TENDÊNCIAS EM CIBERSEGURANÇA: uma análise em grupos de discussão

Erick de Oliveira[1]

Rodrigo Franklin Frogeri[2]

RESUMO

O presente trabalho apresenta um relato de experiência sobre tendências em cibersegurança, com o objetivo de analisar, por meio de grupos de discussão, as principais perspectivas, desafios e estratégias emergentes debatidas nesses ambientes virtuais, buscando identificar padrões temáticos e percepções recorrentes relevantes para o setor. A experiência fundamenta-se na literatura recente sobre segurança cibernética e nas interações ocorridas em redes sociais especializadas. Os dados analisados nesta pesquisa englobam posts, interações e debates extraídos de comunidades online dedicadas à cibersegurança, referentes ao período entre 2022 e 2025, totalizando 2.108.803 registros brutos. As informações foram armazenadas em arquivos nos formatos .txt e .csv, provenientes, inicialmente, das comunidades *Reddit* e *Discord*, às quais foram posteriormente adicionadas outras comunidades, com o intuito de ampliar a abrangência da análise. Para o tratamento e a organização dos dados obtidos no processo científico, foi utilizado o *software* IRaMuTeQ (Interface do R para Análises Multidimensionais de Textos e de Questionários), que possibilitou a realização de análises lexicográficas e estatísticas multivariadas no extenso corpus textual obtido. Os resultados ampliam o debate sobre as tendências em cibersegurança, oferecendo novas perspectivas acerca dos desafios, práticas e impactos observados em ambientes virtuais especializados. As análises indicaram que estes espaços funcionam como espaços de aprendizado colaborativo e desenvolvimento profissional. Observou-se a centralidade de termos ligados à segurança, ao trabalho e ao conhecimento, refletindo o equilíbrio entre dimensões técnicas e formativas. As discussões abordaram desde práticas de defesa digital até trajetórias de carreira, evidenciando a integração entre teoria e prática no setor.

---

[1] Graduando em Bacharelado em Sistemas de Informação no Centro Universitário do Sul de Minas.

[2] Doutor em Sistemas de Informação e Gestão do Conhecimento. Docente no Centro Universitário do Sul de Minas - UNIS. rodrigo.frogeri@professor.unis.edu.br

Palavras-chave: Tendências em cibersegurança. Grupos de discussão. Análise lexicográfica. Segurança cibernética.

1 INTRODUÇÃO

Na atual era digital, a cibersegurança consolidou-se como um tema essencial para a sociedade e para as organizações, em função do aumento da sofisticação e da recorrência das ameaças no ambiente virtual (Sharma et al., 2024). O cenário tecnológico contemporâneo destaca-se pela ampla adoção de redes de fibra óptica, que impulsionam a interconectividade global e o expressivo avanço nas velocidades de transmissão de dados (Paliwal, 2025). Esse movimento é potencializado pelo surgimento das redes móveis de quarta e quinta geração (4G e 5G), que não só ampliam a capacidade de integração de bilhões de dispositivos e oferecem suporte às crescentes demandas de conectividade da sociedade (Salahdine et al., 2023), como também expandem a exposição e a complexidade da segurança digital.

Incidentes cibernéticos podem causar perdas financeiras, responsabilidades legais, violações de privacidade e danos à reputação, afetando também a segurança nacional e a continuidade de operações estratégicas (Falowo et al., 2022).

No cenário atual de cibersegurança, os grupos online de discussão representam espaços colaborativos essenciais para troca de conhecimento entre profissionais, pesquisadores e entusiastas da área (Wu et al., 2021). A cooperação entre esses integrantes e o compartilhamento de experiências são fundamentais para identificar e compreender ameaças cibernéticas, viabilizando a adoção rápida e eficaz de medidas preventivas e corretivas. Nesse contexto, a instituição de mecanismos destinados ao intercâmbio de dados desempenha papel estratégico no fortalecimento das capacidades de segurança e na promoção de um ecossistema cibernético mais resiliente e confiável (Kanca et al., 2021).

Assim, este estudo tem como objetivo analisar as principais tendências em cibersegurança discutidas em grupos online de comunidades virtuais especializadas, buscando compreender as discussões e os direcionamentos atuais no campo da segurança cibernética. A questão central que orientou esta análise foi: Quais são as principais tendências em cibersegurança discutidas em grupos online?

Espera-se que os resultados deste estudo proporcionem uma compreensão das preocupações e discussões emergentes sobre o tema da cibersegurança. Os resultados obtidos podem contribuir para que profissionais desenvolvam iniciativas proativas em sintonia com as tendências atuais. No âmbito acadêmico, tais achados podem revelar temáticas emergentes, fornecendo bases para o aprofundamento de pesquisas.

2 DINÂMICA EVOLUTIVA DAS AMEAÇAS DIGITAIS

A *internet* atual, caracterizada por sua rapidez e eficiência, teve origem em um projeto denominado ARPANET (*Advanced Research Projects Agency Network*), desenvolvido em 1969 pela Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos, destinado a interligar centros de pesquisa e universidades (WALDEN, 2019). Nestas redes que precederam a internet, na década de 1970, a segurança não era uma preocupação central, pois tais estruturas funcionavam em ambientes restritos, experimentais e sob controle institucional. (SILVA, 2023).

A ARPANET operava inicialmente com o *Network Control Protocol* (NCP), mas, à medida que a rede se expandia, tornou-se necessária a adoção de um protocolo mais flexível e escalável, surgia assim, em 1983 o TCP/IP (*Transmission Control Protocol/Internet Protocol*) por proposição de Robert Kahn e Vinton Cerf (IEEE COMMUNICATIONS SOCIETY, 2025) que, incorporado à ARPANET, possibilitou a interconexão de múltiplas redes independentes.

O avanço contínuo da internet acarretou o surgimento de novos riscos e vulnerabilidades, sendo o *Morris Worm*, em 1988, um marco nesse contexto, reconhecido como o primeiro *malware* de grande impacto, infectando aproximadamente 10% dos sistemas conectados à rede (FBI, 2018).

As primeiras iniciativas de segurança incluíam a implementação de *firewalls* básicos, a criação de equipes de resposta a incidentes (CERTs), a utilização de senhas locais e criptografia, esta última restrita a ambientes militares ou acadêmicos (RADWARE, s. d.). Paralelamente, surgiram os primeiros antivírus comerciais (ISLAM et al., 2025), ainda que a conscientização sobre segurança ainda fosse restrita entre usuários comuns, evidenciando a necessidade de maior educação digital e práticas mais robustas de proteção.

No início da década de 1990, Tim Berners-Lee, então pesquisador do Conselho Europeu para a Pesquisa Nuclear (CERN) desenvolveu a *World Wide Web* (WWW),

integrando conceitos de hipertexto e protocolos TCP/IP e DNS (*Domain Name System*), estabelecendo uma forma padronizada de acessar e compartilhar informações através da *internet* (CERN, 2019).

Empresas começaram a oferecer serviços online, originando assim o comércio eletrônico com pioneiros como *Amazon* e *eBay* marcando uma nova era de interatividade e negócios digitais (Ntumba et al., 2023).

A difusão da rede entre usuários leigos propiciou o surgimento dos primeiros vírus de macro, como *Concept* (1995) e *XM/Laroux* (1996), demonstrando como documentos do *Word* e planilhas *Excel* podiam ser usados para propagar *malwares* através de macros, destacando sua vulnerabilidade (TREND MICRO, 2015). No mesmo período, surgiram os primeiros ataques de engenharia social, impulsionados pelo desenvolvimento do *software AOHell*, o qual automatizou ataques de roubo de senhas, dando origem ao termo *phishing* (REKOUCHE, 2011).

Com o intuito de resguardar as transações online, a rede passou a adotar o protocolo HTTPS (*HyperText Transfer Protocol Secure*), baseado em SSL (*Secure Sockets Layer*) (NETSCAPE COMMUNICATIONS CORPORATION, 2025) ao passo em que os *firewalls* evoluíram, adquirindo maior sofisticação.

Com o surgimento da Web 2.0 e a "explosão" de dados ocorrida na primeira década dos anos 2000, a *internet* passou a assumir um caráter altamente interativo, transformando a forma como indivíduos e organizações se relacionam, promovendo a colaboração social e a inteligência coletiva, e oferecendo novas oportunidades para engajar os usuários de maneira mais efetiva (MURUGESAN, 2007).

Redes sociais, *blogs*, *wikis* e serviços em nuvem surgiram como plataformas centrais para comunicação, colaboração e aprendizagem, com destaque para sistemas como *Facebook*, *YouTube* e *Twitter*, permitindo que usuários compartilhem informações, criem conteúdos coletivos e participem ativamente de comunidades digitais (HSU, 2014).

À época, embora as medidas de segurança se concentrassem na proteção de redes, transações e *malwares,* elas não acompanhavam o crescimento do número de usuários e do tráfego de rede, sendo que, no primeiro semestre de 2004, foram identificadas mais de 1.200 vulnerabilidades em *softwares*, quase 5.000 vírus e *worms* e um aumento de *botnets* de 2.000 para mais de 30.000 casos, ampliando o impacto de ameaças como *spyware*, *spam* e *phishing* (SYMANTEC, 2004, apud WIRED, 2004).

O aumento da volumetria de dados favoreceu ataques DDoS (*Distributed Denial of Service*) como o ocorrido contra a empresa *Yahoo!*, que manteve seu sistema inoperante pelo período de 2 horas, causando perdas publicitárias e evidenciando a necessidade de estratégias de segurança mais sofisticadas e políticas robustas de proteção da informação (PRINCETON, 2003).

Com a difusão da *internet* móvel e a consolidação da computação em nuvem, a conectividade tornou-se plenamente portátil, viabilizada por *smartphones* e redes de alta velocidade, como a rede móvel 4G (LORENZI et al., 2022). Concomitantemente, a difusão do conceito de computação em nuvem, materializado por plataformas como *AWS*, *Microsoft Azure e Google Cloud,* possibilitou que usuários e empresas armazenassem e processassem dados remotamente, redefinindo o paradigma da infraestrutura digital (LORENZI et al., 2022).

Entretanto, o crescimento exponencial dos dispositivos móveis aumentou a incidência de ataques direcionados a aplicativos, incluindo a disseminação de *malwares* específicos para as plataformas *Android* e *iOS*, que exploram vulnerabilidades e executam ações maliciosas (ASHAWA et al., 2021).

Vazamentos massivos de dados atingiram redes sociais e empresas de grande porte como o *Yahoo!* e *LinkedIn* (WIRED, 2016), o que levou ao surgimento de normas e regulamentações de proteção de dados como o GDPR (*General Data Protection Regulation*) na Europa e a LGPD (Lei Geral de Proteção de Dados) no Brasil.

Impulsionada pela ascensão da *Internet* das Coisas (IoT), a conectividade deixou de ser restrita somente a computadores e dispositivos móveis, englobando uma ampla variedade de dispositivos do cotidiano e do setor industrial, tais como câmeras de segurança, veículos e sensores industriais (GEORGAKOPOULOS, 2016).

A tecnologia móvel 5G, ao ampliar de forma significativa tanto a velocidade de transmissão quanto a densidade das conexões, favoreceu a configuração de um ecossistema digital altamente complexo e interconectado (ZHENG et al., 2019).

Na cibersegurança, novos desafios emergiram com ataques a dispositivos IoT, como evidenciado pela *Mirai Botnet* (ANTONAKAKIS et al., 2017), revelando vulnerabilidades decorrentes de configurações inadequadas.

A segurança digital passou a ser estratégica, com governos e empresas reconhecendo ataques cibernéticos como ameaças nacionais, de modo que a proteção deixou de ser uma

preocupação exclusivamente corporativa, para se tornar uma questão de soberania nacional (COMPUTER WEEKLY, 2025).

A Inteligência Artificial (IA) passou a ser aplicada tanto na defesa, com a detecção de comportamento anômalo, autenticação e controle de acesso, quanto no ataque viabilizando *phishing* e *spoofing* automatizados, geração assistida de *malwares* e ataques DDoS baseados em IA (GAO, 2024).

De acordo com estudos recentes, a expansão da *internet* e a evolução da cibersegurança ocorreram de forma interdependente, uma vez que o aumento da conectividade, da complexidade das redes e da interatividade online impulsionou também o desenvolvimento de mecanismos de defesa cada vez mais sofisticados, baseados em prevenção, governança e tecnologias emergentes (BOUMAN et al., 2023).

3 MATERIAIS E MÉTODOS

Para alcançar o objetivo proposto neste estudo, optou-se por uma abordagem descritiva, qualitativa e observacional, concentrando-se na análise indireta de conteúdos textuais produzidos espontaneamente em ambientes online (ex. grupos de discussão) sem qualquer tipo de interferência, mediação, sugestão ou interação nos debates estabelecidos pelos participantes, por parte do pesquisador.

A obtenção dos dados concentrou-se nas plataformas *Reddit e Discord*, eleitas por abrigarem comunidades digitalmente engajadas e intensamente ativas no âmbito da segurança cibernética. O período analisado compreendeu os anos de 2022 a 2025. A delimitação inicial das comunidades selecionadas apoiou-se em recomendações de entidades de referência na área de cibersegurança, tais como o portal *medium.com*, que menciona a comunidade *TryHackMe Community* no *Discord*, e o portal *guardz.com*, que destaca a comunidade *r/netsec* no *Reddit*. Essas comunidades foram, portanto, adotadas como núcleo inicial da investigação, sendo posteriormente incluídos grupos abertos ou de acesso público, com objetivo de ampliar o corpus textual e abarcar discussões representativas sobre cibersegurança (A listagem completa de comunidades pode ser consultada no repositório da pesquisa, disponível em: https://drive.google.com/drive/folders/1sXojwXfSZSoIvfutBQ9067QDGsA0J46Z?usp=drive_link). Comunidades fechadas, como servidores privados ou grupos restritos, foram

excluídas, considerando-se as limitações de acesso e a necessidade de se preservar princípios éticos e de transparência na coleta e análise de dados.

Para a plataforma *Reddit*, a coleta de dados foi realizada por meio de *scripts* desenvolvidos em linguagem *Python* (ver respositório da pesquisa em: https://drive.google.com/drive/folders/1sXojwXfSZSoIvfutBQ9067QDGsA0J46Z?usp=drive_link), utilizando a biblioteca PRAW (*Python Reddit API Wrapper*, versão 7.8.1), elaborado e executado em ambiente *vscode* (*Visual Studio Code* versão 1.103.0 *system setup*). O uso dessas ferramentas e ambientes possibilitou o acesso direto e o *download* das publicações e comentários da comunidade *r/netsec*, bem como as demais comunidades que integraram a base de dados organizadas no formato *Excel* (.csv). Quanto à plataforma *Discord*, a coleta de dados foi conduzida por meio da ferramenta *DiscordChatExporter* (versão 2.46.0) que possibilitou a exportação completa das mensagens do servidor *TryHackMe Community,* bem como dos servidores complementares que compuseram a base de dados, organizadas em arquivos no formato texto (.txt). A base de dados coletada encontrava-se em língua inglesa, e a análise foi conduzida neste idioma, a fim de preservar a terminologia técnica e o sentido original das expressões. Após o processo de formatação, detalhado a seguir, o corpus textual resultante apresentou um arquivo de 4,54 MB, contendo um total de 831.838 palavras e 22.404 formas distintas.

Os dados provenientes das comunidades e servidores analisados foram submetidos a um procedimento de organização por meio de *scripts* elaborados em linguagem *Python* (ver repositório da pesquisa em: https://drive.google.com/drive/folders/1sXojwXfSZSoIvfutBQ9067QDGsA0J46Z?usp=drive_link). Esse procedimento incluiu a remoção de linhas em branco, URLs, *emojis* e demais conteúdos irrelevantes, ao mesmo tempo em que preservou frases contendo termos relacionados à cibersegurança. Esses termos foram selecionados com base em dicionários e *frameworks* amplamente reconhecidos na literatura da área, como MITRE ATT&CK, OWASP, NIST e SANS, os quais definem conceitos, técnicas, vulnerabilidades, ferramentas e práticas consolidadas entre profissionais de segurança (CYBERTZAR, 2023). A seleção buscou contemplar as principais categorias da cibersegurança, incluindo autenticação e controle de acesso, *malware* e ataques, engenharia social, vulnerabilidades e explorações, técnicas de defesa e ataque, segurança em redes e nuvem, ferramentas e plataformas, práticas de *Blue/Red/Purple Team*, certificações e tendências contemporâneas. Dessa forma, foi

possível construir um corpus filtrado, relevante e tecnicamente robusto, garantindo que a análise textual capturasse informações representativas do domínio da cibersegurança nas postagens analisadas.

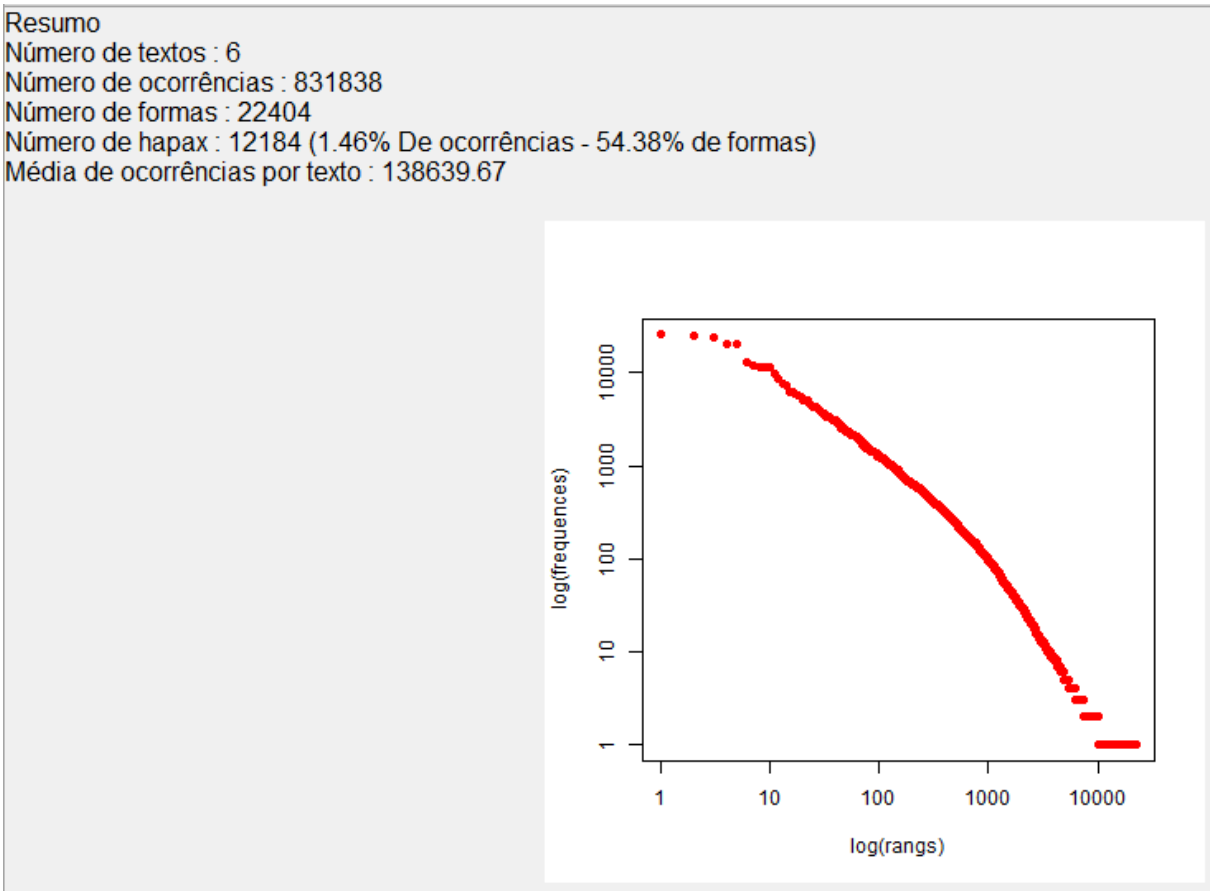
A preparação e a formatação do corpus textual seguiram as orientações apresentadas na documentação oficial IRaMuTeQ, particularmente no que diz respeito à exclusão de conteúdos indesejados e a padronização do arquivo segundo as exigências do sistema (IRaMuTeQ, [s.d.]).

As análises realizadas foram efetivadas utilizando o *software* IRaMuTeQ (versão 0.8 alpha 7), ferramenta de código aberto desenvolvida na linguagem R, reconhecida no meio acadêmico por sua solidez metodológica na análise estatística e textual de dados qualitativos (SOUZA, 2021). Dentre os recursos analíticos mobilizados, salientam-se a Análise de Similitude, a Nuvem de Palavras e a Classificação Hierárquica Descendente (CHD) de *Reinert*, procedimentos que possibilitaram a identificação de padrões lexicais subjacentes, a recorrência de termos significativos e a sistematização de categorias temáticas emergentes a partir do corpus examinado. O emprego destas três técnicas se justifica pela complementaridade de suas abordagens, pois, enquanto a Nuvem de Palavras fornece uma visão imediata dos termos mais frequentes, a Análise de Similitude evidencia as relações semânticas entre eles, e a CHD organiza o corpus em classes temáticas coerentes, permitindo uma análise aprofundada das discussões. Neste sentido, tais recursos têm sido aplicados de forma conjunta em estudos que utilizaram o *software* IRaMuTeQ para análise de textos complexos (SANTOS et al., 2017).

4 RESULTADO E DISCUSSÃO

As análises iniciais possibilitaram a visualização de um primeiro panorama quantitativo, totalizando 6 textos, 831.838 palavras e 22.404 formas distintas. Identificaram-se 12.184 hapax (termos que aparecem uma vez), o que representa 1,46% das ocorrências e 54,38% das formas únicas. Além disso, observou-se uma média de aproximadamente 138.639 palavras por texto (ver Figura 1).

Figura 1: Resumo estatístico do corpus



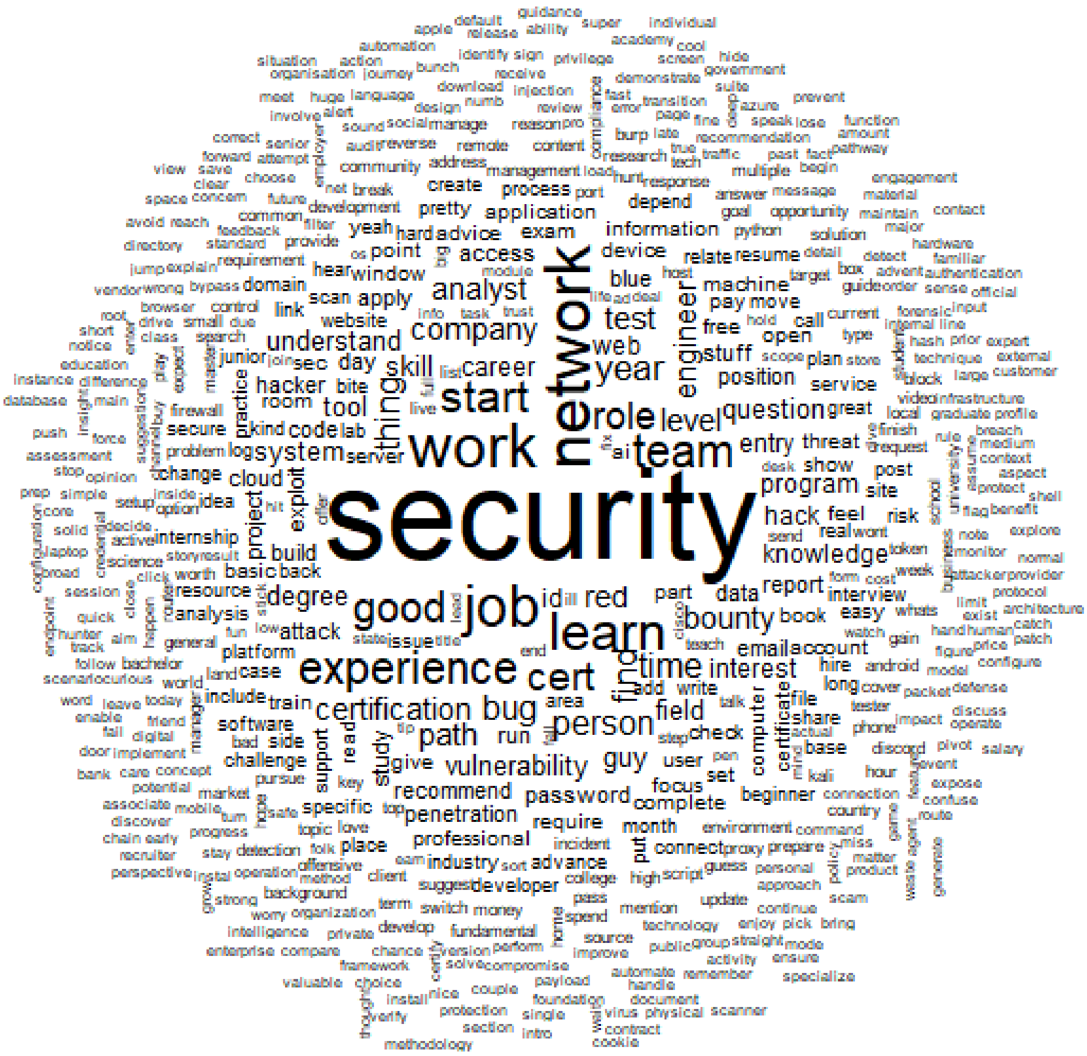
Fonte: Elaborado pelo autor a partir do *software* IRaMuTeQ (2025)

Para compreender a estrutura e os temas predominantes do corpus, foram utilizadas três técnicas complementares do software IRaMuTeQ: análise de nuvem de palavras, análise de similitude e classificação hierárquica descendente (CHD). Isso permitiu uma exploração mais detalhada e organizada do conteúdo textual, conforme seções a seguir.

4.1 Análise por Nuvem de Palavras

A visualização dos termos mais comuns no corpus foi realizada por meio de uma nuvem de palavras, ilustrada na Figura 2. Essa técnica permite identificar graficamente os termos mais frequentes, evidenciando os conceitos que predominam nos textos analisados.

Figura 2: Nuvem de palavras



Fonte: Elaborado pelo autor a partir do *software* IRaMuTeQ (2025)

A análise da nuvem de palavras evidencia a predominância de vocábulos como *security*, *work, network, job e learn*, indicando que as interações nas comunidades digitais estão fortemente orientadas para aspectos técnicos e profissionais da cibersegurança. O termo *security*, com 7.381 ocorrências, destaca a centralidade das discussões voltadas à proteção de sistemas, identificação de riscos e mitigação de vulnerabilidades. Já *network*, com 3.238 ocorrências, revela a relevância da construção de conexões e da colaboração entre membros da comunidade. Em seguida, *work* com 3.098 e *job* com 2.835, evidenciam o interesse dos participantes nas dinâmicas do mercado de trabalho e nas oportunidades profissionais em

tecnologia. Por fim, *learn,* com 2.549 ocorrências, reforça o caráter formativo desses espaços, voltados à aquisição de conhecimento técnico, compartilhamento de experiências e aprimoramento contínuo de habilidades.

A presença de termos como *team*, *experience*, *cert* e *start* evidencia diferentes dimensões das interações nas comunidades digitais de cibersegurança. O termo *team* destaca a importância do trabalho colaborativo e da troca de conhecimentos entre profissionais e aprendizes. *Experience* indica que os usuários valorizam relatos práticos e a partilha de vivências profissionais, que auxiliam no desenvolvimento de competências técnicas.

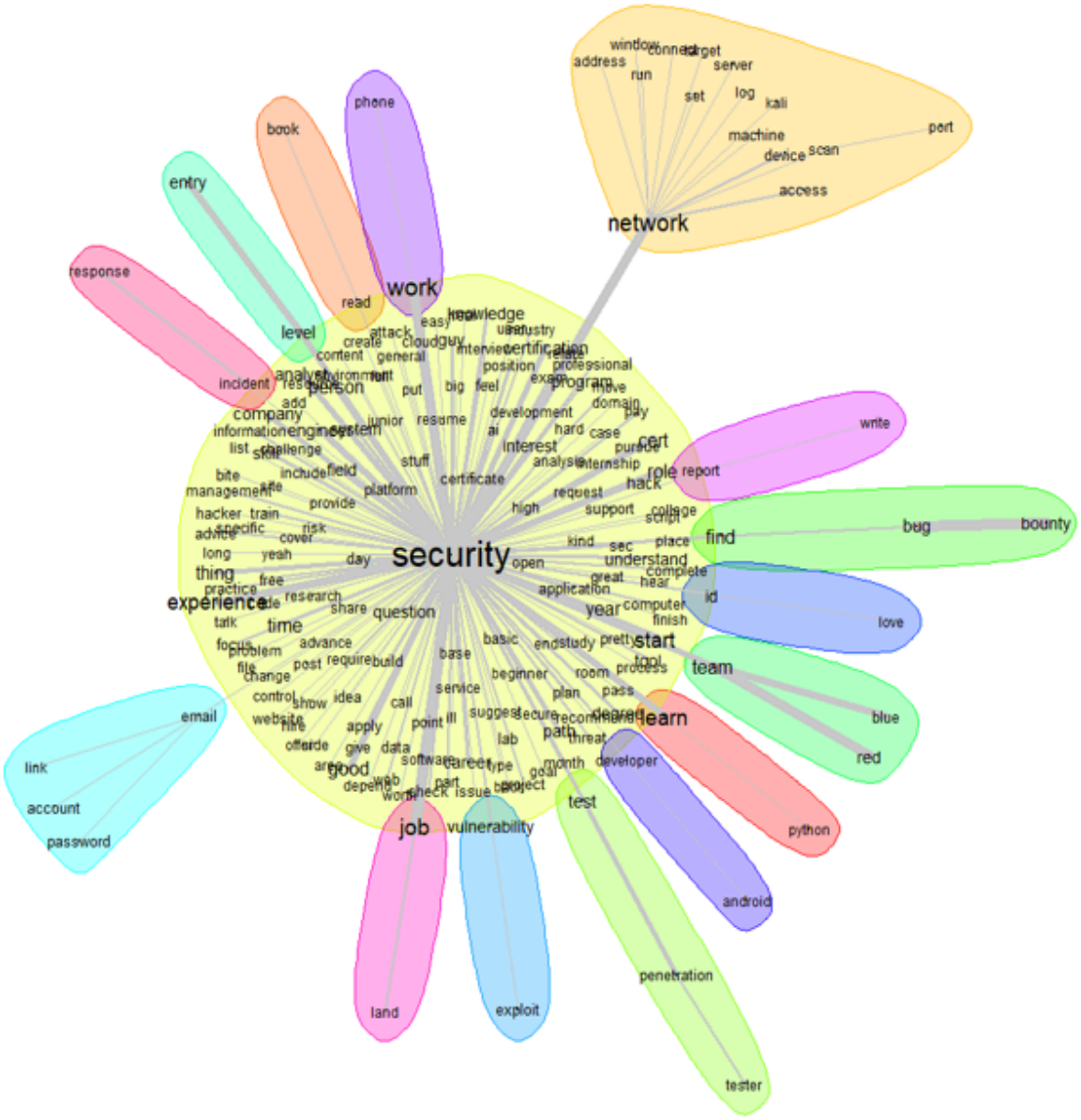
Cert remete às certificações profissionais, mostrando que essas conquistas são vistas como marcos importantes de qualificação e reconhecimento na carreira. Por fim, *start* evidencia o interesse de muitos participantes em iniciar sua trajetória na área da cibersegurança.

Assim, a presença recorrente desses termos sugere que os fóruns e comunidades analisados atuam como ambientes híbridos, nos quais aprendizado, prática profissional e networking se articulam de forma integrada, funcionando como espaços relevantes para o compartilhamento de conhecimento, a discussão de vulnerabilidades e a disseminação de boas práticas no campo da cibersegurança (WU et al., 2021).

4.2 Análise de Similitude

A análise de similitude, realizada a partir do corpus textual e apresentada na Figura 3, evidenciou a centralidade do termo *security*, que se destaca como núcleo semântico do conjunto, articulando-se com diferentes campos lexicais. Essa centralidade indica que o conceito de segurança constitui o eixo em torno do qual se organizam os principais temas abordados nas discussões, evidenciando sua relevância e refletindo a natureza multidisciplinar da cibersegurança, que exige a integração de conhecimentos técnicos especializados, práticas educacionais colaborativas e uma forte conexão com o mercado de trabalho (FURNELL, 2021).

Figura 3: Análise de Similitude



Fonte: Elaborado pelo autor a partir do *software* IRaMuTeQ (2025)

Entre os agrupamentos periféricos, observa-se o campo relacionado a *network*, associado a palavras como *machine*, *port*, *device*, *scan* e *access* remetendo a aspectos técnicos da infraestrutura de redes e à proteção de sistemas, demonstrando a ênfase em práticas voltadas à administração e à defesa de ambientes computacionais.

Os agrupamentos de *work* e *job* sugerem a presença de discursos voltados à atuação profissional e à aplicação prática dos conhecimentos adquiridos, já o polo formado pelo agrupamento *learn* e *start*, revelam o interesse dos participantes por processos de aprendizado inicial e formação técnica. O agrupamento formado por *vulnerability* e *exploit*

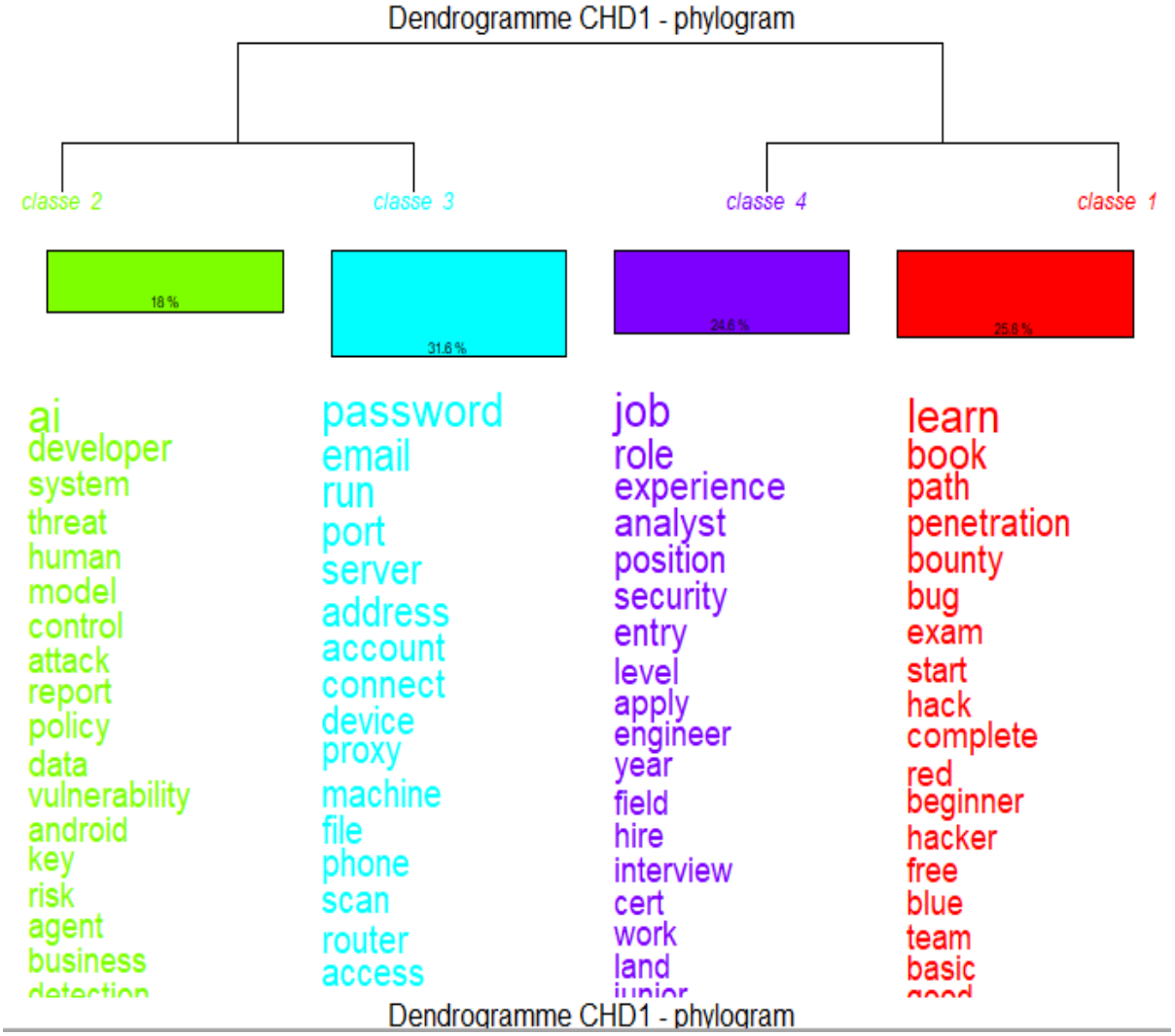
reflete a dimensão prática da cibersegurança nas comunidades estudadas, onde a troca de conhecimento não se limita a conceitos teóricos, mas envolve o desenvolvimento de competências aplicadas, como identificação e exploração ética de falhas, que fortalecem o aprendizado técnico e a preparação para o mercado de trabalho. Por sua vez, os termos *team* e *find* aparecem vinculados a *bug*, *bounty* e *report*, remetendo à colaboração em equipe e à cultura de programas de recompensa por vulnerabilidades (*bug bounty*), aspectos que destacam a dimensão cooperativa e aplicada das atividades de cibersegurança.

Conclui-se que as discussões analisadas se organizam em dimensões técnica, educacional e profissional, evidenciando que as comunidades de cibersegurança atuam como espaços híbridos de aprendizado, prática e desenvolvimento profissional. Os termos mais recorrentes, como *network, vulnerability, exploit, learn, start, experience, work, job* e *company*, refletem esta organização. Essa associação reforça o papel das comunidades digitais como espaços de capacitação e troca de conhecimento entre iniciantes e profissionais experientes (GROSS et al., 2021).

4.3 Classificação Hierárquica Descendente de *Reinert* (CHD)

A análise da Classificação Hierárquica Descendente, identificou quatro agrupamentos distintos de mensagens no corpus, definidos a partir das proximidades lexicais entre os termos, que evidenciam os principais eixos temáticos abordados pelos participantes das comunidades digitais de cibersegurança. A Figura 4 apresenta o dendrograma resultante da segmentação, destacando os conceitos e discussões predominantes nos grupos analisados.

Figura 4: Dendograma da classificação hierárquica descendente de Reinert (CHD)



Fonte: Elaborado pelo autor a partir do *software* IRaMuTeQ (2025)

A seguir, descrevem-se as quatro classes obtidas a partir do corpus, considerando a estrutura do dendrograma apresentado na Figura 4 e suas respectivas análises.

4.3.1. Classe 1 – Formação e prática de aprendizagem

Esta Classe, responsável por 25,8% do corpus analisado, reúne termos como *learn*, *book*, *path*, *penetration, bounty, exam*, *start*, *beginner*, e *basic*. O conjunto lexical indica que essa classe está associada à dimensão formativa e prática da aprendizagem em cibersegurança, com ênfase no aprendizado técnico inicial e na experimentação prática.

O termo *learn*, núcleo central da classe, evidencia que o discurso dos participantes gira em torno da aquisição de conhecimento , característica típica de comunidades voltadas ao aprendizado colaborativo (FISK et al., 2023) Vocábulos como *book*, *path* e *exam* sugerem a presença de recursos educacionais, rotas de aprendizado (*learning paths*) e avaliações de certificação, já a presença dos termos *penetration*, *bug*, *hack* e *bounty* demonstra o foco prático da aprendizagem, com ligação a atividades de simulação e prática ética de invasão de sistemas.

4.3.2. Classe 2 – Inteligência artificial e proteção

A análise lexical da Classe 2, que corresponde a 18% do corpus, evidencia discussões centradas na relação entre inteligência artificial e proteção de sistemas. Os termos mais recorrentes *ai*, *developer*, *system*, *threat*, *human, model*, *control, attack* e *vulnerability* revelam preocupações técnicas, abordando modelos de IA e proteção de sistemas e dados.

Vocábulos como *ai*, *developer*, *system* e *threat* indicam discussões ligadas ao desenvolvimento de modelos de inteligência artificial, sugerindo aprendizado de máquina aplicado à segurança (PROTIVITI, 2025). Outros termos relevantes como *attack*, *vulnerability*, *risk* e *detection,* refletem preocupações com ameaças cibernéticas e mitigação de riscos, típicas de contextos de segurança ofensiva e defensiva.

4.3.3. Classe 3 – Infraestrutura e credenciais

A Classe 3, que representa 31,6% do corpus textual, sugere um núcleo temático voltado à infraestrutura técnica e à segurança de credenciais, conforme evidenciado pela frequência dos termos *password*, *email* e *account*, que remetem à autenticação e à proteção da identidade digital. A presença de palavras como *run*, *file* e *scan* sugere ações operacionais e análise de sistemas, possivelmente vinculadas a práticas de monitoramento e detecção de ameaças. Além disso, a ocorrência de *port*, *server*, *router*, *proxy*, *device* e *machine* evidencia foco em aspectos de conectividade e configurações de rede, fundamentais para o gerenciamento seguro de ambientes digitais. Termos como *connect*, *access* e *address* complementam esse campo semântico, apontando para interações entre usuários e sistemas, incluindo processos de autenticação e controle de acesso. Em conjunto, essa classe reflete

uma dimensão fortemente técnica das discussões sobre cibersegurança, voltada à proteção da infraestrutura e à gestão segura de identidades e dispositivos conectados (LIMA et al., 2022).

4.3.4. Classe 4 – Trabalho e carreira

Compondo 24,6% do corpus textual, a Classe 4 demonstra discussões relacionadas ao mercado de trabalho e ao desenvolvimento de carreira em cibersegurança. Os termos mais frequentes, tais como *job, role, experience, analyst, position, security, engineer, field, hire, interview, cert* e *work*, evidenciam que esta classe reflete o interesse dos participantes em oportunidades profissionais, recrutamento e progressão na carreira dentro do campo de segurança da informação. A presença dos vocábulos *entry* e *junior* indicam a ênfase em posições iniciais ou de entrada, enquanto *cert* e *interview* sinalizam discussões sobre certificações profissionais e processos seletivos. Termos como *experience*, *role* e *position* reforçam a importância de adquirir experiência profissional e compreender responsabilidades específicas em diferentes cargos de cibersegurança. Esse padrão indica que a comunidade analisada valoriza a preparação para o emprego, o aprendizado prático e a progressão em carreiras técnicas, reforçando a interdependência entre conhecimento teórico e aplicação prática no campo da segurança da informação (TOWHIDI; PRIDMORE, 2023).

Para compilar os resultados da análise, desenvolveu-se o Quadro 1:

Quadro 1. Compilados dos achados da pesquisa

Classe	**Tema central**	**Abordagens emergentes**	**Relevância para o setor**
Classe 1 – Formação e prática de aprendizagem (25,8%)	Aprendizagem técnica inicial e prática em cibersegurança	Uso de simulações (*pentest* ético, *bug bounty*), estudo por livros e certificações, comunidades de aprendizagem.	Fundamento para o desenvolvimento de profissionais qualificados, especialmente em níveis iniciais.
Classe 2 – Inteligência artificial e proteção (18,0%)	Integração entre IA e segurança cibernética	Aplicação de *machine learning* em segurança ofensiva e defensiva; desenvolvimento de modelos seguros e controláveis.	Resposta às ameaças emergentes impulsionadas pela evolução tecnológica; inovação em defesa cibernética.
Classe 3 – Infraestrutura e credenciais (31,6%)	Segurança da infraestrutura técnica e gestão de identidades digitais	Monitoramento contínuo, escaneamento de vulnerabilidades, boas práticas de rede e autenticação.	Base técnica essencial para a segurança de ambientes digitais corporativos e pessoais.

Classe 4 – Trabalho e carreira (24,6%)	Mercado de trabalho e desenvolvimento profissional em cibersegurança	Preparação para entrevistas, obtenção de certificações, busca por *roles* específicas (ex: *analyst, engineer*).	Reflete a profissionalização do campo e a demanda por profissionais qualificados e certificados.

Fonte: Desenvolvidos pelos autores.

A Classe 3 é a mais representativa do *corpus*, destacando a centralidade da infraestrutura e gestão de identidades nas discussões de cibersegurança. As quatro classes, em conjunto, revelam uma interdependência entre formação, prática técnica, inovação tecnológica e carreira.

5 CONSIDERAÇÕES FINAIS

O presente estudo buscou analisar as tendências, padrões e aspectos conceituais presentes em comunidades digitais voltadas à cibersegurança. A partir das análises realizadas, foi possível identificar os principais eixos temáticos que estruturam as interações nesses ambientes, revelando que esses ambientes não apenas funcionam como espaços de troca de informações técnicas, mas também como ecossistemas formativos e profissionais, em que o aprendizado, a colaboração e o desenvolvimento de carreira se complementam.

De forma geral, os resultados sugerem que a comunidade analisada se orienta tanto por necessidades educacionais quanto por demandas profissionais e operacionais. Os padrões temáticos identificados (ex. análise CHD) são consistentes com tendências globais no setor, como a ascensão da IA em segurança, a escassez de talentos e o foco em cyber-higiene básica (ex: senhas, autenticação). Observamos que as comunidades *online* de cibersegurança desempenham um papel importante na formação de profissionais e na difusão de conhecimento técnico. Elas operam como ambientes colaborativos, nos quais teoria e prática se articulam, aprendizado contínuo e *networking* se integram, e o desenvolvimento profissional é estimulado. Tais espaços configuram redes de ensino informal e podem promover não apenas a capacitação técnica, mas também o engajamento social e profissional, fomentando uma cultura colaborativa e dinâmica no campo da segurança da informação.

Para o campo prático, acredita-se que este estudo contribui para reflexões sobre o futuro da cibersegurança ao demonstrar que a construção de competências não depende

apenas de ensino formal, mas também envolve interações *online*, colaboração e troca contínua de conhecimento. Ao mapear essas dinâmicas, o estudo oferece subsídios para estratégias educacionais, políticas organizacionais e práticas profissionais que podem fortalecer a segurança digital de forma proativa e sustentável.

Para pesquisas futuras, recomenda-se ampliar o *corpus* de análise, incorporando comunidades multilíngues e outros fóruns relevantes e referenciados ainda não explorados no campo da cibersegurança. Além disso, sugere-se a utilização combinada de métodos quantitativos e qualitativos, de modo a aprofundar a compreensão sobre a produção, validação e disseminação do conhecimento técnico.

TRENDS IN CYBERSECURITY: an analysis of online discussion communities

ABSTRACT

This study presents an experience report on trends in cybersecurity, aiming to analyze, through discussion groups, the main perspectives, challenges, and emerging strategies debated in these virtual environments, seeking to identify thematic patterns and recurring perceptions relevant to the field. The experience is grounded in recent literature on cybersecurity and in interactions that occurred within specialized social networks. The data analyzed in this research include posts, interactions, and debates extracted from online communities dedicated to cybersecurity, covering the period between 2022 and 2025, totaling 2,108,803 raw records. The information was stored in .txt and .csv files, initially collected from Reddit and Discord communities, to which other communities were later added to broaden the scope of the analysis. For data processing and organization, the IRaMuTeQ software (Interface for Multidimensional Analysis of Texts and Questionnaires) was used, enabling lexicographic and multivariate statistical analyses of the extensive textual corpus. The results expand the discussion on cybersecurity trends, offering new perspectives on the challenges, practices, and impacts observed in specialized virtual environments. The analyses indicated that these spaces function as environments for collaborative learning and professional development. A centrality of terms related to security, work, and knowledge was observed, reflecting a balance between technical and formative dimensions. The discussions ranged from digital defense practices to career paths, highlighting the integration between theory and practice in the field.

Palavras-chave: Cybersecurity trends. Discussion groups. Lexicographic analysis. Cybersecurity.

REFERÊNCIAS

ANTONAKAKIS, M. et al. **Understanding the Mirai Botnet.** USENIX Security Symposium, 2017. Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

ASHAWA, Moses; MORRIS, Sarah. **Analysis of Mobile Malware: A Systematic Review of Evolution and Infection Strategies.** 2021. Disponível em: https://www.researchgate.net/publication/357432557_Analysis_of_Mobile_Malware_A_Systematic_Review_of_Evolution_and_Infection_Strategies

BOUMAN, Erwin; VAN EETVELDE, Guido. **Tracing the evolution of cyber resilience: a historical and conceptual review.** International Journal of Information Security, v. 23, p. 239–264, 2023. DOI: https://doi.org/10.1007/s10207-023-00811-x

CERN. **The birth of the Web**. Disponível em: https://home.cern/science/computing/birth-web

COMPUTER WEEKLY. **A nova Estratégia Nacional de Cibersegurança reconhece que "a proteção eficaz requer coordenação entre governo, setor privado e sociedade civil"**. Disponível em: https://www.computerweekly.com/br/reportagen/Por-que-a-gestao-inteligente-de-vulnerabilidades-virou-questao-de-Estado-no-Brasil

CYBERTZAR. **Cyber risk management frameworks.** Cybertzar, 27 jan. 2023. Disponível em: https://cybertzar.com/cyber-risk-management-frameworks

FBI. **The Morris Worm: 30 Years Since First Major Attack on the Internet.** Disponível em: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Falowo, O., Popoola, S., Riep, J., Adewopo, V., & Koch, J. **Tenacidade dos Atores de Ameaças em Disrupção: Análise de Grandes Incidentes de Segurança Cibernética.** IEEE Access, 10, 134038-134051, 2022. https://doi.org/10.1109/ACCESS.2022.3231847

Fisk, N. (2023). **Cybersecurity communities of practice: Strategies for creating gateways to participation.** Computers & Security, 103188. https://doi.org/10.1016/j.cose.2023.103188

FURNELL, S. **The cybersecurity workforce and skills.** Technology in Society, v. 64, p. 101479, 2021. DOI: https://doi.org/10.1016/j.techsoc.2020.101479

GAO, Yukai. **Ataques cibernéticos e defesa: abordagens e técnicas baseadas em IA.** Revista Acadêmica de Computação e Ciência da Informação, v. 7, n. 7, p. 41-46, 2024. Disponível em: https://doi.org/10.25236/AJCIS.2024.070706

Georgakopoulos, D.; Jayaraman, P. **Internet das coisas: do sensoriamento em escala da internet aos serviços inteligentes.** Computação, v. 98, p. 1041–1058, 2016. Disponível em: https://doi.org/10.1007/s00607-016-0510-0

Gross, M.; Ho, S. M. (2021). **Collective Learning for Developing Cyber Defense Consciousness: An Activity System Analysis.** Journal of Information Systems Education, v. 32, n. 1, p. 65-76. Disponível em: https://jise.org/Volume32/n1/JISE2021v32n1pp65-76.pdf

HSU, Y.; CHING, Y.; GRABOWSKI, B. **Aplicações e práticas da Web 2.0 para aprendizagem por meio da colaboração.** In: [s.l.], 2014. p. 747-758. Disponível em: https://doi.org/10.1007/978-1-4614-3185-5_60

IEEE COMMUNICATIONS SOCIETY. **TCP design published.** IEEE Communications Society, 2025. Disponível em: https://www.comsoc.org/node/19581

IRaMuTeQ. **Formatage des corpus texte**. [s.l.]: IRaMuTeQ, [s.d.]. Disponível em: http://www.iramuteq.org/documentation/formatage-des-corpus-texte

ISLAM, M.; LI, X. **Guardiões da Web: A evolução e o futuro da segurança da informação em sites**. 2025. Disponível em: https://arxiv.org/abs/2505.04308

Kanca, A., & Sağiroğlu, Ş. **Compartilhando Inteligência e Colaboração sobre Ameaças Cibernéticas.** Conferência Internacional sobre Segurança da Informação e Criptologia de 2021 (ISCTURKEY), 167-172. 2021. https://doi.org/10.1109/ISCTURKEY53027.2021.9654328

LIMA, Paulo Ricardo Silva; FERREIRA, Leonardo Matheus Marques; PEIXOTO, Ana Lydia Vasco de Albuquerque. **Gestão da segurança da informação: análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira**. P2P – Perspectivas em Políticas Públicas, v. 9, n. 1, p. 206–221, 2022

LORENZI, U. M.; GREIN, W. B.; CORCINI, L. F. **Computação em nuvem: conceitos, aplicações e novas tecnologias.** Revista das Faculdades Santa Cruz, v. 13, n. 1, 2022. Disponível em: https://periodicos.unisantacruz.edu.br/index.php/revusc/article/view/8

MURUGESAN, S. **Compreendendo a Web 2.0. Profissional de TI**, v. 9, 2007. Disponível em: https://doi.org/10.1109/MITP.2007.78

NETSCAPE COMMUNICATIONS CORPORATION. **What is HTTPS**? Disponível em: https://www.akamai.com/glossary/what-is-https

NTUMBA, C.; AGUAYO, S.; MAINA, K. **Revolucionando o varejo: uma minianálise da evolução do e-commerce.** Revista de Marketing e Comunicação Digital, 2023. Disponível em: https://doi.org/10.53623/jdmc.v3i2.365

PALIWAL, D. **Comunicação por fibra óptica. Revista Internacional de Pesquisa Científica em Engenharia e Gestão**, 2025. Disponível em: https://doi.org/10.55041/ijsrem47650

PRINCETON. **Distributed Denial of Service (DDoS) Survey Pape**r. Princeton University, 2003. Disponível em: https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSSurveyPaper_20030516_Final.pdf

PROTIVITI. **Avanços e riscos da inteligência artificial na cibersegurança.** 2025. Disponível em: https://www.protiviti.com.br/cybersecurity/avancos-e-riscos-da-inteligencia-artificial-na-cibersegurança/

RADWARE. **A history of network security.** [S. l.], [s. d.]. Disponível em: https://www.radware.com/resources/network_security_history.aspx

REKOUCHE, H. **Early phishing**. arXiv preprint, arXiv:1106.4692, 2011. Disponível em: https://arxiv.org/abs/1106.4692

SALAHDINE, F.; HAN, T.; ZHANG, N. **5G, 6G e além: avanços recentes e desafios futuros.** Annals of Telecommunications, p. 1-25, 2023. Disponível em: https://doi.org/10.1007/s12243-022-00938-3

SANTOS, A. R.; SILVA, B. L.; OLIVEIRA, C. M. **Uso do software IRaMuTeQ na análise da produção científica sobre decisões judiciais.** Anais da ANPAD, 2017. Disponível em: https://anpad.com.br/uploads/articles/120/approved/6a13382a520e0420014027350a0b3eb4.pdf

SHARMA, S.; AGRAWAL, S.; KUMAR, S. **Desvendando horizontes da cibersegurança: explorando tecnologias, estratégias e tendências de ponta no cenário dinâmico de ameaças cibernéticas.** In: CONFERÊNCIA INTERNACIONAL SOBRE COMPUTAÇÃO INTELIGENTE E TECNOLOGIAS DE COMUNICAÇÃO EMERGENTES (ICEC), 2024, 2024. Anais… p. 1-6. Disponível em: https://doi.org/10.1109/ICEC59683.2024.10837210

SILVA, Michel Bernardo Fernandes da. **Cibersegurança: uma visão panorâmica sobre a segurança da informação na internet.** Rio de Janeiro: Freitas Bastos, 2023. E-book. Disponível em: https://plataforma.bvirtual.com.br

SOUZA, Y. S. O. **O uso do software IRAMUTEQ: fundamentos de lexicometria para pesquisas qualitativas.** Estudos e Pesquisas em Psicologia, v. 21, esp., p. 1541–1560, 2021. DOI: 10.12957/epp.2021.64034

SYMANTEC. **Internet Security Threat Report.** Relatório semestral, 1º semestre de 2004. Disponível em: https://www.wired.com/2004/09/symptoms-of-our-3/

TOWHIDI, G.; PRIDMORE, J. **Alinhando a cibersegurança no ensino superior com as necessidades da indústria**. Journal of Information Systems Education, v. 34, n. 1, p. 70–83, 2023. Disponível em: https://jise.org/Volume34/n1/JISE2023v34n1pp70-83.html

TREND MICRO. **20 Years of Macro Malware: From Harmless Concept to Targeted Attacks.** 31 jul. 2015. Disponível em: https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/20-years-of-macro-malware-from-harmless-concept-to-targeted-attacks

WALDEN, D. **50º aniversário da ARPANET comemorado na Reunião Anual da AAAS de 2019**. Anais da História da Computação do IEEE, v. 41, p. 61-63, 2019. Disponível em: https://doi.org/10.1109/MAHC.2019.2913715

WIRED. **Symptoms of Our Time, Part One.** Wired, 22 set. 2004. Disponível em: https://www.wired.com/2004/09/symptoms-of-our-3/

WIRED. **The biggest hacks of 2016**. 2016. Disponível em: https://www.wired.com/story/biggest-hacks-2016

Wu, M., Aranovich, R., & Filkov, V. **Evolução e diferenciação das comunidades de segurança cibernética em três sites sociais de perguntas e respostas: uma análise de métodos mistos**. PLoS ONE, 16, 2021. https://doi.org/10.1371/journal.pone.0261954

WU, Shaosong; ARANOVICH, Robert; FILKOV, Vladimir. **Community and Discussion Dynamics in Reddit Security Forums**. University of California, 2021. Disponível em: https://escholarship.org/uc/item/7c57s7m9

Zheng, Z.; Xiao, M.; Xiao, Y.; Pang, Z.; Vucetic, B. **Comunicação sem fio de alta confiabilidade e baixa latência para a Internet das Coisas: desafios, fundamentos e tecnologias facilitadoras.** IEEE Internet of Things Journal, v. 6, p. 7946–7970, 2019. Disponível em: https://doi.org/10.1109/JIOT.2019.2907245