

THIAGO ARAUJO MONTEIRO

Licenciatura em Engenharia Informática

CRIANDO UM PROTOCOLO DE MODELAGEM DE AMEAÇAS PARA ORGANIZAÇÕES NÃO-HIERÁRQUICAS

Plano de Dissertação
MESTRADO EM ENGENHARIA INFORMÁTICA

Universidade NOVA de Lisboa

Draft: 20 de janeiro de 2025

CRIANDO UM PROTOCOLO DE MODELAGEM DE AMEAÇAS PARA ORGANIZAÇÕES NÃO-HIERÁRQUICAS

THIAGO ARAUJO MONTEIRO

Licenciatura em Engenharia Informática

Orientador: Kevin Gallagher

Full Professor, NOVA University Lisbon

Plano de Dissertação
MESTRADO EM ENGENHARIA INFORMÁTICA

Universidade NOVA de Lisboa

Draft: 20 de janeiro de 2025

RESUMO

Independentemente da língua em que a dissertação está escrita, geralmente esta contém pelo menos dois resumos: um resumo na mesma língua do texto principal e outro resumo numa outra língua.

Palavras-chave: Primeira palavra-chave, Outra palavra-chave, Mais uma palavra-chave, A última palavra-chave

ABSTRACT

Regardless of the language in which the dissertation is written, usually there are at least two abstracts: one abstract in the same language as the main text, and another abstract in some other language.

Keywords: One keyword, Another keyword, Yet another keyword, One keyword more, The last keyword

ÍNDICE

| | |
|---|-----------|
| Siglas | v |
| 1 Introdução | 1 |
| 1.1 Modelagem de Ameaças: Relevância e Desafios | 1 |
| 1.2 A Segurança Horizontal em Tempos de Interconexão | 2 |
| 1.3 Governança Organizacional: Uma Perspectiva Histórica | 2 |
| 1.4 Protocolo de Segurança para Organizações Não-Hierárquicas | 3 |
| 1.5 Delimitando o Escopo da Pesquisa | 3 |
| 1.6 Contribuições Esperadas | 4 |
| 1.7 Estrutura da Tese | 4 |
| 2 Background | 5 |
| 2.1 Fundamentos da Modelagem de Ameaças | 5 |
| 2.1.1 Definições Conceituais | 5 |
| 2.1.2 Principais Metodologias | 6 |
| 2.2 Taxonomia de Estruturas Organizacionais | 6 |
| 2.2.1 Estruturas Tradicionais Hierárquicas | 7 |
| 2.2.2 Organizações Horizontais | 7 |
| 2.2.3 Modelos Organizacionais Sem Liderança | 8 |
| 2.3 Centralismo Democrático | 9 |
| 2.3.1 Princípios Fundamentais e Origens Teóricas | 9 |
| 2.3.2 Modelos Contemporâneos de Aplicação | 9 |
| 2.3.3 Implicações e Potenciais para Governança | 10 |
| 3 Trabalhos Relacionados | 11 |
| 3.1 Abordagens Tradicionais de Modelagem de Ameaças | 11 |
| 3.1.1 STRIDE | 11 |
| 3.1.2 Attack Trees | 13 |
| 3.2 Metodologias Emergentes | 13 |

| | | |
|----------|---|-----------|
| 3.2.1 | PASTA | 13 |
| 3.2.2 | Security Cards | 15 |
| 3.2.3 | Personae Non Grata | 15 |
| 3.3 | Abordagens Híbridas e Colaborativas | 16 |
| 3.4 | Confiança Descentralizada e Frameworks Criptográficos | 16 |
| 3.4.1 | COLBAC | 16 |
| 3.4.2 | ABCCrypto | 17 |
| 3.4.3 | PGP e o Web of Trust | 18 |
| 3.5 | Perspectivas Comparativas | 19 |
| 3.5.1 | Critérios de Avaliação | 19 |
| 3.5.2 | Aplicabilidade em Organizações Não-Hierárquicas | 20 |
| 4 | Design | 22 |
| 4.1 | Conceito Preliminar do Protocolo | 22 |
| 4.2 | Requisitos de Segurança e Governança | 22 |
| 4.3 | Estratégia de Avaliação | 22 |
| 4.4 | Desenho Experimental | 23 |
| 4.5 | Questões de Pesquisa | 23 |
| 5 | Conclusão | 24 |
| 6 | Plano de Trabalho | 25 |
| 6.1 | Tarefas e Milestones | 25 |
| 6.2 | Gant Chart | 25 |
| | Bibliografia | 26 |

SIGLAS

| | |
|---------------|---|
| ABC | Asset-Based Cryptocurrency (<i>pp. 17, 18, 20, 21</i>) |
| CGTP | Confederação Geral dos Trabalhadores Portugueses (<i>p. 10</i>) |
| COLBAC | Collective based access control system (<i>pp. 9, 16, 17, 20, 21</i>) |
| CoReTM | Collaborative and Remote Threat Modeling (<i>p. 16</i>) |
| DAC | Discretionary Access Control (<i>p. 16</i>) |
| DFDs | Diagramas de Fluxo de Dados (<i>p. 11</i>) |
| DREAD | Damage, Reproducibility, Exploitability, Affected users, Discoverability (<i>pp. 12, 20</i>) |
| hTMM | Hybrid Threat Modeling Method (<i>p. 16</i>) |
| MAC | Mandatory Access Control (<i>p. 16</i>) |
| PASTA | Process for Attack Simulation and Threat Analysis (<i>pp. 12–14, 20</i>) |
| PGP | Pretty Good Privacy (<i>pp. 18, 19</i>) |
| PnGs | Personae Non Gratae (<i>pp. 15, 16</i>) |
| PTM | Participatory Threat Modeling (<i>pp. 16, 21</i>) |
| RBAC | Role-Based Access Control (<i>p. 16</i>) |
| STRIDE | Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (<i>pp. 2, 6, 7, 11–13, 16, 17, 20, 21</i>) |
| WoT | Web of Trust (<i>p. 19</i>) |

INTRODUÇÃO

1.1 Modelagem de Ameaças: Relevância e Desafios

A modelagem de ameaças é uma disciplina essencial no âmbito da segurança da informação, cuja principal função é identificar, classificar e mitigar vulnerabilidades em sistemas tecnológicos antes que estas possam ser exploradas por adversários. Em um contexto onde os sistemas se tornam cada vez mais complexos e integrados, a modelagem de ameaças se destaca como uma ferramenta crítica para antecipar riscos e estabelecer medidas de segurança eficazes [13].

As organizações hierárquicas, devido à centralização do controle e de recursos, geralmente aplicam metodologias de modelagem de ameaças que dependem de fluxos de decisão lineares e centralizados, como é o caso da metodologia STRIDE, desenvolvida pela Microsoft [34]. Esse modelo centralizado reflete uma estrutura organizacional que facilita a implementação de políticas de segurança homogêneas, mas carece de flexibilidade para lidar com as dinâmicas horizontais [38].

Em contrapartida, estruturas organizacionais horizontais, caracterizadas por uma distribuição equitativa de poder e responsabilidades, apresentam desafios específicos para a modelagem de ameaças [8]. A ausência de uma hierarquia clara muitas vezes resulta em incompatibilidades estruturais, como sistemas de controle de acesso que forçam a hierarquização, dificultando a implementação de políticas democraticamente acordadas [8]. Adicionalmente, a centralização de segredos organizacionais, como senhas, pode gerar conflitos durante transições de liderança, o que é exemplificado no fenômeno conhecido como password wars [18].

A utilização de ferramentas digitais por movimentos sociais também revela um fenômeno conhecido como vanguard digital. Isso ocorre quando indivíduos que controlam plataformas e contas digitais assumem posições de poder que podem contrariar os princípios de igualdade estrutural [9]. Além disso, ataques a processos democráticos, como falsificação de identidades (Sybil attacks) e manipulação de quorum, destacam vulnerabilidades exclusivas de sistemas horizontais devido à dependência em processos participativos [43, 6]. Finalmente, a falta de ferramentas tecnológicas que acomodem transições

entre centralizações temporárias e estruturas horizontais limita a eficiência em cenários que demandam respostas rápidas ou especialização [8].

Esses desafios evidenciam a necessidade de adaptações nos métodos de segurança e na modelagem de ameaças para que possam atender às especificidades das organizações horizontais. A modelagem de ameaças para esses contextos deve equilibrar aspectos técnicos e dinâmicas organizacionais, promovendo a resiliência e a segurança em ambientes onde o poder e a responsabilidade são compartilhados [36].

1.2 A Segurança Horizontal em Tempos de Interconexão

No mundo interconectado atual, as organizações horizontais desafiam o pressuposto de que a segurança depende de uma cadeia clara de comando. A ausência de hierarquia formal pode se transformar em um ativo estratégico ao dificultar ataques centralizados e ao permitir uma reconfiguração da gestão da confiança, promovendo a resiliência organizacional [39]. Em sistemas de confiança distribuída, como os utilizados em organizações baseadas em blockchain, a segurança é promovida por mecanismos colaborativos que substituem líderes formais por processos participativos e soluções orientadas à transparência e consenso [31].

Metodologias tradicionais de análise de ameaças, tais como Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) e árvores de ataque, fornecem fundamentos valiosos, mas enfrentam limitações em ambientes descentralizados, destacando a necessidade de abordagens mais adequadas às especificidades de estruturas horizontais [13]. Contextos menos hierárquicos requerem abordagens adaptadas que compreendam a complexidade da confiança horizontal e dos potenciais riscos associados.

Nesse sentido, tecnologias como a criptografia colaborativa [8, 1] e abordagens de modelagem de ameaças que adotam a perspectiva global da organização podem promover um entendimento mais realista da segurança em estruturas descentralizadas. A horizontalidade, frequentemente vista como um desafio, deve ser explorada como um ativo estratégico capaz de diluir pontos únicos de falha e fortalecer a resiliência organizacional.

1.3 Governança Organizacional: Uma Perspectiva Histórica

A governança organizacional reflete as estruturas sociais, econômicas e tecnológicas de cada época. Desde os primeiros agrupamentos humanos até as organizações complexas da contemporaneidade, as formas de organizar o poder e a tomada de decisão foram moldadas para responder a contextos específicos. O modelo hierárquico, amplamente adotado, emergiu como solução para demandas de controle e eficiência. Contudo, a história também registra experimentos que desafiaram essa lógica, sugerindo a possibilidade de novas abordagens na gestão e coordenação de atividades.

Mesmo em sistemas considerados pioneiros na horizontalidade, como a democracia ateniense, a governança enfrentou limitações significativas relacionadas à inclusão e à aplicabilidade prática, evidenciando fragilidades na operacionalização da participação igualitária [2]. Com o avanço da Revolução Industrial, a centralização hierárquica intensificou-se para lidar com o crescimento e a complexidade organizacional [47]. Adicionalmente, experiências como as cooperativas e os movimentos sindicalistas do século XIX delinearam alternativas à centralização absoluta, enquanto tecnologias modernas, oferecendo estruturas descentralizadas que desafiam paradigmas tradicionais de controle [14, 39].

Enquanto tecnologias de vigilância em massa reforçam estruturas centralizadoras, bloqueando a adoção plena de governança horizontal, inovações como o blockchain abrem novas possibilidades de descentralização, ainda que enfrentem desafios na distribuição equitativa de poder e recursos, como evidenciado na concentração de mineradores em redes públicas [46].

Essas evoluções históricas e tecnológicas não apenas moldam as estruturas de governança, mas também introduzem desafios únicos na modelagem de ameaças. A análise crítica dessas tentativas permite identificar vulnerabilidades e forças que fundamentam a construção de protocolos de segurança em organizações horizontais.

1.4 Protocolo de Segurança para Organizações Não-Hierárquicas

Esta pesquisa propõe um protocolo de segurança que integra a horizontalidade como elemento estratégico, indo além da simples adaptação de metodologias tradicionais. Em vez disso, busca demonstrar como a descentralização, quando bem estruturada, reforça a resiliência frente a ameaças complexas, mitigando pontos únicos de falha.

A proposta preenche uma lacuna na literatura sobre segurança em estruturas horizontalizadas, abordando desafios apontados em estudos como o uso limitado de metodologias tradicionais em contextos descentralizados [13] e a necessidade de criptografia adaptada [8]. Considere organizações descentralizadas que gerenciam ativos digitais sensíveis. A pergunta central é como garantir proteção contra fraudes internas e ataques externos, preservando a governança horizontal.

O protocolo proposto oferecerá mecanismos de consenso, transparência e uma modelagem de ameaças adaptada, como a inclusão de abordagens colaborativas e participativas descritas em [8] e [1], fornecendo soluções pragmáticas para tais desafios.

1.5 Delimitando o Escopo da Pesquisa

A variedade de arranjos horizontais é ampla, e analisar todos em um único estudo seria pouco produtivo. Para permitir uma análise detalhada e alinhada com os objetivos da pesquisa, este trabalho concentra-se em estruturas plenamente horizontais que exemplifiquem confiança distribuída, governança democrática e mecanismos colaborativos para

a tomada de decisão [8]. Ambientes híbridos ou parcialmente horizontalizados, onde a governança é compartilhada entre níveis hierárquicos e horizontais, ficam fora do escopo, permitindo avaliar com maior precisão a eficácia do protocolo em um cenário idealizado e mais controlado.

Futuras investigações poderão expandir este protocolo, adaptando suas diretrizes a contextos organizacionais híbridos ou altamente dinâmicos, como redes sociais e plataformas cooperativas digitais [17, 10]. A escolha por cooperativas de trabalhadores e redes comunitárias também reflete a relevância prática dessas estruturas em demonstrar a viabilidade de governança descentralizada e segurança distribuída [14, 39].

1.6 Contribuições Esperadas

A pesquisa entregará um protocolo de modelagem de ameaças específico para organizações horizontais, integrando os princípios de governança distribuída, participação coletiva e transparência. Esse protocolo será projetado para identificar, avaliar e mitigar ameaças em estruturas descentralizadas, fornecendo diretrizes práticas adaptadas às particularidades dessas organizações. Além disso, será acompanhado por um método de avaliação para validar sua eficácia e sua aplicação em casos reais ou simulados.

Espera-se que o protocolo demonstre como a horizontalidade pode ser um ativo estratégico, reforçando a segurança e a resiliência organizacional frente a ameaças complexas. Além de contribuir para o avanço teórico sobre segurança em estruturas descentralizadas, a pesquisa busca oferecer uma solução prática que fortaleça a autonomia e promova a integração entre segurança e governança democrática.

1.7 Estrutura da Tese

Após a introdução, o capítulo de Background apresenta os fundamentos da modelagem de ameaças e segurança em estruturas horizontais. O capítulo de Related Work analisa estudos prévios, identificando lacunas e oportunidades relevantes.

O capítulo de Design detalha o protocolo proposto, suas metodologias e critérios de avaliação. O capítulo de Work Plan descreve as etapas e cronograma da pesquisa, assegurando a execução estruturada e viável do projeto. Por fim, o capítulo de Conclusão sintetiza os resultados, discute limitações e propõe direções futuras, destacando a horizontalidade como ativo estratégico para a segurança organizacional.

BACKGROUND

2.1 Fundamentos da Modelagem de Ameaças

A modelagem de ameaças é um componente central da cibersegurança, pois permite identificar ativos valiosos, analisar potenciais vetores de ataque e estabelecer controles capazes de mitigar riscos. Essa prática vai além de fatores técnicos, incorporando elementos organizacionais e humanos que moldam a segurança em contextos diversos, especialmente em estruturas horizontais, onde processos internos e relações de confiança se tornam ainda mais críticos devido à ausência de hierarquias formais. Em um cenário de rápida evolução tecnológica e diversificação constante das ameaças, uma abordagem ampla e flexível ganha relevância, atendendo às particularidades de contextos em transformação.

Estudos como [26], [27] e [42] demonstram a necessidade de métodos estruturados, porém adaptáveis, para acompanhar ambientes em mutação. A adoção da perspectiva do adversário [25] é crucial para antecipar cenários complexos e fortalecer a resiliência em ambientes descentralizados, onde a multiplicidade de atores e a distribuição de poder requerem uma análise holística das ameaças. Esse ponto é especialmente relevante quando se consideram organizações horizontais, nas quais não há um ponto central de comando. Nesse tipo de contexto, a modelagem de ameaças precisa refletir a distribuição de poder e a multiplicidade de atores, incluindo as possíveis ameaças internas, externas e híbridas.

Além disso, a experiência da Microsoft, documentada em [35], enfatiza a importância de envolver stakeholders diversos e de aplicar ferramentas colaborativas. Esses elementos tornam-se cruciais quando a tomada de decisão é democrática ou descentralizada, pois a identificação e mitigação de riscos demandam engajamento coletivo e flexibilidade estratégica, conectando o exercício de modelagem de ameaças às dinâmicas organizacionais.

2.1.1 Definições Conceituais

A modelagem de ameaças pode ser entendida como um esforço sistemático de proteção que considera tanto vulnerabilidades técnicas quanto fatores sociais e organizacionais. Ao adotar uma visão holística, conforme sugerem [26] e [27], a análise de segurança não fica restrita à infraestrutura, mas incorpora práticas internas, fluxos de informação e a cultura

da organização. Em contextos não-hierárquicos, a ausência de linhas claras de autoridade e o caráter participativo tornam essencial uma análise que considere a distribuição de responsabilidades e a dependência de mecanismos coletivos de mitigação [8].

Por sua vez, [42] enfatiza que não existe uma solução única para modelagem de ameaças, especialmente em cenários onde a descentralização exige abordagens diversificadas e adaptáveis. Nesse sentido, a modelagem de ameaças torna-se um processo iterativo, adaptando-se a alterações estruturais e incorporando inovações como ferramentas de tomada de decisão participativa e práticas de segurança colaborativa.

2.1.2 Principais Metodologias

Metodologias amplamente discutidas, como o Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE), as árvores de ataque e frameworks baseados em cenários [38], fornecem um ponto de partida testado, mas frequentemente não capturam a complexidade de estruturas horizontais.

A documentação [34] apresenta um panorama de métodos existentes, alertando que a eficácia de cada abordagem depende do contexto. Por exemplo, STRIDE e árvores de ataque são úteis para identificar vetores de ataque diretos, mas a ausência de hierarquias formais intensifica a necessidade de explorar cenários complexos, como ameaças internas associadas a ataques externos, bem como falhas em mecanismos distribuídos de autenticação, consenso e governança, como sugerido em [8].

A integração de métodos diversos, como práticas de criptografia colaborativa [1] e abordagens híbridas [45], permite que organizações horizontais identifiquem padrões de risco menos óbvios e fortaleçam sua resiliência coletiva. Essa integração se torna crucial em estruturas distribuídas, onde a ausência de um 'centro' transforma a segurança em um esforço coletivo, e a resiliência emerge da interação contínua entre membros, sistemas e mecanismos de governança descentralizada.

2.2 Taxonomia de Estruturas Organizacionais

Entender a relação entre forma organizacional e segurança é essencial para ajustar a modelagem de ameaças à realidade de cada instituição. Enquanto estruturas hierárquicas confiam em pontos centrais de decisão para controle e coordenação, esses mesmos pontos podem se tornar vulnerabilidades críticas. Organizações horizontais ou cooperativas podem dispersar vulnerabilidades e aumentar a resiliência por meio da governança descentralizada, embora também possam criar múltiplos pontos de entrada que exigem controle colaborativo. A análise desta taxonomia, conforme [14, 20], oferece uma base para identificar como a distribuição de poder em diferentes formas organizacionais afeta a eficácia de medidas de segurança, incluindo a capacidade de resposta a ameaças internas e externas.

2.2.1 Estruturas Tradicionais Hierárquicas

Organizações hierárquicas apresentam linhas claras de autoridade, o que facilita o controle, mas pode concentrar vulnerabilidades em pontos críticos. Essas organizações são caracterizadas por uma cadeia de comando bem definida, onde as decisões fluem do topo para a base. Exemplos clássicos incluem grandes corporações multinacionais, onde a diretoria estabelece políticas que são implementadas por camadas de gerentes, supervisores e funcionários. Por outro lado, em pequenas empresas, como escritórios familiares, a hierarquia pode ser menos formal, mas ainda assim baseada em uma estrutura de comando clara e centralizada [14].

Em grandes organizações, como bancos ou indústrias automotivas, a hierarquia permite uma alocação eficiente de recursos e um controle rigoroso sobre as operações. Por exemplo, as divisões de TI desses ambientes frequentemente utilizam frameworks de segurança como o STRIDE para modelagem de ameaças, focando na proteção de ativos críticos e no gerenciamento de acessos centralizados [48]. A centralização facilita a resposta rápida a incidentes, mas também cria pontos únicos de falha, como vulnerabilidades em servidores principais ou credenciais administrativas [46].

Em contrapartida, pequenas empresas enfrentam desafios diferentes. Nesses contextos, a falta de recursos pode levar a menos camadas hierárquicas, mas as decisões ainda se concentram em um único proprietário ou gerente. Isso reduz a complexidade organizacional, mas aumenta a dependência de indivíduos específicos, tornando-os alvos prioritários em ataques [14]. Ademais, a ausência de equipes dedicadas de segurança pode limitar a capacidade de implementar frameworks sofisticados, como STRIDE, exigindo soluções mais simplificadas.

A diferença entre organizações grandes e pequenas também reflete no impacto sobre a modelagem de ameaças. Em empresas maiores, as estruturas hierárquicas permitem segmentações detalhadas para identificar e mitigar riscos em níveis específicos da organização. No entanto, essa segmentação pode levar a lacunas de comunicação entre departamentos, dificultando a implementação de soluções integradas [48]. Por outro lado, organizações menores têm maior flexibilidade para adaptar rapidamente suas estratégias de segurança, embora frequentemente careçam de recursos para implementar soluções robustas [47].

Portanto, enquanto organizações hierárquicas oferecem vantagens em termos de controle e clareza, elas também introduzem desafios específicos para a modelagem de ameaças. Esses desafios variam significativamente com o tamanho e a complexidade da organização, exigindo adaptações nos frameworks tradicionais para atender às necessidades específicas de cada tipo de hierarquia.

2.2.2 Organizações Horizontais

Organizações horizontais se distinguem pela rejeição de hierarquias tradicionais, priorizando processos decisórios distribuídos e participação equitativa de todos os membros.

Este modelo contrasta diretamente com estruturas hierárquicas, que centralizam o poder em níveis superiores, perpetuando desigualdades no acesso à informação e controle organizacional [10, 29].

A horizontalidade é tanto uma ferramenta quanto um objetivo em si. Nos movimentos sociais argentinos, como analisado por Marina Sitrin, a horizontalidade emergiu como um mecanismo essencial para estabelecer relações baseadas na confiança e no consenso, superando formas tradicionais de organização. Assembleias de bairro e coletivos de trabalhadores desempregados exemplificam como a horizontalidade pode ser aplicada para autogestão e planejamento coletivo [39].

No campo da cibernética, o protocolo COLBAC demonstra a relevância da horizontalidade em sistemas de segurança digital, promovendo um controle de acesso colaborativo que reduz a centralização de poder. Este modelo evita as vulnerabilidades criadas pela dependência de proprietários únicos de senhas ou permissões, reforçando a coerência entre práticas organizacionais e ferramentas tecnológicas [8].

Adicionalmente, exemplos históricos, como a democracia ateniense, ilustram que estruturas horizontais podem ser complementadas por mecanismos temporários de centralização em momentos de crise, garantindo flexibilidade e eficiência sem comprometer os princípios básicos da governança distribuída [2].

Apesar dos desafios, como o risco de dominação por vozes mais influentes ou a gestão de conflitos em espaços coletivos, as organizações horizontais demonstram que, com mecanismos adequados, é possível promover autonomia, participação inclusiva e eficiência em estruturas descentralizadas [9].

2.2.3 Modelos Organizacionais Sem Liderança

O discurso de organizações sem liderança esconde uma complexidade adicional, onde a ausência de uma hierarquia formal não implica necessariamente uma horizontalidade genuína. Estudos críticos destacam como essas organizações frequentemente replicam dinâmicas de poder veladas e centralizações informais.

Marina Sitrin, em sua análise sobre movimentos horizontais na Argentina, aponta que, embora a horizontalidade seja declarada como objetivo, muitos movimentos enfrentam desafios significativos para sustentar práticas realmente participativas. A falta de hierarquia formal frequentemente leva a estruturas de poder informais, onde vozes dominantes assumem papéis de liderança sem supervisão ou responsabilidade coletiva clara [39].

No contexto digital, movimentos como Occupy Wall Street demonstram que a ausência de uma liderança reconhecível não elimina conflitos internos. Estudos sobre as equipes de mídia social desses movimentos revelam que a administração de contas, como no Twitter, foi frequentemente marcada por disputas de controle, ilustrando como poder e influência podem se consolidar mesmo em estruturas supostamente horizontais [9].

Além disso, pesquisas sobre cooperativas de trabalhadores nos Estados Unidos indicam que essas organizações, embora frequentemente vistas como alternativas não hierárquicas,

tendem a desenvolver líderes informais que influenciam decisões de maneira significativa, questionando a narrativa de horizontalidade absoluta [47].

Tecnologias utilizadas por essas organizações também carregam implicações políticas. Langdon Winner argumenta que artefatos técnicos podem perpetuar estruturas de poder existentes, mesmo quando empregados em contextos descentralizados. Por exemplo, plataformas digitais, muitas vezes projetadas para usos individuais, criam desafios na construção de governança coletiva efetiva, exacerbando desigualdades latentes [46].

Esses exemplos destacam que, embora a ideia de ausência de liderança formal seja atraente, sua execução prática frequentemente resulta em formas informais de hierarquia. Assim, o sucesso dessas organizações depende da capacidade de identificar e mitigar as dinâmicas de poder ocultas, promovendo mecanismos claros de governança coletiva e responsabilidade mútua que realmente sustentem a horizontalidade desejada.

2.3 Centralismo Democrático

Em meio a cenários cada vez mais desafiadores em termos de coordenação organizacional, seja na gestão de grandes corporações ou na manutenção de redes descentralizadas como a blockchain, surge a necessidade de se conciliar a eficiência na tomada de decisões com a participação ativa de todos os envolvidos. O centralismo democrático, formulado para atender às exigências de movimentos revolucionários, mantém sua relevância ao propor um equilíbrio dinâmico entre deliberação coletiva e execução centralizada. Essa abordagem tem se mostrado pertinente tanto em contextos políticos e sociais quanto em cenários tecnológicos contemporâneos.

2.3.1 Princípios Fundamentais e Origens Teóricas

O centralismo democrático fundamenta-se na ideia de que a coleta de opiniões e a deliberação (democracia) devem ser harmonizadas com a capacidade de implementar decisões de forma unificada (centralismo). Esse sistema foi originalmente concebido como resposta à necessidade de organização em contextos de alta complexidade estrutural [49, 29].

Sua formulação inicial, associada ao Partido Comunista da União Soviética, inspirou a adoção do modelo por diferentes grupos ao redor do mundo. Na China, por exemplo, as práticas de centralismo democrático demonstram uma resiliência notável, sendo reconfiguradas à medida que variam as conjunturas políticas e sociais [41].

2.3.2 Modelos Contemporâneos de Aplicação

A transposição dos preceitos do centralismo democrático para contextos modernos tem sido observada em diferentes estruturas organizacionais e tecnológicas. Um exemplo é o protocolo Collective based access control system (COLBAC), que adapta as bases do

centralismo democrático a um ambiente de controle de acesso colaborativo, possibilitando decisões participativas aliadas a uma implementação coesa [8].

Movimentos sindicais e organizações sociais também têm integrado princípios de centralismo democrático. A Confederação Geral dos Trabalhadores Portugueses (CGTP), por exemplo, combina deliberação coletiva e períodos de centralização estratégica para dar respostas eficazes a desafios organizacionais [7].

2.3.3 Implicações e Potenciais para Governança

A influência do centralismo democrático transcende os limites dos partidos políticos, podendo ser estendida a cenários diversos que exijam tanto participação ampla quanto execução eficiente. Organizações horizontais ou distribuídas podem recorrer a esse modelo para conciliar a voz de seus integrantes com a necessidade de tomar decisões de forma centralizada em momentos críticos [49, 41].

Nesse sentido, a aplicação de elementos do centralismo democrático em plataformas digitais evidencia como conceitos históricos podem ser reapropriados para atender às demandas de governança contemporâneas.

TRABALHOS RELACIONADOS

3.1 Abordagens Tradicionais de Modelagem de Ameaças

3.1.1 STRIDE

O Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE), desenvolvido pela Microsoft, é uma metodologia sistemática para a modelagem de ameaças, projetada para identificar potenciais vulnerabilidades em sistemas de software. O acrônimo STRIDE representa seis categorias principais de ameaças[36]. Cada uma dessas categorias reflete uma violação específica das propriedades desejadas de segurança, como autenticidade, integridade, não-repúdio, confidencialidade, disponibilidade e autorização [32].

A aplicação do STRIDE começa com a criação de Diagramas de Fluxo de Dados (DFDs) para mapear a movimentação de informações no sistema [11]. Os DFDs ajudam a identificar elementos como entidades externas, processos, fluxos de dados e armazenamentos de dados. Para cada elemento do diagrama, as seis categorias de ameaças do STRIDE são analisadas para identificar possíveis vulnerabilidades [36].

Cada ameaça no STRIDE tem uma definição clara e exemplos práticos para auxiliar na identificação e mitigação. Por exemplo:

1. **Spoofing:** Ameaças que envolvem a falsificação da identidade de usuários ou processos, comprometendo a autenticidade.
2. **Tampering:** Manipulação de dados em trânsito, no armazenamento ou na memória, afetando a integridade.
3. **Repudiation:** Cenários onde usuários negam ações realizadas, muitas vezes devido à falta de mecanismos adequados de registro.
4. **Information Disclosure:** Exposição de informações sensíveis para partes não autorizadas, comprometendo a confidencialidade.
5. **Denial of Service:** Ataques que sobrecarregam os recursos do sistema, prejudicando a disponibilidade.

6. **Elevation of Privilege:** Casos onde um ator mal-intencionado obtém privilégios superiores aos autorizados, comprometendo a autorização.

A metodologia STRIDE pode ser adaptada para diferentes contextos. Por exemplo, em sistemas ciberfísicos, é possível avaliar ameaças relacionadas a componentes de hardware e software, como falhas em sincronização ou comunicação [19]. Além disso, variantes como STRIDE-per-Element e STRIDE-per-Interaction oferecem abordagens mais focadas para identificar ameaças em elementos específicos ou em interações entre componentes [36].

Embora amplamente utilizada, o STRIDE tem limitações. Ele depende significativamente da experiência dos analistas e pode não capturar ameaças emergentes em sistemas descentralizados ou ambientes dinâmicos [12]. Por isso, é frequentemente complementado com outros frameworks, como o Damage, Reproducibility, Exploitability, Affected users, Discoverability (DREAD), para priorizar ameaças com base em impacto e probabilidade [21].

Em resumo, o STRIDE fornece uma base sólida para a identificação de ameaças, mas sua aplicação eficaz exige integração com outras metodologias e adaptações para atender às necessidades específicas de sistemas modernos e descentralizados [11].

3.1.1.1 Modelos Complementares ao STRIDE

Diversos modelos complementares foram derivados ou utilizados em conjunto com o STRIDE para aprimorar sua eficácia e adaptabilidade em diferentes contextos. Entre esses, destaca-se o modelo DREAD, que complementa o STRIDE ao fornecer uma abordagem quantitativa para priorização de ameaças [21]. O DREAD utiliza cinco categorias principais: Damage Potential, Reproducibility, Exploitability, Affected Users e Discoverability, permitindo que analistas atribuam valores e criem escores para classificar ameaças de acordo com sua severidade [30].

O uso combinado do STRIDE e do DREAD pode melhorar a avaliação de riscos em sistemas mais complexos. No entanto, a subjetividade inerente à atribuição de valores no DREAD pode comprometer a consistência das análises, especialmente em contextos colaborativos ou descentralizados [21]. Para mitigar essas limitações, algumas organizações têm integrado o STRIDE a frameworks mais abrangentes, como o Process for Attack Simulation and Threat Analysis (PASTA), que adota uma abordagem iterativa para identificar e priorizar ameaças [30].

Adicionalmente, o uso de árvores de ataque tem se mostrado eficaz para complementar o STRIDE, permitindo que equipes representem visualmente cenários de ameaça complexos e identifiquem múltiplas vias de ataque. Essa integração é particularmente útil em organizações horizontais, onde a ausência de centralização aumenta a necessidade de mapeamentos colaborativos de ameaças [36].

3.1.2 Attack Trees

As árvores de ataque, introduzidas por Bruce Schneier [33], oferecem uma estrutura hierárquica para modelagem de ameaças, onde o objetivo do ataque é representado pelo nó raiz, e os subobjetivos e etapas necessárias para alcançá-lo são dispostos em nós filhos. Cada nó pode ser detalhado com operadores lógicos como AND e OR, representando condições que devem ser cumpridas conjuntamente ou alternativamente [23].

Uma das principais vantagens das árvores de ataque é sua capacidade de decompor ameaças complexas em componentes menores e mais gerenciáveis, permitindo uma análise sistemática [16]. Essa metodologia facilita a identificação de múltiplos caminhos de ataque, permitindo que as organizações priorizem contramedidas com base em métricas como custo, impacto e probabilidade [15].

Aplicações práticas das árvores de ataque incluem sua utilização em redes de sensores sem fio para avaliar riscos à privacidade de localização [15], bem como na detecção de roubo de energia em infraestruturas avançadas de medição, como redes elétricas inteligentes [16]. Em ambos os casos, a abordagem possibilita que as organizações mapeiem cenários de ameaça específicos e projetem contramedidas eficazes.

Além disso, estudos como [23] destacam a reutilização de subárvores para aumentar a eficiência em sistemas complexos. Essa prática permite que elementos compartilhados entre diferentes cenários sejam modelados uma única vez e incorporados em análises futuras, economizando tempo e recursos.

Embora sejam amplamente aplicáveis, as árvores de ataque apresentam desafios relacionados ao esforço necessário para sua construção inicial e à complexidade em sistemas de grande escala [33]. A colaboração entre stakeholders, incluindo especialistas técnicos e operacionais, é essencial para garantir que a representação das ameaças seja precisa e abrangente [16].

As árvores de ataque também se destacam como ferramentas complementares a metodologias como STRIDE e podem ser utilizadas tanto para identificar ameaças quanto para organizar as já descobertas. Além disso, a reutilização de árvores existentes, como aquelas voltadas para fraudes ou eleições, economiza tempo e fornece uma base sólida para análise. Apesar de sua versatilidade, o uso eficaz das árvores depende de representações claras de nós AND/OR e da avaliação contínua para evitar excessos ou lacunas [36].

3.2 Metodologias Emergentes

3.2.1 PASTA

O PASTA é uma metodologia de modelagem de ameaças centrada no risco, projetada para integrar segurança ao longo do ciclo de vida do desenvolvimento de software. Proposto por Tony UcedaVelez e Marco M. Morana [44], o framework consiste em sete estágios sequenciais que permitem uma análise aprofundada e iterativa de ameaças e vulnerabilidades.

O objetivo principal do PASTA é alinhar as preocupações de segurança com os objetivos de negócio, garantindo que as medidas de mitigação abordem tanto os riscos técnicos quanto os impactos organizacionais. A metodologia promove uma abordagem orientada ao risco, integrando simulações de ataques para avaliar a eficácia das contramedidas propostas [44].

1. **Definition of the Objectives (DO):** Neste estágio inicial, são definidos os requisitos de segurança, o perfil de risco e os impactos potenciais nos negócios.
2. **Definition of the Technical Scope (DTS):** Este estágio detalha os aspectos técnicos, como usuários, componentes de software, infraestrutura de terceiros e dependências externas.
3. **Application Decomposition and Analysis (ADA):** A aplicação é dividida em elementos funcionais básicos para identificar fluxos de dados, tipos de usuários, e controles de segurança existentes.
4. **Threat Analysis (TA):** Identificação de possíveis ameaças com base nos elementos e ativos analisados, considerando os vetores de ataque mais prováveis.
5. **Weakness and Vulnerability Analysis (WVA):** Neste estágio, as ameaças são associadas a vulnerabilidades específicas, avaliando a eficácia dos controles existentes e identificando fraquezas.
6. **Attack Modeling and Simulation (AMS):** Realização de simulações para determinar os caminhos de ataque mais prováveis, utilizando árvores de ataque e outros modelos para explorar cenários de risco.
7. **Risk Analysis and Management (RAM):** Identificação dos impactos técnicos e de negócio, propondo medidas para mitigar os riscos prioritários [44].

O PASTA se destaca por sua flexibilidade e profundidade analítica, tornando-o particularmente eficaz em ambientes dinâmicos e distribuídos. A metodologia incentiva a colaboração entre stakeholders de diferentes áreas, promovendo uma compreensão unificada dos riscos e das prioridades organizacionais. Além disso, a integração de simulações de ataques permite que as organizações testem a eficácia de suas estratégias de segurança em condições realistas, aprimorando sua resiliência contra ameaças emergentes [44].

Um dos aspectos mais relevantes do PASTA é sua compatibilidade com organizações horizontais. A abordagem colaborativa da metodologia, que envolve múltiplos stakeholders em todas as etapas do processo, está alinhada com os princípios de governança distribuída. Em estruturas não hierárquicas, onde a responsabilidade pela segurança é compartilhada, o PASTA oferece um framework estruturado para identificar e mitigar riscos de forma participativa e eficiente.

3.2.2 Security Cards

Os Security Cards são uma ferramenta desenvolvida para facilitar o brainstorming de ameaças de segurança, utilizando um baralho de cartas que aborda diferentes aspectos de possíveis ataques [5]. Criados por Tamara Denning, Batya Friedman e Tadayoshi Kohno, os cartões cobrem quatro dimensões principais: motivações do adversário, recursos do adversário, métodos do adversário e impacto humano [4]. Esta abordagem busca promover a criatividade e a colaboração entre stakeholders, incentivando uma análise mais holística e abrangente das ameaças [37].

Cada carta oferece exemplos e cenários relacionados à sua dimensão, ajudando as equipes a explorar vulnerabilidades que poderiam não ser identificadas por métodos tradicionais [5]. Por exemplo, na dimensão de "Impacto Humano", os cartões podem destacar como violações de segurança podem afetar a privacidade, o bem-estar emocional ou financeiro, fornecendo uma perspectiva mais centrada no usuário [4].

Os Security Cards têm sido utilizados em diversas aplicações, como a proteção de sistemas biométricos contra ataques de apresentação [22]. Sua estrutura flexível permite adaptação a diferentes contextos organizacionais, incluindo ambientes descentralizados. Em organizações horizontais, os Security Cards facilitam a participação de diversos stakeholders, promovendo a governança distribuída e reforçando a colaboração [37].

Apesar de seu potencial, a metodologia pode gerar um número elevado de falsos positivos, o que exige esforço adicional para filtrar ameaças relevantes [4]. No entanto, sua ênfase na criatividade e inclusão de múltiplas perspectivas faz dos Security Cards uma ferramenta valiosa para explorar ameaças emergentes e fortalecer a resiliência organizacional.

3.2.3 Personae Non Grata

Personae Non Gratae (PnGs) representam uma abordagem inovadora para a modelagem de ameaças, destacando-se por seu foco em usuários mal-intencionados e comportamentos indesejáveis [3]. Inspiradas pelas personas tradicionais do design de experiência do usuário, as PnGs ajudam a antecipar como adversários podem explorar vulnerabilidades em um sistema, fornecendo uma perspectiva adversarial detalhada [24].

As PnGs são criadas por meio de técnicas como crowd-sourcing, permitindo que diferentes stakeholders contribuam com insights para a identificação de ameaças [24]. Esta abordagem colaborativa aumenta a abrangência e a diversidade dos perfis de atacantes considerados, permitindo uma modelagem mais robusta e adaptada a diferentes contextos [3].

Uma das principais vantagens das PnGs é sua capacidade de capturar motivações, capacidades e comportamentos específicos de atacantes. Por exemplo, uma PnG pode descrever um adversário que utiliza phishing para obter credenciais ou explora falhas de segurança em transações financeiras [3]. Este nível de detalhamento auxilia na priorização de contramedidas e na alocação de recursos de segurança [24].

Além disso, as PnGs são particularmente eficazes em contextos onde as ameaças internas e externas se sobrepõem. Em organizações horizontais, onde a governança é distribuída e a responsabilidade é compartilhada, as PnGs ajudam a mapear potenciais riscos que podem surgir de atores internos, como colaboradores, ou externos, como competidores [3].

Apesar de seus benefícios, a implementação de PnGs requer esforço significativo para garantir que os perfis sejam precisos e relevantes. No entanto, quando integradas a outras metodologias, como árvores de ataque ou STRIDE, as PnGs oferecem uma camada adicional de análise, tornando-as uma ferramenta indispensável para organizações que buscam compreender e mitigar ameaças de forma abrangente [24].

3.3 Abordagens Híbridas e Colaborativas

As abordagens híbridas e colaborativas buscam integrar diferentes metodologias para criar frameworks adaptáveis e eficazes em contextos variados. Dentre essas, destaca-se o Hybrid Threat Modeling Method (hTMM), que combina elementos de diferentes frameworks para uma análise abrangente de riscos. Ele é particularmente útil em cenários que envolvem múltiplos stakeholders e requerem alinhamento entre objetivos de segurança e prioridades de negócio [25].

Outro exemplo é o Collaborative and Remote Threat Modeling (CoReTM), projetado para facilitar a modelagem de ameaças em equipes distribuídas ou remotas. Utilizando ferramentas colaborativas, como plataformas de anotação compartilhada, o CoReTM torna o processo mais acessível e inclusivo, sendo ideal para organizações horizontais e globais [45].

Por fim, o Participatory Threat Modeling (PTM) promove a inclusão de uma ampla gama de stakeholders no processo de modelagem de ameaças. Esta abordagem valoriza a diversidade de perspectivas, sendo especialmente relevante em contextos descentralizados onde a transparência e a participação coletiva são essenciais [40]. Essas metodologias reforçam a governança distribuída e fortalecem a resiliência organizacional, complementando o trabalho desenvolvido por frameworks mais tradicionais.

3.4 Confiança Descentralizada e Frameworks Criptográficos

3.4.1 COLBAC

O Collective based access control system (COLBAC) é um modelo de controle de acesso projetado para abordar as especificidades de organizações horizontais, promovendo uma abordagem democrática e participativa para a autorização de acessos. Sua proposta busca superar os desafios impostos por modelos tradicionais de controle de acesso, como Discretionary Access Control (DAC), Mandatory Access Control (MAC) e Role-Based

Access Control (RBAC), que frequentemente reforçam dinâmicas hierárquicas inadequadas para estruturas horizontalizadas [8].

Uma das características mais marcantes do COLBAC é sua capacidade de alinhar o controle de acesso às práticas de governança horizontal, permitindo que decisões sejam tomadas coletivamente por meio de processos democráticos. O modelo organiza recursos e processos em três esferas principais: a Esfera Coletiva, que concentra recursos críticos sujeitos à aprovação coletiva; a Esfera do Usuário, que abrange recursos gerenciados individualmente com base em controles tradicionais; e a Esfera Imutável, responsável por armazenar logs e registros de maneira inalterável, assegurando transparência e rastreabilidade [8].

No contexto do COLBAC, interações com a Esfera Coletiva seguem um processo estruturado em três fases: na Fase de Rascunho, o usuário cria um token que especifica as permissões e objetivos da ação; na Fase de Petição, o token é submetido à votação pelos membros da organização; e, finalmente, na Fase de Autorização, os resultados da votação determinam a aprovação ou rejeição da ação, com todos os registros sendo armazenados na Esfera Imutável [8]. Essa estrutura oferece flexibilidade ao permitir a adaptação do nível de horizontalidade de acordo com as necessidades da organização, inclusive em situações de crise que possam demandar centralizações temporárias.

Apesar de suas vantagens, o COLBAC enfrenta desafios inerentes à sua abordagem democrática. Processos de votação frequentes podem resultar em fadiga dos usuários, especialmente em organizações maiores. Além disso, ataques democráticos, como a manipulação de quóruns ou o uso abusivo de tokens de emergência, representam riscos significativos. Tais problemas podem ser mitigados com a implementação de auditorias independentes, ajustes dinâmicos nos critérios de quórum e mecanismos que limitem o uso de tokens de emergência. Outra questão importante é a curva de aprendizado associada ao modelo, que requer familiaridade com práticas democráticas e a compreensão do funcionamento dos tokens [8].

O COLBAC oferece uma solução inovadora para organizações que desejam alinhar sua governança horizontal com práticas robustas de segurança digital. Sua transparência, flexibilidade e compromisso com a participação democrática o posicionam como uma ferramenta estratégica para superar os desafios de segurança em estruturas descentralizadas, transformando potenciais vulnerabilidades em oportunidades para fortalecer a autonomia coletiva.

3.4.2 ABCcrypto

O Asset-Based Cryptocurrency (ABC) é um framework de modelagem de ameaças desenvolvido especificamente para abordar as peculiaridades de criptomoedas e sistemas baseados em blockchain. Em contraste com frameworks generalistas como o STRIDE, o ABC foi projetado para lidar com os desafios de segurança únicos apresentados por sistemas distribuídos e permissionless, onde atores desconfiam uns dos outros e os incentivos

econômicos desempenham um papel central [1].

O principal diferencial do ABC é a introdução de matrizes de conluio (collusion matrices), que permitem analisar cenários de ameaças que envolvem colaborações entre diferentes atores maliciosos. Essa abordagem sistemática reduz a complexidade do processo de modelagem ao eliminar casos irrelevantes e agrupar cenários com efeitos semelhantes. Além disso, o framework utiliza categorias de ameaças específicas para criptomoedas, considerando não apenas os ativos tangíveis, como blockchains e tokens, mas também ativos abstratos, como privacidade e reputação [1].

Uma característica fundamental do ABC é sua capacidade de adaptar as categorias de ameaças aos objetivos e ativos de cada sistema. O processo começa com a caracterização detalhada do modelo de sistema, identificando participantes, ativos e motivações financeiras. Em seguida, categorias de ameaças são derivadas a partir das violações potenciais das propriedades de segurança dos ativos, como corrupção de serviços, roubo de pagamentos e inconsistências na blockchain. Por fim, cenários concretos de ataque são enumerados e analisados por meio da matriz de conluio, que considera todas as combinações possíveis de atacantes e alvos [1].

O ABC também destaca a importância de incorporar análises econômicas e incentivos financeiros no processo de mitigação de riscos. Por exemplo, mecanismos de "detectar e punir" podem ser implementados para desencorajar comportamentos desonestos ao torná-los financeiramente inviáveis. Este uso de teoria dos jogos e modelagem econômica é particularmente eficaz para endereçar ameaças que não podem ser neutralizadas exclusivamente por meios criptográficos [1].

A eficácia do ABC foi demonstrada em estudos de caso envolvendo sistemas reais, como Bitcoin, Filecoin e CacheCash. No caso do Filecoin, o framework revelou lacunas significativas no design público, particularmente em cenários de conluio que não haviam sido previamente considerados. Já no CacheCash, o ABC foi usado desde as etapas iniciais do design para identificar 525 casos de conluio e implementar contramedidas baseadas em incentivos [1].

Embora apresente benefícios claros, o ABC não é isento de desafios. A criação de matrizes de conluio e a análise detalhada de categorias de ameaças podem ser intensivas em termos de recursos, especialmente em sistemas com múltiplos participantes e ativos complexos. No entanto, esses esforços são recompensados pela identificação de ameaças críticas e pela robustez das soluções propostas [1].

O ABC oferece uma abordagem avançada e adaptável para a modelagem de ameaças em criptomoedas, demonstrando que frameworks especializados podem melhorar significativamente a segurança e a resiliência de sistemas distribuídos.

3.4.3 PGP e o Web of Trust

Pretty Good Privacy (PGP), desenvolvido por Philip Zimmermann, é um sistema de criptografia que combina privacidade, autenticação e conveniência para proteger mensagens

e arquivos. O PGP utiliza a criptografia de chave pública para viabilizar a comunicação segura entre indivíduos, mesmo sem confiança prévia ou troca de chaves em canais seguros [28].

No modelo de funcionamento do PGP, cada indivíduo possui um par de chaves — uma pública, amplamente divulgada, e uma privada, mantida em sigilo. A chave pública é utilizada para criptografar mensagens, enquanto a privada é usada para descriptografá-las. Esse esquema não apenas garante a privacidade das mensagens, mas também permite a autenticação por meio de assinaturas digitais, assegurando a integridade e a origem de um conteúdo [28].

Uma característica central do PGP é o modelo de Web of Trust (WoT), que adota uma abordagem descentralizada para a validação de identidades. Diferentemente das hierarquias centralizadas de Autoridades Certificadoras, o WoT permite que qualquer usuário assine digitalmente a chave pública de outro, certificando sua autenticidade. Essas assinaturas criam uma rede de confiança distribuída, na qual a validação de uma chave pública depende da confiança acumulada das assinaturas de outros usuários confiáveis [28].

No PGP, cada usuário pode atribuir diferentes níveis de confiança a outros indivíduos para atuarem como "introdutores confiáveis". Esse mecanismo permite que a rede de confiança seja construída de forma orgânica, refletindo as relações sociais naturais. Por exemplo, um usuário pode confiar plenamente em outro para certificar chaves, ou apenas marginalmente, dependendo de sua percepção sobre a competência e integridade do introdutor [28].

Além de promover a descentralização, a WoT também oferece resiliência contra ataques. Em vez de depender de um único ponto de falha, como ocorre em sistemas centralizados, o WoT permite que os usuários validem chaves públicas com base em múltiplas assinaturas, reduzindo o impacto de compromissos individuais. No entanto, essa abordagem também apresenta desafios, como a dificuldade de gerenciar grandes anéis de chaves e a subjetividade na atribuição de níveis de confiança [28].

A relevância do PGP e da WoT para organizações horizontais é evidente. Estruturas não hierárquicas podem aproveitar a natureza descentralizada do WoT para criar sistemas de segurança alinhados aos princípios de autonomia coletiva e governança distribuída. Ao permitir que cada participante construa sua própria rede de confiança, o PGP reforça a segurança sem comprometer a horizontalidade dessas organizações.

3.5 Perspectivas Comparativas

3.5.1 Critérios de Avaliação

A avaliação de frameworks de modelagem de ameaças requer critérios objetivos para comparar sua eficácia, aplicabilidade e adequação a diferentes contextos organizacionais.

Crítérios fundamentais incluem a capacidade de identificar ameaças específicas, adaptabilidade às mudanças no ambiente operacional, custos de implementação e a integração de dimensões sociais, econômicas e técnicas no processo de modelagem. Além disso, a escalabilidade e a habilidade de lidar com estruturas organizacionais complexas são fatores críticos.

O STRIDE, por exemplo, é amplamente utilizado por sua simplicidade e aplicabilidade em sistemas de software tradicionais. No entanto, ele enfrenta limitações em ambientes descentralizados, como criptomoedas ou organizações horizontais, devido à sua dependência de categorias de ameaças predefinidas. Em contraste, frameworks como o ABC oferecem uma abordagem especializada, utilizando matrizes de conluio para explorar ameaças em sistemas distribuídos e permissionless, enquanto o PASTA foca na avaliação iterativa de riscos para sistemas dinâmicos.

Frameworks como o COLBAC, por outro lado, destacam-se por integrar processos democráticos à modelagem de ameaças, permitindo que organizações horizontais alinhem segurança e governança participativa. Apesar de sua inovação, o COLBAC enfrenta desafios de usabilidade devido à necessidade de familiarização com processos democráticos e o risco de fadiga de votação em grandes grupos. Alternativamente, frameworks como o DREAD, que utiliza uma abordagem quantitativa para priorização de ameaças, podem complementar modelos existentes, embora sua subjetividade possa limitar a eficácia em cenários colaborativos.

Por fim, a escalabilidade é essencial para organizações que lidam com múltiplos participantes e interações complexas. Técnicas como a fusão de cenários no ABC demonstram que frameworks especializados podem mitigar custos operacionais enquanto mantêm a robustez analítica. Isso os torna adequados para sistemas modernos que exigem tanto precisão técnica quanto flexibilidade organizacional.

3.5.2 Aplicabilidade em Organizações Não-Hierárquicas

A aplicabilidade de frameworks de modelagem de ameaças em organizações não-hierárquicas depende de sua capacidade de abordar dinâmicas específicas dessas estruturas. Organizações horizontais operam com base em governança distribuída, participação equitativa e ausência de centralização formal, exigindo abordagens que respeitem e fortaleçam esses princípios.

Frameworks como o COLBAC e o ABC demonstram forte compatibilidade com organizações horizontais devido à sua ênfase em processos colaborativos e adaptabilidade a contextos descentralizados. O COLBAC utiliza tokens de autorização coletiva para alinhar segurança e governança democrática, permitindo flexibilidade entre centralização temporária e controle horizontal. Já o ABC incorpora análise econômica e incentivos financeiros para mitigar riscos em ecossistemas de blockchain, oferecendo ferramentas como matrizes de conluio para mapear cenários de ameaça complexos.

Frameworks tradicionais, como STRIDE e árvores de ataque, fornecem uma base sólida para a identificação de ameaças, mas sua aplicabilidade é limitada em organizações horizontais devido à sua dependência de hierarquias formais e pontos de controle centralizados. Em contraste, abordagens emergentes, como o PTM, promovem maior alinhamento com as necessidades dessas organizações, integrando stakeholders em todas as etapas do processo.

A escolha de um framework para organizações horizontais deve equilibrar eficácia técnica com transparência e engajamento coletivo. Soluções como o ABC e o COLBAC destacam-se ao integrar dimensões sociais e econômicas, demonstrando que a segurança pode ser fortalecida por meio de práticas colaborativas e governança inclusiva. Essas abordagens são particularmente relevantes para organizações que buscam alinhar segurança com autonomia e resiliência organizacional.

4.1 Conceito Preliminar do Protocolo

TODO

4.2 Requisitos de Segurança e Governança

Para garantir que o protocolo atenda às demandas de segurança e governança horizontal, os seguintes requisitos são definidos:

- **Transparência:** Todos os processos de autorização devem ser registrados de forma imutável, permitindo auditorias completas.
- **Participação Democrática:** A tomada de decisão deve ser inclusiva, com processos que permitam contribuições de todos os membros.
- **Flexibilidade:** O protocolo deve suportar mudanças rápidas entre modos de governança centralizados e descentralizados, dependendo das necessidades da organização.
- **Escalabilidade:** Deve ser capaz de operar eficientemente em organizações de diferentes tamanhos e níveis de complexidade.

4.3 Estratégia de Avaliação

A estratégia de avaliação será baseada em estudos de caso e simulações que envolvam cenários realistas de organizações horizontais. O desempenho do protocolo será analisado considerando os seguintes critérios:

- **Eficiência:** Tempo necessário para concluir processos de autorização e tomadas de decisão.
- **Eficácia:** Capacidade de identificar e mitigar ameaças relevantes.

- **Aceitação pelos Usuários:** Facilidade de uso e nível de adoção pelos membros da organização.
- **Resiliência a Ameaças:** Desempenho sob ataques simulados, incluindo manipulações de quórum e falhas de consenso.

4.4 Desenho Experimental

TODO

4.5 Questões de Pesquisa

1. Como o protocolo pode equilibrar eficiência e participação democrática em organizações horizontais?
2. Quais são as melhores práticas para integrar segurança e governança em estruturas descentralizadas?
3. Como o protocolo pode se adaptar a diferentes níveis de horizontalidade e dinâmicas organizacionais?
4. De que forma ele pode melhorar a resiliência contra ameaças internas e externas, mantendo a transparência e a participação inclusiva?

CONCLUSÃO

TODO

PLANO DE TRABALHO

6.1 Tarefas e Milestones

TODO

6.2 Gant Chart

TODO

BIBLIOGRAFIA

- [1] G. Almashaqbeh, A. Bishop e J. Cappos. «ABC: A Cryptocurrency-Focused Threat Modeling Framework». Em: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2019, pp. 859–864. DOI: [10.1109/INFOCOMW.2019.8845101](https://doi.org/10.1109/INFOCOMW.2019.8845101) (ver pp. 2, 3, 6, 18).
- [2] C. W. Blackwell. «Athenian Democracy: An Overview». Em: *Dēmos: Classical Athenian Democracy*. Ed. por C. W. Blackwell. www.stoa.org: The Stoa: A Consortium for Electronic Publication in the Humanities, 2003. URL: <http://www.stoa.org> (ver pp. 3, 8).
- [3] J. Cleland-Huang. «How Well Do You Know Your Personae Non Gratae?» Em: *IEEE Software* 31.4 (2014), pp. 28–31. DOI: [10.1109/MS.2014.85](https://doi.org/10.1109/MS.2014.85) (ver pp. 15, 16).
- [4] J. Cleland-Huang et al. «Keeping Ahead of Our Adversaries». Em: *IEEE Software* 33.3 (2016), pp. 24–28. DOI: [10.1109/MS.2016.75](https://doi.org/10.1109/MS.2016.75) (ver p. 15).
- [5] T. Denning, B. Friedman e T. Kohno. *The Security Cards: A Security Threat Brainstorming Toolkit*. Accessed: 2024-12-09. 2013. URL: <http://securitycards.cs.washington.edu/assets/security-cards-information-sheet.pdf> (ver p. 15).
- [6] J. R. Douceur. «The Sybil Attack». Em: *Peer-to-Peer Systems*. Ed. por P. Druschel, F. Kaashoek e A. Rowstron. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 251–260. ISBN: 978-3-540-45748-0 (ver p. 1).
- [7] *Estatutos da Confederação Geral dos Trabalhadores Portugueses – Intersindical Nacional: Declaração de Princípios e Objectivos Programáticos*. Acesso em: 08 dez. 2024. Confederação Geral dos Trabalhadores Portugueses (CGTP), 2020. URL: <https://www.cgtp.pt/images/images/2020/02/ESTATUTOSCGTP.pdf> (ver p. 10).
- [8] K. Gallagher et al. «COLBAC: Shifting Cybersecurity from Hierarchical to Horizontal Designs». Em: *Proceedings of the 2021 New Security Paradigms Workshop*. NSPW '21. Virtual Event, USA: Association for Computing Machinery, 2022, pp. 13–27. ISBN: 9781450385732. DOI: [10.1145/3498891.3498903](https://doi.org/10.1145/3498891.3498903). URL: <https://doi.org/10.1145/3498891.3498903> (ver pp. 1–4, 6, 8, 10, 17).

- [9] P. Gerbaudo. «Social media teams as digital vanguards: The question of leadership in the management of key Facebook and Twitter accounts of Occupy Wall Street, Indignados and UK Uncut». Em: *Information, Communication & Society* 20.2 (2017), pp. 185–202. DOI: [10.1080/1369118X.2016.1161817](https://doi.org/10.1080/1369118X.2016.1161817). URL: <https://doi.org/10.1080/1369118X.2016.1161817> (ver pp. 1, 8).
- [10] P. Herbst. «Non-Hierarchical Forms of Organization». Em: *Acta Sociologica* 19.1 (1976), pp. 65–75. DOI: [10.1177/000169937601900106](https://doi.org/10.1177/000169937601900106). URL: <https://doi.org/10.1177/000169937601900106> (ver pp. 4, 8).
- [11] S. Hernan et al. *Uncover Security Design Flaws Using The STRIDE Approach*. Accessed: 2024-Dec-09. 2006-11. URL: <https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach> (ver pp. 11, 12).
- [12] M. Howard e S. Lipner. *The Security Development Lifecycle: SDL, a Process for Developing Demonstrably More Secure Software*. Secure software development series. Microsoft Press, 2006. ISBN: 978-07356-2214-2 (ver p. 12).
- [13] S. Hussain et al. «Threat Modelling Methodologies: A Survey». Em: vol. 26. 2014-01, pp. 1607–1609. URL: <https://api.semanticscholar.org/CorpusID:111533730> (ver pp. 1–3).
- [14] R. Jackall e H. M. Levin, eds. *Worker Cooperatives in America*. Berkeley e Los Angeles, California: University of California Press, 1984. ISBN: 0-520-05117-3 (ver pp. 3, 4, 6, 7).
- [15] R. Jiang, J. Luo e X. Wang. «An Attack Tree Based Risk Assessment for Location Privacy in Wireless Sensor Networks». Em: *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*. 2012, pp. 1–4. DOI: [10.1109/WiCOM.2012.6478402](https://doi.org/10.1109/WiCOM.2012.6478402) (ver p. 13).
- [16] R. Jiang et al. «Energy-theft detection issues for advanced metering infrastructure in smart grid». Em: *Tsinghua Science and Technology* 19.2 (2014), pp. 105–120. DOI: [10.1109/TST.2014.6787363](https://doi.org/10.1109/TST.2014.6787363) (ver p. 13).
- [17] A. Kavada. «Creating the collective: social media, the Occupy Movement and its constitution as a collective actor». Em: *Information, Communication & Society* 18.8 (2015), pp. 872–886. DOI: [10.1080/1369118X.2015.1043318](https://doi.org/10.1080/1369118X.2015.1043318). eprint: <https://doi.org/10.1080/1369118X.2015.1043318>. URL: <https://doi.org/10.1080/1369118X.2015.1043318> (ver p. 4).
- [18] A. Kavada e T. Poell. «From Counterpublics to Contentious Publicness: Tracing the Temporal, Spatial, and Material Articulations of Popular Protest Through Social Media». Em: *Communication Theory* 31.2 (2020-10), pp. 190–208. ISSN: 1050-3293. DOI: [10.1093/ct/qtaa025](https://doi.org/10.1093/ct/qtaa025). eprint: <https://academic.oup.com/ct/article-pdf/31/2/190/37900340/qtaa025.pdf>. URL: <https://doi.org/10.1093/ct/qtaa025> (ver p. 1).

- [19] R. Khan et al. «STRIDE-based threat modeling for cyber-physical systems». Em: *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. 2017, pp. 1–6. DOI: [10.1109/ISGT-Europe.2017.8260283](https://doi.org/10.1109/ISGT-Europe.2017.8260283) (ver p. 12).
- [20] J. W. Kuyper e J. S. Dryzek. «Real, not nominal, global democracy: A reply to Robert Keohane». Em: *International Journal of Constitutional Law* 14.4 (2017-01), pp. 930–937. ISSN: 1474-2640. DOI: [10.1093/icon/mow063](https://doi.org/10.1093/icon/mow063). eprint: <https://academic.oup.com/icon/article-pdf/14/4/930/9607155/mow063.pdf>. URL: <https://doi.org/10.1093/icon/mow063> (ver p. 6).
- [21] D. LeBlanc. *DREADful*. Accessed: 2024-Dec-09. 2007-08. URL: https://learn.microsoft.com/en-us/archive/blogs/david_leblanc/dreadful (ver p. 12).
- [22] E. Marasco et al. «Attack Trees for Protecting Biometric Systems Against Evolving Presentation Attacks». Em: *16th Annual IEEE International Conference on Technologies for Homeland Security (HST) 2017*. 2017 (ver p. 15).
- [23] S. Mauw e M. Oostdijk. «Foundations of Attack Trees». Em: *Information Security and Cryptology - ICISC 2005*. Ed. por D. H. Won e S. Kim. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 186–198. ISBN: 978-3-540-33355-5 (ver p. 13).
- [24] N. Mead et al. «Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling». Em: *2017 IEEE 25th International Requirements Engineering Conference (RE)*. 2017, pp. 412–417. DOI: [10.1109/RE.2017.63](https://doi.org/10.1109/RE.2017.63) (ver pp. 15, 16).
- [25] N. R. Mead et al. «A hybrid threat modeling method». Em: *Carnegie Mellon University-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002* (2018) (ver pp. 5, 16).
- [26] S. Myagmar, A. J. Lee e W. Yurcik. «Threat modeling as a basis for security requirements». Em: (2005) (ver p. 5).
- [27] P. Nancy R. Mead. *Advanced Threat Modeling (ATM)*. Rel. téc. Pittsburgh, PA 15213: Carnegie Mellon University, 2017. URL: permission@sei.cmu.edu (ver p. 5).
- [28] P. Zimmermann. *PGP User's Guide, Volume I: Essential Topics*. Revised Edition. PGP Version 2.6.2. Massachusetts Institute of Technology: Phil's Pretty Good Software, 1994. URL: <https://web.pa.msu.edu/reference/pgpdoc1.html> (ver p. 19).
- [29] P. C. Português. *Programa e Estatutos do PCP*. Revisão tipográfica: Edições «Avante!». Lisboa, Portugal, 2013. URL: <https://www.pcp.pt/estatutos-do-pcp> (ver pp. 8, 9).
- [30] B. Potteiger, G. Martins e X. Koutsoukos. «Software and attack centric integrated threat modeling for quantitative risk assessment». Em: *Proceedings of the Symposium and Bootcamp on the Science of Security*. HotSos '16. Pittsburgh, Pennsylvania: Association for Computing Machinery, 2016, pp. 99–108. ISBN: 9781450342773. DOI: [10.1145/2898375.2898390](https://doi.org/10.1145/2898375.2898390). URL: <https://doi.org/10.1145/2898375.2898390> (ver p. 12).

- [31] Y. Saito e J. A. Rose. «Reputation-based Decentralized Autonomous Organization for the Non-Profit Sector: Leveraging Blockchain to Enhance Good Governance». Em: *Frontiers in Blockchain* 5 (2023). ISSN: 2624-7852. DOI: [10.3389/fbloc.2022.1083647](https://doi.org/10.3389/fbloc.2022.1083647). URL: <https://www.frontiersin.org/articles/10.3389/fbloc.2022.1083647> (ver p. 2).
- [32] R. Scandariato, K. Wuyts e W. Joosen. «A Descriptive Study of Microsoft's Threat Modeling Technique». Em: *Requirements Engineering* 20.2 (2015-06), pp. 163–180. ISSN: 1432-010X. DOI: [10.1007/s00766-013-0195-2](https://doi.org/10.1007/s00766-013-0195-2). URL: <https://doi.org/10.1007/s00766-013-0195-2> (ver p. 11).
- [33] B. Schneier. *Attack Trees*. Rel. téc. 12. 1999. URL: <https://tnlandforms.us/cs594-cns96/attacktrees.pdf> (ver p. 13).
- [34] N. Shevchenko et al. «Threat modeling: a summary of available methods». Em: *Software Engineering Institute | Carnegie Mellon University* (2018), pp. 1–24 (ver pp. 1, 6).
- [35] A. Shostack. «Experiences Threat Modeling at Microsoft». Em: *MODSEC@ MoDELS* (2008) (ver p. 5).
- [36] A. Shostack. *Threat modeling: Designing for security*. John Wiley & Sons, 2014 (ver pp. 2, 11–13).
- [37] F. Shull e N. Mead. *Cyber Threat Modeling: An Evaluation of Three Methods*. Carnegie Mellon University, Software Engineering Institute's Insights (blog). Accessed: 2024-Dec-9. 2016-11. URL: <https://insights.sei.cmu.edu/blog/cyber-threat-modeling-an-evaluation-of-three-methods/> (ver p. 15).
- [38] F. Shull et al. *Evaluation of Threat Modeling Methodologies*. Rel. téc. Carnegie Mellon University, Software Engineering Institute, 2016-10. URL: https://insights.sei.cmu.edu/documents/4027/2016_017_001_474200.pdf (ver pp. 1, 6).
- [39] M. A. Sitrin. *Everyday Revolutions: Horizontalism and Autonomy in Argentina*. London, UK; New York, USA: Zed Books Ltd, 2012. ISBN: 9781780320502 (ver pp. 2–4, 8).
- [40] J. Slupska et al. «Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity». Em: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI EA '21. Yokohama, Japan: Association for Computing Machinery, 2021. ISBN: 9781450380959. DOI: [10.1145/3411763.3451731](https://doi.org/10.1145/3411763.3451731). URL: <https://doi.org/10.1145/3411763.3451731> (ver p. 16).
- [41] P. M. Thornton. «Of Constitutions, Campaigns and Commissions: A Century of Democratic Centralism under the CCP». Em: *The China Quarterly* 248.S1 (2021), pp. 52–72. DOI: [10.1017/S0305741021000758](https://doi.org/10.1017/S0305741021000758) (ver pp. 9, 10).
- [42] P. Torr. «Demystifying the threat modeling process». Em: 3.5 (2005), pp. 66–70. DOI: [10.1109/MSP.2005.119](https://doi.org/10.1109/MSP.2005.119) (ver pp. 5, 6).

- [43] Z. Trifa e M. Khemakhem. «Sybil Nodes as a Mitigation Strategy Against Sybil Attack». Em: *Procedia Computer Science* 32 (2014). The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable Energy Information Technology (SEIT-2014), pp. 1135–1140. ISSN: 1877-0509. DOI: <https://doi.org/10.1016/j.procs.2014.05.544>. URL: <https://www.sciencedirect.com/science/article/pii/S1877050914007443> (ver p. 1).
- [44] T. UcedaVelez e M. M. Morana. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons, 2015-05, p. 696. ISBN: 978-0-470-50096-5 (ver pp. 13, 14).
- [45] J. Von Der Assen et al. «CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling». Em: *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. 2022, pp. 189–196. DOI: [10.1109/CSR54599.2022.9850283](https://doi.org/10.1109/CSR54599.2022.9850283) (ver pp. 6, 16).
- [46] L. Winner. «Do Artifacts Have Politics?» Em: *Daedalus* 109.1 (1980), pp. 121–136. ISSN: 00115266. URL: <http://www.jstor.org/stable/20024652> (acedido em 2024-12-08) (ver pp. 3, 7, 9).
- [47] C. Wright. *Worker Cooperatives and Revolution: History and Possibilities in the United States*. Bradenton, Florida, USA: BookLocker.com, Inc., 2014. ISBN: 978-1-63263-432-0 (ver pp. 3, 7, 9).
- [48] W. Xiong e R. Lagerström. «Threat modeling - A systematic literature review». Em: 84 (2019), pp. 53–69. ISSN: 0167-4048. DOI: <https://doi.org/10.1016/j.cose.2019.03.010>. URL: <https://www.sciencedirect.com/science/article/pii/S0167404818307478> (ver p. 7).
- [49] G. Yang. «Still a Century of the Chinese Model? Exploring Dimensions of Democratic Centralism». Em: *Chinese Political Science Review* 1.1 (2016), pp. 171–189. DOI: [10.1007/s41111-016-0005-3](https://doi.org/10.1007/s41111-016-0005-3). URL: <https://doi.org/10.1007/s41111-016-0005-3> (ver pp. 9, 10).

