SOLUÇÃO INTEGRADA PARA ANÁLISE E MONITORAMENTO DE REDES EMPRESARIAIS

Mateus Oliva Soares[1], **Marcelo Marchioro Cordeiro**[1], **Erico Hoff do Amaral**[1], **Gabriel Haab**[2]

[1]Universidade Federal do Pampa (UNIPAMPA)
– Bagé – RS – Brazil

[2]Microchip Technology – Chandler – Arizona – U.S.A

{mateusoliva,marcelocordeiro}.aluno@unipampa.edu.br,

ericoamaral@unipampa.edu.br,gabrielhaab@gmail.com

Abstract. *Computer network security consists of strategies administrators adopt to protect the network against threats, for example, intrusion attempts, brute force attacks, and port scanning. Thus, it is observed in the business scope the indispensability of establishing security standards to ensure data integrity. The current project aims to build a* software *capable of centralizing and managing the primary security needs of computer networks. In addition, it is envisaged to make available, through this tool, incident alerts and a proactive way to reduce the impacts caused by different anomalies in computer networks.*

Resumo. *A segurança de redes de computadores consiste em um conjunto de estratégias adotadas pelos administradores para a proteção contra ameaças, por exemplo, tentativa de invasão, ataques de força bruta, escaneamento de portas, entre outros. Desse modo, observa-se no âmbito empresarial, a imprescindibilidade do estabelecimento de padrões de segurança para prover a garantia da integridade dos seus dados. O presente trabalho tem como objetivo a construção de um* software *capaz de centralizar e gerir as principais necessidades de segurança no âmbito de redes de computadores. Além disso, vislumbra-se disponibilizar, através dessa ferramenta, alertas de incidentes e uma forma proativa para a redução dos impactos causados por diferentes anomalias nas redes de computadores.*

1. Introdução

A segurança dos dados que trafegam na Internet é um assunto recorrente, considerando o aumento do uso de dispositivos computacionais para a execução de atividades do dia-a-dia e de âmbito profissional. Segundo [Izumi and Tomazeti 2019] a "Segurança da Informação mostrou-se necessária para a preservação de todas as categorias de informações que circulam nas redes sociais e na Internet, assim como, manter a integridade das mesmas".

Em decorrência das medidas sanitárias para controle da pandemia da COVID-19, houveram mudanças na configuração do modelo de trabalho das empresas, substituindo majoritariamente as atividades presenciais para um modelo em *home office*. É indiscutível que antes da crise sanitária mundial, as atividades remotas ou um modelo *home office* eram

crescentes, contudo o processo foi acelerado de modo a preservar a saúde dos colaboradores, conforme afirma [Bridi et al. 2020]. Ainda em relação à segurança, a privacidade de dados vem ganhando cada vez mais atenção, o que esta claro pela implementação e publicação da Lei Geral de Proteção de Dados (LGPD), obrigando, desta forma, as organizações a ampliarem os investimentos em segurança da informação.

Ao entender esse panorama, algumas considerações devem ser realizadas, como o entendimento sobre as falhas no monitoramento das redes empresariais e, também sobre a necessidade da identificação de formas pertinentes para a resolução destes problemas. É necessário discutir métodos de controle, capazes de prover e suprir as necessidades básicas de segurança em redes de computadores, tendo como referência o crescente número de serviços online e a proteção de todos os recursos de TI das organizações.

Tendo em vista o aumento nos casos de crimes cibernéticos a proposta deste estudo é o desenvolvimento de um software capaz de integrar ferramentas de segurança abstraindo a complexidade inerente as configurações destas soluções. Além disso, prover recursos mínimos de proteção para empresas do segmento SMB (Small and Medium Business), principalmente organizações que não possuam um departamento de segurança em TI. Sendo assim, tem-se a questão norteadora deste estudo: É possível a implementação de uma solução de software integrada para o monitoramento de redes de computadores, que disponibilize uma interface de controle centralizada, permitindo o maior controle do ambiente e a inserção de respostas proativas aos incidentes de segurança no âmbito de pequenas e médias empresas?.

O presente artigo apresenta a seguinte organização: uma contextualização do tema nesta introdução. Na Seção 2 são apresentados os métodos de pesquisa empregados no trabalho e as etapas de desenvolvimento do mesmo. Seguindo para a Seção 3 é apresentado a proposta do software que será desenvolvido e a definição dos seus requisitos. Na Seção 4 são apresentados as tecnologias definidas para o desenvolvimento do protótipo, seguido pela Seção 5 onde são demostrado a funcionalidade da ferramenta na sua fase atual de desenvolvimento, além do resultado de um teste realizado com a mesma. Por fim a Seção 6 é destinada a apresentação das conclusões da proposta e sua viabilidade.

2. Materiais e Métodos

A proposta deste trabalho é implementar uma solução capaz de centralizar e gerir as principais necessidades de segurança no âmbito das redes de computadores empresariais. Desse modo, a metodologia adotada é de natureza aplicada. Na pesquisa aplicada, o pesquisador busca orientação prática à solução imediata de problemas concretos do cotidiano, conforme afirmam [da Silveira Barros and de Souza Lehfeld 2014]. A definição do problema de pesquisa foi implementada a partir do entendimento da necessidade de segurança no ambiente de redes das empresas de pequenos e médio porte. A metodologia de pesquisa e as etapas do projeto pode ser visualizada na Figura 1.

Esta pesquisa também pode ser classificada como um método indutivo, a base dos objetivos adotada foi caracterizada como exploratória, pois visa entender o problema de pesquisa e suas possíveis soluções, através de estudo de casos já existentes e de suas bases bibliográficas. A abordagem do problema deverá ser quali-quantitativo, o método quantitativo se aplica na obtenção de valores gerados pelas ferramentas de monitoramento, as quais permitem a conversão dos dados coletados em gráficos para os usuários e, quali-

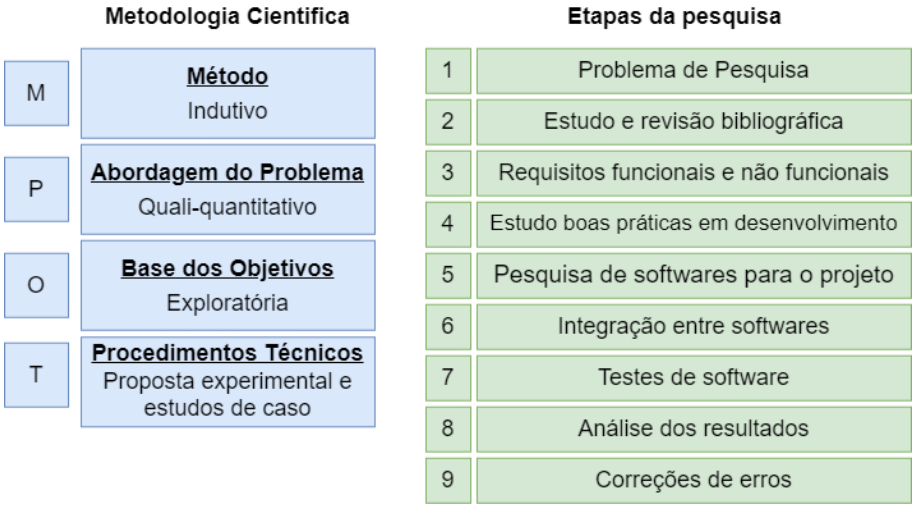

Figura 1. Metodologia Cientifica e Etapas de pesquisa

tativa na busca de uma relação entre esses dados, à proporção que usa como base para criação de alerta para a rede. Por fim, em relação aos procedimentos técnicos esse estudo se qualifica como uma pesquisa experimental e estudo de caso.

O objetivo da pesquisa será alcançado com amparo de estudos de casos e pesquisas em periódicos relacionados a área de segurança. Os requisitos para implementação da solução de monitoramento integrada estarão diretamente relacionados com as principais demandas de segurança identificadas no referencial teórico estudado.

Para alcançar os objetivos o presente projeto foi organizado em etapas, onde a primeira é caracterizada pela delimitação do problema de pesquisa, o qual foi identificado a partir do entendimento da necessidade de padrões de segurança e escassez de investimento nesta área pelas organizações. A etapa 2 compreende o estudo e revisão bibliográfica sobre o problema de pesquisa. Por sua vez, a etapa 3 corresponde ao levantamento de requisitos, o qual deverá contemplar as principais necessidades de segurança voltadas para o ambiente de redes das organizações. O conjunto de informações resultantes desta etapa permitirá a construção da arquitetura de uma solução para o problema de pesquisa. Na quarta etapa será realizado um estudo sobre técnicas e padrões de desenvolvimento para a construção do sistema de monitoramento integrado. A etapa 5 se destinará ao estudo de ferramentas e tecnologias que poderão ser empregadas para a implementação do *software*. Na etapa 6, após o estudo das ferramentas serão configurados os serviços necessários para integração entre as diferentes ferramentas elencadas para este estudo, além da definição do frontend/backend da aplicação. Os testes, análise de resultados nas etapas 7,8 respectivamente. Ao final, na nona etapa será realizado correções de erros e ajustes necessários identificado nos testes realizados.

3. Solução integrada para análise e monitoramento de redes empresarias

O objetivo deste trabalho de pesquisa é implementar uma solução capaz de centralizar e gerir as principais necessidades de monitoramento e segurança no âmbito de redes de computadores, definindo as principais métricas de monitoramento de redes, sendo capaz de prover o mínimo de segurança ao ambiente. Conforme, [Kamienski et al. 2005] a vigilância constante do sistema e da rede promove uma maior segurança para empresas.

A coleta destes dados permite a realização da uma análise minuciosa dos sistemas com o objetivo de de expor vulnerabilidades de segurança.

Contudo, não apenas a atividade de monitoramento é o foco deste trabalho, assim como, a proposição maneiras proativas para o tratamento de incidentes ou anomalias identificadas na rede.

3.1. Proposta de uma arquitetura para integração de soluções para monitoramento de redes de computadores

Com o objetivo de criar uma proposta para atender o problema de pesquisa foi realizado um estudo teórico com o objetivo de reconhecer diferentes tecnologias de redes e, a partir do resultado desta atividade, propor um conjunto de ferramentas capazes de fornecer dados pertinentes e, com uma integração viável. O conjunto de soluções identificadas em um primeiro momento focavam no controle e monitoramento das redes, contudo uma pesquisa sobre soluções de *firewall* também foi realizada, buscando a integração deste tipo de ferramenta ao projeto, como um recurso proativo para viabilização das demandas de segurança desta proposta. Como resultado destas atividades é demonstrado na Figura 2 o protótipo da arquitetura sugerida, a qual é composta por 3 camadas *frontend*, *backend* e módulos.

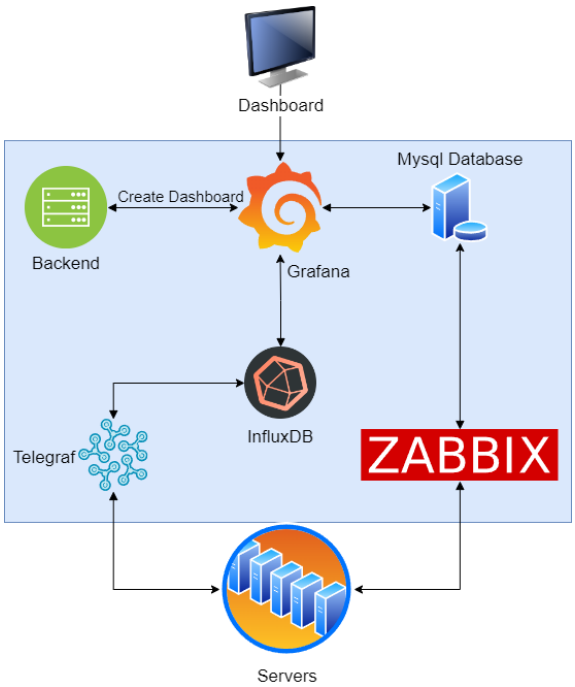

Figura 2. Arquitetura proposta

Na camada de *frontend* é disponibilizada a área de interação do usuário com o software, permitindo de forma simples o monitoramento da rede através desta interface. O foco na implementação deste recurso é oferecer ao administrador do sistema um *dashboard* simples e de complexidade reduzida, que permita a estes profissionais realizarem o controle da rede de uma forma eficiente e otimizada. Como destaque na interface gráfica do *frontend* cita-se a área de alertas para anomalias ou incidentes, que possibilitarão ao usuário identificar em tempo real problemas na rede. Estes alertas serão gerados a partir da análise e cruzamento de informações de *logs* geradas pelas ferramentas

integradas no sistema. Pretende-se ainda, por meio da *dashboard* prover ao usuário controle sobre a configuração de alertas. A segunda camada do *software* proposto, o backend, será responsável pelas principais atividades da ferramenta, fornecendo uma API de comunicação para realização de configurações de Firewall, criação de dashboard automatizados e inserção de novos hosts para serem monitorados. Também, caso seja necessário, o mesmo realizará o tratamento de todos os dados coletados (logs), normalizando os mesmo e gerando informações pertinentes para serem apresentadas através do *dashboard* da solução. A interpretação destes dados pelo usuário permitirá a geração de diferentes alertas, além da possibilidade de integração de regras de *firewall*, para garantir o nível de segurança esperado desta solução. A camada 3 disponibilizará todos os recursos necessários para que as diferentes ferramentas de monitoramento e de *firewall* possam ser instaladas e integradas a presente proposta. Todas as configurações e ajustes nesta camada serão realizadas de forma automatizada, ou seja, este recurso permitirá aos administradores de redes um reduzido nível de interação com o *software*, facilitando o processo de monitoramento da rede.

4. Implementação do protótipo

Realizado o estudo sobre as tecnologias e definição da arquitetura do projeto, deu-se o início da implementação do protótipo. Na sequência foi realizado a instalação dos *softwares* de monitoria e *dashboard*. Para a configuração da solução utilizou-se a documentação oficial das ferramentas Zabbix, Ntop e Grafana. Vale salientar, que simultaneamente a instalação foram desenvolvidos *scripts* para a automatização destes processos.

A solução vislumbra propor uma interface para configuração e visualização das regras de *firewall*, monitoramento das interfaces de redes e dos recursos de hardware. Observa-se que os dados coletados já estão sendo expostos no Grafana, entretanto a configuração destes ocorre de forma manual. Posteriormente, a camada de *backend* será responsável por realizar essas etapas, além de ser capaz de detectar novos *hosts* e produzir uma *dashboard* correspondente.

Analisando o protótipo da *dashboard* desenvolvida (Figura 3) observa-se métricas e logs de identificação do trafego e protocolos na interface de rede, juntamente com a identificação do *host* monitorado utilizando seu *hostname*.

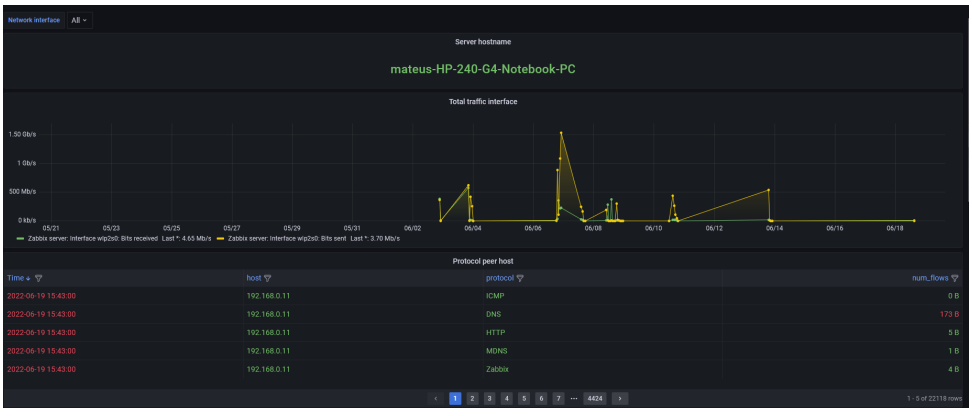

Figura 3. Dados coletados na Dashboard

Descrevendo os próximos painéis presente na *dashboard* (Figura 4) é possível

identificar informações do sistema operacional, como total de alertas da ferramenta Zabbix, informações do número de usuários logados no sistema, total de tempo de *uptime*, atividades de bloqueio do Firewall e total de atividades no registro de logs do Firewall.

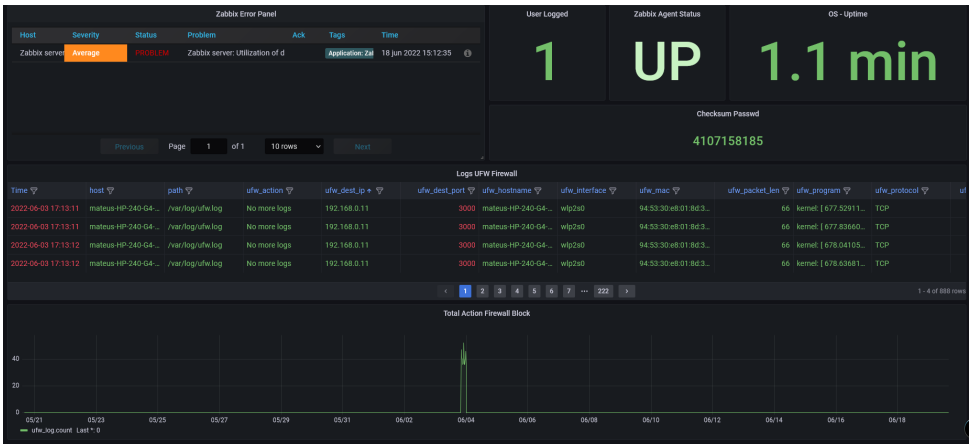

Figura 4. Dados coletados na Dashboard métricas de SO

Deste modo, a visualização deste dados de forma centralizada é possível através integração realizadas das ferramentas Zabbix, Ntop e Grafana. Com isso, é garantido aos administradores um aumento de produtividade, além da identificação rápida de incidentes de segurança, pois as principais informações sobre a rede estarão disponibilizadas em uma única solução.

Entretanto, este projeto prevê um nível de flexibilidade que permitirá a integração de novos recursos de monitoramento e segurança, assim como, a adição de outros painéis no *dashboard*, disponibilizando métricas relevantes para os operadores.

5. Resultados e Discussões

Com o protótipo desenvolvido, observou-se sua capacidade de prover a coleta de métricas da rede e *hardware*, bem como fornecer ao usuário uma interface gráfica centralizada para a visualização dos dados apurados. Além disso, os resultados obtidos podem ser analisados de forma geral ou especifica, por exemplo, o trafego total da rede e o trafego de uma interface de rede, respectivamente. Nesse sentido, para os dados de *hardware* coletados é exibido: utilização de CPU, memória principal e unidades de armazenamento. Portando, a análise vislumbra uma monitoria absoluta dos sistemas. Dessa forma, com a finalidade de validar de detecção das ameaças pela ferramenta foi realizado a simulação de um ataque do tipo DDoS utilizando o *software* Raven-Storm Toolkit [1]. Sendo assim, estruturou-se um plano de testes sobre uma arquitetura hipotética, apresentada na Figura 5.

Dessa maneira, a arquitetura é composta por um computador denominado atacante, o qual possui o *software* Raven-Storm Toolkit instalado e está fora da rede monitorada. Ademais, essa organização é constituída também por outros 2 computadores conectados na mesma rede, sendo que apenas 1 contém o *software* de monitoramento integrado

[1]O software Raven-Storm Toolkit está disponível no Github e pode ser acessado pelo link: https://github.com/Tmpertor/Raven-Storm

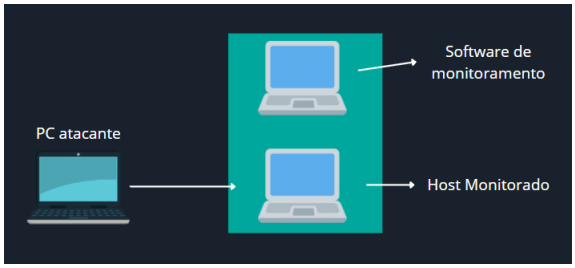

Figura 5. Arquitetura do laboratório de testes

e o outro receberá o ataque. Dessa maneira, na Figura 6, é possível perceber a estabilidade da rede até o início do ataque, tendo em vista o inicio do ataque foi possível observar o aumentou de forma acelerada na quantidade de dados recebidos na rede. Nesse instante, se o alerta estivesse habilitado para esse gráfico analisado, os administradores receberiam informações acerca do estado da rede.

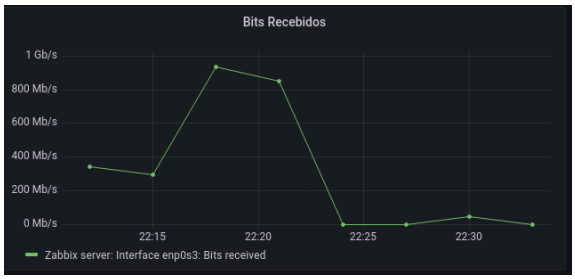

Figura 6. Gráfico do trafego de rede

No entanto, nesse cenário de protótipo, o desenvolvimento de funções da camada de *backend*, o qual realizaria a resposta ativa ao incidente através de regras de *firewall*, ainda não foram desenvolvidas, visto que estará compondo a versão final do projeto. Diante dessa perspectiva, observa-se com o fim do ataque, há normalização do tráfego de dados na rede. A partir do protótipo, percebe-se que a integração de ferramentas amplia as possibilidades de um *software*, centralizando a coleta de dados e entregando ao usuário uma aplicação completa e de fácil utilização, pois transfere a responsabilidade de configuração e instalação para os processos automatizados. Por fim, o modelo não dispõe de todas as funções propostas para a implementação final, sendo necessário principalmente o desenvolvimento da camada *backend* para realizar as devidas organizações e automatização de processos. Ademais, posteriormente, necessita-se realizar uma pesquisa por novas tecnologias que extendam as funcionalidades desta solução. Logo, serão agregadas ao projeto final recursos para respostas ativa a incidentes, implementação da camada do *backend*, criação de *dashboards* automatizadas e uma interface gráfica provendo a configuração do *firewall*.

6. Conclusão

Este estudo tem como objetivo o projeto e desenvolvimento de um software capaz de centralizar e gerir as principais necessidades de monitoramento e segurança no âmbito das redes de computadores. Como resultado da pesquisa foi proposto uma arquitetura com a finalidade de automatizar os processos de configuração e instalação da solução proposta.

O projeto visa centralizar em uma única interface utilizando o *software* Grafana os dados pertinentes para uma gerencia proativa a incidentes ocasionados por atividades maliciosas, identificadas através das regras de firewall, que conforme [Belentani et al. 2018] permitem controlar os recursos do ambiente, além de identificar e prevenir impactos indesejáveis. A construção da arquitetura tem como base 3 camadas sendo duas para comunicação e uma para os módulos de segurança, os quais concentram as ferramentas que serão integradas ao sistema. O *backend* será responsável pela gerência das comunicações, administração do Firewall e por realizar a criação de novos *dashboards* e *hosts* na rede. O *frontend* por sua vez, tem como finalidade disponibilizar os os dados coletados. A concepção do projeto mostrou-se viável através da implementação de um protótipo, o qual integrou um conjunto de ferramentas com o intuito de coletar métricas de *hardware* e rede.

A prototipação desta proposta de *software* ocorreu com base nas tecnologias avaliadas e, com a utilização de *scripts* para o auxilio na automatização dos processos. Nesta etapa da pesquisa foi possível realizar a instalação dos serviços, de forma ágil e com baixa intervenção do usuário, necessitando apenas informações de configuração como credenciais para os serviços. Salienta-se que no futuro tais dados serão coletadas a partir de um arquivo de configuração do ambiente. Visto esta ser uma solução inicial, ainda passará por atualizações com o intuito de prover uma ferramenta ativa para a resposta de incidentes em redes de computadores empresariais. É importante salientar que a coleta de dados ocorreu em tempo real durante a utilização do protótipo, contudo a apresentação dos mesmos na interface apresentou um *delay* de 5 segundos, resultante do tempo necessário para atualização do *dashboard* no Grafana. Ainda, para um nível satisfatório de segurança, além de um processo de monitoramento bem definido para identificar ameaças constantes, é importante que as organizações adotem boas práticas e protocolos de segurança.

Referências

Belentani, L. C., Marcello, J., and Florian, F. (2018). A utilizaÇÃo de ferramentas de monitoramento para a otimizaÇÃo do gerenciamento da rede. *Revista Interface Tecnológica*, 15(2):99–110.

Bridi, M. A., Bohler, F. R., Zanoni, A. P., Braunert, M. B., Bernardo, K., Maia, F. L., FREIBERGER, Z. B., and GU, O. (2020). O trabalho remoto/home-office no contexto da pandemia covid-19. *Curitiba: Universidade Federal do Paraná, Grupo de Estudos Trabalho e Sociedade*.

da Silveira Barros, A. J. and de Souza Lehfeld, N. A. (2014). *Fundamentos de Metodologia Científica*. Pearson Prentice Hall, 3 edition.

Izumi, P. T. and Tomazeti, D. M. (2019). Segurança e privacidade: Proteção e tratamento de dados nos aplicativos de redes sociais.

Kamienski, C., Souza, T., Fernandes, S., Silvestre, G., and Sadok, D. (2005). Caracterizando propriedades essenciais do tráfego de redes através de técnicas de amostragem estratificada. SBRC.