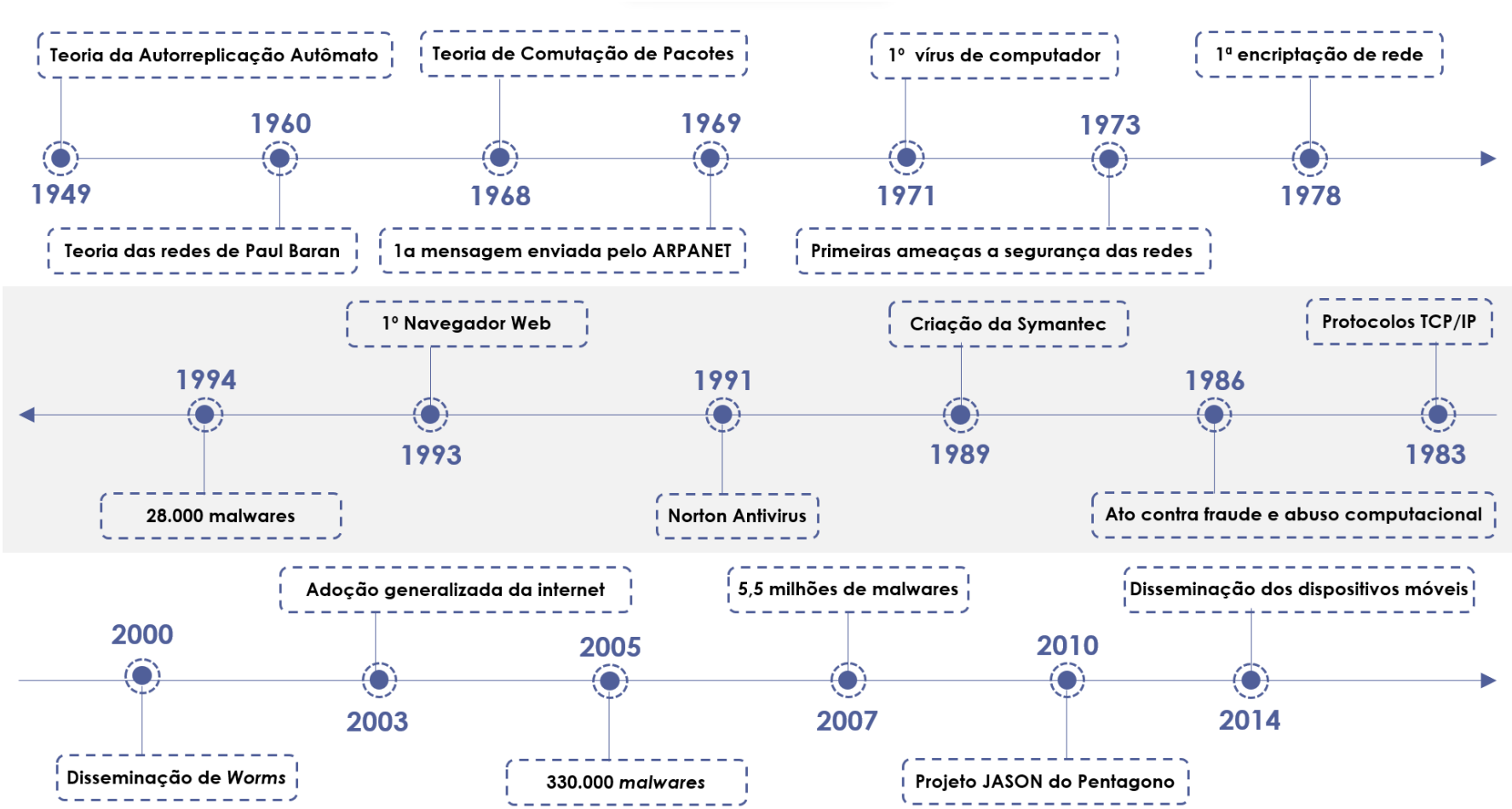

Figura 1- Linha do Tempo das ameaças cibernéticas. Fonte: elaboração própria do autor.

Uma breve descrição dos fatos em cada um dos anos presentes na figura:

- 1949: o cientista Húngaro Jon Von Neuman publicou a "Teoria da Autorreplicação Automata";
- 1960: O engenheiro Paul Baran desenvolve a teoria das redes, permitindo que redes de comunicação pudessem operar mesmo se houvesse algum dano devido a uma redundância;
- 1968: Donald Davies desenvolve a teoria da comutação de pacotes tornando possível mais de um usuário acessar a mesma linha e também diminuía a informação em pacotes menores otimizando a capacidade de transmissão
- 1969: 1ª mensagem enviada pela ARPANET, rede de troca de dados do governo dos Estados Unidos, considerada a precursora da internet;
- 1971: 1º vírus de computador chamado: *The creeper*. Em decorrência dele, criou-se o primeiro antivírus. Essa data é considerada o início da história do cibercrime;
- 1973: rede ARPANET já sofria de diversos casos de intrusões, começando a ser uma ameaça constante;
- 1978: 1ª encriptação de redes de comunicação digital;
- 1983: padronização da comunicação com a rede ARPANET por meio de protocolos de TCP/IP. Neste mesmo ano foi mencionado pela primeira vez o termo "vírus de computador" em um artigo acadêmico se referindo a um software que pode alterar outro computador e se replicar;
- 1986: com o avanço da internet e dos usuários, o congresso americano aprova um ato para conter roubo de dados, acesso não-autorizado a redes e outros crimes cibernéticos;
- 1988/1989: proliferação das companhias de antivírus, lançamento da Symantec, uma das maiores empresas de cibersegurança até os dias de hoje;
- 1991: lançamento do primeiro Norton Antivirus pela Symantec;
- 1993: lançamento do primeiro navegador web, democratização do acesso a internet e crescimento dos ciberataques. Primeiros usos de robôs digitais para realizar DDoS[10] ataque;

[10] *Distributed Denial of Service Attacks*, negação de serviço distribuída

- 1994: número de malwares únicos alcança 28 mil;
- 1996: expansão da complexidade de navegadores com a adição de *add-ons Flash Players*, ao mesmo tempo que *phisihing* se torna um problema para os usuários de e-mail;
- 2000: disseminação de *computer Worms*[11] e sofisticação dos cibercriminosos (*hacker*), utilizando ferramentas como *Adware* e *Spyware*, para espionar e apagar informações;
- 2003: uso da internet decola, informação criada na internet só em 2003 supera toda a informação criada na história. Nesse cenário, *malwares, phishing* e *zero-day attacks*[12] se tornam comuns. Número de malwares alcança 333 mil, incremento de 1100% em 10 anos;
- 2007: 5,5M de malwares detectados apenas neste ano;
- Desde 2014: a complexidade e o número de conexões das redes cresceram de maneira exponencial com o uso de dispositivos móveis com conexão à internet;

De maneira complementar à linha do tempo exposta acima, na figura abaixo, descreve-se a tecnologia da informação que estava sendo desenvolvida ou ganhando tração naquela década. Assim como as ameaças de CS que surgiam e as soluções de cibersegurança implementadas em decorrência fenômenos. Vale ressaltar que tal tabela não busca ser exaustiva a respeito de nenhum dos aspectos abordados.

[11] *Computer Worm* ou W*orm* são programas independentes desses do tipo malware que se replica com o objetivo de se espalhar para outros computadores.
[12] *Zero-day-attacks* é uma vulnerabilidade de software de computador desconhecida para aqueles que deveriam estar interessados em sua mitigação ou conhecida e um patch não foi desenvolvido.

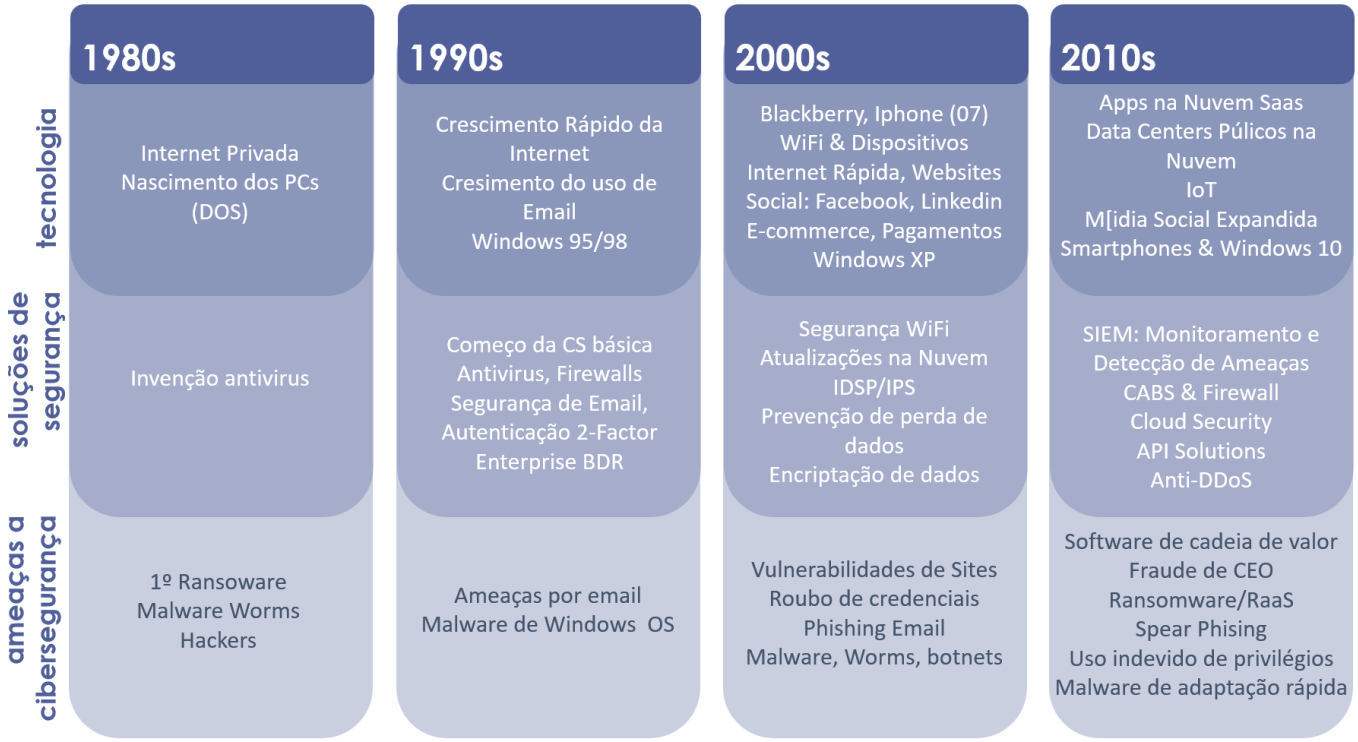

Figura 2 - Panorama temporal de tecnologia, ameaças e soluções de cibersegurança no decorrer do tempo. Fonte: elaboração própria do autor.

2.2 Futuro da cibersegurança

Como mencionado na seção “Panorama Atual”, há diversas razões que justificam o crescimento da importância da cibersegurança no contexto mundial. Em grandes linhas, a evolução digital das empresas e pessoas, faz com que haja mais oportunidade e valor a ser extraído de um ataque cibernético. Isto leva as empresas a investir cada vez mais nessa frente. Buscando se blindar e conter os danos de uma provável tentativa de invasão.

Vale ressaltar que essa vulnerabilidade não está relacionada apenas com grandes empresas. Com o aumento do investimento em CS para estruturação de barreiras de proteção, os ataques cibernéticos também se tonaram mais complexos e mais difíceis de serem detectados. Assim, empresas médias e pequenas, que não tem tanto orçamento para se blindar dessas ameaças, também se tornaram alvos para os cibercriminosos.

Outro fator que apresenta um grande risco no futuro da cibersegurança é a evolução da capacidade de processamento dos computadores e dos modelos de inteligência artificial (HAI, 2017).

No caso da evolução exponencial da capacidade de processamento, o evento mais emblemático é o uso da computação quântica para invasão de sistemas. Embora essa seja uma realidade distante, estima-se que leve mais de 20 anos para que essa tecnologia alcance o mercado de uma maneira minimamente acessível (MIT TECHNOLOGY REVIEW, 2022), essa capacidade de processamento certamente mudará totalmente a maneira como é a estruturada a segurança cibernética de qualquer pessoa ou instituição.

Já no caso da inteligência artificial, ela vem sendo usada tanto para ajudar a defender sistemas de segurança, buscando anomalias e inconsistências em interações e entidades, quanto para o orquestrar ataques em massa a empresas com baixo nível de proteção. O crescente uso e evolução dessa tecnologia permite utilizações cada vez mais complexas. (HAI, 2017)

Por fim, o ganho de relevância da Web 3.0 e da descentralização das redes também é um fator que vai tornar ataques e riscos cibernéticos mais atrelados ao dia a dia das pessoas. Um exemplo bastante óbvio disso é o metaverso[13], no qual, um risco cibernético estaria diretamente ligado às informações pessoais e vidas das pessoas.

2.3 Polos de Cibersegurança

Justamente por não haver fronteiras de atuação para acessar qualquer rede do mundo, os cibercriminosos podem atuar independente da localidade. Com isso, observa-se uma concentração de ataques cibernéticos provenientes de países como Rússia, China e Korea do Norte. Estes países, são conhecidos por "permitirem" ou até mesmo incentivarem a operação de cibercriminosos que tenham como alvo países da Europa e do eixo ocidental (PERLROTH, 2021).

No caso da Korea do Norte, diversas são as alegações que há um programa do governo que utiliza os crimes cibernéticos como uma via de receita para financiamento interno do país (MASCELLINO, 2022).

O próprio Estados Unidos desenvolve armas cibernéticas para utilizar em caso de ameaça internacional (PERLROTH, 2021).

[13] Metaverso é uma rede de mundos virtuais, que tenta replicar a realidade, com foco na conexão social. No limite, entusiastas defendem que será no ambiente virtual que as principais relações interpessoais vão ocorrer.

Além da exportação de ataques cibernéticos, temos o desenvolvimento e exportação de soluções de cibersegurança. Na vanguarda desse movimento, três países se destacam como os pivôs Estados Unidos, Israel, Cingapura, onde grandes empresas do setor e incentivos do governo estão presentes.

2.4 Principais motivações de ataques e setores alvo

As motivações por trás de um ciber-ataques podem ser diversas e como principais temos: (i) financeira; (ii) política; (iii) acesso de dados sigilosos/pessoais (SOLMS e NIEKERK, 2013). Independente do motivo, os alvos finais são chamados de ativos críticos.

Com o intuito de proteger esses ativos críticos, uma séria de precauções é tomada para: (i) garantir que os dados possam ser acessados somente por usuários autorizados (confidenciabilidade); (ii) assegurar a veracidade e a acurácia dos dados (integridade); (iii) manter as aplicações e dispositivos disponíveis e acessíveis para os usuários (acessibilidade). Estes são conhecidos como os pilares da cibersegurança (TCHERNYKH, SCHWIEGELSOHN, *et al.*, 2019)

Naturalmente há uma diferença na maneira como os setores da indústria interagem com esses ativos críticos. Fazendo com que alguns setores sejam mais propensos a serem alvos de cibercriminosos. Cinco dos principais setores que são mais almejados são: *e-commerce*[14], setor financeiro, educacional, saúde e transporte (aviação em especial) (MISHRA, ALZOUBI, *et al.*, 2022).

Saúde: saúde online (*e-healthcare)* vem impulsionando a evolução das tecnologias usadas na medicina. Isto tanto nos procedimentos médicos e exames, como também no contato com o paciente. Com o coronavírus, a *tele saúde* ganhou uma relevância gigantesca (BARR, D'AURIA e PERSIA, 2020), além das tele consultas, muitos foram os ganhos na interface do cliente e no atendimento por plataformas digitais (GRANJA, JANSSEN e JOHANSEN, 2018). Isso garantiu acesso a informações de exames, procedimentos e servindo como fonte confiável para diagnósticos pré-maturos (HERZIG e WALSH, 2020).

[14] E-Commerce: comércio eletrônico, refere-se aos negócios que estruturam seu processo de compra e venda na Internet. Assim, todas as transações comerciais são realizadas por meio de ferramentas online

Todos esses serviços necessitam de um sistema de cibersegurança (CS[15]) confiável por tratarem com informações e procedimentos sensíveis (ALZOUBI, OSMANAJ, *et al.*, 2021).

Serviços financeiros: esse é um setor de forte dependência na CS. A enorme maioria dos serviços financeiros e de gestão financeira dos usuários já pode ser acessada por meio da plataforma de *e-banking*[16]. Permitindo a centralização do acesso aos recursos financeiros de um cliente em um dispositivo digital (ALJAAFREH, AL-ADAILEH, *et al.*, 2014) (PELTIER, 2016). Essa autonomia leva a uma alta dependência de serviços de CS para garantir autenticidade, integridade e acessibilidade aos clientes.

Educação e aprendizado online: com a pandemia do COVID-19, houve uma explosão da utilização de plataformas de comunicação online para suporte das aulas de grande maioria das instituições de ensino em meio aos *lockdowns*[17]. Por exemplo, podemos citar Zoom, Microsoft Teams e Google Meets (HERRERA, RON e RABADÃO, 2017). Com essas plataformas os estudantes eram capazes de interagir com outros alunos e com os próprios professores durante as aulas (CRANE, 2016). Graças a tecnologia, foi possível disponibilizar bibliotecas de conteúdo para consumo 100% digital (BUJA, 2021), assim como plataformas para que os alunos pudessem ter visibilidade e gestão da sua performance (BANDARA, IORAS e MAHER, 2014).

Aviação: a tecnologia da indústria de aviação sempre foi considerada vanguardista frente aos outros setores. Isto justamente pela crescente dependência dela para operar instrumentos e plataformas cada vez mais complexas. Essa relação com a tecnologia tem sua presença evidente nas plataformas digitais dos clientes para compra, reserva e gestão de passagens de avião. Acesso que está disponível a todo momento e de qualquer lugar (YANG, XIONG e REN, 2020). Além disso, todo o processo de treinamento dos pilotos, softwares de gestão de tráfego, otimização de voo e muitas as outras tecnologias empregadas na cadeia do transporte aéreo dependem de acesso à internet e interconectividade com outros dispositivos (KANIA, 2018). Exigindo assim um setor de CS robusto.

E-commerce: a pandemia do COVID-19 impulsionou um crescimento monumental no setor de comércio eletrônico, exigindo soluções de computação em nuvem e medidas de

[15] CS: Cibersegurança, denotação que será utilizada no decorrer do trabalho
[16] E-Banking: Plataforma que permite acesso ao portal do banco por meio de um dispositivo pessoal
[17] Lockdown: Medida dos governos do mundo para conter a disseminação do COVID-19, no qual, foi-se imposto um toque de recolher obrigatório para todas as atividades não essenciais.

proteção de CS para garantir a integridade e disponibilidade desse serviço online de qualquer lugar do mundo e para qualquer lugar do mundo (CHUKWU e IDOKO, 2021). Além disso, outros serviços como pagamentos online e crédito estão encrustados no fluxo do e-commerce (VILLA, RUIZ, *et al.*, 2018). Sendo assim, robustez nas soluções de CS providas é necessária.

2.5 Estruturação da cibersegurança de acordo com a dimensão da empresa

Um dos principais fatores que moldam as necessidades de cibersegurança de cada uma das empresas é sua maturidade. Não só as necessidades como também a disponibilidade de recursos para desenvolver essa frente, tanto recursos humanos, quanto financeiros. Visto que o porte da empresa é de grande importância, a seguir discorre-se um pouco mais sobre cada um dos possíveis estágios da empresa e os desafios enfrentados.

2.5.1 Grande empresa

Uma grande empresa pode ser caracterizada por sua maturidade e impacto gerado pela operação. De forma abrangente, uma companhia com mais de 200 funcionários já deve ter maturidade operacional e impacto em forma de receita suficiente para ser considerada uma grande empresa. No Brasil, grandes empresas tem uma receita anual média superior a 1 bilhão de reais ou próxima a isso.

No quesito de nível de ameaça, as grandes empresas são as mais visadas por cibercriminosos. Além de terem uma maior exposição dos seus ativos digitais ao público, têm um sistema mais crítico para a operação, que, em caso de interrupção, pode incorrer em perdas proporcionais a sua escala (muitas vezes global). Por isso, tudo no setor de grandes empresas está atrelado ao superlativo desde as ameaças, até os crescentes orçamentos para o segmento de cibersegurança. Estima-se que esse mercado em grandes empresas crescerá a uma taxa de 15% ao ano até 2025 (BRAUE, 2021).

Essas preocupações com a segurança da informação provêm de uma série de características intrínsecas à operação da companhia, como (i) uma grande cadeia de fornecedores, que exige uma gestão do risco de terceiros; (ii) uma maior visibilidade e interface com o consumidor final, que torna o ativo muito mais atrativo para um ciber-ataque (maiores impactos refletem diretamente em uma maior possibilidade de retorno em caso de ataque bem sucedido); (iii) uma questão estrutural de sistemas muito mais complexa da companhia, exigindo diversos níveis de segurança para garantir a integridade dos processos;

(iv) riscos desproporcionais para o atacante em relação à companhia, enquanto o atacante pode fazer ataques em massa, com enorme taxa de impunidade (SILVESTER, 2015), a companhia pode sofrer um risco capital caso uma brecha seja explorada. Podendo gerar prejuízos à imagem, financeiros ou judiciais, caso seja julgada má conduta de segurança da informação.

Todas essas preocupações justificam os crescentes orçamentos que vêm sendo destinados para a estruturar uma robusta cibersegurança em grandes companhias. Mesmo com recursos financeiros, estas companhias sofrem da falta de mão de obra qualificada para atuar neste setor. Isso resulta no aumento da remuneração destes trabalhadores acompanhando a escassez de oferta.

2.5.2 Pequena empresa

Em contraposição às grandes empresas, as pequenas por sua vez têm um caráter de impacto gerado pela companhia muito mais contido e, por conseguinte, uma receita e um orçamento mais modestos. Desta forma, há uma limitação de recursos por parte das pequenas empresas para a estruturação de um setor dedicado de cibersegurança.

Associada a essa falta de recursos está uma desinformação a respeito dos riscos cibernéticos que a companhia está sujeita, além dos conhecimentos acerca de como se prevenir de possíveis ataques. No início do milênio 2000, mesmo desguarnecidos de alguma forma, essas empresas eram alvos pouco visados, por não oferecerem grandes recompensas aos cibercriminosos. Contudo, com os cibercriminosos usando de Inteligência Artificial e *Machine Learning*[18] para viabilizar ataques em massa, esses ataques vêm se tornando cada vez mais frequentes (SEGAL, 2022).

O principal ponto explorado nesse caso é, mais uma vez, o elo humano. Utilizando engenharia social, os cibercriminosos buscam credenciais e acessos restritos de pessoas de altas patentes (CEOs, CFOs e CTOs). São ataques direcionados (*spear phishing*) e customizados para aumentar as chances de sucesso.

[18] *Machine Learning*: é um método de análise de dados que automatiza a construção de modelos analíticos. Esses modelos são capazes de serem treinados com alguma base de dados e ir continuamente se otimizando.

2.5.3 Média empresa

Por fim, as empresas médias, que se situam entre a pequena e a grande tanto em impacto operacional causado, quanto em maturidade da companhia. Muitas das empresas cresceram rapidamente e recentemente entraram nesse setor, de forma que muitos dos processos ainda não estão estruturados e prontos para escalar[19]. Esta transição de maturidade da companhia pode gerar vulnerabilidades intrínsecas nos processos da companhia. Deixando-a desguarnecida para enfrentar a realidade de sua nova escala.

Em decorrência dessa escala, a companhia alcança muito mais pessoas e tem muito mais exposição no mundo digital. Tornando-se um alvo cobiçado por cibercriminosos.

Como agravante, a companhia ainda não conta com recursos suficientes para estruturar seu setor de cibersegurança de maneira abrangente. Isto é, mesmo os recursos existindo, eles são limitados. Dessa forma, a priorização das frentes que serão desenvolvidas é indispensável, assim como a busca por soluções que sejam condizentes ao risco e ao orçamento disponível da companhia.

Desse cenário surgem uma série de questões:

- Qual frente de cibersegurança devo priorizar e desenvolver primeiro?
- Como evitar uma superespecialização em um segmento de CS, não necessariamente garantindo a segurança do sistema conjunto da companhia?
- Quais as soluções que condizem com as necessidades da empresa? E com o seu orçamento?

2.6 Domínios da Cibersegurança

Definir domínios claros com escopos bem determinados é uma tarefa complexa em um contexto de constante evolução como o da cibersegurança. Há poucos anos, o ideal de cibersegurança seguia uma analogia muito próxima a de um castelo, onde há diversas camadas de proteção até alcançar o que se está protegendo. Dessa forma, propunha-se desenvolver uma série de barreiras para que não fosse possível alcançar os seus ativos digitais de valor (dados pessoais, códigos fonte, APIs internas). Essa superfície de contato entre a rede de acesso público e a rede privada da companhia é comumente chamada de perímetro. (TALBOT, FRINCKE e BISHOP, 2010). No esquema a seguir, tem-se

[19] Escalar: subir de nível, aumentar sua escala (volume)

representado essa ideia em 6 camadas de proteção que protegem o interior da rede de uma empresa com o exterior.

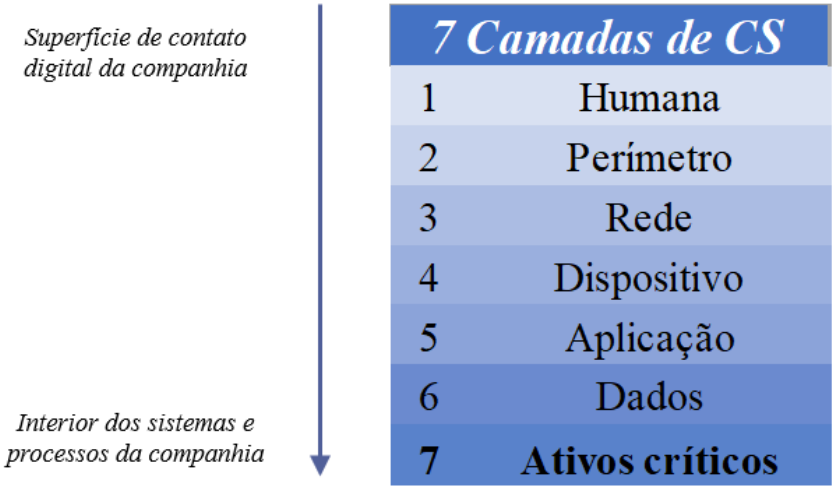

Figura 3 - 7 Camadas de cibersegurança: Humana, Perímetro, Rede, Dispositivo, Aplicação, Dados e Ativos críticos. Fonte: Elaboração própria do autor com base em (MANHATTAN TECH, 2021)

Cada uma dessas camadas tem soluções associadas a ela e que tem como intuito criar barreiras de acesso sequenciais a possíveis ameaças cibernéticas. Embora tenha imensa importância (RAHMAN, ROHAN, *et al.*, 2021) diversos esquemas que descrevem o universo de segurança cibernética, não se incluem a camada de interação humana, por não envolver um software/serviço de proteção.

Em paralelo a estas camadas, é comum estruturar uma frente de prevenção a ciberataques e outra de monitoramento e resposta. A primeira é responsável por tudo que envolva governança, processos, estruturação de sistemas, inteligência etc. e a segunda relacionada à detecção e resposta a incidentes tanto internos a rede quanto externo a rede (fora do perímetro).

A seguir temos um esquema que representa essas camadas de proteção (sem apresentar a camada humana) e suas duas frentes paralelas de prevenção e detecção e resposta. Além de apresentar as soluções mais comuns referentes a cada uma delas:

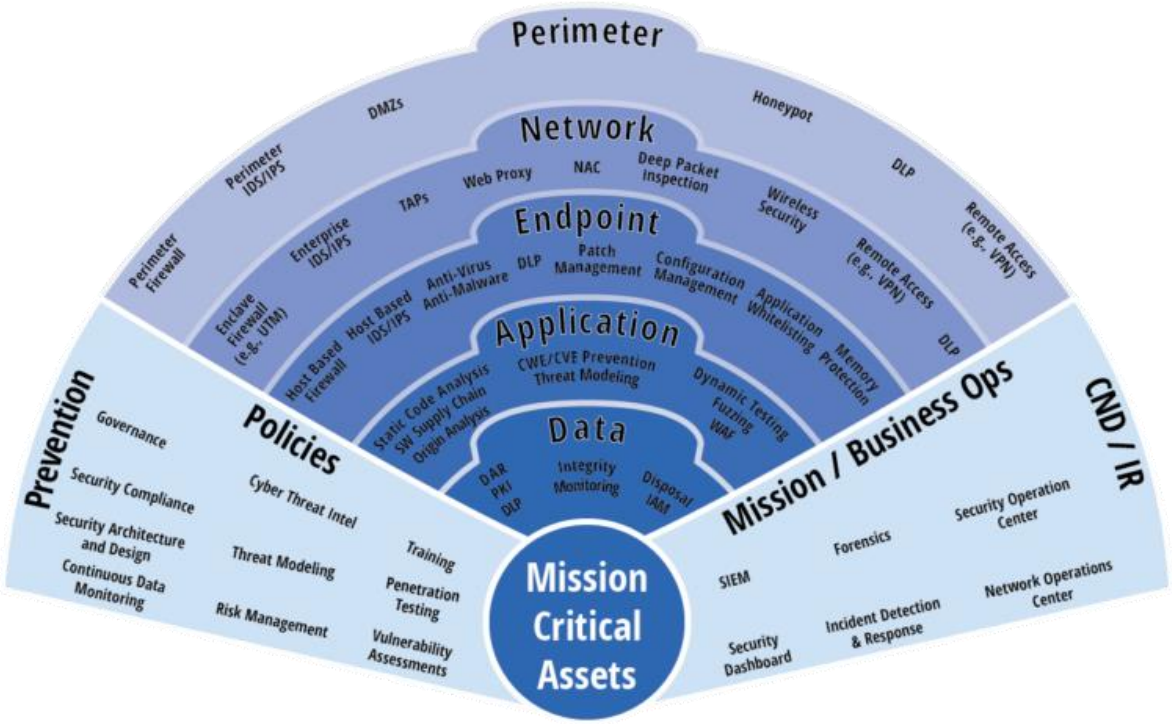

Figura 4 - Camadas de cibersegurança e suas principais funcionalidades internas. Fonte: (TMC² TECHNOLOGIES, 2021)

Um dos "mitos" /erros mais comuns durante a estruturação da cibersegurança de uma instituição é a de que: quanto mais camadas de segurança, mais segura a empresa está. Esse conhecimento legado de gerações anteriores se provou equivocado em estudos mais recentes (TALBOT, FRINCKE e BISHOP, 2010). A defesa em camadas funciona bem para a defesa de ativos físicos, contudo para ativos digitais que tem alta complexidade e grande quantidade de interações com outras entidades, isso não se provou verdadeiro (MCKINSEY, 2019).

Uma nova maneira de entender-se a estruturação das camadas de segurança é um conceito que é chamado de *zero-trust* (zero confiança). A ideia do *zero trust* é que, independentemente da camada de proteção que a entidade esteja, para ela interagir com alguma parte da rede é necessário fazer toda uma revalidação da procedência daquela entidade. Essa redundância na checagem toda vez que a entidade faz uma interação diferente torna o sistema de proteção ainda mais resiliente, impedindo, principalmente, a dispersão horizontal (dentro de uma mesma camada de segurança) de uma ameaça cibernética. (NIST, 2020)

No contexto empresarial, a principal preocupação no fundo é a redução do risco cibernético – referente a perdas no negócio de todos os tipos no domínio digital: financeiro, reputacional, operacional, produtivo ou regulatório (MCKINSEY, 2019)

2.6.1 Elo mais fraco da cadeia: interação humana

Embora haja enormes investimentos para a estruturação de camadas de proteção de CS em todas as companhias, o ponto mais vulnerável de ataques é sempre o mesmo: o ser humano. A enorme maioria dos ciberataques iniciam através de alguma espécie de falha ou exploração da interação humana (RAHMAN, ROHAN, *et al.*, 2021). De tal forma que, uma das maiores lacunas de investimento em CS é justamente o treinamento dos funcionários para (i) boas práticas de CS nos processos e (ii) roteiro de atuação em caso de ataque ou ameaça cibernética.

Quando pensamos na CS e nos seus pilares (usuários, sistemas e usabilidade), observamos uma clara correlação entre os três componentes. Em literaturas passadas, já se explorou muito mais a frente técnica — de sistemas de CS — do que os outros dois pilares. De forma que há uma lacuna de desenvolvimento na frente de usuários e usabilidade (RAHMAN, ROHAN, *et al.*, 2021).

No quesito de usuários, é sempre necessário considerar ao menos dois tipos diferentes: os experts e os não experts de CS. Eles têm diferente características que afetam a maneira como cada um utiliza os sistemas (RAHMAN, ROHAN, *et al.*, 2021). Além disso, vale ressaltar a importância da cultura nesse pilar, uma vez que está diretamente ligado ao comportamento humano. A literatura tem uma clara tendência de generalização cultural dos estudos do hemisfério Ocidental, gerando uma lacuna de conhecimento para culturas Orientais (MINKOV e HOFSTEDE, 2011) (REDMILES, 2019).

Já quanto a usabilidade, em empresas, comumente há um efeito inverso: quanto mais seguro e com mais camadas de proteção um sistema, menor a usabilidade. Uma menor usabilidade também leva a (i) um menor nível de engajamento do usuário, (ii) uma menor produtividade, e (iii) um atrito maior com o sistema e com os processos que podem levar a uma frustração do usuário e a uma negligência nos processos (RUOTI, 2019). De forma geral, os três pilares funcionam em paralelo, mas altamente correlacionados entre si. Não se pode priorizar um em detrimento do outro e todos tem muita importância.

Assim, o foco no elo humano da cadeia deve se dar por meio de treinamentos que não só previnem e ensinem como atuar em caso de ciber-ataque, mas que também tenha essas boas práticas incrustradas na cultura da companhia sempre que se constrói uma funcionalidade/produto/processo novo. Um exemplo dessa frente é uma prática chamada de Segurança por Design (*Security By Design*), que tem como principal função garantir que a segurança esteja diretamente relacionada no processo de design de todos os serviços de

tecnologia. Atentando-se a boas práticas de CS durante o processo de projeto e estruturação (SÁNCHEZ-GORDÓN, 2020).

2.7 Ferramentas de ataque cibernético

Há uma série de ferramentas utilizadas por cibercriminosos para atacar os sistemas de informação das empresas. A seguir, descrevem-se algumas das mais utilizadas e suas principais funcionalidades como descrito no relatório (EUROPOL, 2016):

(i) *Backdoor* – cria-se uma via de acesso escondida para áreas protegidas;

(ii) *Vírus de computador* – software que, estando dentro de um sistema de um computador, destrói, destorce ou interrompe suas operações. Capaz de ser transmitido por linhas de comunicação, redes de dados, entre outros. Além disso, os vírus se reproduzem;

(iii) "bombas lógicas" – software que se pluga no sistema de informação e de controle e é ativado após um tempo específico ou um sinal lógico;

(iv) Cavalo de troia – programa que, após ser instalado, realiza uma sequência de funções pré-definidas em segundo plano;

(v) Neutralizadores de programas de teste que garantem a preservação do código original;

(vi) Analisadores de tráfego (*sniffer*) – programa ou dispositivo que monitora os dados transmitidos através da rede;

(vii) Ataque DDoS (negação de serviço distribuída) – ataque coordenado que tem como objetivo interromper o acesso a uma rede. Comumente realizado através da execução de milhões de requisições cada segundo, resultando em uma sobrecarga no sistema que pode dificultar o acesso ou até mesmo interrompê-lo por completo;

(viii) Email Phishing – utilização de e-mails para obter acesso a credenciais ou dados confidenciais de alguma pessoa;

(ix) *Keylogger* – Software ou hardware que consegue controlar todos os pressionamentos de teclas do dispositivo. Obtendo assim qualquer informação teclada.

2.8 Impactos das Ameaças cibernéticas

Um ataque bem-sucedido pode ter diversos impactos dentro das instituições. Esses ataques se dão, na grande maioria das vezes, em três escopos (i) financeiro, (ii) reputacional, e (iii) legal (NIBUSINESSINFO, 2020):

No mérito financeiro, os impactos comumente incorrem de:

- Roubo de informações corporativas (Informações sigilosas que podem ser monetizadas);
- Roubo de informações financeiras (Dados bancários, cartões de crédito, etc.);
- Roubo de dinheiro (Roubo de criptomoedas);
- Interrupção das operações (Impossibilidade de realizar transações financeiras ou de operar);
- Perda de negócio ou contrato;
- Custos associados ao pagamento de resgate após um ataque de *ransomware;*
- Custos associados à notificação de clientes e provedores afetados;
- Custos associados a prestação de contas aos reguladores;
- Custo associado ao aumento do prêmio do seguro;
- Custos associados com os reparos aos sistemas, redes e dispositivos afetados;

No mérito reputacional, há um dano causado a relação com clientes, fornecedores e com o mercado como um todo. O maior problema aqui é o impacto que pode ser causado à confiança na companhia, este pode levar a:

- Perda de clientes;
- Perda de novas vendas;
- Redução dos lucros;
- Redução da confiança da cadeia de valor (provedores, parceiros de negócio, acionistas);

No mérito legal, há leis (por exemplo LGPD) que exigem cuidado ao gerenciar as informações dos clientes, provedores, investidores e empregados. Caso estas sejam descumpridas e a companhia tenha sido incapaz de aplicar as medidas de segurança apropriadas, esta empresa está passível de multas e sanções no âmbito legal.

Além dessas três categorias, há também (i) impactos operacionais, que podem exigir uma reestruturação da operação ou um causar dano operacional; e (ii) tempo gasto para recuperação das operações, que não podem ser desconsiderados por influenciar diretamente no trabalho dos funcionários da companhia.

2.9 Certificações disponíveis

Existem diversas certificações no mercado que buscam validar se uma companhia/instituição aplica boas práticas de segurança da informação. Isto inclui não só ter os sistemas de CS necessários para atuarem como barreiras de segurança, como também processos que sejam estruturalmente seguros e escaláveis. Dois dos mais utilizados certificados são a ISO27001 e SOC2. Estas são certificações da segurança da informação referentes a qualquer companhia e ou setor.

Com as recentes atualizações da legislação, principalmente da LGPD no Brasil, há um segundo grau de certificação da ISO27001 que é a 27701 – Sistema de Gestão de Segurança Privada. Esta é uma extensão da norma 27001, e tem como objetivo adicionar novos controles no sistema de gestão para garantir a total privacidade especificamente dos dados pessoais (RODRIGUES, 2020).

Um ponto a ser considerado é que essas certificações, não necessariamente garantem que a companhia esteja cumprindo todas as normas regulatórios do setor em que atua. Isso porque cada setor pode ter normas específicas de CS de acordo com o grau de criticidade da TI para as operações. O setor de energia brasileiro por exemplo, está aumentando o rigor regulatório nos mérito de cibersegurança (CANALENERGIA, 2021).

A certificação é especialmente importante se a empresa opera em um modelo B2B (*Business to Business*), onde certamente lhe será exigido a preencher e obter uma certificação em Segurança da Informação, seja ela uma Certificação ISO27001 ou um atestado SOC2, ou até mesmo outros modelos que comprovariam os cuidados com a Segurança da Informação; e, as empresas incapazes de fornecer tal prova de conformidade terão dificuldade em competir e de se estabelecer no mercado (SALGADO, BOCCARDO, *et al.*, 2021). Isso se deve ao risco cibernético proveniente da cadeia de suprimentos e fornecedores, com os quais, há alguma espécie de interação entre os sistemas de Tecnologia da Informação, podendo ser uma via de entrada para ameaças dependendo do grau de integração entre as companhias.

Como principais características da ISO27001 e da SOC2 busca-se garantir que exista a segurança em seus processos, tecnologia e pessoas. Na tabela a seguir, descreve-se os principais pontos de cada um desses atestados/certificações:

Tabela 1- Principais características das normas SOC2 e ISO 27001. Fonte: Elaboração própria do autor.

Certificação/Atestado	SOC2	ISO27001
Objetivo	Garantir que os controles de segurança que protegem as informações e processos da companhia foram implementados	O mesmo que o SOC2, mas também exige-se que a empresa possua um SGSI[1] operacional em vigor para gerenciar seu programa de segurança em uma base contínua e visando o longo prazo
Caráter	Voluntário	Voluntário
Tipo de documento	Atestado, que resulta em um relatório	Selo de certificação
Rigor	Menos rigoroso e mais fácil de manter	Robusto e mais completo
Abrangência	Pessoas, tecnologias e processos	Pessoas, tecnologias e processos
Validade	Principalmente nos EUA	Global
Certificador/fiscal	Executado por um CPA (Contador Público Certificado) licenciado	Necessário contratar um organismo de certificação credenciado pelo CGCRE (Coordenação Geral de Acreditação)/INMETRO no Brasil ou pela ANAB (ANSI National Accreditation Board)
Duração	Duração processo 6 a 12 meses	Duração processo 6 a 12 meses
Período de renovação	Renovação anual	Manutenção anual do selo e recertificação a cada 3 anos
Extensões		Possibilidade de extensão para a ISO27701

De maneira geral, estar de acordo com as normas da SOC2 ou da ISO27001 garante uma segurança abrangente principalmente nos processos da companhia e, de um momento específico no tempo, até que a renovação seja feita. Além disso, na enorme maioria das vezes, a empresa não é capaz de conseguir os selos de aprovação sozinhas, sendo necessária a contratação de uma consultoria, comumente oferecida pela própria agência certificadora.

2.10 Modelos de priorização da cibersegurança

Literaturas passadas (GOODALL, LUTTERS e KOMLODI, 2009) (GUSMAO, SILVA, *et al.*, 2018) (BOJANC, 2008) discorreram acerca de modelos para coordenar a priorização de frentes de cibersegurança. Pode-se segmentar esses estudos em três grandes áreas: (i) a de soluções tecnológicas de detecção e redução de ameaças cibernéticas; (ii) uma

área de priorização dos retornos financeiros dos investimentos em cibersegurança da companhia; e (iii) uma frente do estudo de redução do risco cibernético.

Além desses três movimentos de priorização, a forma tradicional que muitas empresas aplicavam era um modelo de investimento baseado no nível de maturidade da companhia.

2.10.1 Modelo baseado em nível de maturidade da companhia

O modelo legado de estruturação da frente de cibersegurança de muitas companhias é o baseado no nível de maturidade de cada uma das camadas de proteção. A ideia por trás desse modelo consiste em ter como objetivo adicionar novas funcionalidades de segurança à companhia. Dessa forma, há um aumento do número total de soluções de CS e um melhor do rating de segurança gerencial, mas não necessariamente priorizando funcionalidades e controles que diminuam ao máximo o risco cibernético ao que a companhia está exposta.

Este modelo de estruturação pode ser funcional para uma companhia jovem e com poucas soluções de CS em operação, de forma que são óbvias as lacunas de segurança e não faz sentido um estudo mais aprofundado. Assim, o modelo baseado no nível de maturidade funciona como uma primeira exploração a respeito das ameaças cibernéticas e os principais riscos a que empresa está sujeita. (MCKINSEY, 2019)

A prática desse modelo em companhias tem uma série de consequências possíveis, principalmente ao aumentarem o tamanho das operações, como:

(i) crescimento descontrolado do controle sobre os processos, causando o super-monitoramento de atividades que podem não gerar tanto valor;

(ii) necessidade de monitorar tudo, sem um critério claro estabelecido de que processos monitorar e quais realmente são importantes, além de sobrecarregar o time de analistas que fazem o monitoramento;

(iii) aumento dos custos para a empresa, diretamente relacionados às ineficiências estruturais;

(iv) aumento das barreiras para implementação de novas soluções, o setor de cibersegurança sempre será um gargalo caso não haja um olhar crítico sobre o desenvolvimento de novas soluções e suas implicações;

(v) superinvestimento em uma frente, tornando a empresa muito especializada em um setor e desguarnecida em outro.

2.10.2 Modelo baseado na detecção e redução de ameaças cibernéticas

Nessa área de estudo relacionada à tecnologia há foco em detecção e redução de ameaças cibernéticas. **Goodall, Lutters e Komlodi, (2009)** estudaram a análise de cibersegurança sob aspectos práticos de detecção de intrusão no sistema, enfatizando a expertise e complexidade necessária para detectar esses casos. **Kim, Yan e Zhang, (2015)** apresentou um sistema de detecção automatizado chamado DART para identificar páginas falsas na internet. **Bou-Harb, Debbabi e Assi, (2013)** discorreram sobre um método composto de duas técnicas para lidar com os desafios de detectar escaneamento cibernético em corporações e atividade reconhecimento em clusters distribuídos. **Burmester, Magko e Chrissikopoulos, (2012)** desenvolveram uma metodologia estruturada para modelar a segurança de um sistema físico-cibernético com base no comportamento do adversário e os aspectos físicos e cibernéticos do sistema. **Dasgupta, (2007)** focou na construção de um sistema autônomo de defesa, que usa analogias do sistema imunológico para analisar e responder às ameaças e ataques. **Rejeb, Leeson e Green (2006)** propuseram um algoritmo para identificar a fonte de ataques e definir sua natureza em uma rede. Trabalhos mais recentes focaram em redes inteligentes (GAI, 2017), transferência de dados por dispositivos móveis (GAI, 2017) e transmissões usando multicanais para comunicação (GAI, 2018). Contudo, essas ferramentas têm dificuldade para medir os impactos dos ciberataques e de avaliar os investimentos em CS de uma perspectiva gerencial. Além disso, essas ferramentas têm pouca flexibilidade para se adaptar aos novos contextos digitais e de ameaças de CS.

2.10.3 Modelo baseado na análise de retornos financeira

Uma segunda abordagem, busca avaliar os retornos financeiros provenientes de investimentos nos setores de CS – avaliando indicadores quantitativos financeiros. **Bojanc, Jerman-Blažič e Tekavčič (2012)** buscaram uma abordagem da perspectiva financeira que levava em conta o ROIC[20], valor presente líquido (VPL) e IRR[21] para quantificar os custos e os benefícios de investimentos em segurança. Antes disso, **Bojanc e Jerman-Blažič (2008)** apresentaram um modelo matemático para otimizar os investimentos em segurança da tecnologia baseado em um método de tomada de decisão, que levava em conta os riscos de

[20] ROIC – Return on Invested: Retorno sobre o capital
[21] IRR – Internal Rate of Return

segurança e uma avaliação dos ativos digitais. **Chai, Kim e Rao (2011)** examinaram o valor de um investimento na segurança da tecnologia da informação (TI) com base na reação sobre anúncios de investimentos CS de analistas de ações do mercado financeiro. Essas metodologias têm diversas limitações, como a falta de estudos aprofundados mensurando as perdas financeiras decorrentes de ataques cibernéticos. Como **Patal, Graham e Ralston (2008)** afirmaram, avaliar as perdas financeiras de uma falha de segurança digital dificulta ainda mais o desafiador processo de avaliação e mensuração dos riscos da companhia.

2.10.4 Modelo baseado em redução do risco cibernético

Uma outra abordagem para a estruturação da cibersegurança em uma empresa é buscar a redução do risco cibernético global da companhia. Dessa forma, as atividades que estão sendo realizadas vão sempre estar alinhadas com o a estratégia de risco da companhia e os seus objetivos estratégicos. Dando importância para as diretrizes que foram definidas, a priorização do monitoramento e do desenvolvimento de camadas de proteção, a criação de indicadores de performance chave (KPI[22]) e de indicadores do risco de cibersegurança (KRI[23]).

Esse modelo dá visibilidade e controle sobre o desenvolvimento do cenário de cibersegurança da companhia (MCKINSEY, 2019). Um exemplo clássico da importância dessa estratégia é optar pelo investimento em treinamento e conscientização dos funcionários a respeito de boas práticas de cibersegurança ao invés de adicionar mais camadas de segurança que tornam o dia a dia do empregado mais engessado e não necessariamente adiciona segurança ao sistema. Vale lembrar que para o contexto de segurança cibernética o nível de segurança de uma empresa é diretamente relacionado ao seu elo mais fraco, que muitas vezes é o humano. (RAHMAN, ROHAN, *et al.*, 2021).

A ideia de identificação e avalição das principais ameaças, antes de um eventual investimento em tecnologia e processos de CS, é algo sugerido que foi sugerido por **Cowley, Greitzer e Woods (2015).** Isto porque são necessárias métricas de risco para saber como priorizar despesas em um orçamento limitado. De qualquer forma, são poucas as

[22] KPI – Key Performance Indicators
[23] KRI – Key Risk Indicators

metodologias quantitativas de avaliar riscos cibernéticos, quando comparamos com as qualitativas (PATEL, 2008).

Uma outra metodologia proposta é a utilização da teoria de Fuzzy e da Árvores de Análise de Falhas (Fault Tree Analysis, FTA), que busca ajudar tanto no mapeamento das ameaças cibernéticas e os seus principais riscos frente aos processos da companhia, como também ajudar a priorizar qual das frentes desenvolver primeiro com base na probabilidade de ocorrência, no grau do impacto financeiro e no tempo para a recuperação das atividades. (GUSMAO, SILVA, *et al.*, 2018)

Também de acordo com **Patel (2008)**, modelos qualitativos de avaliação do risco cibernético são utilizados em situações em que a avaliação de risco é simples e os cálculos, impossíveis ou desnecessários. Esse era o cenário para PMEs até poucos anos atrás, mas com a digitalização, uma priorização com um embasamento quantitativo se tornou importante (VAN HAASTRECHT, G., *et al.*, 2021). A avalição quantitativa envolve instrumentos matemáticos para avaliar o risco como a teoria de Fuzzy, Árvores de Análise de Falhas (Fault Tree Analysis, FTA), e avaliação multicritérios (PATEL, 2008).

A literatura se refere aos métodos quantitativos de avaliação de risco sempre tendo como uma de suas bases a ideia de uma avalição de risco probabilística (*PRA, probabilistic risk assessment*) que consiste em uma maneira sistemática de avaliar os riscos associados a aquela entidade (RALSTON, 2007). O PRA pode utilizar diferentes métodos. Um deles é justamente o FTA que tem como objetivo determinar as causas de um evento indesejado. Para tal, faz-se o caminho inverso: primeiro mapeia-se os eventos a serem evitados e segue-se a sequência de situações que podem levar a aquele evento. Há outros métodos que fazem justamente o caminho oposto, iniciando-se dos eventos e mapeando as consequências de tal evento.

Shin, Son, Khalil ur e Heo (2015) propuseram um modelo avalição de risco de CS baseado em estatística Bayesiana que permitia avaliar a parte processual e técnica de diversos aspectos da CS. **Jaganathan, Cheruveettl, e Silvashanumugam (2015)** propuseram um modelo matemático para prever o impacto da cibersegurança baseado no número de vulnerabilidades de segurança da informação dado o ambiente, o setor de atuação da companhia e as informações necessárias para o funcionamento dos processos. **Silva, de Gusmão, Poleto, Silva, e Costa (2014)** propuseram uma análise multidimensional que

utilizar a teoria de Fuzzy e Análise de modo e efeito de falha (FMEA, *Faliure Mode and Effect Analysis*) para gestão da segurança da informação. Na mesma linha desse estudo, **Silva, Poleto, Camara, Henriques, e Cabral (2016)** propuseram uma análise de risco baseada em uma perspectiva multidimensional que integra análises de *Big Data* com FMEA (Análise de modo e efeito de falha) e com a GRA (*grey relational analysis*[24]). **Kawanaka, Matsumaru, e Rokugawa (2014)** apresentaram um método para quantificar o risco de ciberataques em sistemas de controle de produção que provém de riscos de software expressando os impactos causados em unidades monetárias. Propostas relevantes de métodos dinâmicos para a tomada de decisão sobre o acesso a informações do sistema de saúde foram feitas por **Shaikh, Adi e Logripppo (2012)**. **Zhango, Ho, e He (2009)** apresentaram uma solução que mede os impactos de ataques nos sistemas de segurança, usando uma análise que leva como base os custos-benefícios e as respostas naturais de mercado.

Um ponto que vale ser ressaltado é que todos os estudos explorados para mapeamento e análise dos riscos cibernéticos de cada instituição envolvem dois atores, que podem ser a mesma pessoa: (i) um expert em segurança da informação que seja capaz de avaliar, mesmo que subjetivamente, os riscos e ameaças a que uma empresa de tal setor está exposta; e/ou (ii) uma pessoa que conheça as atividades e os principais processos da instituição. Com os dois, é possível ter um mapeamento (i) dos processos críticos da companhia, (ii) das eventuais ameaças a que ela está exposta e (iii) às possíveis lacunas de segurança da informação (seja em processos, software ou hardware).

2.11 Modelos em atuação em empresas médias

No contexto das empresas médias do Brasil, a priorização de investimentos de CS é feita de maneira pouco estruturada. O que ocorre em muitas empresas é a utilização parcial de alguns dos métodos de mapeamento de processos para um melhor entendimento da superfície digital. Esse mapeamento, mais conhecido como o processo de *Discovery*, é um serviço oferecido por muitas empresas de software de automação do setor. O resultado deste processo é um mapa de interações de todos os processos e interações da companhia (SERVICENOW, 2022).

[24] GRA: *grey relational analysis*[24], que é um dos modelos dentro da *grey system theory* que define situações sem nenhuma informação como pretas e com informações perfeitas como brancas. Contudo, em situações do mundo real, as informações e o acesso a elas são imperfeitos, sendo denominadas cinzas, difusas, nebulosas. GRA atua na modelagem dessas situações.

O mapa de processos gerado é bastante extensivo e detalhado, e não está associado a uma grande despesa. O que falta, no entanto, é a análise crítica desta cadeia, fazendo uma ponte para o contexto de CS. De forma que, a priorização de investimentos nesse setor fica muito associada aos processos operacionais principais das companhias (ZEIJLEMAKER, 2022).

Outro recurso utilizado para tomada de decisão são os propostos por **Bojanc, Jerman-Blažič e Tekavčič (2012)** de análise com perspectiva financeira que leva em conta o ROIC, valor presente líquido (VPL) e IRR para quantificar os custos e os benefícios de investimentos em segurança. De qualquer forma, o processo de mapeamento da cadeia e o de análise financeira dos investimentos são desconectados em grande parte das empresas brasileiras.

Assim, o ponto que muitas vezes direciona a priorização de investimentos em CS é o orçamento da companhia destinado a essa frente. Valor que pode estar descasado com a necessidade de segurança de um ponto de vista estratégico da companhia.

Em suma, o tomador de decisão está munido do (i) mapeamento, (ii) análise financeira dos investimentos, (iii) orçamento destinado a CS, e (iv) contexto setorial em que a empresa atua. Assim, a priorização está muito atrelada à experiência do profissional encarregado (CISO, CIO, CTO) que analisa essas informações e determina a estratégia de priorização de CS da companhia.

2.12 Modelos em atuação em empresas pequenas

Outra realidade mais direcionada a companhias menores são soluções que buscam dar uma proteção superficial e global para instituições de caráter mais simples. Estas soluções oferecem uma solução satisfatória para o grau de exposição da companhia e o nível de risco que ela está disposta a tomar. De forma que não faz sentido uma análise mais aprofundada dos riscos de CS. Contudo, essas companhias não fazem parte do escopo principal deste trabalho.

2.13 Métodos de avaliação

Os modelos descritos são um conjunto de diferentes ferramentas e métodos que ajudam em diferentes etapas do processo estruturado de priorização. A seguir, discorre-se sobre as principais características dos principais métodos e se justifica a escolha de um modelo conjunto do FTA com teoria de Fuzzy para o contexto de empresas médias em crescimento.

2.13.1 Síntese dos principais métodos

Dentre os modelos e seus respectivos métodos, há diferentes características que os tornam mais orientados para um nicho específico de instituição. O modelo descrito por **Shin, Son, Khalil ur e Heo (2015)** que propõe a utilização de estatística bayesiana tem uma característica bastante técnica, dificultando a adoção e o entendimento do seu funcionamento para muitas companhias.

O modelo estruturado por **Jaganathan, Cheruveettl, e Silvashanumugam (2015)** que descreve um método matemático para prever o impacto da cibersegurança baseado no (i) número de vulnerabilidades de segurança da informação detectadas no ambiente da companhia, (ii) o setor de atuação da companhia e (iii) quão sensíveis são as informações necessárias para o funcionamento dos processos, tem uma dificuldade grande em lidar com a subjetividade de cada um desses valores e exige um robusto monitoramento dos processos da companhia. Estas características o tornam mais orientados a companhias mais maduras e com mais controle dos processos.

A priorização com base puramente no método proposto por **Bojanc, Jerman-Blažič e Tekavčič (2012)** que visa analisar da perspectiva financeira indicadores para quantificar os custos e os benefícios de investimentos em segurança é algo que é utilizado por algumas empresas. Mas sua atuação é muito direcionada para o mérito financeiro, falhando em fazer uma ponte com a estratégia e as lacunas atuais da companhia.

Os métodos propostos por **Kawanaka, Matsumaru, e Rokugawa (2014)**, **Shaikh, Adi e Logripppo (2012)**, são direcionados para indústrias específicas: sistemas de controle de produção e indústria de saúde, respectivamente. De forma que, fogem do escopo deste trabalho.

Há também propostas que utilizam a Análise de modo e efeito de falha (FMEA[25]) que tem como principal ideia mapear a cadeia de eventos que levaram a uma falha específica. Iniciando a partir das falhas, mapeia-se as consequências de tal evento (falha de sistema). Por esta característica, ela é mais indicada para a utilização retroativa após um evento/falha. Isto é, tem um caráter mais reativo, no lugar de uma medida preventiva, idealmente aplicada durante respostas a incidentes para análise forense após ou durante um ataque-cibernético (SILVA, 2016).

2.13.2 Escolha do método a ser proposto

De todos esses modelos que já foram propostos, o proposto por **Gusmão, Silva, Silva, Poleto, e Costa (2018)** que utiliza FTA e teoria Fuzzy para fazer a avaliação de CS da companhia apresenta algumas características interessantes para endereçar os problemas de médias empresas. A primeira é a capacidade de identificar relações de causalidades entre eventos utilizando o FTA. A segunda é criação de uma ponte estruturada entre a análise qualitativa (FTA) e quantitativa por meio de ferramentas da teoria de Fuzzy, considerando não só custo financeiro, como também o tempo de restauração das atividades. Em suma, o uso do FTA possibilita o mapeamento das causas que levam a falhas de segurança, enquanto a análise utilizando a teoria de Fuzzy é capaz de lidar com as incertezas numéricas e avaliações subjetivas de experts de CS.

2.13.3 Teoria de Fuzzy

De acordo com **Zadeh (1965), 1975)** e **Pedrycz, Ekel, e Parreiras, (2011)**, a teoria de Fuzzy, ou teoria de conjunto difuso, pode ser definida como um conjunto de objetos em que o valores de adesão — que expressam o grau em que cada objeto é compatível com as características distintivas da coleção — pode assumir valores entre 0 (exclusão completa da coleção) e 1 (adesão completa à coleção). Em seguida, é descrito um conjunto difuso *C* por uma função de pertinência que mapeia os elementos de um universo *X* para o intervalo de unidade [0,1] (PEDRYCZ, 2011):

[25] FMEA: *Faliure Mode and Effect Analysis*

$$C: X -> [0, 1]$$

Um conjunto difuso também pode ser visto como um conjunto de pares ordenados da forma *{x, C(x)}* onde *x* é um elemento de *X* e *C(x)* denota seu correspondente grau de adesão.

As funções de pertinência podem ser representadas de diferentes formas. As funções de pertinência mais comuns são: triangular; trapezoidal, *T-membership*, S-*membership*, Gaussiano e exponencial. O tipo de uma função pertinência deve refletir o problema que está sendo enfrentado, a percepção do conceito representado e o nível de detalhe requerido.

A função pertinência triangular é a forma que será adotada nesse trabalho para representar a avaliação das alternativas de diferentes investimentos em CS. Este tipo de função de pertinência pode ser descrito da seguinte forma (PEDRYCZ, 2011):

$$C(x, a, m, b) = \begin{cases} 0 & if\ x \leq a \\ \frac{x-a}{m-a} & if\ x \in [a, m] \\ \frac{b-x}{b-m} & if\ x \in [m, b] \\ 0 & if\ x \geq b\ , \end{cases}$$

Onde os três parâmetros *a*, *b* e *m* representam, respectivamente, os limites inferior e superior e o valor modal do conjunto difuso. Uma razão para escolher este tipo de função é que os conjuntos de Fuzzy triangulares são o modelo mais simples possível para estabelecer graus de afiliação.

A aplicação da teoria de Fuzzy em cenários de incerteza foi abordada na literatura de várias formas. Primeiro, no mérito de estruturação do problema **Raiffa (1968)** propôs um esquema para organizar e sistematizar o processo de tomada de decisão. De acordo com este esquema, as consequências de qualquer ação não podem ser consideradas como certas, já que eventos, que não podem ser previstos, podem intervir para afetar os resultados. Estas decisões sob incerteza são necessárias em muitas situações da vida real. Com isto em mente, **Belyaev (1977)** define as etapas necessárias para a resolução de problemas de decisão sob cenários de incerteza:

- Definição do problema;
- Identificação dos estados da natureza que são mais representativos para o problema;
- Cálculo e análise preliminar de alternativas de solução;

- Cálculo da matriz de *payoff*[26];
- Análise da matriz de *payoff* e escolha de ações racionais;
- e escolha e implementação de ações.

Como vários tipos de incerteza são encontrados em problemas de sistemas complexos (EKEL, MARTINI e PALHARES, 2008), a definição de um problema não é uma tarefa fácil. Entre outras coisas, nesta etapa, o tomador de decisão deve estabelecer a forma correta de uma função de avaliação $F(Ai , \theta s)$ que estima a consequência/impacto de i diferentes ações A sob s diferentes estados θ.

Nesta função, é necessário escolher um número finito s de pontos que caracterizam suficientemente o conjunto θ dos estados. O número de estados deve ser estabelecido levando em conta as peculiaridades do problema e o poder computacional disponível. O próximo passo, análise preliminar de alternativas de solução, visa identificar as alternativas com resultados dominantes.

O cálculo da matriz de *payoff* consiste em avaliar cada ação/alternativa $Ai\ (i = 1;...;I)$ para todos os estados selecionados $\theta s\ (s = 1;...;S)$. Uma matriz de *payoff* genérica é ilustrada na tabela seguinte (EKEL, MARTINI e PALHARES, 2008):

	θ_1	…	θ_s	…	θ_S
A_1	$F(A_1, \theta_1)$	…	$F(A_1, \theta_s)$	…	$F(A_1, \theta_S)$
…	…	…	…	…	…
A_i	$F(A_k, \theta_1)$	…	$F(A_k, \theta_s)$	…	$F(A_k, \theta_S)$
…	…	…	…	…	…
A_I	$F(A_K, \theta_1)$	…	$F(A_K, \theta_s)$	…	$F(A_K, \theta_S)$

Figura 5 - Matriz de payoff. Fonte: Ekel, Martini e Palhares, 2008

A etapa de análise que envolve a matriz de *payoff* e a escolha de ações racionais é apoiada em um ou mais (quando o objetivo é comparar as recomendações) critérios propostos para condições de incerteza (os critérios de Wald, Laplace, Savage e Hurwitz). Entretanto, nenhum deles inspira confiança sincera, e nenhum critério pode ser usado para a escolha final da ação. Assim, as escolhas finais costumam ser feitas pelos tomadores de decisão, com base em sua experiência e intuição (EKEL, MARTINI e PALHARES, 2008) (BELYAEV, 1977).

[26] *Payoff*: custo-benefício

Nesse método, assim como descrito em **Ekel et al. (2008)**, utiliza-se o critério de Laplace como auxiliar na tomada de decisão, que é orientado a escolher a alternativa de solução A^L para qual a estimativa de $\bar{F}(A_i)$ seja a máxima.

$$\textbf{[1]}\ \max_{1\le i\le l} \bar{F}(A_i) = \max_{1\le l\le I} \frac{1}{S}\sum_{s=1}^{S} \bar{F}(A_i, \theta_s)$$

Na equação [1], $\bar{F}(A_i)$ é o nível médio da solução objetivo para o par de alternativa e estado de natureza. Assim, $\bar{F}(A_i)$ é estimado por **[2]**.

$$\textbf{[2]}\ \bar{F}(A_i) = \frac{1}{S}\sum_{s=1}^{S} \bar{F}(A_i, \theta_s)$$

$F(A_i)$ representa ou nível máximo da função objetivo ou o nível mínimo, de acordo com o que se busca com a função, maximização ou minimização. Assim, $F(A_i)$ pode ser estimada, respectivamente, por **[3]** e **[4]**.

$$\textbf{[3]}\ F^{max}(A_i) = \max_{1\le s\le S} \bar{F}(A_i, \theta_s)$$

$$\textbf{[4]}\ F^{min}(A_i) = \min_{1\le s\le S} \bar{F}(A_i, \theta_s)$$

Considerando que $R(A_i, \theta_s)$ é um sobre gasto que ocorre com a combinação de θ_s e da alternativa A_i, ao invés da solução ótima local para a alternativa sob o estado de natureza θ_s, o nível máximo de risco é definido por **[5]** (BELYAEV, 1977)**.**

$$\textbf{[5]}\ R^{max}(A_i) = \max_{1\le s\le S} R(A_i, \theta_s)$$

O risco apresenta uma diferença relativa dos valores das funções objetivos em relação a outra e associa um nível de perdas/danos relacionado a situação de incerteza.

Dessa forma, no lugar destes critérios a proposta é utilizar justamente a teoria de Fuzzy para auxiliar a priorização do tomador de decisão. Cada função objetiva $F_p(A)$ é substituída por uma função de pertencimento $\mu_{Cp}(A)$ para um determinado critério *p*, onde *p=1,..., q*.

Uma solução Fuzzy *D* é produzida como resultado da intersecção $D = \cap_{p=1}^{q} \mu_{Cp}$, onde $\mu_{Cp}(A_i) = \min_{1 \le p \le q} \mu_{Cp}(A_i)$ para uma solução fuzzy *D* com os conjuntos difusos do tipoC_p. A interseção leva a uma solução que prova o grau máximo:

$$\textbf{[6]}\ \max \mu_{Cp}(A_i) = \max \min_{1 \le p \le q} \mu_{Cp}(A_i, \theta_s)$$

E reduz a dificuldade de encontrar:

$$\textbf{[7]}\ A = \arg \max \min_{1 \le p \le q} \mu_{Cp}(A_i, \theta_s)$$

Para alcançar a solução de **[7]**, pode-se utilizar a condição

$$\textbf{[8]}\ \mu_{Cp}(A_i, \theta_s) = \frac{F_p(A) - \min F_p(A)}{\max F_p(A) - min F_p(A)}^{\lambda_p}$$

Para maximização da função objetivo ou

$$\textbf{[9]}\ \mu_{Cp}(A_i, \theta_s) = \frac{\max F_p(A) - F_p(A)}{\max F_p(A) - min F_p(A)}^{\lambda_p}$$

Para a minimização da função objetivo, onde λ_p são fatores de importância para a função objetivo correspondente. Finalmente, o critério de Laplace pode ser escrito de acordo com **[10].**

$$\textbf{[10]} \qquad \max_{1 \le i \le I} \mu_D(A_i) = \max_{1 \le i \le I} \frac{1}{S} \sum_{s=1}^{S} \min_{1 \le p \le q} \mu_{Cp}(A_i, \theta_s)$$

Existem outras nuances no método de aplicação da teoria de Fuzzy para problemas com graus de incerteza que podem facilitar a adoção deste modelo proposto por **Ekel (2008)**, mas não serão abordadas nesse trabalho.

Para a aplicação desse método, descrito por em **Ekel et al. (2008)**, é possível utilizar o aplicativo *Adaptitative Interactive Decision Making System (AIDMS2)* desenvolvido pelo Prof. Dr. Petr Ekel, Mateus Alberto Dorna de Oliveira e Igor Marques Reis, coautores de (W.

MAIA, EKEL, *et al.*, 2021). Ele implementa a alocação multiobjetivo de recursos baseadas em conjuntos fuzzy (ou sua escassez), conforme descrito nesta seção **(2.13.3)**. A figura a seguir demonstra a tela principal do aplicativo *AIDMS2*. Esse aplicativo pode ser utilizado em outros contextos onde seja necessária análise de alocação de recursos.

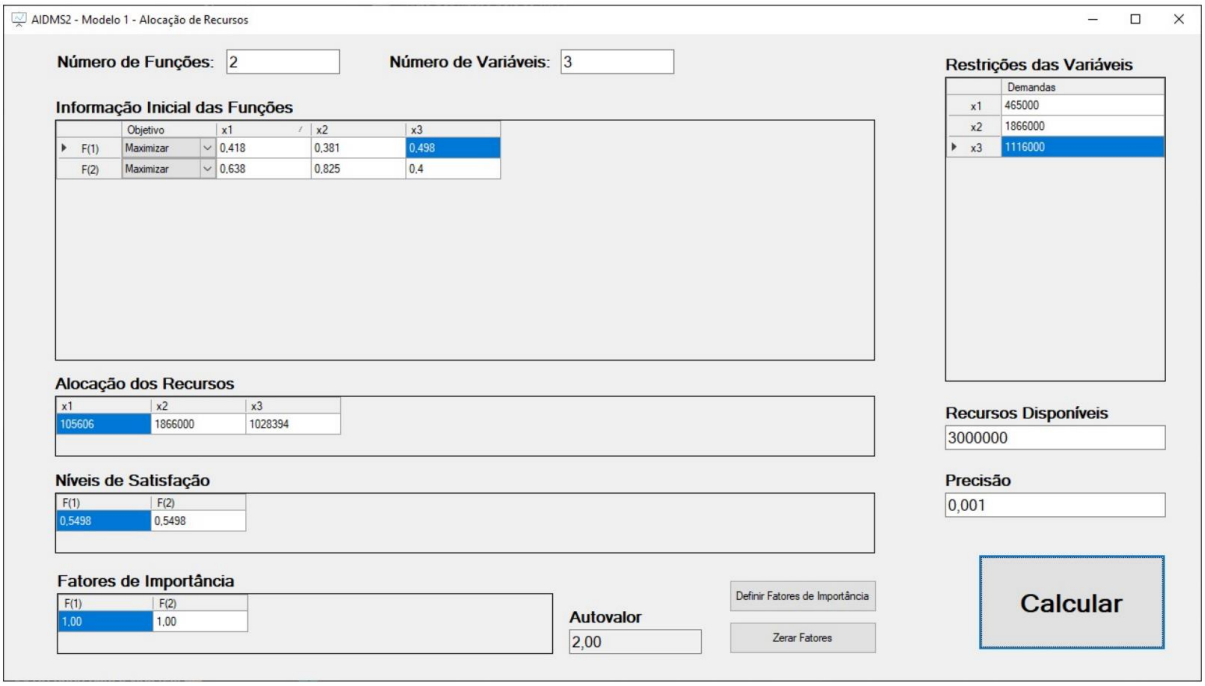

Figura 6 - Captura de tela da página principal do aplicativo AIDMS2. Fonte: (W. MAIA, EKEL, et al.*, 2021)*

2.13.4 FTA – Árvore de Análise de Falhas

Árvore de Análise de Falhas ou FTA (Fault Tree Analysis) é uma técnica para conduzir análises de segurança e confiabilidade de sistemas, usando representações gráficas para modelar cadeias causais que levam a falhas (HAUPTMANNS, 2002) (RUIJTERS, 2015). Esse método também proporciona uma visão estratégica de todo o sistema sem a necessidade de uma análise detalhada, permitindo um mapeamento mais rápido das possíveis cadeias vulneráveis em momentos de ameaça. (FERDOUS, 2009) (HAUPTMANNS, 2004).

Essa técnica já foi adotada em muitos contextos. Por exemplo: a representação da relação causal entre eventos que contribuíram para quedas fatais na indústria de construção (CHI, 2014); modelos de mensuração de confiabilidade de sistemas de energia (RAHMAN, 2013); modelos de predição de falha para redes de transmissão de óleo e gás (YUHUA, 2005); estudos de casos para otimização de inventário e redução de perda de vendas em montadoras de aviões (CHENG, 2013).

No contexto de cibersegurança, o estágio inicial do FTA é definir os possíveis eventos de falhas na CS e rastrear as influências de volta ao evento causador. A partir desse evento inicial é possível visualizar diferentes causas e níveis de profundidade de ciberataques. O intuito do FTA é encontrar o a combinação mais básica de fatores que causam o evento de falha. Ao analisar essas combinações, pode-se tomar decisões de priorização para evitar o evento originário (MAHMOOD, 2013).

3 METODOLOGIA DO TRABALHO

Neste capítulo, são apresentados os métodos de coleta e análise de dados utilizados na evidenciação das seguintes características de empresas brasileiras: estrutura de CS, modelos de priorização de CS, orçamentos e orçamentos de CS. As informações também serviram para um entendimento maior do setor de CS e das tendências desse mercado. Além disso, buscou-se mais informações a respeito da *Empresa A.*

3.1 Método de Amostragem

A principal forma de coleta de informações desse trabalho foi via entrevistas qualitativas com *players* do setor de CS que buscaram traçar uma visão mais concreta da realidade das empresas, principalmente brasileiras, quanto a essa frente de CS. Para tal, estruturou-se estas entrevistas de diferentes formas.

Os dados levantados não são meramente quantitativos, pois são compostos de impressões subjetivas de cada pessoa. Por isso, para obter esses dados, existe a necessidade de alcançar uma descrição completa de cada impressão, algo que ocorre, idealmente, por meio do diálogo, e não apenas por formulários. Isto é, vê-se a necessidade da realização de entrevistas qualitativas, nas quais existe, de fato, um diálogo entre entrevistador e entrevistado. Ou seja, esta pesquisa qualitativa em questão está alinhada com a metodologia fenomenológica sugerida por **Vieira e Boeira (2006)** em **Godoi et al. (2006).**

Como método de amostragem, a amostragem teórica (não aleatória) foi selecionada para esse trabalho, dado que o processo de escolha é pautado por razões teóricas, como revelação de um fenômeno incomum, replicação de descobertas de outros casos, replicação contrária, eliminação de explicações alternativas e elaboração da teoria emergente (EISENHARDT e GRAEBNER, 2007).

Além disso, dada a unidade de análise como o ecossistema, o método de amostragem utilizado para a seleção de respondentes e participantes das entrevistas para a pesquisa foi o método não probabilístico chamado *snowball* (ou “bola de neve”), no qual o pesquisador usa alguns casos para encorajar novos participantes a colaborar na pesquisa (TAHERDOOST, 2016). Na prática, o entrevistador pergunta aos primeiros participantes – os quais normalmente são selecionados por proximidade ou conveniência – se eles conhecem outros possíveis objetos de estudo em situação semelhante que teriam interesse em participar da mesma pesquisa. De maneira geral, a amostragem *snowball* continua até a saturação de dados

- momento no processo de pesquisa no qual novas amostras geram redundância de dados, sem incluir nenhuma informação nova à pesquisa (NADERIFAR, GOLI e GHALJAIE, 2017).

No contexto do presente estudo, para viabilizar a aplicação deste método de amostragem, foi incluído um item no roteiro das entrevistas exclusivamente para pedir aos respondentes informações de contato de players mais próximos que poderiam agregar mais informações ao mapeamento esboçado em conjunto. Vale o adendo de que, dado o período limitado disponível para a realização das entrevistas, não se chegou à saturação de dados, assim como recomendado para o método de amostragem do *snowball*. De qualquer forma, mesmo não sendo um estudo exaustivo de todo o cenário, entende-se que o presente trabalho serve como uma exploração inicial da abordagem proposta.

Utilizou-se como alavancas para chegar a esses *players* da cadeia: a rede de professores da Escola Politécnica da USP, que está repleta de especialistas da área; os contatos que provém do estágio no fundo de *venture capital/private equity*, que são empreendedores de múltiplas empresas, CTO[27]s, CIO[28]s, CISO[29]s e analistas de outros fundos; e, por fim, o acesso à *Empresa A*, sempre mantendo discrição sobre as informações confidenciais dessa companhia.

O perfil dos *players* entrevistados a respeito de "tipo de *player*" que é o escopo de atuação e "Descrição" que são as suas características é descrito na tabela a seguir:

[27] CTO: *Chief Tecnology Officer*, chefe de tecnologia da companhia
[28] CIO: *Chief Information Officer*, chefe de gestão da informação da companhia
[29] CISO: *Chief Information Security Officer*, chefe de segurança da informação da companhia.

Tabela 2 - Perfil dos players entrevistados. Fonte: Elaboração própria do autor

Sigla	Tipo de *player*	Descrição
E1	*Empresa A* - CIO de *Fintech* de soluções financeiras *(múltiplas interações)*	**Porte**: médio, 100 funcionários, BRL 50 milhões de faturamento anual **Público-alvo**: empresas de todos os portes
E2	CISO de um Banco Brasileiro	**Porte**: médio, 200 funcionários, Patrimônio Líquido de BRL 2 bilhões **Público-alvo**: empresas de todos os portes
E3	CEO, CIO, CFO de empresa de software de CS *(múltiplas interações)*	**Porte**: médio, 200 funcionários, BRL 50 milhões de faturamento anual **Público-alvo**: empresas de grande porte
E4	CISO e equipe de CS de grande varejista de vestuário *(múltiplas interações)*	**Porte**: grande, + 10 mil funcionários, BRL 7,5 bilhões de faturamento anual **Público-alvo**: empresas de grande porte
F1	Fundo de *Venture Capital* atuante no setor de CS. Também possui outras frentes.	**Porte**: grande, BRL +60 bilhões de ativos sob gestão **Público-alvo**: Private equity, Venture Capital, Previdência, Fundo imobiliário
P1	Professor da EPUSP Marcos Barreto.	Pesquisador e consultor de empresas na frente de CS.
E5	CISO de *Fintech* de soluções financeiras	**Porte**: média, 300 funcionários, BRL 200 milhões de faturamento anual **Público-alvo**: empresas de todos os portes
F2	Fundo de *Venture Capital* atuante no setor de CS.	**Porte**: média, BRL 1 bilhão de ativos sob gestão **Público-alvo**: Private equity, Venture Capital
E6	CISO de um Banco Brasileiro	**Porte**: grande, 4200 funcionários, Patrimônio Líquido de BRL 1,1 bilhão **Público-alvo**: pessoas físicas
E7	CISO de uma *startup* marketplace multimarcas	**Porte**: grande, 800 funcionários, BRL 300 milhões **Público-alvo**: pessoas físicas
E8	CISO de uma cadeia de supermercados internacional	**Porte**: grande, + 72 mil funcionários, BRL 100 bilhões (operação Brasil) **Público-alvo**: pessoas físicas

Sigla	Tipo de player	Descrição
E9	CEO empresa de software de CS	**Porte**: pequena, 100 funcionários, BRL 10 milhões de faturamento anual **Público-alvo**: empresas de grande porte
E10	Conselheiro administrativo de empresa de CS Brasileira	**Porte**: grande, 450 funcionários, BRL 200 milhões de faturamento anual **Público-alvo**: empresas de grande porte
E11	CISO de uma empresa de *telecom* internacional	**Porte**: grande, + 100 mil funcionários, BRL 40 bilhões (operação Brasil) **Público-alvo**: pessoas físicas
E12	CEO de empresa de software de CS Brasileira	**Porte**: pequena, 30 funcionários, BRL 20 milhões de faturamento anual **Público-alvo**: empresas de grande porte

Além dessas entrevistas qualitativas, também foram usadas entrevistas com 52 fundadores de empresas brasileiras e internacionais como base para o conhecimento geral do setor de *startups*. As indústrias de atuação dessas companhias são: serviços financeiros, cadeia de suprimentos, cadeia logística, agroindústria, seguros e consumo (varejo e *marketplace* de produtos). Essas entrevistas foram realizadas no período contido entre fevereiro de 2022 até outubro de 2022 e são provenientes da atuação como analista de investimentos para a gestora onde o autor realizou estágio. Em relação ao porte das companhias são predominantemente pequenas e médias, salvo algumas exceções. Estas entrevistas auxiliaram no entendimento maturidade estrutural das operações, da governança e da indústria de cada uma das companhias.

3.2 Coleta de dados

A coleta de dados se baseou em três principais fontes além da literatura acadêmica do tema:

1. Entrevistas qualitativas semiestruturadas com players do setor;
2. Serviço de *Due digiligence*[30] para investir em uma empresa de CS brasileira, seguindo o molde descrito por **CFI Teams (2022)**;

[30] *Due Diligence:* no setor de investimentos se refere a uma auditoria aprofundada da empresa, mercado e documentação para assegura-se, previamente ao investimento, que as informações fornecidas pela companhia são autenticas.

3 Estudos de mercado desenvolvidos por empresas e consultorias do setor (MCKINSEY, 2019) (BERKMAN, JONA, *et al.*, 2018) (MCKINSEY & COMPANY, 2022) (PERSISTENCE, 2021).

Considerou-se que, para o problema em questão e o público delimitado, o método mais adequado para a realização das entrevistas seria o de "entrevistas semiestruturadas" segundo **Boni & Quaresma (2005)**, ou "entrevistas baseadas em roteiros", de **Godoi & Mattos (2006)**.

De acordo com **Selltiz et al. (1987)**, a entrevista semiestruturada tem uma vantagem sobre as outras formas de realização de entrevista, visto que as pessoas entrevistadas se sentem mais à vontade para expor suas opiniões a cerca de um assunto. Enquanto métodos estruturados não permitem essa abertura. Também, realizar a entrevista por meio do diálogo permite maior interação do que entrevistas por escrito, devido às maiores interações entre os indivíduos (e dando maior liberdade ao entrevistado para que este possa trazer questões inesperadas para o entrevistador, gerando ideias de grande contribuição para o trabalho).

Esse método é interessante pela posição assumida pelo entrevistador, bem como pela forma de realizar as perguntas: ao realizar esse tipo de pesquisa, o entrevistador se posiciona como alguém que conhece um pouco do meio do entrevistado (por meio de pesquisas prévias), garantindo maior empatia do entrevistado e permitindo que ele compartilhe impressões pessoais e informações mais privadas, alinhadas com a proposta da pesquisa devido ao seguimento de um roteiro. O roteiro acaba servindo mais como macro tópicos a serem abordados, sem a necessidade de uma linearidade do discurso, podendo alterar a ordem cronológica das questões e a forma de realizá-las, bem como trazer novas questões para cada entrevista, se for oportuno.

No começo de cada entrevista, o entrevistador informou o tema de CS e as intenções da entrevista, bem como uma noção geral sobre o tema da estruturação da CS em empresas. Garantiu também anonimato das informações cedidas (no caso, nome do entrevistado e de outras pessoas citadas, e nome das organizações envolvidas); deixou claro que o entrevistador poderia não responder alguma pergunta se não se sentisse à vontade; perguntou se tinha alguma questão que não havia ficado clara; e, em seguida, iniciou-se o bate papo de caráter informal, mas com direcionamento do roteiro.

Em meio a entrevista, tomou-se notas das principais questões levantadas e, ao final, passou-se a limpo a fim de consolidar e estruturar as informações.

Quanto ao serviço de *Due Digiligence*, este foi realizado por uma empresa de auditoria terceira e permitiu um entendimento minuciosos não só do operacional da empresa de CS em questão, mas também uma maior abertura a sua rede de clientes. Dessa maior abertura, obteve-se acesso a dados como orçamentos de CS de cada companhia e modelos de priorização utilizados por alguns clientes.

Já o acesso a estudos de mercado feitos por empresas de consultoria foi possível através dos contatos da gestora de investimentos do estágio do autor. Estes estudos feitos por empresas de consultoria e por empresas especializadas no setor de CS e tem um alto custo. De forma que seria impraticável obtê-los de maneira não institucional e com viés econômico. Os dados desses estudos também foram selecionados e estruturados para guiar este trabalho.

3.3 Análise de dados

Como comentado anteriormente, todos os resultados das entrevistas qualitativas, da *Due Digiligence*, e das pesquisas de mercado foram anotados, estruturados e, em seguida, analisados buscando vieses, entendimentos e fatos sobre os seguintes pontos:

- Tendências do mercado de CS para empresas
- Características gerais da companhia *(quando aplicável)*: porte, segmento, estratégia, posicionamento etc.
- Como a CS é estruturada atualmente nessa instituição? *(quando aplicável)*
- Como é decidido o que priorizar em CS/modelos de priorização? Quem decide? *(quando aplicável)*
- Dimensão do orçamento para CS *(quando aplicável)*
- Principais lacunas da instituição *(quando aplicável)*

Além dessas questões, foi possível se aprofundar mais na *Empresa A*, a qual se teve mais abertura justamente por se tratar de uma das empresas do portfólio administrado de investidas da gestora. Assim, realizaram-se reuniões mensais do conselho administrativo da companhia para os méritos operacionais e 3 entrevistas com o CIO da companhia com foco na estratégia de priorização de CS. Dessas entrevistas foi possível extrair informações como:

- Alocação detalhada do time de CS;
- Falhas passadas de CS e suas causas;

- Impactos causados por ciberataques no passado;
- Principais prioridades de CS atuais;

3.4 Próximos capítulos

Após a coleta de dados e a sua estruturação, realizou-se uma análise crítica a respeito de que modelo de priorização de CS se encaixaria melhor no contexto da *Empresa A.* Essa discussão de resultados e a proposta de novo modelo está descrita no capítulo 4 deste trabalho, Resultados e Discussão.

4 RESULTADOS E DISCUSSÕES

Nesta parte do trabalho são expostos os principais resultados obtidos através da aplicação da metodologia que engloba, principalmente, pontos levantados durante as entrevistas e conhecimentos obtidos através de estudos de mercado. Em seguida, discorre-se a respeito das características levantadas sobre empresas médias e sobre o mercado de CS, e como isso se relaciona com o modelo de priorização de CS a ser proposto pelo autor.

Como as informações coletadas nas entrevistas têm caráter sensível, os resultados serão descritos de maneira geral e não fazendo referência a uma instituição específica.

4.1 Resultados obtidos

Através das entrevistas e dos estudos de mercado, uma questão se destacou: ainda há muita desinformação e despreparo por parte das empresas na sua frente de CS. Muitos dos tomadores de decisão alcançam esse posto por uma escassez generalizada de mão de obra especializada em CS. Dessa forma, sem preparo especializado e sem uma especialização no meio de segurança da informação, essas pessoas acabam desenvolvendo seus conhecimentos conforme vão desempenhando as funções como tomador de decisões.

Além desse ponto, outras questões que se destacaram durante a coleta de dados foram:

- O orçamento disponível para desenvolver a frente de CS: contrastando o presente e passado
- Estruturação de CS da companhia
- Como são as tomadas as decisões de priorização de investimentos de CS da companhia
- Método de escolha de provedores de soluções de CS

Orçamento

Iniciando pelo orçamento destinado à estruturação da CS da companhia, este é um reflexo direto do quão central é a questão da CS para o modelo negócio da companhia. Essa importância está diretamente relacionada a uma série de fatores. Isto é, quanto:

(i) maior a quantidade de dados sensíveis presentes no banco de dados da companhia;

(ii) maior o número de clientes, funcionários e provedores;

(iii) maior a intensidade de troca de informações entre diferentes setores e *players* da cadeia de valor;

(iv) mais regulado a indústria de atuação;

(v) maior o porte da companhia;

mais central é a CS para o funcionamento saudável e seguro das operações de uma empresa e isso está refletido no orçamento.

O orçamento de CS das companhias é destinado principalmente para três frentes. A primeira é orçamento para compor o time de CS. A segunda está destinada à compra de soluções de CS (softwares ou consultorias/serviços terceiros), que serve como ferramental para prevenir, operar e monitorar o dia a dia com segurança. A terceira é a criação de um fundo para lidar com casos de emergência/urgência que possam surgir. Este último geralmente só está presente em empresas bastante maduras, com "fartura" de orçamento e que buscam dar autonomia para o time de CS. Garantindo agilidade e eficiência na hora de lidar com um problema.

A coleta de dados expôs um incremento significativo dos recursos destinados para cibersegurança nos últimos 3 anos, tendo um ponto de inflexão claro na realidade das companhias com a pandemia do COVID-19. Naquele momento, as empresas de grande porte que já tinham um setor de CS estruturado, tornaram essa frente ainda mais robusta com o aumento dos funcionários destinados unicamente para essas iniciativas dentro da companhia. Ampliou-se também os limites de orçamento relacionados a compra de soluções de CS. Esse aumento está diretamente associado ao aumento da percepção de valor dos investimentos preventivos em cibersegurança em meio a um aumento do nível de ameaça cibernética e da incidência de ataques bem-sucedidos.

Um exemplo dessa reestruturação pós pandemia pôde ser observado na empresa E4 que, de 2019 para 2022, duplicou o orçamento de CS e se reestruturou em 7 diferentes grupos de competência para cobrir diferentes flancos da CS. Estes são, em grandes linhas: (i) governança, (ii) operação cibernética, (iii) projetos, soluções e inovações, (iv) inteligência cibernética, (v) c*ompliance*, (vi) auditoria, e (v) fraude, que muitas vezes é considerado um ramo a parte da CS.

Essa mudança no orçamento fica tangível na seguinte frase:

"Imagine que antigamente destinavam-se milhões de reais do orçamento de um banco para a proteção dos bens físicos na forma de seguranças, carros fortes, vidros à prova de bala, monitoramento. Esse orçamento segue relevante, mas o ativo mais precioso de uma

companhia agora não é físico, e sim digital. De forma que, o orçamento de segurança cibernética ultrapassou o da segurança convencional." — CIO do banco E2.

Já no caso de empresas de pequeno e médio porte a frente de CS foi estruturada do zero ou teve um incremento no tamanho do time e dos recursos destinados a essa frente bastante considerável. Das entrevistas feitas, o aumento do orçamento nessa frente foi na ordem de 3 a 5 vezes o que era gasto no período pré-pandemia.

"Não se investia em CS no Brasil há 3 anos atrás." — interação com a empresa E5.

Estrutura

Muito da estrutura de CS encontrada nas empresas hoje é nova, imatura. Isto é, passou por uma restruturação total ou quase total nos últimos anos. Esse foi o caso de todas as empresas entrevistadas. De maneira geral, os resultados apontam diferentes cenários para empresas grandes e médias/pequenas.

As grandes, que já possuíam processos de CS bem definidos, tiveram uma expansão da capilaridade e aprofundamento das medidas de controle dos processos. Isso fica claro com o aumento no número de times mais nichados de CS e aumento do número de pessoas nos times, dobrando, na média. Isso fica bem claro no modelo de reestruturação de E4, passando de 3 times de CS para 7 nos últimos 3 anos.

No caso de empresas médias, os processos de CS tiveram que ser basicamente criados do zero. Saindo de nenhuma relevância no conselho, para uma pauta de prioridade crítica no dia a dia das companhias. Disso os times aumentaram muito, triplicando juntamente com o orçamento, quando comparados com o período pré-COVID 19. Vale ressaltar que uma parte dessa mudança está associada ao crescimento das operações da companhia, mas mesmo em empresas que não houve grande crescimento, houve uma priorização da CS frente outras áreas. Tendência clara no portfólio de companhias do fundo de investimentos do autor, no F1 e no F2 que foram entrevistados.

Empresas que ainda não conseguiram uma estrutura própria que suporte 100% das operações de CS optam, em sua maioria, por serviços de terceiros, os MSSPs[31], para cobrir alguma lacuna ou função capital da integridade da segurança. Grandes empresas fazem esse movimento para garantir proteção de diversos flancos não internalizados.

[31] *MSSP*: *Managed Security Services Providers*, são empresas que proveem serviços gerenciados de segurança para outras empresas, através de um SOC – *Security Operations Center*

Outro ponto é que, em algumas empresas brasileiras, há uma falta de sofisticação de arquitetura digital anterior à questão da CS, que é a migração de aplicações e servidores para a nuvem. Esta, mesmo mais exposta, tem camadas de proteção mais robustas fornecidas pelo *host* daquele sistema em nuvem. Ao operar preponderantemente em sistemas *on-premise* há uma dificuldade constante em se manter atualizado frente às novas ameaças cibernéticas. Dessa forma, muitas empresas brasileiras ainda precisam superar essa barreira tecnológica antes de ter acesso às ferramentas de última geração de segurança da informação.

Das entrevistas, observa-se que empresas médias operam com uma equipe de 3 a 20 empregados destinados unicamente para a CS. Esse número chega a mais de 50 em grandes companhias, como foi exposto nas entrevistas de E6, E7, E8 e E10.

Priorização

Mesmo com esse incremento repentino de orçamento, ainda não há espaço para cobrir todas as lacunas de segurança que as empresas gostariam/necessitam. Obrigando-as a pensar nas principais lacunas estruturais da companhia e como priorizá-las. Como levantado por uma das empresas médias: "(O CISO) Estou devendo um curso de boas práticas para toda a equipe, mas não vai caber no orçamento desse ano. Vai ter que ficar para o próximo". Essa é uma ideia recorrente entre as entrevistas.

A restrição de capital tem feito com que empresas deixem de buscar certificações como a ISO27001, que, de acordo com os entrevistados, serve muito mais como um selo de cuidados mínimos do que como garantia de segurança. Muito em decorrência da rápida mudança do cenário de ameaças, de forma que as normas têm dificuldade de acompanhar essas mutações. Essas características associadas a um preço elevado para obter uma certificação de duração de 6-12 meses faz com que muitas empresas pretiram tais certificações.

As entrevistas também expuseram a realidade a qual essas instituições estão expostas, onde os ataques cibernéticos se manifestam de todas as formas diariamente, sendo milhares de tentativas de intrusões em alguns casos seja por *Brute Force*[32], por *phising* ou por outro método.

[32] *Brute Force:* Em criptografia, um ataque de força bruta, ou busca exaustiva de chave, é um ataque criptoanalítico que pode, em teoria, ser usado contra quaisquer dados criptografados

Um temor comum de diversos dos entrevistados, senão de todos é o *ransomware*. Este sequestro de sistema trava completamente as operações dos serviços comprometidos e obriga a companhia a lidar com os *hackers*, sequestradores digitais, e, muitas vezes optar por pagar o resgate em *criptomoedas* não rastreáveis para obter acesso outra vez aos sistemas.

Esse temor, muito claro durante as entrevistas, torna o processo decisório de priorização muitas vezes míope, emocional para as reais probabilidades dessa falha ocorrer frente outros ataques.

Sobre os modelos de priorização observados nas companhias, foi possível observar três formas distintas de acordo com a maturidade da empresa.

Em grandes empresas com uma CS já mais estruturada e com acesso a um orçamento, o modelo de priorização estratégica é feito junto de uma consultoria de CS. Essa consultoria realiza o mapeamento da estrutura atual da companhia utilizando métodos próprios e ferramentas de *Discovery*. Em seguida pondera o possível impacto financeiro de cada uma das ameaças cibernéticas com um método similar ao proposto por **Bojanc, Jerman-Blažič e Tekavčič (2012)**. Por fim, a consultoria expõe o plano estratégico de priorização para o conselho de segurança da companhia, que na maioria das vezes o aprova sem grandes intervenções. Vale destacar que, nesse modelo, a própria consultoria é uma forte orquestradora da implementação do plano de CS, atuando como um MSSP e articulando a compra e operação das soluções que foram determinadas. Assim, parte das funções de CS mais relacionadas a infraestrutura de software e operação fica nas mãos da própria companhia, enquanto funções de monitoramento, risco externo e resposta a ameaças fica sob o guarda-chuva da consultoria.

Empresas pequenas são o outro extremo. Não tendo acesso a um orçamento suficiente para a criação e execução um plano estratégico extensivo, operam de acordo com as questões que mais lhe doem no momento. Como em muitos casos, estão em plena expansão essas dores estão ligadas ao aumento da exposição da marca e da capacidade operacional. O tomador de decisão não dispõe de ferramentas para realizar o *Discovery* da infraestrutura de tecnologia da empresa, realizando essa etapa junto dos engenheiros de software que mais conhecerem das operações. Por fim, as maiores lacunas são visualizadas e sua priorização vem muito em linha com referências externas de o que outros CIOs e CISOs de diferentes companhias têm feito e qual método de intrusão (*phising, brute force, Worms*) está mais disseminado no momento. Em suma, não há grande estruturação e embasamento para a tomada de decisão de qual frente priorizar. Muitos optam por soluções que oferecem um pacote básico de proteção global, dispensando análise de priorização. Essas informações

proveram, principalmente, das interações com a empresa E12, E10 e E3 que fornecem soluções de CS para empresas de diferentes portes.

Já empresas médias, operam de uma maneira um pouco diferente. Elas possuem orçamento para ter uma equipe de CS dedicada e têm acesso a ferramentas mais simples de *Discovery*, assim como técnicas de mapeamento de ativos digitais. Esse mapeamento, entretanto, tem muito mais uma função operacional, para ser capaz de diagnosticar e otimizar serviços e processos, do que um enfoque em CS, para ressaltar processos vulneráveis e passíveis de intrusões ou vazamentos. De forma que servem com base, mas não são exaustivos. Já na análise quantitativa de possíveis riscos e impactos, o cenário das companhias de médio porte varia consideravelmente, na qual algumas até buscam avaliar o risco/retorno de cada uma das opções, como proposto por **Bojanc, Jerman-Blažič e Tekavčič (2012)**, mas há muitas que tomam a decisão unicamente baseada em critérios qualitativos. Essas informações provêm das entrevistas com as empresas E1, E2, E3, E5 e E10 que expuseram os modelos que já foram empregados em suas companhias. Em suma, o tomador de decisão está munido do (i) mapeamento, (ii) análise financeira dos investimentos (em alguns casos), (iii) orçamento destinado a CS, e (iv) contexto setorial em que a empresa atua. Assim, a priorização está muito atrelada à experiência do profissional encarregado (CISO, CIO, CTO) que analisa essas informações e determina a estratégia de priorização de CS da companhia e tem espaço para ser influenciada por questões externas (lado emocional humano).

Escolha de solução

Algumas tendências puderam ser observadas quanto a escolha da solução e do provedor da solução a serem utilizados por uma companhia. Primeiramente a respeito do porte do provedor e robustez da solução, este é um fator diretamente relacionado com a importância daquela frente e da maturidade do domínio de CS. Tal direcionamento evidencia-se no apontamento da empresa E4:

"Para domínios da CS mais maduros utilizamos grandes empresas, como, a frente de *IAM*[33], Segurança de Aplicação, *Data Security*, *Network Security*, Governança, risco

[33] *IAM: Identity Access Management*, gestor de indentidades para acesso dos sistemas

Compliance. Já para domínios mais novos, pode-se utilizar empresas mais atuais, startups, como segurança de nuvem, segurança para *IoT*[34], *SecOps*[35], *Bug Bounty*[36]."

Outro fenômeno que se observou com frequência foi a utilização de grupos de tomadores de decisão de CS para buscar por referências de soluções. Nesses grupos, CISOs, CIOs e CTOs se conversam a fim de entender as melhores práticas e soluções de CS disponíveis no mercado. Por ser um mercado de pouca maturidade, as empresas buscam inspiração em outras empresas pares para entender o que estão fazendo e espelhar-se.

Esse grupo é, em boa parte das vezes, o voto de minerva para decidir entre diferentes plataformas. De forma que, na hora de optar por uma solução, haja até um excesso de confiança na palavra dos outros, sem nem mesmo entender muito a fundo a plataforma ou software que estão comprando. Em suma, é um mercado onde a marca do provedor faz muita diferença, principalmente para grandes e médias empresas que tem que apresentar essas soluções para o conselho administrativo. Esse conselho administrativo conhece pouquíssimo do setor do CS e exige dos tomadores de decisão de CS empresas com algum renome na CS como garantia de bom trabalho,

Outra questão é, pela imaturidade do mercado e pela preocupação de grandes empresas em relação a possíveis invasões (risco assimétrico entre invadido e invasor), muitas vezes, há uma redundância das soluções de CS. Isto é, mais de uma solução servindo o mesmo propósito. Gera-se assim uma ineficiência de orçamento, por não saber julgar qual das soluções é melhor ou pior: "Por via das dúvidas, pegamos (escolhemos) as duas soluções." – CEO da empresa E9.

Nessa linha de resolver questões especializadas de cibersegurança, as empresas acabam optando por fornecedores diferentes de soluções de segurança justamente por não haver uma "bala de prata" que resolva todos os problemas de uma companhia. Isso fica ainda mais evidente em grandes companhias, que chegam a acumular mais de 10 fornecedores de serviços de segurança, como é o caso das empresas E6, E7, E8 e E10. Explorando essa dor, há grandes empresas de CS que estão seguindo uma tendência de consolidação das soluções do mercado. Ao invés de vários prestadores, apenas uma que faça um pouco de tudo visando

[34] *IoT: Internet of Things,* Internet das coisas é um conceito que se refere à interconexão digital de objetos cotidianos com a internet, conexão dos objetos mais do que das pessoas

[35] *SecOps:* unidade que garante a segurança e privacidade do processo de implementação e operação da companhia. Fazem parte dessa frente o *Security by Design* e o *Privacy by Design*

[36] *Bug Bounty:* Um programa de recompensa por bugs é um programa oferecido por algumas organizações nos quais indivíduos podem receber recompensas por relatar bugs, especialmente aqueles relacionados a explorações de segurança e vulnerabilidades

um mundo ideal onde empresas médias e pequenas seriam capazes de ter apenas um provedor de CS que fizesse tudo. Desde o mapeamento, estudo de priorização até oferecimento das soluções. Um serviço de consultoria na sua essência. Esse serviço até existe, mas está totalmente fora da realidade de orçamento de empresas médias, isto pois há múltiplas funções ainda não conseguem ser 100% automatizadas e requerem o trabalho direto de um especialista.

Todas essas informações expõem a desestruturação do modelo de priorização de CS, que é demasiadamente influenciado por fatores qualitativos e informais. Tendência que é ainda mais exacerbada em pequenas e médias empresas.

Empresa A

Na Empresa A em específico, encontrou-se uma estrutura e método de priorização de CS similar com o de outras empresas médias. Em mais detalhes: a companhia conta com 10-15 funcionários dedicados para garantira segurança da informação e dos processos de toda companhia. Estes estão divididos entre *Blue Team, Red Team, Yellow Team* e *White Team.* O primeiro cuida da segurança defensiva, fazendo o monitoramento de incidentes e condução da resposta ao incidente, responsável por cuidar de vazamentos, fraudes, comprometimentos da infraestrutura, entre outros. O segundo cuida justamente do oposto, a segurança ofensiva, fazendo diversos testes de penetração no sistema de segurança e simulações de ataques. O *Yellow Team* por sua vez é o responsável pela arquitetura do software, tanto de nuvem quanto de tecnologias, garantindo também as boas práticas no setor. Por fim, o White Team está ligado aos passos de governança da segurança da informação, propondo políticas, procedimentos e processos. Dessa forma, garantindo uma concordância com as métricas legais e de *compliance*[37]. Esses 4 times juntos compõem a equipe de CS da *Empresa A* trabalhando muitas vezes entre si para garantir a conformidade e ressonância no desenvolvimento da companhia.

Como a empresa é relativamente nova, criada há 4 anos, e está em plena expansão o orçamento de CS também vem em um crescimento vertiginoso, multiplicando por 4 entre as duas últimas rodadas de captação (entre dezembro de 2020 e dezembro de 2021).

[37] *Compliance* representa as ações que as empresas executam para guiar suas atividades com base em regras e procedimentos legais

Em relação aos processos de priorização, utiliza-se uma ferramenta de *discovery* para mapeamento de seus ativos digitais e sistemas, mas não há uma ponte para os impactos voltados para CS. Em seguida, há uma análise dos impactos financeiros e dos retornos esperados por cada um dos investimentos em CS utilizando um modelo quantitativo similar ao proposto por **Bojanc, Jerman-Blažič e Tekavčič (2012)**. Entretanto, a decisão final fica nas mãos do CIO da companhia e de um conselho de segurança, composto pelo CEO e alguns dos engenheiros principais de software. Essas informações levantadas não estão organizadas em um processo decisório estruturado e que visa levar em consideração tantos as análises quantitativas, quanto qualitativas. Estando sujeitas a decisões sub ótimas, muitas vezes.

Um exemplo de decisão que pode ter sido sub ótima que ocorreu na Empresa A, foi a priorização do incremento das camadas de segurança das aplicações em nuvem, que já possuíam alguma robustez, em detrimento de uma solução de *Ciber Threat Intelligence (CTI)*[38] e *Digital Risk Protection (DRP)*[39], que protege a marca e os clientes de possíveis fraudes. Em um acontecimento recente, essa decisão custou a companhia cerca de R$500 mil em um só mês em casos de fraudes a clientes que foram induzidos a fazer pagamentos em uma plataforma fraudulenta. Caso a companhia tivesse uma solução de CTI/DRP, que custa em média R$80 mil reais/ano, essa perda teria sido totalmente evitada e haveria dano a marca da *Empresa A.*

A utilização de um modelo de priorização mais estruturado teria provavelmente exposto essa lacuna e, frente à possibilidade de alto impacto na companhia, teria sido priorizada.

4.2 Aplicação do modelo de priorização proposto utilizando Teoria de Fuzzy e Análise de Falhas

Tendo em vista a forma como está organizada a tomada de decisão dentro da *Empresa A*, o modelo proposto pelo autor de priorização para estruturação da CS com o uso de teoria de Fuzzy e Análise de falhas pode servir como bom substituto ao modelo atual.

Para aplicar esse modelo proposto, deve-se seguir uma sequência de etapas composta de cinco fases: (i) identificação de um expert; (ii) entendimento das possíveis causas de

[38] *Cyber Threat Intelligence: CTI,* Inteligência de Ameaças Cibernéticas
[39] *Digital Risk Protection:* DRP, Proteção de Riscos Digitais

cenários de ataque; (iii) definição de critérios; (iv) avaliação com o método de Fuzzy; e (v) agregação e ordenação. Essa sequência de etapas está exposta na figura seguinte:

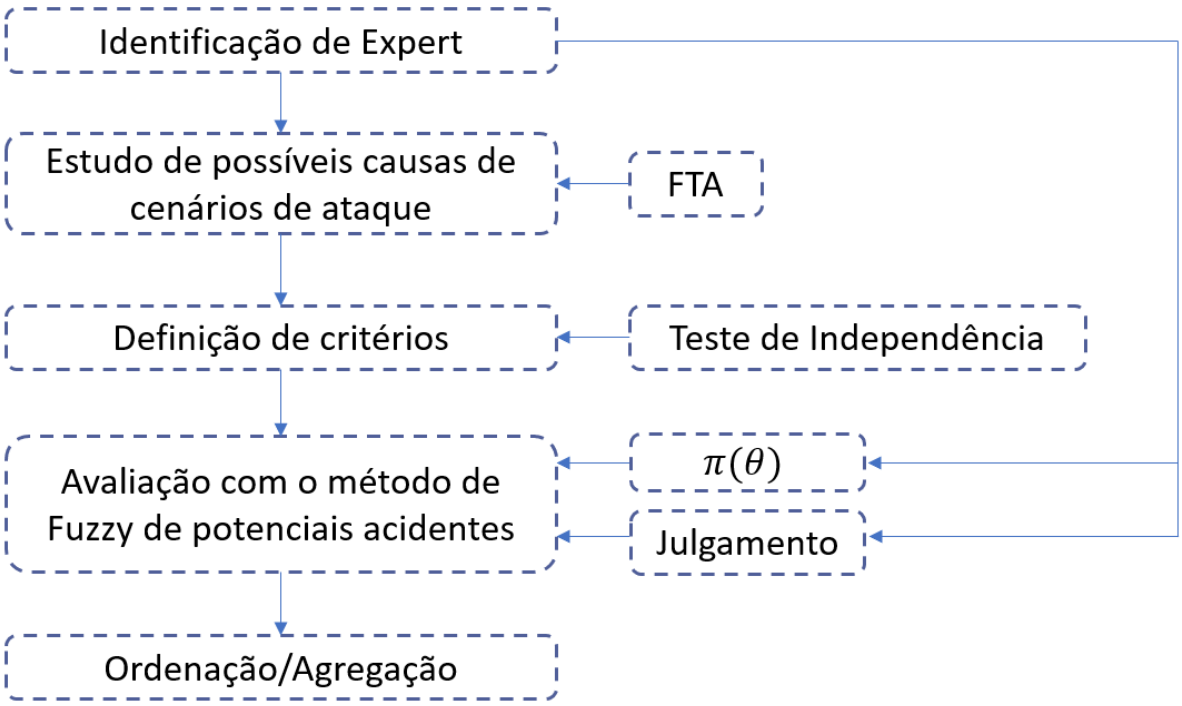

Figura 7 - Etapas do modelo proposto pelo autor. Fonte: Elaboração do próprio autor

(i) Identificação do expert

Nessa etapa inicial é necessário identificar uma pessoa ou um grupo de pessoas que, baseados em suas experiências, atue como um tomador de decisão capaz de maximizar o valor gerado por essa decisão. Isto é, ser capaz de identificar: (i) as vulnerabilidades da organização e, consequentemente, os potenciais acidentes; (ii) possíveis cenários de falhas; e (iii) as chances de ocorrência e os julgamentos sobre cada um desses elementos. Essa etapa chamada *identificação do expert.*

(ii) Estudo de possíveis causa de cenários de ataque

Para entender as possíveis causas e cenário que podem levar a ameaças, o modelo propõe a utilização do Método de Análise de Falhas (FTA). Um exemplo de aplicação se dá na *Figura 7* que é uma árvore que mostra os eventos de falha. Usando essa árvore, é possível identificar os possíveis efeitos de algum evento iniciador e dos eventos subsequentes gerados.

Os passos para a aplicação do FTA no contexto de ciberataques está descrito na tabela a seguir:

Tabela 3 - Procedimento para aplicação da árvore de análise de falhas. Fonte: elaboração do próprio autor.

Passo	Definição
Passo 1	Definir o sistema de interesse em relação aos ciberataques e como causas condicionais iniciais de falhas no sistema de segurança
Passo 2	Defina o evento principal para a análise e especifique o problema de interesse que a análise abordará
Passo 3	Defina a estrutura do topo da árvore. Determine os eventos e condições (ou seja, eventos intermediários) que levam mais diretamente ao evento principal, que neste caso pode ser uma rede defeituosa e uma falha no sistema de informação
Passo 4	Explore cada ramo em níveis sucessivos de detalhe. Determine os eventos e as condições que levam mais diretamente a cada evento intermediário.

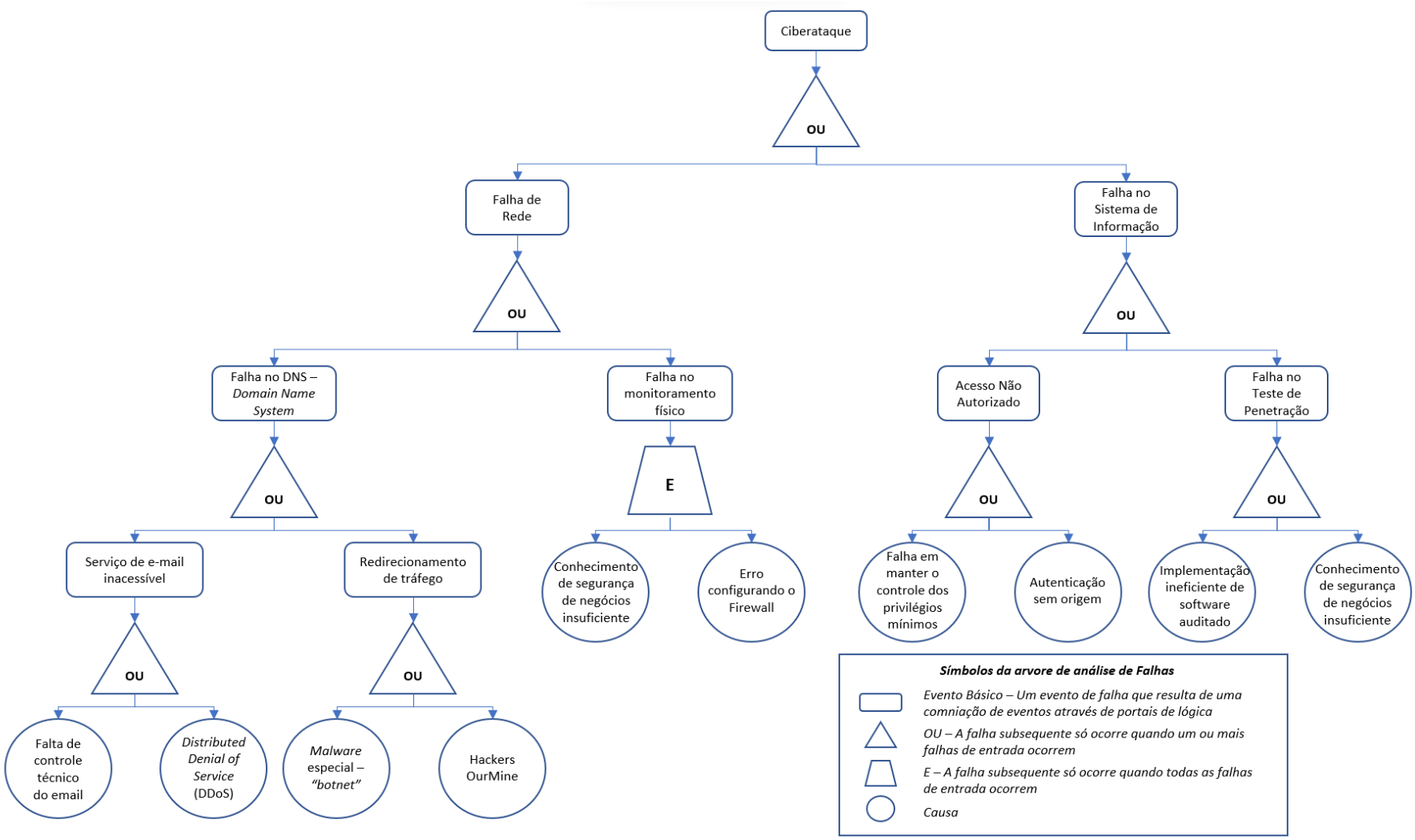

Figura 8- Estrutura produzida pela aplicação do FTA sobre um caso de ciber-ataque em um computador. Fonte: elaboração do próprio autor

(iii) Definição de critérios

Considerando as incertezas da análise de risco, este trabalho propõe o uso de modelos apresentados em **Ekel et al., (2008)**. Além disso, como este documento trata da análise de risco de CS, parece inadequado estimar as consequências da solução com base em um único critério.

Portanto, este documento se baseia em dois critérios para avaliação: (i) perdas financeiras (em milhares de dólares) e (ii) tempo para restauração das operações (em horas). O segundo critério considera a capacidade de reparar, reconstituir ou substituir rapidamente serviços danificados/desabilitados e retornar a um nível aceitável de funcionalidade. Também pode envolver reparo ou substituição de peças que tenham sofrido danos físicos devido a um ataque cibernético. Algumas dessas peças podem exigir longos prazos de entrega para substituição, devido a problemas de instalação ou disponibilidade de força de trabalho qualificada. Por exemplo, um atacante pode ter acesso a informações valiosas e sabotar os serviços da rede. Embora este trabalho considere apenas estes dois critérios, o processo que ele esboça não se restringe a eles.

(iv) Avaliação com o método de Fuzzy de potenciais acidentes

Essa etapa consiste na avaliação de cada uma das alternativas a_i para os critérios j identificados pelo especialista em gestão. Três alternativas foram escolhidas como exemplo de aplicação, com base em sua importância para o contexto organizacional da *Empresa A* e sua vulnerabilidade a ataques. As alternativas de investimento estão relacionadas ao (i) website da companhia; (ii) motor de transações financeiras, *gateways* de pagamentos internos; e (iii) *ERP*[40] da companhia. Na *Tabela 4*, descreve-se cada uma dessas frentes.

Com os critérios e as alternativas estabelecidos, falta a definição dos estados de natureza e suas potenciais consequências, que estão expressos na *Tabela 5*. No passo seguinte uma avaliação deve ser feita pelo expert, usando teoria de Fuzzy e as probabilidades ($p(s_j)$), representada por $\pi(\theta)$.

[40] *ERP:* Enterprise Resource Planning

Tabela 4 - Alternativas potenciais de investimento e as consequências de um possível ciberataque. Fonte: elaborado pelo próprio autor.

Alternativa	Descrição
Web Site Fraudulento	Um alvo comum para ciberataques é o servidor web público que conecta uma rede corporativa à Internet. O servidor web normalmente executa serviços http e ftp, e o atacante ganha controle sobre o servidor explorando as vulnerabilidades nestes serviços.
Gateway de pagamentos	As ferramentas de pagamento online que sustentam pagamentos com cartão de crédito, caso a caso, podem de dados sensíveis do portador do cartão, o que pode envolver grandes multas e, em muitos casos, má fama e perda de confiança e credibilidade
Enterprise Resource Planning (ERP)	Essas plataformas armazenam as informações mais valiosas e executam os principais processos comerciais de uma organização. Os componentes podem ser propensos a vulnerabilidades que podem ser exploradas para comprometer o sistema. Assim, os ciberataques que violarem uma plataforma ERP serão capazes de impor ataques de alto impacto contra a organização das vítimas

Tabela 5 - Potenciais consequências de um ciberataque. Fonte: elaboração própria do autor

Estados de Natureza (θ)	Descrição
Disseminação de dados (θ1)	Distribuição ou transmissão de dados confidenciais a outros usuários não autorizados.
Modificação de dados (θ2)	Eliminação, inserção ou alteração de informações de forma não autorizada.
Perda ou destruição de dados (θ3)	Roubo de informação confidencial
Interrupção dos serviços (θ4)	Interrupção parcial ou total da performance das operações da companhia

(v) Ordenação/Agregação

A parte final implica em agregar todos os critérios utilizados e ordenar as alternativas, de acordo com a magnitude de suas consequências e aplicando o método da teoria de Fuzzy. Essa etapa exige atuação do expert em CS identificado. Ele que será o responsável pelo preenchimento das tabelas e mapeamento das possíveis causas de falhas. Avaliando cada uma das alternativas a_i (levantadas na *Tabela 4)* associadas a cada um dos estados de natureza θ (descritos na *Tabela 5*) em relação aos critérios definidos (financeiro e tempo de recuperação

do sistema). Essa avaliação pode ser feita utilizando uma escala linguística de 5-pontos, que varia entre muito baixo (MB), baixo (B), médio (M), alto (A) e muito alto (MA). Essa abordagem se vê útil uma vez que é difícil estabelecer um valor numérico fixo para cada caso, visto as incertezas envolvidas e por muitos dos riscos não serem quantitativamente mensuráveis. Esse modelo facilita essa dificuldade.

Essa avaliação do impacto foi feita de maneira demonstrativa para cada um dos pares de alternativas e estados de natureza nas *Tabelas 6 e 7*.

Tabela 6 - Avaliação do expert quanto ao critério financeiro. Fonte: elaboração própria do autor.

Avaliação do expert a respeito do critério financeiro

Alternativas	θ1	θ2	θ3	θ4
Web Site Fraudulento	MB	B	M	MB
Gateway de pagamentos	A	MA	A	MA
ERP	MB	A	A	A

Tabela 7- Avaliação do expert a respeito do critério de tempo de restauração. Fonte: elaboração própria do autor.

Avaliação do expert a respeito do critério de tempo de restauração

Alternativas	θ1	θ2	θ3	θ4
Web Site Fraudulento	B	MB	M	A
Gateway de pagamentos	M	A	A	MA
ERP	M	A	M	MA

Nas *Tabelas 8 e 9*, utiliza-se conjuntos de Fuzzy triangulares de acordo com a escala linguística adotada. Em ambos os critérios definidos, quanto maior o valor (financeiro ou de tempo de recuperação) pior para a companhia. De forma que se priorizará a as alternativas de maior impacto.

Tabela 8 - Escala verbal relacionada a variação financeira. Fonte: elaboração própria do autor.

Escala verbal relacionada a variação financeira

Termos Lingísticos	Tipo de conjunto Fuzzy	Valores	Unidade
Muito Baixo	Triangular	(100; 150; 250)	milhares de BRL
Baixo	Triangular	(200; 350; 450)	milhares de BRL
Moderado	Triangular	(350; 600; 800)	milhares de BRL
Alto	Triangular	(650; 1000; 1300)	milhares de BRL
Muito Alto	Triangular	(1000; 1600; 2000)	milhares de BRL

Tabela 9 - Escala verbal relacionada a variação de tempo de recuperação. Fonte: elaboração prórpria do autor.

Escala verbal relacionada a variação de tempo de recuperação

Termos Lingísticos	Tipo de conjunto Fuzzy	Valores	Unidade
Muito Baixo	Triangular	(1; 3; 8)	Horas
Baixo	Triangular	(6; 12; 30)	Horas
Moderado	Triangular	(24; 36; 48)	Horas
Alto	Triangular	(40; 72; 120)	Horas
Muito Alto	Triangular	(96; 160; 240)	Horas

As *Tabelas 10 e 11* foram obtidas através da utilização do aplicativo *AIDMS2*, como descrito em (W. MAIA, EKEL, *et al.*, 2021). O método aplicado pelo *AIDMS2* segue **(8)** e **(9)**. A matriz de impacto agregada foi ilustrada na Tabela 12. Esta consiste em eleger a avaliação entre os dois critérios que represente o maior impacto para cada par de alternativa e estado de natureza.

Por fim, outra vez através do aplicativo *AIDMS2* gerou-se a matriz de risco com base em **(4)** e **(5)** e o ranking de alternativas foi criado utilizando o critério de LaPlace **(10)**. Esses resultados estão expostos na *Tabela 13.*

Tabela 10 - Matriz de retornos modificada com base no critério financeiro. Fonte: elaboração própria do autor.

Matriz de retornos modificada com base no critério financeiro

Alternativas	01	02	03	04
Web Site Fraudulento	(1; 1; 1)	(0,89; 0,86; 0,86)	(0,72; 0,69; 0,69)	(1; 1; 1)
Gateway de pagamentos	(0,39; 0,41; 0,4)	(0; 0; 0)	(0,39; 0,41; 0,4)	(0; 0; 0)
ERP	(0,72; 0,69; 0,69)	(0,39; 0,41; 0,4)	(0,39; 0,41; 0,4)	(0,39; 0,41; 0,4)

Tabela 11 - Matriz de retornos modificada com base no critériode tempo de restauração. Fonte: elaboração própria do autor.

Matriz de retornos modificada com base no critério de tempo de restauração

Alternativas	01	02	03	04
Web Site Fraudulento	(0,95; 0,94; 0,91)	(1; 1; 1)	(0,76; 0,79; 0,83)	(0,59; 0,56; 0,52)
Gateway de pagamentos	(0,76; 0,79; 0,83)	(0,59; 0,56; 0,52)	(0,59; 0,56; 0,52)	(0; 0; 0)
ERP	(0,76; 0,79; 0,83)	(0,59; 0,56; 0,52)	(0,76; 0,79; 0,83)	(0; 0; 0)

Tabela 12 - Matriz de retornos agregada. Fonte: elaboração própria do autor.

Matriz de retornos agregada

Alternativas	θ1	θ2	θ3	θ4	$\mu_D^{Max}(A_i)$	$\mu_D^{Min}(A_i)$	$\bar{\mu}_D^{Min}(A_i)$
Web Site Fraudulento	(0,95; 0,94; 0,91)	(0,89; 0,86; 0,86)	(0,72; 0,69; 0,69)	(0,59; 0,56; 0,52)	(0,95; 0,94; 0,91)	(0,59; 0,56; 0,52)	(0,79; 0,76; 0,75)
Gateway de pagamentos	(0,39; 0,41; 0,4)	(0; 0; 0)	(0,39; 0,41; 0,4)	(0; 0; 0)	(0,39; 0,41; 0,4)	(0; 0; 0)	(0,19; 0,21; 0,2)
ERP	(0,72; 0,69; 0,69)	(0,39; 0,41; 0,4)	(0,39; 0,41; 0,4)	(0; 0; 0)	(0,72; 0,69; 0,69)	(0; 0; 0)	(0,38; 0,38; 0,37)
$\mu_D^{Max}(\theta_i)$	(0,95; 0,94; 0,91)	(0,89; 0,86; 0,89)	(0,72; 0,69; 0,69)	(0,59; 0,56; 0,52)			

Tabela 13 - Matriz de Risco. Fonte: elaboração própria do autor.

Matriz de Risco

Alternativas	θ1	θ2	θ3	θ4	Rmax(Ai)	Ranking
Web Site Fraudulento	(0; 0; 0)	(0; 0; 0)	(0; 0; 0)	(0; 0; 0)	(0; 0 ;0)	3o
Gateway de pagamentos	(0,56; 0,5; 0,51)	(0,89; 0,86; 0,89)	(0,33; 0,28; 0,29)	(0,59; 0,56; 0,52)	(0,89; 0,86; 0,89)	1o
ERP	(0,23; 0,25; 0,22)	(0,50; 0,45; 0,49)	(0,33; 0,28; 0,29)	(0,59; 0,56; 0,52)	(0,59; 0,56; 0,52)	2o

Com base na avaliação teórica em questão, o *gateway* de pagamentos se mostrou a alternativa mais arriscada, seguido do ERP e website fraudulento. Vale ressaltar que quando esse mesmo método é aplicado em outras empresas, os resultados podem variar. Refletindo o tipo de negócio, tamanho da empresa e percepção do expert.

4.3 Discussão do modelo e justificativa de modelo proposto

O modelo proposto pelo autor é capaz de organizar de maneira estruturada o processo decisório de priorização em companhias, abordando o mapeamento das possíveis falhas e, com ajuda de um expert, fazendo a ponte entre critérios qualitativos e quantitativos de priorização de CS. Esse modelo poderia ser aplicado na *Empresa A* afim de reduzir ao máximo os impactos de critérios subjetivos e externos na hora da priorização por parte do tomador de decisão da companhia. Hoje, embora haja ferramentas para munir o tomador de decisão a respeito de possíveis riscos, como (i) a ferramenta de *Discovery* de mapeamento de ativos digitais e sistemas; (ii) o uso do modelo de análise de retorno sobre o capital investido proposto por **Bojanc, Jerman-Blažič e Tekavčič (2012)** para uma análise da perspectiva financeira; (iii) e um conselho de segurança para a discussão de diferentes pontos, ainda há uma desestruturação do processo como um todo. De forma que, não se estabelece pesos claros para cada uma das medidas qualitativas e quantitativas e se sujeita a decisões sub ótimas.

Extrapolando a aplicação do modelo proposto para todas as empresas médias em crescimento, é possível ter um ganho do ponto de vista de governança e de segurança da companhia como um todo. De governança, por tirar o fardo de decisão unicamente do tomador de decisão e fornecendo um modelo estruturado como suporte, e de segurança, por garantir uma visão global da companhia por meio do mapeamento. Além disso, o modelo não se restringe a uma única indústria: tanto a Árvore de Análise de Falhas (FTA), quanto os métodos da teoria de fuzzy podem ser aplicados em diferentes situações.

No caso da análise utilizando teoria de fuzzy, pode-se escolher os critérios, alternativas de investimento de CS e estados de natureza de acordo com a maneira como a companhia está estruturada e o modelo de negócio. Garantindo a aplicabilidade em basicamente qualquer cenário.

Embora o modelo utilize ferramentas matemáticas não óbvias para qualquer pessoa, como a Teoria de Fuzzy e o critério de LaPlace, sua aplicação é relativamente simples com o

auxílio da ferramenta *AIDMS2* desenvolvida em (W. MAIA, EKEL, *et al.*, 2021). Uma vez que o passo a passo é definido, basta adicionar no aplicativo cada uma das variáveis que os resultados já são produzidos pela aplicação. Dessa forma, funcionaria bem para o modelo de empresas médias, que requerem alguma sofisticação e ampla abordagem no modelo de priorização aplicado.

Para empresas pequenas, a aplicação de um modelo como esse provavelmente não faz sentido, uma vez que a empresa é imatura não só nos processos, mas principalmente na frente de CS. Além disso, há uma limitação de recursos orçamentários dificultando a justificativa dos investimentos nesse estudo de priorização. Nesse caso, opta-se na maioria das vezes por soluções que fornecem soluções generalistas que protejam a companhia de maneira abrangente, mas sem grandes especificidades para cada uma das companhias.

Já nas companhias grandes, há sim a necessidade de um modelo de estruturado de priorização de CS. Entretanto, o porte da companhia dificulta a utilização do FTA para mapeamento global, uma vez que a rede de sistemas e ativos digitais de grandes companhias são excessivamente complexos.

Além disso, a frente de CS da companhia já é madura (em boa parte das vezes) de forma que há diferentes times (subdivisões dentro da CS) cujas prioridades de investimento são distintas. Isso segmenta o poder de tomada de decisão na mão de vários grupos e torna a priorização de uma tomada de decisão global difícil de ser orquestrada. Devido a essas características, faria mais sentido grandes companhias utilizarem um modelo de priorização semelhante ao proposto de maneira localizada, ou seja, no escopo dos próprios times (subdivisões dentro da CS).

Por fim, vale ressaltar que as grandes companhias terceirizam uma parte relevante dos serviços de CS. De forma que, junto desses serviços pode estar incluído uma consultoria estratégica de priorização de CS, que aborda as lacunas da companhia de maneira muito mais detalhada e estratégica do que o modelo proposto pelo autor neste trabalho.

5 CONCLUSÕES

O tema cibersegurança vem ganhando mais relevância cada dia. Com o aumento da superfície digital, digitalização dos serviços, democratização do acesso à internet e uma população cada vez mais dependente das tecnologias, esse crescimento na importância da CS veio para ficar. Mesmo crescendo e com muito dinheiro fluindo para esse setor, ele ainda é bastante jovem e pouco maduro, com falta de pessoas capacitadas no mercado e com uma enorme desinformação a respeito dos riscos cibernéticos a que as pessoas estão expostas. Essa falta de maturidade fica ainda mais evidente em países em desenvolvimento, como o Brasil, que começaram a investir no ramo recentemente.

Em paralelo a esse cenário, desde 2020 vive-se um *boom*[41] no mercado de *venture capital/private equity*, onde nunca na história, viu-se tanto dinheiro ser investido em *startups* para financiar o aumento exponencial das suas operações. Esse crescimento abrupto gera grandes dificuldades estruturais para suportar esse aumento de escala, levando vários dos setores das companhias ao estresse máximo, e a cibersegurança é um deles.

Nesse contexto, o presente trabalho buscou uma maneira de auxiliar empresas médias em crescimento acelerado a priorizarem os seus investimentos em CS, alavancando-se na entrada que o autor tinha no mercado de *venture capital/private equity* para entender as maiores dores no processo de tomada de decisão na frente de CS das companhias. Entrevistou-se uma série de empresas e players do setor de CS e se constatou que havia uma grande desestruturação do modelo de tomada de decisão de companhias médias. As maiores dificuldades identificadas foram a falta de uma maneira de analisar quantitativamente os investimentos de CS de uma companhia e a susceptibilidade do tomador de decisão a influências externas na hora de optar por uma solução. Observou-se, também, nas entrevistas, que parte das companhias não dava a importância necessária para o segmento de CS, despriorizando-o frente outros investimentos.

Dessa forma, nesse trabalho realizou-se uma revisão bibliográfica contextualizando sobre o panorama atual da CS no mundo e sobre a importância do investimento em CS. Em seguida, discorreu-se sobre as diferentes características de pequenas, grandes e médias empresa no contexto de CS e as vulnerabilidades específicas de cada uma delas. Caracterizou-se também quais são os principais domínios e soluções da CS, e conceitos

[41] Boom: crescimento exponencial

chaves da cadeia de ataques cibernéticos, explorando seus principais atores e impactos. Após essa contextualização, explorou-se literaturas passadas para entender os modelos de priorização de CS que já haviam sido propostos.

Como objeto de estudo desse trabalho, elegeu-se a *Empresa A*, uma *fintech* de porte médio em crescimento acelerado com a qual o autor tinha proximidade e foi capaz de estudar com mais detalhes a estruturação da CS dessa companhia. Com base nas entrevistas e nos modelos de priorização de CS de literaturas passadas, discutiu-se qual seria a melhor opção para ser aplicada em uma companhia com características similares a da *Empresa A*. A opção escolhida foi a proposta por **Gusmão, Silva, Silva, Poleto, e Costa (2018)** que utiliza FTA e teoria Fuzzy para fazer a avaliação de CS da companhia por apresentar algumas características interessantes para endereçar os problemas de médias empresas: uma ponte estruturada entre a análise qualitativa e quantitativa e um método quantitativo para lidar com incertezas da análise.

Em seguida, aplicou-se de maneira demonstrativa o modelo proposto para três diferentes alternativas de investimento em CS. Elegeu-se como critérios para serem analisados as perdas financeiras e o tempo de recuperação do sistema pós ataque cibernético. Sugeriu-se também a utilização do programa *AIDMS2* para auxiliar nos cálculos da teoria de Fuzzy e aplicação do critério de LaPlace. Assim, chegou-se ao resultado de priorização do investimento na alternativa referente ao *gateway de pagamentos* da companhia. Vale ressaltar que, para a aplicação em um caso real, é necessário um expert para realizar as análises subjetivas de impacto.

O trabalho sugere que há um ganho operacional e estratégico a ser feito ao utilizar o modelo proposto de priorização de investimento em CS em companhias médias. A aplicação desse método deve ter um caráter de recorrência, anual por exemplo, para garantir o direcionamento correto dos investimentos de CS da companhia visto que (i) as ameaças digitais estão em constante evolução e (ii) o crescimento acelerado das empresas leva a uma mudança nas prioridades estratégicas.

Da mesma forma, companhias pequenas e grandes também sofrem com a priorização da CS e têm demandas diferentes, que não são 100% satisfeitas utilizando o modelo proposto neste trabalho. De forma que há espaço para futuros estudos direcionados para esses outros segmentos de empresas: as pequenas que sofrem de uma falta de orçamento estrutural e as

grandes que têm uma operação complexa demais para a aplicação do modelo proposto em sua essência.

Por fim, além de conhecimentos em tópicos diversos do setor de cibersegurança e a respeito de métodos como o FTA e a teoria de Fuzzy adquiridos pelo autor durante a produção deste trabalho final, espera-se que os estudos feitos e as propostas de modelos de priorização de CS para empresas deste trabalho contribuam para uma melhor estruturação da CS nas companhias brasileiras. De forma que essas instituições sejam capazes de trabalhar contra a desinformação sobre o setor da CS – capacitando experts ou educando funcionários a respeito de boas práticas – e de atuar contra o risco assimétrico que as empresas correm em relação a possíveis ciberataques e suas consequências, democratizando o acesso a CS para empresas e para pessoas.

6 REFERÊNCIAS BIBLIOGRÁFICAS

[1] ALJAAFREH, A. et al. A review of literature of initial trust in e-services: The case of internet banking services in Jordanian context. **J. Electron. Bank. Syst.**, 2014.

[2] ALZOUBI, Y. I. et al. Fog computing security and privacy for the Internet of Thing applications. **Secur. Priv.**, 2021. 4.

[3] AMERICANAS SA. **resultados 1T22**. Americanas SA. [S.l.]. 2022.

[4] BABANINA, V. et al. Cybercrime: History of formation, current state and ways of counteraction. **Amazonia Investiga**, v. 10, n. 38, fev. 2021. ISSN 2322-6307.

[5] BANDARA, I.; IORAS, F.; MAHER, K. **Cyber security concerns in e-learning education**. ICERI2014 Conference, IATED. Sevilha: [s.n.]. 2014. p. 728-734.

[6] BARR, J. R.; D'AURIA, D.; PERSIA. Homecare in the Era of COVID-19 & Beyond. **In Proceedings of the Third International Conference on Artificial Intelligence for Industries (AI4I)**, Irvine, September 2020. 48-51.

[7] BBC NEWS. President Rodrigo Chaves says Costa Rica is at war with Conti hackers. **BBC**, 2022. Disponivel em: <https://www.bbc.com/news/technology-61323402>. Acesso em: 17 jun. 2022.

[8] BELYAEV, L. S. A practical approach to choosing alternative solutions to complex optimization problems under uncertainty. **International Institute for Applied Systems Analysis**, v. 1, 1977.

[9] BERKMAN, H. et al. Cybersecurity awareness and market valuations. **Journal of Accounting and Public Policy**, v. 37, n. 6, p. 508-526, 2018.

[10] BOEIRA, S. L.; VIEIRA, P. F. Estudos organizacionais: dilemas paradigmáticos e abertura interdisciplinar. **Pesquisa qualitativa em estudos organizacionais: paradigmas, estratégias e métodos**, São Paulo, p. 17-51, 2006.

[11] BOJANC, R. . &. J.-B. B. Standard approach for quantification of the ICT security investment for cybercrime prevention. **Proceedings - The 2nd International Conference on the Digital Society**, v. 30, p. 7-14, 2008.

[12] BOJANC, R. . J.-B. B. . &. T. M. Managing the investment in information security technology by use of a quantitative modeling. **Information Processing & Management,** v. 48(6), p. 1031--1052, 2012.

[13] BONI, V.; QUARESMA, S. J. Aprendendo a entrevistar: como fazer entrevistas em. **Revista Eletrônica dos Pós-Graduandos em Sociologia Política da UFSC**, v. 2, n. 1, p. 68-80, 2005.

[14] BOU-HARB, E. . D. M. . &. A. C. A systematic approach for detecting and clustering distributed cyber scanning. **Computer Networks**, v. 57(18), p. 3826-3839, 2013.

[15] BRAUE, D. Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025. **Cybercrime Magazine**, 2021. Disponivel em: <https://cybersecurityventures.com/cybersecurity-spending-2021-2025/>. Acesso em: 26 out. 2022.

[16] BUJA, A. G. Cyber Security Featuresfor National E-Learning Policy. **Turk. J. Comput. Math. Educ. (TURCOMAT)**, p. 1729-1735, 2021.

[17] BURMESTER, M. . M. E. . &. C. V. Modeling security in cyber-physical physical. **International Journal of Critical Infrastructure Protection**, v. 5(3-4), p. 118-126, 2012.

[18] BUSINESS INSIDER. The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. **Insider**, 2021. Disponivel em:

<https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12>. Acesso em: 17 jun. 2022.

[19] BUSINESS WIRE. EC-Council to Increase Development of Ethical Hackers to Address Mounting Shortage of Cybersecurity Professionals. **Business Wire**, 2022. Disponivel em: <https://www.businesswire.com/news/home/20220907005072/en/EC-Council-to-Increase-Development-of-Ethical-Hackers-to-Address-Mounting-Shortage-of-Cybersecurity-Professionals>. Acesso em: 17 September 2022.

[20] CANALENERGIA. Norma regulamenta política de cibersegurança de empresas do setor elétrico. **CanalEnergia**, 2021. Disponivel em: <O que é ISO 27701?>. Acesso em: 28 out. 2022.

[21] CFI TEAMS. Types of Due Diligence. **CFI**, 2022. Disponivel em: <https://corporatefinanceinstitute.com/resources/valuation/types-of-due-diligence/>. Acesso em: 19 nov. 2022.

[22] CHAI, S. . K. M. . &. R. H. R. Firms' information security investment decisions: Stock market evidence of investors' behavior. **Decision Support Systems**, v. 50(4), 2011.

[23] CHENG, C.-Y. . L. S.-F. . C. S.-J. . Y. C.-Y. . &. S. R. J. Application of fault tree analysis to assess inventory risk: A practical case from aerospace manufacturing. **International Journal of Production Research**, v. 51, n. 21, p. 6499-6514, 2013.

[24] CHI, C.-F. . L. S.-Z. . &. D. R. S. Graphical fault tree analysis for fatal falls in the construction industry. **Accident; Analysis and Prevention**, v. 72, p. 359-369, 2014.

[25] CHUKWU, M. A.; IDOKO, E. C. Inhibitors of Electronic Banking Platforms' Usage Intention in Deposit Money Banks: Perspectives of Elderly Customers in Developing Economy. **Sch. Bull.**, n. 7, p. 134-145, 2021.

[26] CNN. Hackers steal over $600 million from video game Axie Infinity's Ronin network. **CNN**, 2022. Disponivel em: <https://edition.cnn.com/2022/03/29/tech/axie-infinity-ronin-hack/index.html>. Acesso em: 17 jun. 2022.

[27] COWLEY, J. A. . G. F. L. . &. W. B. Effect of network infrastructure factors on information system risk judgments. **Computers & Security**, v. 52, p. 142-158, 2015.

[28] CRANE, B. E. Online Teaching and Learning: A Practical Guide for Librarians. **Rowman & Littlefield: Lanham,** v. 29, 2016.

[29] DATAREPORTAL. **Digital 2022: Global Overview Report**. Datareportal. [S.l.]. 2022.

[30] DOVGAN, O. Cybersecurity in the information society: Information-analytical digest. **Artek**, Kiev, 2018.

[31] DOVHAN, O.; TKACHUK, T. U. System of information security of Ukraine: ontological dimensions. **Information and law**, v. 24, n. 1, p. 89-103, 2018.

[32] DW. Kaseya cyberattack: Hackers want $70 million for decryption. **DW**, 2021. Disponivel em: <https://www.dw.com/en/kaseya-cyberattack-hackers-want-70-million-for-decryption/a-58158481>. Acesso em: 17 jun. 2022.

[33] EISENHARDT, K.; GRAEBNER, M. E. Theory building from cases: opportunities and challenges. **Academy of Management Journal**, v. 50, n. 1, p. 25-32, 2007.

[34] EKEL, P. Y.; MARTINI, J. S. C.; PALHARES, R. M. Multicriteria analysis in decision making under information uncertainty. **Applied Mathematics and Computation**, v. 200, n. 2, p. 501-516, 2008.

[35] EU. General Data Protection Regulation GDPR. **Intersoft consulting**, 2022. Disponivel em: <https://gdpr-info.eu/>. Acesso em: 15 September 2022.

[36] EUROPOL. **Public Awareness and Prevention Guides.** [S.l.]. 2016.

[37] FERDOUS, R. . K. F. . V. B. . &. A. P. R. Methodology for computer aided fuzzy fault tree analysis. **Process Safety and Environmental Protection**, v. 87, n. 4, 2009.

[38] GAI, K. . Q. L. . C. M. . Z. H. . &. Q. M. SA-EAST : Security-Aware Efficient Data Transmission for ITS in Mobile Heterogeneous Cloud Computing. **ACM: Transactions on Embedded Computing Systems**, v. 16(2), p. 1-22, 2017.

[39] GAI, K. . Q. M. . M. Z. . Z. H. . &. Q. L. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. **IEEE Transaction on Smart Grid**, v. 8(5), p. 2431-2439, 2017.

[40] GAI, K. . Q. M. . X. Z. . &. L. M. Privacy-preserving multi-channel communication in Edge-of-Things. **Future Generation Computer Systems**, v. 85, p. 190-200, 2018.

[41] GALOV, N. Cloud Adoption Statistics for 2022. **Web Tribunal**, 2022. Disponivel em: <https://webtribunal.net/blog/cloud-adoption-statistics/#gref>. Acesso em: 14 September 2022.

[42] GODOI, C. K.; MELLO, R. B.-D.; SILVA, A. B. D. **Pesquisa qualitativa e o debate sobre a propriedade de pesquisar**. [S.l.]: [s.n.], 2006.

[43] GOODALL, J. R.; LUTTERS, W. G.; KOMLODI, A. Developing expertise for network. **Information Technology and People,** v. 22(2), p. 92-108, 2009.

[44] GRANJA, C.; JANSSEN, W.; JOHANSEN, M. A. Factors determining the success and failure of eHealth interventions: Systematic review. **J. Med. Internet Res.**, 2018. 20.

[45] GUSMAO, A. P. H. et al. Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. **International Journal of information management**, v. 43, p. 248-260, 2018.

[46] HAI, T. Artificial Intelligence in Cybersecurity. **Academia**, January 2017.

[47] HASAN, M. **State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally**. IOT Analytics. [S.l.]. 2022.

[48] HAUPTMANNS, U. Analytical propagation of uncertainties through fault trees. **Reliability Engineering & System Safety**, v. 76, p. 327-329, 2002.

[49] HAUPTMANNS, U. Semi-quantitative fault tree analysis for process plant safety using frequency and probability ranges. **Journal of Loss Prevention in the Process Industries Industries**, v. 17, n. 5, p. 339-345, 2004.

[50] HERRERA, A. V.; RON, M.; RABADÃO, C. **National cyber-security policies oriented to BYOD (bring your own device):** Systematic review. 12th Iberian Conference on Information Systems and Technologies (CISTI). Liboa: [s.n.]. 2017. p. 21-24.

[51] HERZIG, T.; WALSH. T. Implementing Information Security in Healthcare: Building a Security Program. **CRC Press:** Boca Raton, 2020. Acesso em: 02 September 2022.

[52] INMETRO. O que significa a ABNT NBR ISO 9001 para quem compra? **InMetro**, 2022. Disponivel em: <http://www.inmetro.gov.br/qualidade/pdf/cb25docorient.pdf>. Acesso em: 17 September 2022.

[53] JAGANATHAN, V. . C. P. . &. S. P. M. Using a prediction model to manage cyber security threats. **The Scientific World Journal,** v. 2015, p. 1-5, 2016.

[54] KANIA, D. D. The Ethical Issues of Aviation Business in Indonesia. **J. Manaj. Transp. Logist.**, v. 5, p. 1-10, 2018.

[55] KAWANAKA, T. . M. M. . &. R. S. Software measure in cyber-attacks on production control system. **Computers & Industrial Engineering**, v. 76, p. 378-386, 2014.

[56] KIM, D. W. . Y. P. . &. Z. J. Detecting fake anti-virus software distribution. **Computers & Security**, v. 49, p. 95-106, 2015.

[57] LE VPN. WHEN DID THE INTERNET START: HISTORY OF CYBER SECURITY. **Le VPN**, 2021. Disponivel em: <https://www.le-vpn.com/internet-privacy-cyber-security/>. Acesso em: 23 out. 2022.

[58] MAHMOOD, Y. A. . A. A. . V. A. K. . S. A. . &. K. U. Fuzzy fault tree analysis: A review of concept and application. **International Journal of System Assurance Engineering and Management**, v. 4, n. 1, p. 19-32, 2013.

[59] MANHATTAN TECH. The Seven Layers of IT security. **Manhattan Tech Support.com**, 2021. Disponivel em: <https://www.manhattantechsupport.com/blog/the-seven-layers-of-it-security/>. Acesso em: 19 nov. 2022.

[60] MASCELLINO, A. Cybercrime a Key Revenue Stram For North Korea`s Weapons Program. **Info Security Magazine**, 2022. Disponivel em: <https://www.infosecurity-magazine.com/news/cybercrime-revenue-stream-north/>. Acesso em: 12 September 2022.

[61] MCKINSEY & COMPANY. **New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers**. McKinsey & Company. [S.l.]. 2022.

[62] MCKINSEY. **The risk-based approach to cybersecurity**. McKinzsey. [S.l.]. 2019.

[63] MEYER, A. IoT Devices are Dramatically Expanding Your Digital Footprint. **Security Week**, 2017. Disponivel em: <https://www.securityweek.com/iot-devices-are-dramatically-expanding-your-digital-footprint>. Acesso em: 12 September 2022.

[64] MINKOV, M.; HOFSTEDE, G. The evolution of Hofstede's doctrine. **Cross Cultural Management: An International Journal.**, v. 18, n. 1, p. 10-20, 2011.

[65] MISHRA, A. et al. Cybersecurity Enterprises Policies: A Comparative Study. **MDPI**, 11 January 2022.

[66] MIT TECHNOLOGY REVIEW. O alarde sobre a computação quântica é um problema. **MIT Technology review**, 2022. Disponivel em: <https://mittechreview.com.br/o-alarde-sobre-a-computacao-quantica-e-um-problema/?utm_campaign=tr_weekreview_30042022&utm_medium=email&utm_source=RD+Station>. Acesso em: 10 January 2022.

[67] MOISEEV, N. Information Society as a Stage of Contemporary History. **Free Thought**, v. 1, p. 81-83, 2016.

[68] NADERIFAR, M.; GOLI, H.; GHALJAIE, F. Snowball Sampling: A Purposeful Method of Sampling in Qualitative Research. **Strides in Development of Medical Education**, v. 14, n. 3, 2017.

[69] NIBUSINESSINFO. Impact of cyber attack on your business. **NIInfoBusiness.co.uk**, 2020. Disponivel em: <https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business>. Acesso em: 26 out. 2022.

[70] NIST. Zero Trust Architecture, August 2020.

[71] PATEL, S. C. . G. J. H. . &. R. P. A. S. Quantitatively assessing the vulnerability of critical information systems : A new method for evaluating security. **International Journal of Information Management**, p. 483-491, 2008.

[72] PATEL, S. C. . G. J. H. . &. R. P. A. S. Quantitatively assessing the vulnerability of critical information systems : A new method for evaluating security enhancements. **International Journal of Information Management**, v. 28, p. 483-491, 2008.

[73] PEDRYCZ, W. . E. P. . &. P. R. Methods and applications. Fuzzy multicriteria decision-making: Models. **JohnWiley Sons**, 2011.

[74] PELTIER, T. R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. **CRC Press: Boca Raton**, Boca Raton, 2016.

[75] PERLROTH, N. **This Is How They Tell Me the World Ends:** The Cyberweapons Arms Race. [S.l.]: Bloomsbury Publishing, 2021.

[76] PERSISTENCE. **Global Market Study on Cyber Security: Demand Buoyed by Ever-Expanding Connected Environment**. [S.l.]. 2021.

[77] PRESIDÊNCIA DA REPÚBLICA SECRETARIA GERAL. **LEI Nº 13.709**. Presidência da República Secretaria Geral. Brasília. 2018.

[78] RAHMAN, A. F. . V. A. . K.-M. M. . &. L. J. C. Application of fault tree analysis for customer reliability assessment of a distribution power system. **Reliability Engineering & System Safety**, v. 111, p. 76-85, 2013.

[79] RAHMAN, T. et al. Human Factors in Cybersecurity: A Scoping Review, Bangkok, Thailand, July 2021. ISSN 978-1-4503-9012-5/21/06.

[80] RAIFFA, H. Decision analysis. **Wesley Reading**, 1968.

[81] RALSTON, P. A. S. . G. J. H. . &. H. J. L. Cyber security risk assessment for SCADA and DCS networks. **ISA Transactions**, v. 46, p. 583-594, 2007.

[82] REDDY, E.; MINNAAR, A. Cryptocurrency : a tool and target for cybercrime. **Acta Criminologica : African Journal of Criminology & Victimology**, December 2021.

[83] REDMILES, E. M. **"Should IWorry?" A Cross-Cultural Examination of Account Security Incident Response**. IEEE Symposium on Security and Privacy (SP). [S.l.]: [s.n.]. 2019. p. 920-934.

[84] RODRIGUES, R. O que é ISO 27701? **ProMove**, 2020. Disponivel em: <https://promovesolucoes.com/o-que-e-iso-27701/>. Acesso em: 28 out. 2022.

[85] RUIJTERS, E. . &. S. M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. **Computer Science Review**, p. 15-16, 29-62, 2015.

[86] RUOTI, S. E. A. **A comparative usability study of key management in secure email**. Proceedings of the 14th Symposium on Usable Privacy and Security, SOUPS. [S.l.]: [s.n.]. 2019. p. 375-394.

[87] SALGADO, B. et al. [Artigo] ISO 27001 x SOC2 – Qual é a melhor certificação de Segurança da Informação para a minha organização? **SegInfo**, 2021. Disponivel em: <https://seginfo.com.br/2021/06/09/artigo-iso-27001-x-soc2-qual-e-a-certificacao-de-seguranca-da-informacao-para-a-minha-organizacao/>. Acesso em: 16 out. 2022.

[88] SALGADO, B. et al. ISO 27001 x SOC2 – Qual é a melhor certificação de Segurança da Informação para a minha organização? **SegInfo**, 2021. Disponivel em: <https://seginfo.com.br/2021/06/09/artigo-iso-27001-x-soc2-qual-e-a-certificacao-de-seguranca-da-informacao-para-a-minha-organizacao/>. Acesso em: 28 out. 2022.

[89] SÁNCHEZ-GORDÓN, M. A. C.-P. R. **Security as Culture:** A Systematic Literature Review of DevSecOps. Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops. Nova York: [s.n.]. 2020. p. 266-269.

[90] SEGAL, E. Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report. **Forbes**, 2022. Disponivel em: <https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=2ff01c1352ae>. Acesso em: 26 out. 2022.

[91] SELLTIZ, C. **Métodos de pesquisa nas relações sociais. Tradução de Maria Martha**. 2. ed. [S.l.]: [s.n.], 1987.

[92] SERVICENOW. Discovery. **ServiceNow**, 2022. Disponivel em: <https://docs.servicenow.com/en-US/bundle/tokyo-it-operations-management/page/product/discovery/reference/r-discovery.html>. Acesso em: 28 out. 2022.

[93] SHAIKH, R. A. . A. K. . &. L. L. Dynamic risk-based decision methods for access control systems. **Computers & Security**, v. 31, n. 4, p. 447-464, 2012.

[94] SHIN, J. . S. H. . K. U. R. . &. H. G. Development of a cyber security risk model using Bayesian networks. **Reliability Engineering & System Safety,** v. 134, p. 208-217, 2015.

[95] SILVA, M. M. . D. G. A. P. H. . P. T. . S. L. C. E. . &. C. A. P. C. S. A multidimensional approach to information security risk management using FMEA and fuzzy theory. **International Journal of Information Management**, v. 34, n. 6, p. 733-740, 2014.

[96] SILVA, M. M. . P. T. . C. E. S. L. . H. D. G. A. P. . &. C. S. C. A. P. A. Grey theory based approach to big data risk management using FMEA. **Mathematical Problems in Engineering**, p. 1-15, 2016.

[97] SILVESTER, A. Impunity for cyber criminals simply isn't good enough. **City A.M**, 2015. Disponivel em: <https://www.cityam.com/impunity-for-cyber-criminals-simply-isnt-good-enough/>. Acesso em: 26 out. 2022.

[98] SOLMS, R.; NIEKERK, J. From information security to cyber security. **Computers & Security**, v. 38, p. 97-102, 2013. ISSN 0167-4048.

[99] STATISTA. The level of Internet penetration in the world as of September 2021, broken down by region. **Statista**, 2021. Disponivel em: <https://www.statista.com/statistics/269329/penetration-rate-of-the-internetby-region/>. Acesso em: 17 jun. 2022.

[100] TAHERDOOST, H. **Sampling methods in research methodology:** How to choose a sampling technique for research. [S.l.]: [s.n.], 2016.

[101] TALBOT, E. B.; FRINCKE, D.; BISHOP, M. Demythifying Cybersecurity. **IEEE**, 24 maio 2010. 56-59.

[102] TCHERNYKH, A. et al. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity and availability. **J. Comput. Sci.**, 2019. 36.

[103] TENCH, R.; YEOMANS, L. **Exploring Public Relations. US: Pearson Education**. [S.l.]. 2014.

[104] TERRA. Fundos captaram US$ 617 mi em 2022 para investir em startups no Brasil. **Terra**, 2022. Disponivel em: <https://www.terra.com.br/economia/dinheiro-em-dia/meu-negocio/fundos-captaram-us-617-mi-em-2022-para-investir-em-startups-

no-brasil,11d1e8e724e22d8bf7e7f78e56ea962fwlyhnmfu.html>. Acesso em: 23 out. 2022.

[105] TIA. SCS 9001: THE FIRST GLOBAL SUPPLY CHAIN SECURITY STANDARD. **Telecomunications Industry Association**, 2022. Disponivel em: <https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/>. Acesso em: 13 September 2022.

[106] TMC² TECHNOLOGIES. Cyber Security and Information Assurance. **TMC² Technologies**, 2021. Disponivel em: <https://www.tmctechnologies.com/cyber/>. Acesso em: 19 nov. 2022.

[107] VAN HAASTRECHT, M. et al. A Shared Cyber Threat Intelligence Solution for SMEs. **Eletronics**, v. 10, p. 2193, 2021.

[108] VILLA, E. et al. Electronic commerce: Factors involved in its adoption from a bibliometric analysis. **J. Theor. Appl. Electron. Commer. Res.**, v. 13, p. 39-70, 2018.

[109] W. MAIA, P. et al. Evaluation of Operational Risk in Power Substations and. **IEEE**, v. 1, p. 1, 2021. ISSN 2169-3536.

[110] WIRED. Russia Is Being Hacked at an Unprecedented Scale. **Wired**, 2022. Disponivel em: <Wired.co.uk>. Acesso em: 17 jun. 2022.

[111] YANG, P.; XIONG, N.; REN, J. Data security and privacy protection for cloud storage: A survey. **IEEE Access**, p. 8, 2020. ISSN 131723–131740.

[112] YAR, M. The Novelty of 'Cyber crime': An Assessment in Light of Routine Activity. **Theory European Journal of Criminology**, v. 2, n. 4, p. 407-427, 2015.

[113] YUHUA, D. . &. D. Y. Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis. **Journal of Loss Prevention in the Process Industries**, v. 18, n. 2, p. 83-88, 2005.

[114] ZADEH, L. A. Fuzzy sets. **Information and Control**, 1985. 338-353.

[115] ZADEH, L. B. The concept of a linguistic variable and its application to approximate reasoning—II. **Information Sciences**, 1975. 301-357.

[116] ZEIJLEMAKER, S. Unraveling the dynamic complexity of cyber-security towards identifying core systemic structures driving cyber-security investment decision-making. **Radboud Repository**, 2022.

[117] ZHANG, Z. . H. P. H. . &. H. L. Measuring IDS-estimated attack impacts for rational. **Computers & Security**, v. 28, n. 7, p. 605-614, 2009.