UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de Bauru

Luiz Felipe de Camargo

Visualização da Informação Aplicada ao Monitoramento de Redes de Computadores: Um Estudo de Caso sobre a Rede sem Fio da Unesp

Bauru, São Paulo, Brasil

Agosto 2019

Luiz Felipe de Camargo

Visualização da Informação Aplicada ao Monitoramento de Redes de Computadores: Um Estudo de Caso sobre a Rede sem Fio da Unesp

Dissertação de Mestrado elaborada junto ao Programa de Pós-Graduação em Ciência da Computação – Área de Concentração em Computação Aplicada, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

Universidade Estadual Paulista "Júlio de Mesquita Filho"

Instituto de Biociências, Letras e Ciências Exatas

Programa de Pós-Graduação em Ciência da Computação

Orientador: Dr. José Remo Ferreira Brega

Bauru, São Paulo, Brasil

Agosto 2019

Este trabalho é dedicado à minha família, o meu maior ponto de apoio, desde sempre.

C172v

Camarogo, Luiz Felipe de
Visualização da informação aplicada ao monitoramento de redes de computadores : um estudo de caso sobre a rede sem fio da Unesp / Luiz Felipe de Camarogo. -- , 2019
154 p. : il., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências Farmacêuticas, Araraquara,
Orientador: José Remo Ferreira Brega

1. Ciência da computação. 2. Visualização da informação. 3. Redes de computadores. 4. Redes de computadores Monitorização. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências Farmacêuticas, Araraquara. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de São José do Rio Preto

IBILCE

ATA DA DEFESA PÚBLICA DA DISSERTAÇÃO DE MESTRADO DE LUIZ FELIPE DE CAMARGO, DISCENTE DO PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, DO INSTITUTO DE BIOCIÊNCIAS, LETRAS E CIÊNCIAS EXATAS - CÂMPUS DE SÃO JOSÉ DO RIO PRETO.

Aos 23 dias do mês de agosto do ano de 2019, às 14:00 horas, no(a) UNESP/ Câmpus de Bauru, reuniu-se a Comissão Examinadora da Defesa Pública, composta pelos seguintes membros: Prof. Dr. JOSE REMO FERREIRA BREGA - Orientador(a) do(a) Departamento de Computação / UNESP/Câmpus de Bauru, Prof. Dr. HELIO PEDRINI do(a) Instituto de Computação / Universidade Estadual de Campinas, Prof. Dr. KELTON AUGUSTO PONTARA DA COSTA do(a) Departamento de Computação / Faculdade de Tecnologia de Bauru, sob a presidência do primeiro, a fim de proceder a arguição pública da DISSERTAÇÃO DE MESTRADO de LUIZ FELIPE DE CAMARGO, intitulada ***Visualização da Informação Aplicada ao Monitoramento de Redes de Computadores: Um Estudo de Caso sobre a Rede sem Fio da Unesp***. Após a exposição, o discente foi arguido oralmente pelos membros da Comissão Examinadora, tendo recebido o conceito final: APROVADO _____. Nada mais havendo, foi lavrada a presente ata, que após lida e aprovada, foi assinada pelos membros da Comissão Examinadora.

Prof. Dr. JOSE REMO FERREIRA BREGA

Prof. Dr. HELIO PEDRINI Hélio Pedrini

Prof. Dr. KELTON AUGUSTO PONTARA DA COSTA

Luiz Felipe de Camargo

Visualização da Informação Aplicada ao Monitoramento de Redes de Computadores: Um Estudo de Caso sobre a Rede sem Fio da Unesp

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Ciência da Computação, junto ao Programa de Pós-Graduação em Ciência da Computação, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Comissão Examinadora

Prof. Dr. José Remo Ferreira Brega
UNESP – Câmpus de Bauru
Orientador

Prof. Dr. Hélio Pedrini
Unicamp – Campinas

Prof. Dr. Kelton Augusto Pontara Costa
FATEC – Bauru

Bauru
23 de agosto de 2019

Agradecimentos

Expresso aqui meus agradecimentos ao meu orientador Prof. José Remo Ferreira Brega, pelas produtivas conversas, sempre repletas de conselhos e ideias, agradeço ao Prof. Diego Roberto Colombo Dias, pela dedicação, pelos conselhos e pelo auxílio nas revisões de texto, agradeço à equipe da DTI-FMB onde presto serviço, pela paciência e auxílio com minhas dúvidas e pelos conselhos e sugestões que agregaram bastante qualidade a este trabalho, agradeço aos colegas de mestrado, pelo compartilhamento de conhecimento, pela colaboração e pelo crescimento conjunto, agradeço aos professores do programa e do Departamento de Computação da Faculdade de Ciências em Bauru por toda a colaboração na minha formação. Agradeço a todos os colegas das diversas unidades da Unesp que colaboraram comigo durante o processo de avaliação da ferramenta desenvolvida. Agradeço a minha família e demais amigos por serem sempre meu suporte. E, por fim, acima de tudo, agradeço a Deus, em especial pelo dom da minha vida.

"A vitória mais bela que se
pode alcançar é vencer a si mesmo."
Santo Inácio de Loyola

Resumo

Cada vez mais as redes de computadores se tornam vitais para as atividades das organizações, sendo necessário seu monitoramento para garantir o correto funcionamento. A utilização do processo cognitivo humano nas tomadas de decisões por meio da visualização da informação se mostra uma opção viável para grandes quantidades de dados, como os gerados no monitoramento de redes. Considerando a necessidade de se monitorar as redes de computadores modernas e o ganho de qualidade ao se utilizar técnicas de visualização, objetivou-se realizar um estudo de revisão para compreender o processo de construção de uma ferramenta de monitoramento utilizando recursos de Visualização da Informação e, a partir desta revisão, seguir com um estudo de caso por meio de uma ferramenta para aplicação de visualização na gestão da rede sem fio da Universidade Estadual Paulista "Júlio de Mesquita Filho"(Unesp). Para tanto, procedeu-se com a técnica de revisão sistemática da literatura e posteriormente um levantamento de requisitos junto aos gestores da rede da universidade. Com a análise dos dados provenientes da revisão e do levantamento, foi realizada a especificação e o desenvolvimento de uma ferramenta, avaliada em diversas unidades da universidade. Desta forma, em tempo são observados os resultados provenientes da revisão e do levantamento de requisitos, o que permitiu o desenvolvimento de uma solução utilizando as tendências constatadas, validando-as na utilização e avaliação da ferramenta. A principal contribuição do trabalho é a ferramenta resultante e seu impacto na gestão da rede sem fio da universidade, facilitando as atividades dos gestores.

Palavras-chave: visualização da informação. redes. segurança. gestão. monitoramento de redes.

Abstract

Increasingly, computer networks become vital to the activities of organizations, and their monitoring is necessary to ensure their proper functioning. Using the human cognitive process in decision making through information visualization is a viable option for large amounts of data, such as those generated in network monitoring. Considering the need to monitor modern computer networks and the quality gain by using visualization techniques, the objective was to conduct a review study to understand the process of building a monitoring tool using Information Visualization resources and, from this review, follow up with a case study through a tool for visualization application in the management of wireless network of the Paulista State University "Júlio de Mesquita Filho" (Unesp). For this, we proceeded with the technique of systematic review of the literature and later a survey of requirements with the managers of the university network. With the analysis of the data from the review and the survey, the specification and development of a tool were performed, evaluated in several university units. Thus, in time, the results from the review and survey of requirements are observed, which allowed the development of a solution using the observed trends, validating them in the use and evaluation of the tool. The main contribution of the work is the resulting tool and its impact on the university wireless network management, facilitating the activities of managers.

Keywords: information visualization. networking. security. management. network monitoring.

Lista de ilustrações

Lista de quadros

Lista de tabelas

Lista de abreviaturas e siglas

ACM	Association of Computing Machinery
AP	Access Point
API	Application Programming Interface
BGP	Border Gateway Protocol
CAFe	Comunidade Acadêmica Federada
CSS	Cascading Style Sheets
CSV	Comma Separated Values
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ELK	Elasticsearch, Logstash e Kibana
FMB	Faculdade de Medicina de Botucatu
GRC	Grupo de Redes de Computadores
GIF	Graphics Interchange Format
GOMS	Goals, Operators, Methods, Selections Rules
HTML	Hypertext Markup Language
HTML5	Hypertext Markup Language versão 5
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Eletronics Engineering
IIS	Internet Information Services
IP	Internet Protocol
IPS	Intrusion Prevention System
JS	Javascript
JSON	JavaScript Object Notation

LaPES	Laboratório de Pesquisa em Engenharia de Software
LDAP	Lightweight Directory Access Protocol
LLD	Low-level discovery
MIB	Management Information Base
MIT	Massachusetts Institute of Technology
OSI	Open System Interconnection
PHP	PHP: Hypertext Preprocessor
QUIS	Questionnaire for User Interaction Satisfaction
SNMP	Simple Network Management Protocol
StArt	State of the Art through Systematic Review
TCP	Transmission Control Protocol
UFSCar	Universidade Federal de São Carlos
Unesp	Universidade Estadual Paulista "Júlio de Mesquita Filho"
VAST	Visual Analytics Science and Technology
RADIUS	Remote Authentication Dial In User Service
RNP	Rede Nacional de Ensino e Pesquisa
SaaS	Software as a Service
SGBD	Sistemas de Gestão de Base de Dados
SQL	Structured Query Language
SVG	Scalable Vector Graphics
VoIP	Voice over Internet Protocol
XML	Extensible Markup Language

Sumário

1 Introdução

1.1 Considerações Iniciais do Capítulo

As Redes de Computadores se tornam cada vez mais uma parte vital das estruturas tecnológicas de qualquer organização. Toda e qualquer comunicação entre equipamentos, prédios e unidades de uma organização ou organizações parceiras dependem destas redes. Por meio delas, dados importantes são recebidos e transmitidos a todo instante, para os mais diversos lugares. Todo esse fluxo deve ser transmitido de maneira segura, garantindo a disponibilidade das redes para a transmissão sempre que necessária, com o grau de segurança que as informações demandarem (TANENBAUM; WETHERALL, 2010).

Quando as Redes de Computadores eram ainda projetos experimentais de pesquisa, não existia uma estrutura organizada e nem mesmo a necessidade de monitoramento ou gerência destas. Quando ocorriam problemas, os mesmos eram isolados e rapidamente detectados por meio de testes simples e ajustes básicos, pois, o uso, o número de usuários e o número de dispositivos conectados eram pequenos e as falhas não causavam grande impacto. Porém, essa situação mudou quando o mercado percebeu o potencial de evolução possível por meio destas redes. O crescimento passou a ser exponencial, junto também cresceram os problemas e a necessidade de segurança, principalmente no aspecto da disponibilidade das redes, que deveriam estar executando 24 horas por dia, 7 dias por semana. A necessidade de controlar, monitorar e coordenar os dispositivos de hardware e software era evidente (KUROSE; ROSS, 2013).

A fim de monitorar suas redes e garantir sua segurança e disponibilidade, o administrador de redes de computadores deve utilizar sistemas de software que sirvam como ferramentas para realizar o monitoramento de sua rede, obtendo informações em tempo real e históricos sobre os estados dos serviços e equipamentos que a compõe.

Entretanto, o monitoramento efetivo de modo a garantir o funcionamento pleno de uma rede, por meio de registro de todos os incidentes ocorridos, acaba por gerar uma quantidade considerável de dados, causando problemas para o administrador de redes ao analisar e obter novas informações a partir destes dados. De modo a solucionar este problema, pode-se fazer uso das técnicas de Visualização da Informação, utilizando a visão humana para auxiliar a interpretação dos dados (JACOBS, 2014b).

1.2 Trabalhos Relacionados

Diversos trabalhos já foram realizados explorando o contexto da Visualização da Informação aplicada ao Monitoramento de Redes de Computadores, de modo que vários autores realizaram estudos analisando essa área (LANGTON; NEWEY, 2010; BIERSACK et al., 2012; DAVEY et al., 2012; ZHANG et al., 2012; GUIMARAES et al., 2016; DASGUPTA et al., 2017).

Tratando-se especificamente de rede sem fio, tem-se o trabalho de Prole et al. (2008) utilizando a visualização para desenvolver um protótipo para monitoramento de ativos de rede sem fio, considerando sua localização e seus atributos de segurança. Lu et al. (2011) descreveram uma abordagem robusta para detecção de ataques analisando estatisticamente a topologia das redes sem fio. Ainda sobre redes sem fio, pode-se citar o trabalho de Gelenbe et al. (2013) que trata de redes móveis, entre elas redes sem fio e de telefonia celular, através também de visualização.

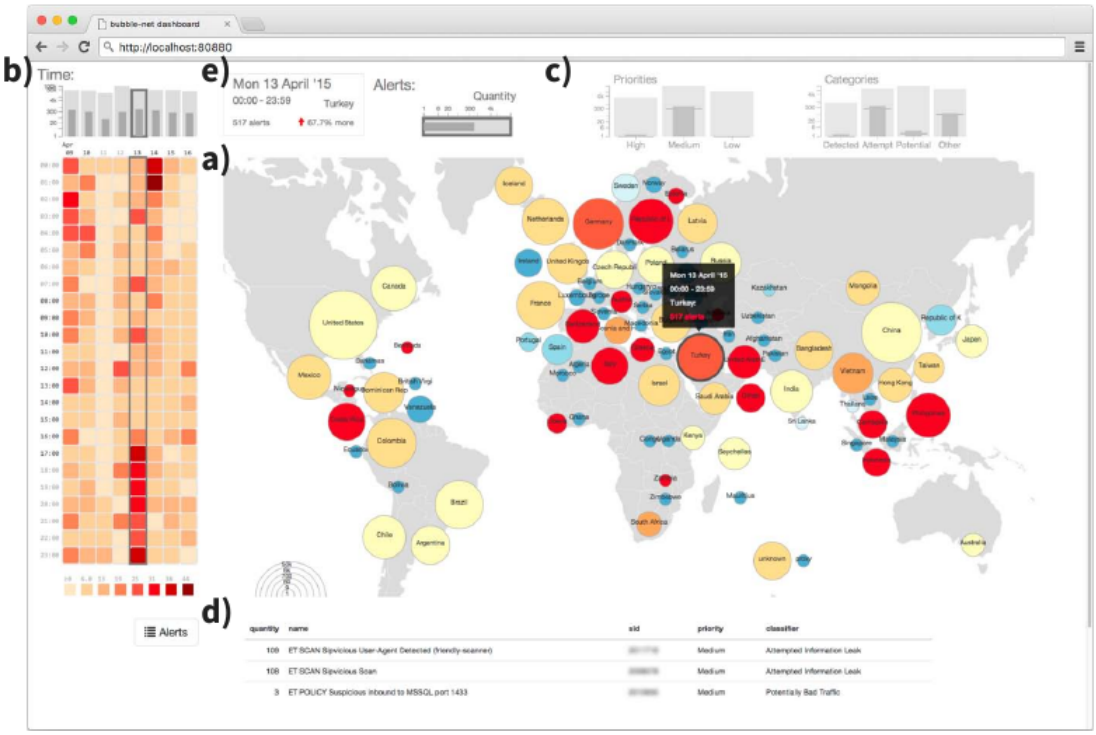
A biblioteca de programação D3.js vem ganhando cada vez mais destaque no cenário de visualização através de aplicações web. Escrita em linguagem Javascript, ela permite a criação de visualizações interativas com praticidade. Nos últimos anos diversos trabalhos utilizaram a biblioteca D3.js para criação de visualizações sobre Segurança de Redes, entre eles, pode ser citar o trabalho desenvolvido por Chen et al. (2014), que permite por meio de fontes de dados heterogêneas, obter *insights* profundos para análise de eventos de rede. Wang, Yang e Chen (2015) utilizaram a D3.js para análise de ataques de redirecionamento de servidores. Yuen, Turnbull e Hernandez (2015) abordaram em seu trabalho o desenvolvimento do componente visual de um sistema para análise de ataques multi-estágios. Guerra, Catania e Veas (2017) utilizaram visualização para detecção de comportamentos hostis em *logs* de rede. Angelini et al. (2017) aplicaram visualização na análise de *downloads* de arquivos potencialmente maliciosos. Yoon e Choi (2018) abordaram a análise e o monitoramento de segurança através dos chamados tomogramas de fluxo de redes. Tabash e Happa (2018) utilizaram a visualização aplicada à segurança e a biblioteca D3.js para análise de ameaças internas.

Bem semelhante à solução apresentada no presente trabalho, utilizando a biblioteca D3.js para tratar eventos de rede por meio de um *dashboard*, pode-se citar o trabalho realizado por McKenna et al. (2016), um resultado da aplicação pode ser vista na Figura 1.

1.3 Justificativa

A Unesp, com suas diversas unidades e seu grande número de usuários, gera uma quantidade considerável de dados monitorando sua estrutura de rede sem fio, quantidade

Figura 1 – O painel do BubbleNet identificado por suas codificações correspondentes: a) mapa de localização baseado em um cartograma de Dorling, b) gráfico temporal e mapa de calor, c) gráficos de barras com marcadores de atributos, d) tabela de detalhes de registros e e) visão geral de seleção.



Fonte — (MCKENNA et al., 2016).

esta que impossibilita muitas vezes a extração de novas informações úteis para os gestores de rede.

Após consulta ao órgão responsável pela gestão da rede no âmbito da Unesp, foi apresentada esta demanda dentro da rede sem fio, desta forma, busca-se solucionar o problema de análise de dados de rede provenientes da rede sem fio da Unesp, de modo a desenvolver e oferecer uma ferramenta aos gestores de rede da universidade, buscando a melhoria no processo de gestão, identificando problemas e possibilidades de melhorias. Atualmente se é utilizada uma solução de monitoramento que se mostra um tanto quanto ineficaz por conta de sua interface.

1.4 Objetivos

Esta monografia tem como objetivo apresentar uma ferramenta para auxiliar os gestores de redes, em alguns dos principais problemas apresentados no início deste capítulo.

Quanto à solução apresentada nesta dissertação, seu objetivo principal consiste em elaborar a arquitetura e implementar uma aplicação baseada em web para visualização

das informações relacionadas a rede sem fio da Unesp por meio de um painel de controle, um *dashboard*, permitindo a visualização das informações de estado dos pontos de acesso e controladoras que compõem a rede em questão.

A contribuição almejada por essa aplicação é facilitar o acesso as essas informações aos gestores de rede sem fio de grandes organizações distribuídas em diversas localidades, nos seus mais diversos níveis de responsabilidade, permitindo assim melhor gestão das redes e identificação de problemas.

Como um dos objetivos secundários do trabalho, visa-se realizar uma revisão sistemática de conteúdo acerca da utilização da Visualização da Informação aplicada à Segurança de Redes de Computadores. Outros objetivos secundários são: compreender profundamente a área de estudo selecionada, estudar e especificar a arquitetura de um software de visualização para monitoramento de rede, desenvolver o software com as melhores técnicas e colocar em funcionamento a ferramenta validando seu uso.

A contribuição almejada pelo trabalho como um todo é a demonstração de viabilidade do uso de aplicações de Visualização da Informação para gestão de redes, em termos de usabilidade.

1.5 Metodologia

Partiu-se da hipótese de que a utilização da Visualização da Informação pode auxiliar na de problemas relacionados a quantidade de dados produzidos pelo monitoramento de redes. Desta forma, se executou uma revisão sistemática de literatura sobre a aplicação da Visualização da Informação na Segurança de Redes de Computadores. A partir desta revisão se elaborou um projeto com a especificação de uma ferramenta para monitoramento visual dos dados provenientes da rede sem fio da Unesp. Buscou-se comparar a propostas com outras ferramentas semelhantes disponíveis no mercado, avaliando sua viabilidade. Após a avaliação da viabilidade foi dado continuidade ao desenvolvimento da ferramenta, finalizando este processo com a avaliação da ferramenta por um conjunto de usuários, validando sua utilização no cenário da universidade e comprovando a hipótese levantada anteriormente.

1.6 Organização do Trabalho

Esta dissertação está organizada em mais 8 capítulos e 4 apêndices, além da presente introdução. No Capítulo 2 são expostos conceitos para fundamentar o restante do trabalho. No Capítulo 3 é apresentada a revisão sistemática de literatura realizada. No Capítulo 4 é descrito o cenário onde o trabalho se encontra inserido, será detalhado o problema tratado e será apresentada a especificação de solução. No Capítulo 5 a especificação de ferramenta

é comparada com outras ferramentas disponíveis no mercado, o desenvolvimento da ferramenta será detalhado no Capítulo 6, o processo de avaliação da ferramenta é exposto no Capítulo 7. Por fim, o Capítulo 8 contém a discussão de resultados e a conclusão deste trabalho. O Apêndice A apresenta os dados dos estudos incluídos na revisão sistemática, o Apêndice B apresenta uma lista dos estudos excluídos na revisão, o Apêndice C apresenta o tutorial de utilização da ferramenta desenvolvida e o Apêndice D apresenta o questionário de avaliação da ferramenta.

2 Fundamentação Teórica

2.1 Considerações Iniciais do Capítulo

O presente capítulo busca ser um ponto de partida teórico para o desenvolvimento do trabalho, apresentando a definição dos conceitos principais que são utilizados do decorrer do desenvolvimento.

Nas seções que compõem o presente capítulo são apresentados conceitos que foram importantes no desenvolvimento da solução apresentada neste trabalho, são conceitos para entendimento acerca de Segurança de Informação (Seção 2.2), Gestão e Gerenciamento de Redes de Computadores (Seção 2.3), Visualização da Informação (Seção 2.4) e Avaliação de Usabilidade de Software (Seção 2.5).

2.2 Segurança da Informação

A Segurança da Informação é descrita como a proteção das informações de diversas ameaças que buscam colocar em risco a continuidade de um negócio. Através da Segurança da Informação se busca minimizar o risco decorrente destas ameaças, maximizando sempre o retorno sobre as oportunidades de negócio e investimentos (ABNT, 2005).

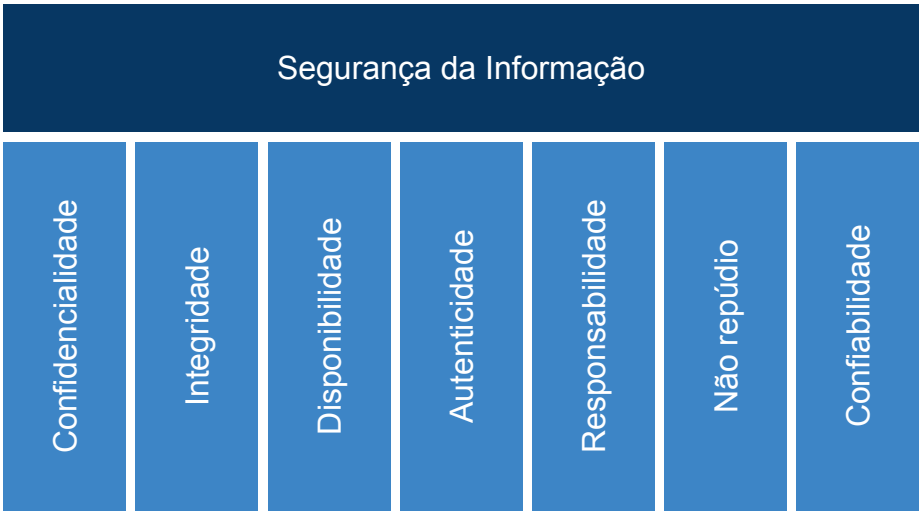
A segurança está estruturada em três principais pilares: confidencialidade, integridade e disponibilidade. No entanto, pode-se citar também outras propriedades: autenticidade, responsabilidade, não repúdio e confiabilidade (ABNT, 2005). Os pilares são ilustrados na Figura 2.

A Segurança da Informação, mesmo que focada em Redes de Computadores, é um assunto muito abrangente. De maneira simplificada, tem como preocupação o acesso das informações transmitidas pela rede por pessoas não autorizadas, para leitura ou mesmo modificação. Outras preocupações que podem ser citadas são o acesso a serviços oferecidos por pessoas não autorizadas, veracidade e o não repúdio das informações transmitidas (TANENBAUM; WETHERALL, 2010).

Caso não sejam tomadas as devidas contramedidas, existe a possibilidade de ocorrência de uma grande gama de ataques que comprometem a segurança de uma rede, tais como: monitoramento não autorizado das informações, falsificação de credências, sequestro de uma seção de comunicação em andamento, sobrecarga de um sistema, tornando o mesmo indisponível a todos, inclusive a usuários autorizados (KUROSE; ROSS, 2013).

Dentre as propriedades já citadas, o monitoramento de redes de computadores está

Figura 2 – Os pilares da Segurança da Informação.



Fonte — Produzida pelo autor.

estritamente ligado ao conceito de disponibilidade, que pode ser definido como a capacidade de estar acessível e utilizável sob demanda, ou seja, quando necessária e solicitada por entidade autorizada (ISO/IEC, 2004).

2.3 Gestão e Gerenciamento de Redes de Computadores

Todos os recursos tecnológicos devem ser utilizados com consciência, uma vez que toda a matéria-prima utilizada para produção destes vem de recursos naturais findáveis, como, por exemplo, o papel e demais suprimentos utilizados em um parque de impressoras. Neste ponto, entra o processo de gestão. Pode-se definir gestão ou administração como o ato de combinar os recursos e os objetivos de uma organização, na proporção adequada, sendo, para isso, necessário tomar decisões constantemente em um contexto de restrições, pois, nenhuma organização dispõe de todos os recursos e a capacidade de processamento de informações do ser humano é limitada (CHIAVENATO, 2003). Recursos de redes de computadores também são limitados e precisam ser geridos, para isso é necessário ter o máximo de conhecimento sobre a rede em questão.

Segundo as normas técnicas vigentes, é conveniente o correto gerenciamento e controle das redes de computadores, de modo a protegê-las de ameaças e garantir a segurança de sistemas e aplicações que fazem uso destas redes e de toda informação trafegada por ela (ABNT, 2005).

De forma mais detalhada, os seguintes itens devem ser considerados:

- a) Todas as responsabilidades relacionadas ao gerenciamento de redes e procedimentos

necessários para executá-las, incluindo equipamentos remotos e em áreas de usuários, devem ser previamente estabelecidos;

- b) Controles necessários sejam estabelecidos a fim de garantir os três pilares básicos da Segurança da Informação, confidencialidade, integridade e disponibilidade, sejam em redes públicas, sem fio, computadores e sistemas a elas conectadas;
- c) Utilizar mecanismos adequados para monitoramento e registro de ações relevantes no que diz respeito à segurança;
- d) Aplicar as atividades de gerenciamento de maneira uniforme e consistente sobre toda infraestrutura; e
- e) Os requisitos de gerenciamento devem ser definidos em níveis de serviços, de acordo com os serviços e suas necessidades, tanto para serviços de rede interno quanto para terceirizados.

A definição de Gerenciamento de Redes é sintetizada em uma única sentença por Saydam:

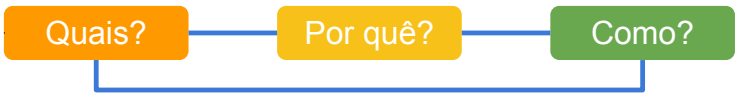
> "Gerenciamento de rede inclui o desenvolvimento, a integração e coordenação de todo o hardware, software e elementos humanos para monitorar, testar, consultar, configurar, analisar, avaliar, e controlar os recursos da rede e seus elementos para atender em tempo real os requisitos de desempenho operacional e de qualidade de serviço a um custo razoável."(SAYDAM; MAGEDANZ, 1996).

2.4 Visualização da Informação

À medida que a quantidade de informações de auditoria de rede produzidas a cada dia cresce exponencialmente, a comunicação destes dados se torna uma tarefa cada vez mais complexa, sendo a comunicação visual destas informações algo que permite a compreensão dessas grandes quantidades de dados de maneira mais simplificada e intuitiva. Um único gráfico ou imagem tem a capacidade de resumir um mês de alertas de intrusão, possivelmente mostrando tendências e exceções, ao invés de percorrer várias páginas de dados de auditoria brutos com pouco senso dos eventos subjacentes.

A Visualização da Informação busca representar conjuntos de dados como imagens, auxiliando na compreensão e tornando a interpretação destes mais eficiente. O uso da visualização é adequado quando há necessidade de aumentar as capacidades cognitivas humanas em vez de substituí-las por métodos de tomada de decisão computacional. A criação de uma ferramenta de visualização deve ser realizada respondendo três perguntas: por que a tarefa está sendo executada, quais dados são exibidos nas visualizações, e como

Figura 3 – Modelo de análise de três partes para visualização.



Fonte — Munzner e Maguire (2015) - Adaptado pelo autor.

a linguagem de expressão é construída como opção de design (MUNZNER; MAGUIRE, 2015). O processo cíclico de questionamentos pode ser visto na Figura 3.

Os três questionamentos são: "Quais?"se referindo a quais os dados utilizados na construção da visualização, "Por quê?"se referindo a motivação e o objetivo da visualização e "Como?"se referindo as técnicas de visualização e o processo de construção escolhidos.

O autor Ware (2004) justifica o uso da visualização através da potencialidade do cérebro humano para processar informações:

> Por que deveríamos nos interessar em visualização? Porque o sistema visual humano é um buscador de padrões de enorme poder e sutileza. O olho e o córtex visual do cérebro formam um processador massivamente paralelo que fornece o canal com maior banda nos centros cognitivos humanos (WARE, 2004).

Para situações onde a quantidade de dados tende a crescer de maneira acelerada, o dispositivo de exibição ou mesmo a visão humana pode limitar a utilização de técnicas visuais. Nestas situações pode ainda aplicar técnicas de interação para mudanças na visão. Diferente de uma visualização estática, que pode mostrar somente um aspecto do conjunto de dados, visualizações interativas podem mostrar simultaneamente diversos aspectos, suportando diversos níveis de detalhes (MUNZNER; MAGUIRE, 2015).

Dentro do campo de estudo da visualização existe um famoso mantra de autoria de Ben Shneiderman que diz: “Visão geral primeiro, depois zoom e filtro e, finalmente, detalhes sobre demanda”. Com esse mantra ele define o processo de interação básico com uma ferramenta de visualização, por meio do qual grandes quantidades de dados podem ser analisadas de maneira mais simples (SHNEIDERMAN, 1996).

2.4.1 *Dashboards*

O autor Few (2006), em seu livro sobre design de *dashboards*, define um *dashboard* da seguinte maneira: é uma exibição visual das informações necessárias para alcançar um ou mais objetivos que se ajustam inteiramente a uma única tela de computador, de modo que possa ser monitorado rapidamente.

O termo *dashboard*, em português algo como painel de bordo, indica um painel de indicadores, como, por exemplo, o painel de indicadores de um automóvel (indicador de

velocidade, indicador de rotações do motor, indicador de temperatura do motor, indicador do nível do óleo, etc.), de uma aeronave (indicador de altitude de voo, indicador de velocidade do vento, etc.), entre outros veículos. Não apenas veículos, mas todo tipo de sistema que depende de diversas variáveis e possui diversos estados pode contar com um *dashboard*. Um exemplo de *dashboard* de um veículo por ser visto na Figura 4.

Figura 4 – Painel de um carro com seu *dashboard*, mostrando diversas informações sobre o estado atual do veículo.

Fonte — (WheelZine Staff. "New Technology in Cars".
Acessado em 04 de julho de 2018. https://wheelzine.com/new-technology-in-cars.)

É indicado, no processo de criação de um *dashboard*, tomar certos cuidados, de modo a garantir a qualidade na utilização do painel:

- Definir o objetivo de um *dashboard*;
- Definir o público alvo do *dashboard*;
- Utilizar cores com moderação;
- Não utilizar imagens desnecessárias;
- Não apresentar dados/informações desnecessárias ou pouco relevantes de acordo com o objetivo do *dashboard* e o público alvo; e
- Não trabalhar com barras de rolagem em um *dashboard*, o ideal é ter todas as informações em uma única tela.

Pode-se classificar os *dashboards* em três grupos principais, de acordo com o público alvo que se deseja atingir, no contexto de Segurança de Redes de Computadores pode-se definir esses três tipos da seguinte maneira:

- Operacional: esse tipo é utilizado no acompanhamento de processos, métricas e estado principais de um sistema ou rede. Ele comunica informações de baixo nível rapidamente e é usado para monitoramento em tempo real das informações. O público alvo desse *dashboard* é o analista de segurança que precisa de informações precisas em tempo real.

- Tático: tipo usado para monitorar processos de departamentos, redes, estados de máquinas, etc. Ele ajuda a analisar as condições de exceção/problema e sumariza os dados para analisar a raiz da situação. Os gerentes de operações de segurança ou supervisores costumam ser o público alvo desse tipo de *dashboard*.

- Estratégico: esse tipo ajuda a monitorar a execução de objetivos estratégicos de uma organização. As visualizações de tendências são comumente encontradas nesse tipo de *dashboards*. A necessidade de informação em tempo real é "relaxada". Esses *dashboards* são usados para melhorar a coordenação e a colaboração, e o público alvo geralmente inclui o chefe da equipe de Segurança da Informação, o chefe de Segurança e outros executivos.

Independente do tipo utilizado, um dos conceitos mais comuns e importantes dentro do assunto *dashboard* é o conceito de comparação de valores. É a capacidade de ver tendências e mudanças ao longo do tempo que devem atrair a atenção do espectador. Isso não significa que apenas as alterações devam ser mostradas em *dashboards*, muitas vezes, é o fato de que alguma medida não mudou, o que a torna digna de nota.

O Quadro 1 mostra alguns exemplos de medidas comparativas. Também são mostrados no quadro exemplos de como essas medidas podem ser aplicadas e que tipo de *dashboard* usaria geralmente essa medida.

O fluxo de informações de um *dashboard* não deve ser unidirecional. Os indicadores técnicos não são somente agregados, resumido e reportado até o *dashboard* do responsável pela rede, mas o fluxo também funciona ao contrário. Os indicadores coletados devem resultar em ajustes de políticas, melhorias de processos e novos controles. O fluxo de informações deve ser um processo de aprendizado que ajuda a rastrear exceções para melhorar as arquiteturas e políticas de segurança e permitir que os processos de gerenciamento sejam ajustados, inclusive de maneira automatizada se o grau de integração alcançado permitir, possibilitando assim novas estratégias aplicando inteligência computacional para fazer o melhor uso da estrutura disponível.

Quadro 1 – Medidas comparativas do *dashboard*

Medida	Exemplo	Tipo de *dashboard*
Comparação com a mesma medida no passado	Número de ataques no último ano comparado com hoje	Tático / Estratégico
O estado atual de uma medida	Número de vulnerabilidades expostas atualmente	Operacional / Tático / Estratégico
A relação com um futuro objetivo que a medida deve alcançar	Percentual de máquinas sem um determinado *patch* de segurança	Tático
A predição de uma medida estabelecida em algum momento do passado	Previsão dos custos para manter as assinaturas de antivírus atualizadas	Tático / Estratégico
A relação com a predição futura de uma medida	Percentual de máquinas atualizadas para o novo sistema operacional nesse trimestre	Tático / Estratégico
Um valor refletindo o normal para essa medida	Número médio de falhas de login por pessoa, ou o intervalo de tempo normal que as pessoas logam em seus *desktops*, ou o número de horas levado em média para corrigir sistemas críticos	Operacional / Tático
Predição futura de uma medida	Número de máquinas que precisam serem trocadas em um ano ou o tamanho da população de usuários em um mês	Estratégico
Uma versão diferente de uma mesma medida	Como é a postura de risco se comparada a outras empresas do mesmo setor	Estratégico
Uma medida relacionada para comparar com	Custo de execução do monitoramento de segurança interna em comparação com a postura de segurança e risco que resultaria se o monitoramento de segurança fosse terceirizado.	Estratégico

Fonte: (JACOBS, 2014a) - Traduzido e adaptado pelo autor

2.5 Avaliação de Usabilidade de Software

Dentro do estudo de interfaces, uma das etapas mais importantes no desenvolvimento é a avaliação. Por meio dela é possível verificar se todos os requisitos definidos foram atendidos e como está o relacionamento do usuário com o que está sendo desenvolvido.

Norman e Nielsen (2003) observam: "A experiência do usuário engloba todos os aspectos da interação do usuário final... o primeiro requisito para uma experiência de usuário exemplar é atender às necessidades exatas do cliente, sem problemas ou incômodos. Em seguida vem a simplicidade e a elegância, que produzem produtos que são uma alegria para si próprios, uma alegria de usar."

Com o advento e a popularização dos *smartphones*, *tablets* e outros dispositivos com interfaces que vão além do mouse e teclado, houve um aumento na conscientização sobre usabilidade. Entretanto, muitas vezes os projetistas ainda levam a si mesmos como referência no momento de avaliar a usabilidade. A avaliação com outros usuários permite verificar se as escolhas de design estão apropriadas para uma população de usuários mais ampla, evitando problemas futuros (PREECE; ROGERS; SHARP, 2015).

2.6 Considerações Finais do Capítulo

Neste capítulo foram apresentados conceitos que norteiam os demais capítulos do presente trabalho, estes conceitos são apresentados de forma breve, mas que permitem a contextualização sobre os assuntos tratados e compreensão da solução a ser apresentada.

3 Revisão Sistemática da Literatura

3.1 Considerações Iniciais do Capítulo

Neste capítulo é exposta a revisão sistemática de literatura realizada para nortear o desenvolvimento da ferramenta.

A revisão sistemática da literatura é uma técnica que busca executar revisões abrangentes da literatura acerca de um tema, avaliando os resultados de forma não tendenciosa, explicitando sempre seus critérios de seleção, de modo que o pesquisador que for utilizar a revisão possa avaliar a qualidade da mesma e executá-la novamente. Esta técnica foi desenvolvida inicialmente para utilização na área de medicina, porém, vem cada vez mais sendo utilizada em outras áreas do conhecimento (BRERETON et al., 2007).

3.2 Metodologia de Busca

Nesta Seção são apresentados os métodos e dados acerca do processo de pesquisa realizado neste estudo.

Durante a revisão os estudos são categorizados da seguinte forma:

- Estudos identificados: são os estudos retornados pelo sistema de busca selecionado, seja ele manual ou eletrônico. São registradas a quantidade de estudos encontrada e a fonte destes estudos;
- Estudos duplicados: são aqueles estudos que estão presentes em mais de uma base de dados selecionada, são contabilizados somente uma vez;
- Estudos não selecionados: são aqueles estudos que de maneira objetiva não atendem os critérios de inclusão. São excluídos durante a fase de seleção. É registrada apenas a quantidade destes estudos;
- Estudos selecionados: são aqueles que aparentemente atendem os critérios de inclusão, são incluídos na fase de seleção. Registram-se as referências completas destes estudos;
- Estudos excluídos: são aqueles estudos que, após avaliação do texto completo, não atendem aos critérios de inclusão, são excluídos na etapa de extração; e
- Estudos incluídos: são aqueles estudos que, após avaliação do texto completo, atendem aos critérios de inclusão, se mantém durante todo o processo e são utilizados na etapa de extração.

3.2.1 Objetivos da revisão

A revisão executada tem como objetivo obter um panorama geral da utilização das técnicas de Visualização da Informação na Segurança de Redes de Computadores e, através disso, compreender profundamente o campo de pesquisa de Visualização da Informação aplicada à Segurança de Redes de Computadores.

3.2.2 Questões de pesquisa

Após diversas discussões e pesquisas prévias, chegou-se à seguinte questão principal de pesquisa:

Como as ferramentas que utilizam técnicas de Visualização da Informação aplicadas ao contexto de Segurança de Redes de Computadores são construídas?

Esta pergunta principal pode ser expandida nas seguintes questões:

- Qual a linguagem de programação utilizada na construção deste tipo de ferramenta?

- Quais técnicas visuais são exploradas neste tipo de ferramenta?

- Quais dados são utilizados na construção e validação deste tipo de ferramenta?

- Qual o objetivo específico da ferramenta?

3.2.3 Desenvolvimento do protocolo

Nesta seção é descrito o desenvolvimento do protocolo definido para guiar a presente revisão. Foram detalhadas as seguintes etapas: escolha da estratégia de busca, escolha das bases de dados, definição dos critérios de inclusão e exclusão, definição da avaliação de qualidade, definição do processo de extração de dados com o formulário de extração e do processo de síntese dos estudos.

3.2.4 Estratégia de busca

Definiu-se uma revisão sistemática utilizando os termos:

analysis defense, analysis security, analysis visualization, data defense, data security, data visualization, defense data, defense data visualization, defense visualization, information defense, information security, information visualization, internet availability, internet defense, internet security, internet security visualization, network availability, network defense, network security, network security visualization, security data, security data visualization, security visualization, visual analytics.

As bases de dados oferecem o recurso de busca avançada, onde os termos de buscas podem ser concatenados utilizando caracteres adequados que servem como operadores,

formando assim a chamada *string* de busca. Para o presente trabalho, a *string* de busca inicialmente utilizada foi:

(("information"OR "data"OR "analysis") AND ("visualization"OR ("security"OR "defense"))) AND (("network"OR "internet") AND (("security"OR "defense") OR "availability"OR "security visualization")) AND (("security"OR "defense") AND ("visualization"OR "data"OR "data visualization")) AND "visual analytics"

Foram considerados como estudos válidos artigos publicados na língua inglesa em periódicos e conferências. Não foi imposta nenhuma restrição relacionada à data de publicação dos estudos envolvidos, sendo considerados somente os estudos localizados até a execução das buscas e da fase de identificação dos estudos em 12/12/2018.

3.2.5 Bases de dados

As buscas iniciais foram realizadas utilizando *strings* de busca nas bases de dados ACM Digital Library, IEEE Xplore Digital Library, Science Direct, Scopus e Engineering Village.

A seleção destas foi realizada considerando a relevância, afinidade com as áreas de estudo e quantidade de resultados obtidos nos testes preliminares.

3.2.6 Critérios de inclusão e exclusão

Nesta etapa foram definidos os critérios para avaliar quais estudos avançam para a próxima etapa da revisão. Os critérios devem ser definidos a partir das questões de pesquisa. Outros critérios que podem ser utilizados na execução de uma revisão são: restrição por idioma, por exemplo, restringir a revisão a somente artigos em Inglês, restrição por área, restrição por artigos primários, excluindo estudos secundários como outras revisões sistemáticas, etc. (NEIVA; SILVA, 2016).

Não foram encontrados trabalhos correlatos escritos em língua portuguesa, desta forma optou-se pela inclusão somente de artigos escritos na língua inglesa.

3.2.6.1 Critérios de inclusão

Para a presente revisão, os seguintes critérios de inclusão foram definidos:

- Afinidade do estudo com os temas desejados – buscou-se incluir na revisão os estudos que possuíam relação com o tema Visualização da Informação aplicada à Segurança de Redes de Computadores e similares, estudos sem relação ao assunto ou com relação a somente uma das áreas: Visualização da Informação ou Segurança de Redes de Computadores, foram excluídos; e

- Apresenta uma aplicação prática – foram selecionados e identificados todos os estudos que apresentaram uma aplicação prática e concreta dos temas desejados, de modo que se pudesse entender o processo de desenvolvimento desta aplicação.

3.2.6.2 Critérios de exclusão

Como critérios de exclusão, foram definidos os seguintes critérios:

- Falta de afinidade do estudo com os temas desejados – estudos retornados na busca, porém, que não apresentavam afinidade com os temas desejados, Visualização da Informação e Segurança de Redes de Computadores, foram excluídos. Estudos que tratavam de somente um dos temas, sem relacionar com o outro também foram excluídos por este motivo;
- Não é um artigo – resultados retornados que não poderiam ser considerados estudos foram desconsiderados, entre eles estão artigos de opinião, índices de anais de eventos, entre outros;
- Estudo não está disponível completo no idioma Inglês – estudos retornados na pesquisa, como o resumo disponível na língua inglesa, porém, com o texto completo somente disponível em outro idioma foram excluídos da revisão pela impossibilidade de leitura; e
- Trata de ferramenta já analisada – situações onde foram identificados mais de um artigo proveniente de um mesmo grupo de autores e se tratando da mesma ferramenta optou-se por avaliar o estudo mais recente, excluindo os demais por já terem a ferramenta em questão analisada.

3.2.7 Avaliação de qualidade

Em determinadas situações é interessante definir um ponto de corte para que artigos menos qualificados de acordo com parâmetros previamente definidos, de modo que uma parte dos estudos que não atenderem o nível de qualidade definido possam ser excluídos, reduzindo a quantidade de estudos a um número plausível (NEIVA; SILVA, 2016).

No presente trabalho, por conta da quantidade satisfatória de estudos retornadas, optou-se por não executar a avaliação de qualidade.

3.2.8 Extração de Dados

Na etapa de extração de dados, a questão de pesquisa deve ser respondida por meio da análise dos artigos selecionados na etapa anterior, mediante um formulário de extração previamente elaborado com questões que detalhem aspectos da pergunta de pesquisa

principal. Os dados são registrados de maneira que fiquem vinculados aos estudos a que se referem, esse registro pode ser realizado utilizando ferramentas especificas ou métodos mais simplificados, como uma planilha. Ao se executar a leitura completa dos estudos, as possíveis respostas ao formulário de extração são registradas (NEIVA; SILVA, 2016).

Para o presente estudo, as seguintes questões compuseram o formulário de extração:

- Tipos de rede abordados: por meio desta pergunta se busca obter qual tipo de rede de computadores se trata no estudo, exemplos delas são baseadas no conjunto de protocolos Transmission Control Protocol/Internet Protocol (TCP/IP), em português, Protocolo de Controle de Transmissão/Protocolo de Internet, no protocolo BGP, redes de telefonia celular, redes exclusivamente *wireless*, etc;

- Técnicas de visualização utilizadas: por meio desta pergunta se busca identificar quais técnicas de visualização e quais recursos gráficos são utilizados no estudo e na construção de ferramenta em questão, as informações obtidas nesta pergunta respondem a uma das perguntas fundamentais sobre uma ferramenta de visualização: como os dados são exibidos? (MUNZNER; MAGUIRE, 2015);

- Objetivos das visualizações: conforme entendimento dos autores Munzner e Maguire (2015), toda visualização dever responder à pergunta do porque ela foi criada. Sendo assim através desta questão se busca identificar a motivação por trás do desenvolvimento da visualização em questão. As mais diversas motivações foram encontradas, de modo a facilitar a manipulação dos resultados, elas foram sintetizadas em três (3) categorias: "Categoria 1 — Análise de atividade anormal em grandes volumes de dados históricos ou a longo prazo", "Categoria 2 — Compreender comportamento da rede e detectar anomalias"e "Categoria 3 — Detectar, analisar e responder a ataques específicos". O detalhamento destas categorias será realizado na Seção 3.3.9;

- Fonte de dados utilizadas nas visualizações: por meio desta questão se busca identificar quais são as fontes de dados utilizadas na construção das visualizações, desta forma se responde a terceira pergunta dos autores Munzner e Maguire (2015): o que será visualizado?;

- Camada de rede utilizada: conforme proposto no modelo de referência *Open System Interconnection (OSI)* e implementado no protocolo IP, busca-se identificar com qual camada de rede os dados analisados estão relacionados, as respostas possíveis definidas foram: “aplicação”, “transporte”, “rede” e “enlace e física”;

- Houve desenvolvimento de ferramenta: esta pergunta busca identificar se houve desenvolvimento de uma nova ferramenta de visualização ou somente aplicação de uma ferramenta já existente, dessa forma a pergunta poderia ser respondida de forma binária, com sim ou não;

- Nome da ferramenta: esta pergunta busca identificar o nome dado a ferramenta e verificar se a ferramenta em questão já não foi analisada em outro estudo;
- Linguagens utilizadas na construção da ferramenta: por meio desta pergunta foram analisadas as linguagens de programação utilizada durante o desenvolvimento das ferramentas, de forma a buscar tendências de utilização; e
- É um estudo de revisão (*survey*, revisão sistemática, etc): por meio desta pergunta busca-se identificar os estudos tidos como secundários, ou seja, estudos anteriores que já buscaram realizar um trabalho com caráter de revisão sobre uma área, tendo como respostas as opções binárias sim e não.

3.2.9 Síntese de estudos

A síntese e sumarização das informações coletadas foram reunidas e expostas através de tabelas, de forma a mostrar a divisão dos estudos baseada nas perguntas que compõem o formulário de extração.

Sempre que possível foram utilizados gráficos e recursos visuais para exposição da informação, utilizando as boas práticas de visualização, de modo a facilitar a compreensão dos dados.

3.2.10 Ferramenta StArt

Para apoio à realização da presente revisão, foi utilizada a ferramenta StArt, desenvolvida pelo Laboratório de Pesquisa em Engenharia de Software (LaPES) da Universidade Federal de São Carlos (UFSCar).

A ferramenta StArt permite aos pesquisadores preencher todo o protocolo de uma revisão sistemática de forma facilitada. Ela possui informações sobre todas as fases presentes em uma revisão, desde o objetivo, questão de pesquisa, busca, estratégias de seleção, critérios de inclusão e exclusão, formulário de extração, formulários de critérios de qualidade até as estratégias de sintetização de resultados (FABBRI et al., 2016).

3.3 Análise e Discussão dos Resultados

Nesta seção são apresentados e discutidos os resultados obtidos ao aplicar o protocolo de revisão nas bases científicas e extrair seus dados.

3.3.1 Condução

De maneira preliminar, foram obtidas as seguintes quantidades de estudos por base de dados, após a fase de identificação, conforme visto na Tabela 1:

Tabela 1 – Resultados — Fase de Identificação

Base de dados	Estudos
ACM Digital Library	24
IEEE Xplore Digital Library	94
Science Direct	3
Scopus	164
Engineering Village	205
Total	490
Duplicados	219
Estudo únicos	271

Fonte: Produzida pelo autor.

3.3.2 Estudos

A quantidade de estudos obtida ao final da revisão, de acordo com a classificação pode ser observada na Tabela 2.

Tabela 2 – Quantidades de estudos durante as fases da revisão

Categorias	Quantidades
Estudos identificados	490
Estudos duplicados	219
Estudos não selecionados	165
Estudos selecionados	106
Estudos excluídos	33
Estudos secundários	7
Estudos incluídos	66

Fonte: Produzida pelo autor.

Na Figura 5, o total de 490 estudos é dividido de acordo com a classificação final de cada trabalho, após a realização da presente revisão.

Na Figura 6, pode-se visualizar a evolução da quantidade de estudos aceitos em cada fase da revisão sistemática.

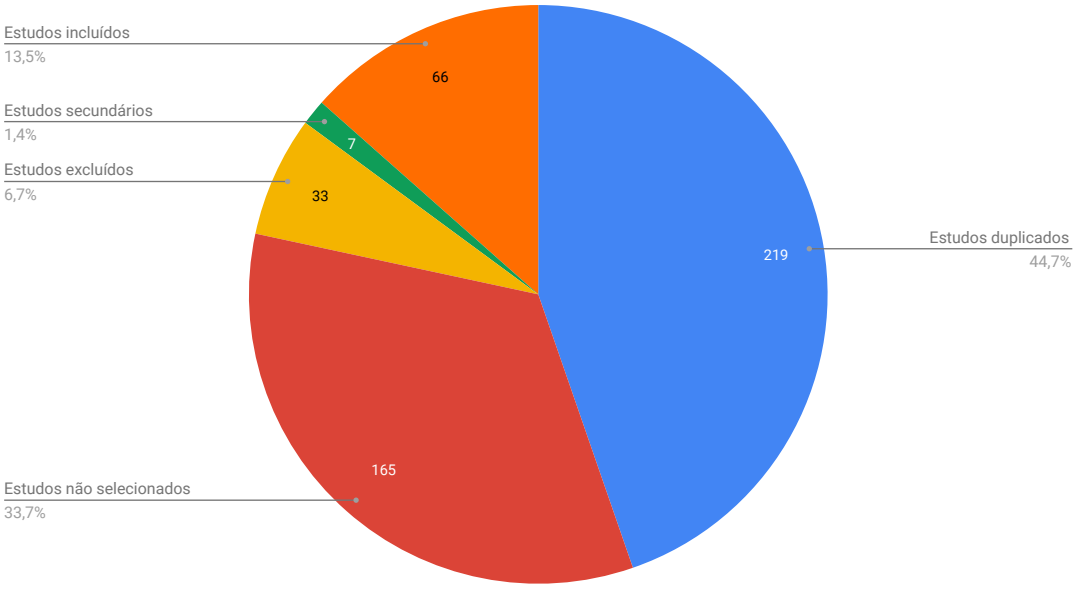
3.3.3 Estudos excluídos

Durante a fase de extração, 33 estudos foram excluídos, pois mesmo após a análise inicial do título e resumo, durante a leitura completa, foi verificado que não atendiam os critérios de inclusão. Estes estudos estão listados no Apêndice B.

3.3.4 Estudos secundários

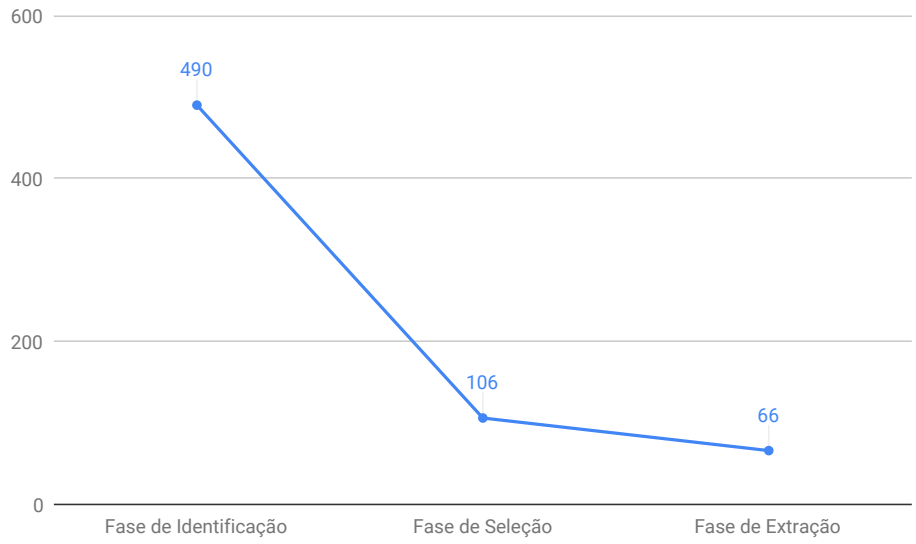
Os estudos secundários identificados serão analisados na Seção 3.3.12.

Figura 5 – Classificação final dos estudos



Fonte — Produzida pelo autor.

Figura 6 – Evolução da quantidade de estudos



Fonte — Produzida pelo autor.

3.3.5 Estudos incluídos

Os dados detalhados e referências dos 66 estudos analisados são apresentados no Apêndice A deste trabalho. As próximas seções detalham os dados obtidos após análise destes estudos.

3.3.6 Tipos de redes de computadores

O assunto redes de computadores é amplo, dessa forma se desejou identificar de maneira geral qual tipo de rede tratada em cada estudo. O conjunto maior que forma a Internet e as redes atuais tem grande base na tecnologia TCP/IP, um conjunto de protocolos, baseado no modelo de referência OSI, onde cada camada é responsável por um certo grupo de tarefas, fornecendo uma interface bem definida de serviços para a camada imediatamente superior, quanto mais alta a camada, mais próxima da aplicação e mais abstratos são os dados (FERREIRA, 2003).

Desta forma, buscou-se identificar a relação dos estudos com os tipos de rede existentes, com foco maior no conjunto de protocolos TCP/IP e suas partes específicas, desta forma se constatou os resultados apresentados na Tabela 3:

Tabela 3 – Ocorrência de tipos de rede

Tipo de rede	Ocorrência
BGP	3
Mobile: wireless e celular	1
TCP/IP	57
Wireless	3
4G LTE	1
VoIP	1

Fonte: Produzida pelo autor.

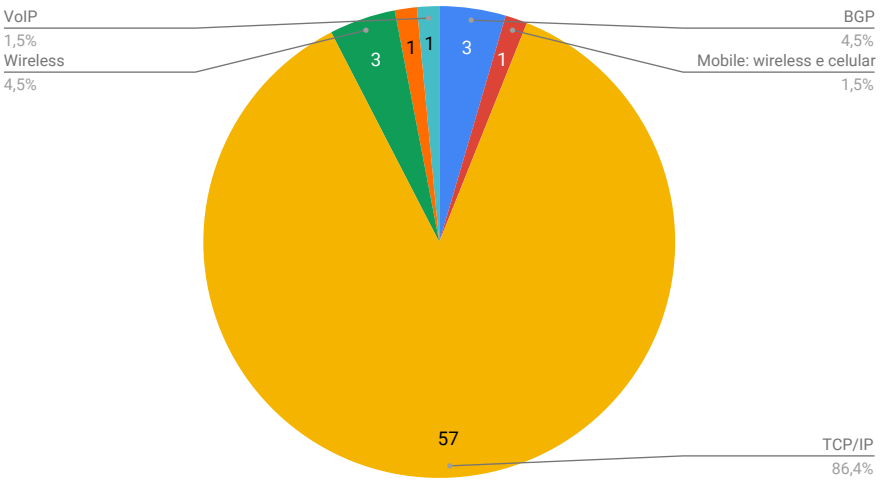
As redes citadas como BGP, *Wireless*, *Mobile* e VoIP acabam por ser baseadas também no conjunto TCP/IP, porém os estudos tratam exclusivamente desses tipos de rede, não se aplicando a todo tipo de rede baseada em TCP/IP. A Figura 7 representa a divisão por tipo de rede.

3.3.7 Camada de rede

Dentro do conjunto de protocolos TCP/IP, se tem as seguintes camadas:

- Camada 1 — Enlace e Física: responsável pela comunicação com o meio físico da rede, como placas e cabos;
- Camada 2 — Rede: também chamada de camada de Internet, serve para identificação da máquina em uma rede ou na Internet. Nesta camada funcionam os roteadores;
- Camada 3 — Transporte: responsável pela transferência eficiente, confiável e econômica dos dados entre a máquina de origem e a máquina de destino, garantindo ainda que os dados cheguem sem erros e na sequência correta. O controle da camada de transporte é feito pelo sistema operacional; e

Figura 7 – Tipos de rede presentes nos estudos



Fonte — Produzida pelo autor.

- Camada 4 — Aplicação: esta camada realiza a função de 3 camadas do modelo OSI, aplicação, apresentação e sessão. É a camada onde rodam as aplicações;

Dentro da utilização do conjunto de protocolos TCP/IP, buscou-se identificar com quais camadas de rede os dados estavam relacionados, conforme Tabela 4.

Tabela 4 – Ocorrências das camadas de rede

Camadas	Ocorrências
Camada 1 — Enlace e Física	7
Camada 2 — Rede	51
Camada 3 — Transporte	3
Camada 4 — Aplicação	9
Não informada	3

Fonte: Produzida pelo autor.

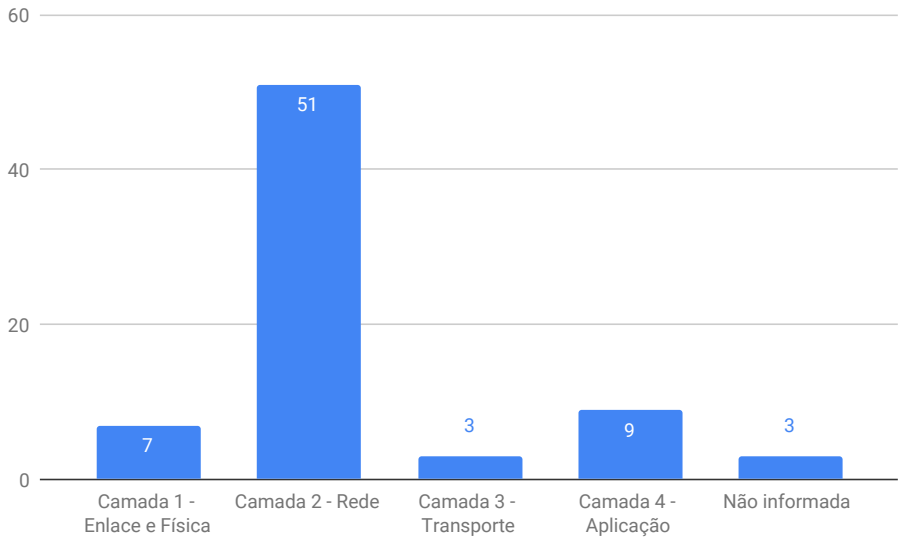
Pode-se perceber uma grande tendência a se obter os dados provenientes da Camada 2, a camada de rede, mais especificamente dados no formato de fluxo de rede (*netflow*). Esta tendência pode ser visualizada na Figura 8.

A Figura 9 mostra a distribuição no tempo dos artigos que indicam a camada de rede utilizada. Pode-se observar uma lacuna entre 2009 e 2013 onde dados provenientes da camada 4 não foram utilizados no desenvolvimento de ferramentas.

3.3.8 Técnicas visuais

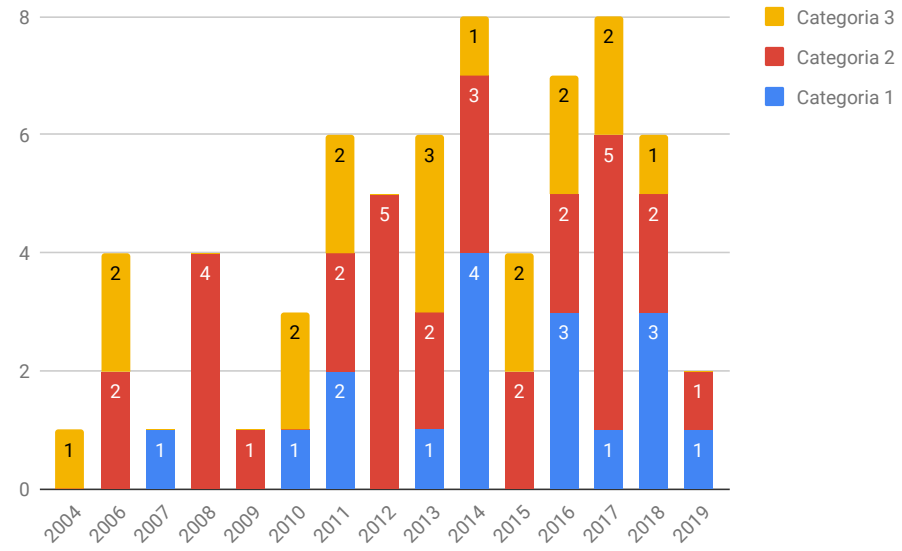
As mais diversas técnicas visuais foram aplicadas nas ferramentas abordadas nos estudos participantes, agrupando técnicas semelhantes pode-se citar a presença de 83

Figura 8 – Estudos separados por camadas de rede utilizadas



Fonte — Produzida pelo autor.

Figura 9 – Camadas utilizadas no decorrer dos anos.



Fonte — Produzida pelo autor.

técnicas visuais diferentes utilizadas nas construções das visualizações. Na Tabela 5, são mostradas as técnicas utilizadas em mais de um estudo.

Destaca-se a utilização maior de técnicas consideradas clássicas como o gráfico de barras, muito usado em diversas situações permitindo fácil interpretação e coordenadas paralelas, utilizadas na exibição de grandes quantidades de relacionamentos entre os dados.

Na Figura 10 tem-se uma visualização utilizando a técnica *word cloud* para de-

Tabela 5 – Técnicas visuais mais utilizadas

Técnica	Ocorrências
diagrama de voronoi	2
geoespacial	2
grafico circular	2
gráfico de linha	2
gráfico de radar	2
mapa	2
matriz	2
nós	2
tomografia de network flows	2
visualização geográfica	2
diagrama nó-link	3
espaços 3D	3
geográficas	3
grafo	3
linha do tempo	3
séries temporais	3
curva de série temporal	4
histograma	4
radial	5
treemap	5
mapa de calor	7
gráfico de dispersão	9
coordenadas paralelas	10
gráfico de barras	12

Fonte: Produzida pelo autor.

monstrar todas as técnicas presentes nos estudos. Optou-se pela utilização da técnica *word cloud* pela possibilidade que ela oferece de se visualizar uma grande quantidade de categorias, relacionando a relevância de cada uma delas, sem ocupar muito espaço.

3.3.9 Objetivos da visualização

De acordo com os objetivos da visualização utilizada e da ferramenta desenvolvida ou aplicada, os estudos foram divididos em três (3) categorias:

- Categoria 1 — Análise de atividade anormal em grandes volumes de dados históricos ou a longo prazo: ferramentas que possuíam como objetivo a análise posterior ao evento ocorrido, com foco em grandes quantidades de dados históricos, avaliando tendências;
- Categoria 2 — Compreender comportamento da rede e detectar anomalias: ferramentas que possuíam como foco principal o estado atual da rede, oferecendo maior compreensão sobre seu comportamento e exibindo anomalias em tempo real; e

Figura 10 – *Word cloud* com todas as técnicas de visualização citadas

Fonte — Produzida pelo autor através da ferramenta disponível em http://www.wordart.com

- Categoria 3 — Detectar, analisar e responder a ataques específicos: ferramentas focadas em ataques específicos, buscando comportamentos predeterminados e proporcionando informações úteis para a realização da defesa.

Definidas as categorias, os estudos ficaram distribuídos da seguinte maneira, conforme Tabela 6. De maneira gráfica visualiza-se na Figura 11.

Tabela 6 – Objetivos das ferramentas

Objetivo	Estudos
Categoria 1 - Análise de atividade anormal em grandes volumes de dados históricos ou a longo prazo	17
Categoria 2 - Compreender comportamento da rede e detectar anomalias	31
Categoria 3 - Detectar, analisar e responder a ataques específicos	18

Fonte: Produzida pelo autor.

A Figura 12 mostra a distribuição no tempo de acordo com os objetivos das ferramentas.

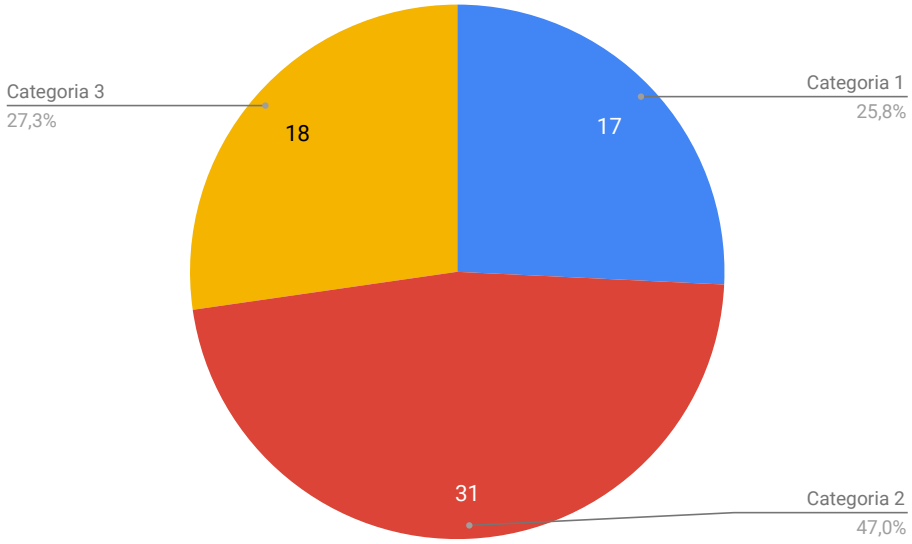
3.3.10 Fontes de dados

Foram citadas 56 fontes de dados diferentes para extração de dados e geração das visualizações. Na Tabela 7 pode-se verificar as fontes que possuem mais de uma citação:

Na Figura 13, visualiza-se através da técnica de *word cloud* todas as fontes citadas.

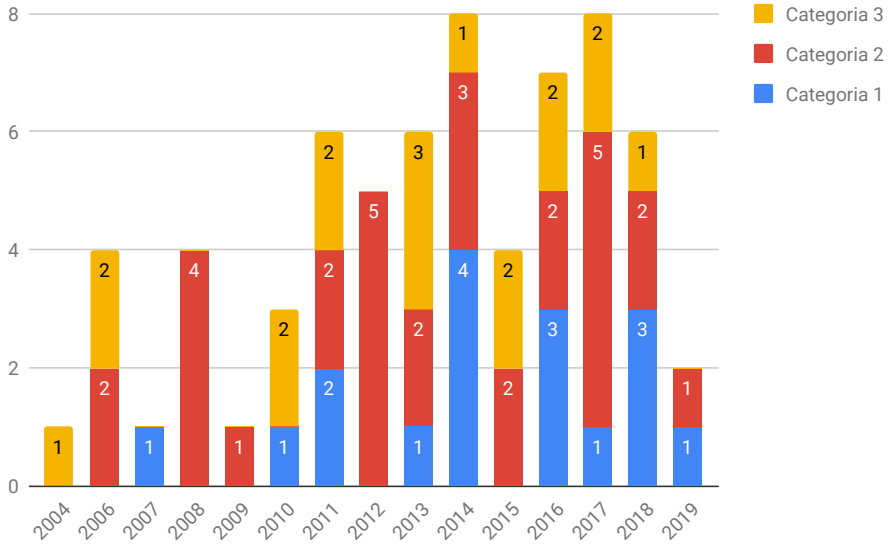
Pode-se verificar a grande presença das fontes de dados Visual Analytics Science and Technology (VAST) e *netflow*.

Figura 11 – Estudos separados por objetivo



Fonte — Produzida pelo autor.

Figura 12 – Objetivos no decorrer dos anos.



Fonte — Produzida pelo autor.

O VAST Challenge é um concurso anual com o objetivo de avançar o campo da análise visual por meio de competições. Os problemas do VAST Challenge fornecem aos pesquisadores tarefas e conjuntos de dados realistas para avaliar seu software, bem como uma oportunidade para avançar no campo, resolvendo problemas mais complexos (VAST, 2017).

Netflow é um recurso que foi introduzido em roteadores Cisco, cuja função é coletar características e informações sobre o tráfego de redes IP, tanto na saída quanto na entrada

Tabela 7 – Fontes de dados utilizadas

Fonte de dados	Citações
dados de IDS	2
dados de topologia	2
dados do WinPcap	2
informações de negócios	2
dados do SNORT	3
log de IDS	4
log de firewall	6
VAST	17
network flow	19

Fonte: Produzida pelo autor.

Figura 13 – Fontes de dados utilizadas nos estudos exibidas através da técnica de *word cloud*

Fonte — Produzida pelo autor através da ferramenta disponível em http://www.wordart.com

de uma interface. Analisando os dados fornecidos pelo *Netflow*, um gerente de rede pode determinar tarefas como a origem e o destino do tráfego e as causas de congestionamento. Com o tempo acabou por se tornar um recurso padrão em equipamentos de rede e um padrão de notação de dados de uma rede.

3.3.11 Desenvolvimento e linguagem

O chamado desenvolvimento de software é definido como o ato de elaborar e implementar um sistema computacional, ou seja, transformar a necessidade de um utilizador ou de um mercado em um software (BIRREL; OULD, 1988).

Dos 66 estudos avaliados, na grande maioria deles (62) houve desenvolvimento

de uma nova ferramenta e apenas 4 deles trataram da implantação de uma ferramenta existente.

As linguagens de programação são conjuntos de regras que permitem que um programador especifique de maneira precisa sobre quais dados um computador vai atuar, de que forma estes dados serão armazenados ou transmitidos e quais ações devem ser tomadas sob várias circunstâncias (FISCHER; GRODZINSKY, 1993).

Foram levantadas as linguagens de programação utilizadas no desenvolvimento de cada ferramenta, entretanto, 30 estudos não informaram em seu texto qual foi a linguagem de programação utilizada. Já 7 estudos informaram utilizar 2 linguagens combinadas durante o desenvolvimento. As linguagens identificadas podem ser vistas na Tabela 8.

Tabela 8 – Linguagens de programação utilizadas

Linguagem	Utilizações
Android	1
C#	1
C++	2
C++, Javascript	1
DOT language	1
Java	12
Java, Javascript	1
Java, Processing	1
Javascript	5
Javascript, Processing	1
Perl	1
PHP, Javascript	2
Processing	1
Python, Javascript	1
R	1
Não informado	30
Sem desenvolvimento	4

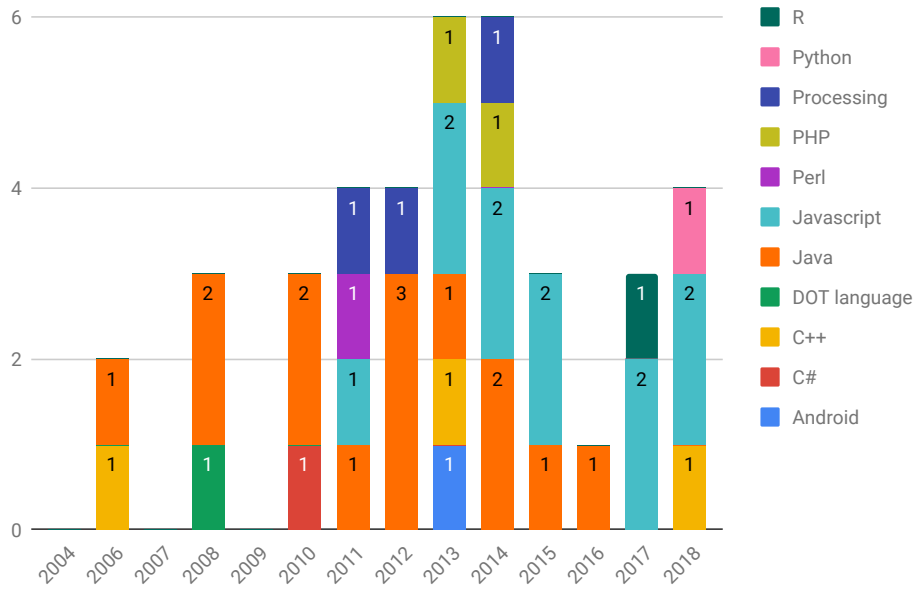
Fonte: Produzida pelo autor.

Pode-se perceber uma tendência de utilização da linguagem Java para aplicações *server-side* e Javascript para aplicações que possam ser executadas no *client-side*, através do navegador do usuário.

A Figura 14 mostra a distribuição no tempo dos artigos que indicam a linguagem de programação utilizada. Pode-se perceber pela Figura 14 que a distribuição das linguagens no decorrer dos anos não apresenta tendência conclusiva.

Durante o estudo, foi constatada a grande utilização de diversas bibliotecas e *frameworks* para desenvolvimento visual, dentre elas pode-se citar a biblioteca D3.js escrita em Javascript e citada em 6 estudos, que permite a criação de visualizações através do suporte nativo dos navegadores web a padrões de desenho do HTML5.

Figura 14 – Linguagens no decorrer dos anos.



Fonte — Produzida pelo autor.

3.3.12 Estudos comparativos

Durante a execução do presente trabalho, foram encontrados estudos comparativos ou secundários, ou seja, estudos que já propunham, dentro do tema, uma revisão de conteúdo, seja ela por meio de uma revisão sistemática, um *survey*, entre outras técnicas. A seguir uma descrição breve destes estudos:

- (LANGTON; NEWEY, 2010): neste trabalho é avaliada uma certa quantidade de métodos e ferramentas de visualização em segurança cibernética, essas ferramentas foram selecionadas para revisão de acordo com a disponibilidade, presença em artigos publicados e popularidade em postagens no site http://www.vizsec.org. Ferramentas proprietárias não foram avaliadas, somente ferramentas gratuitas, com código aberto e em constante evolução;

- (BIERSACK et al., 2012): levantamento dos métodos de visualização desenvolvidos para o monitoramento de redes BGP, em especial para a identificação de sequestro de prefixos, por meio de padrões de roteamento anormais. Apresenta análise de caso real ocorrido entre abril e agosto de 2011;

- (DAVEY et al., 2012): apresenta por meio de duas facetas, conteúdo e infraestrutura, exemplos concretos do benefício da análise visual para a chamada Internet do Futuro. Foca em como a junção de ambos os temas têm potencial de abrir novas oportunidades para o mercado de tecnologia;

- (ZHANG et al., 2012): apresenta uma pesquisa sobre projetos que aplicam a Visualização da Informação para Segurança de Redes por meio de arquivos de *logs*, os estudos identificados são separados em cinco (5) categorias de acordo com taxonomia criada;

- (GUIMARAES et al., 2016): estudo avalia o uso de técnicas de Visualização da Informação no apoio do processo de gerenciamento de redes e serviços, através da execução de uma revisão sistemática de literatura. Nele foram classificados 285 artigos publicados entre 1985 e 2013, classificando eles de acordo com taxonomias de Visualização da Informação e Gerenciamento de Redes;

- (DASGUPTA et al., 2017): trata de um estudo acerca da utilização do fator humano na análise de fluxos de dados. Busca através de uma pesquisa *(survey)* entender o estado da arte do assunto e compreender as lacunas e desafios existentes acerca do tema; e

- (ZHAO et al., 2019): estudo trata de sistemas de visualização para segurança cibernética, analisa 15 ferramentas, divididas em 3 categorias, através de 6 atributos: alertas, interoperabilidade, colaboração, flexibilidade, consciência situacional e filtros.

3.4 Discussão

Na presente seção são discutidos os resultados obtidos, de forma a extrair deles novas informações e tendências.

3.4.1 Relevância do estudo

A presente revisão contempla o que se acredita ser a quase totalidade do campo de estudo desejado, uma vez que os termos de busca foram selecionados e posteriormente aperfeiçoados de forma a contemplar o maior número possível de resultados relacionados. As bases de dados também colaboraram para a força das evidências criadas, pois foram selecionadas as mais relevantes na área da Computação e também algumas outras de modo a ampliar o número e a variedade dos resultados obtidos. Além do que a quantidade de estudos analisados de maneira completa, 66, número superior ao padrão exigido para aceitação na revista ACM Computing Surveys, que exige no mínimo revisões tratando de 50 estudos.

3.4.2 Limitações do estudo

Para a realização de uma revisão sistemática, diversos métodos de busca podem ser utilizados, entre eles pode-se citar: busca manual em periódicos, busca automatizada

por *string* de busca em bases de dados, busca por meio da metodologia de "bola de neve", incluindo na revisão as referências dos resultados obtidos inicialmente, além de se combinar métodos de busca. Optou-se pela realização somente da busca automatizada em bases de dados, o que pode limitar o escopo da pesquisa em comparação com uma abordagem combinada de diversos métodos.

A partir do estudo realizado percebeu-se a possibilidade de um aprofundamento da revisão realizada, aplicando uma avaliação de qualidade dos estudos, expandindo o número de estudos avaliados e selecionando os que apresentassem maior relevância.

Foi constatada a ausência em diversos estudos de informações de extrema importância na construção das ferramentas como: fonte de dados utilizadas descritas de forma objetiva, linguagem de programação utilizada durante o desenvolvimento, nome da ferramenta, entre outros. A ausência destes dados enfraquece as tendências encontradas, mesmo com um número relevante de estudos analisados.

3.4.3 Tendências

Diversas tendências puderam ser averiguadas durante a execução da presente revisão, entre elas, podem ser citadas:

- Tipo de rede: os estudos, em sua grande maioria, abordaram redes que utilizam o conjunto de protocolos TCP/IP. Mesmo com algumas ferramentas tratando de tipos específicos de rede, a tendência percebida é a de criação de uma ferramenta generalista, que possa ser aplicada a qualquer rede TCP/IP;

- Técnicas visuais: percebe-se uma tendência na criação de técnicas próprias, partindo muitas vezes de técnicas clássicas e executando as adaptações que se julgam necessárias. Entretanto, o uso de técnicas clássicas como gráfico de barras e coordenadas paralelas, é bem frequente em comparação com as demais técnicas. Percebe-se também a presença de uma quantidade relevante de técnicas ligadas a variação temporal utilizadas em conjunto com outras técnicas, que permitem a visualização histórica dos dados e da situação anterior da rede;

- Objetivos da visualização: os estudos avaliados apresentaram os objetivos mais diversos, porém, de modo a facilitar a análise de tendências, os objetivos foram simplificados e separados em três categorias. A categoria com mais estudos foi "Compreender comportamento da rede e detectar anomalias", pode-se perceber a tendência na criação de ferramentas generalistas, que auxiliem no acompanhamento do estado geral da rede e de como este é afetado por anomalias. Os outros objetivos que não foram tão presentes estão ligados a análise de dados históricos e detecção de ataques específicos;

- Linguagens de programação: percebe-se a tendência de uso das linguagens Java e Javascript, linguagens flexíveis com foco em programação para web. Como a evolução dos padrões web, como o HTML 5, por exemplo, e a necessidade de portabilidade das informações, a opção por uma opção de linguagem focada em web se mostra uma tendência e uma boa opção. A utilização de *frameworks* e bibliotecas de apoio para o desenvolvimento visual é constante nos estudos, mostrando assim a tendência de utilização destas ferramentas de apoio que agilizam o desenvolvimento; e

- Fontes de dados e camada de rede: percebe-se a forte tendência na utilização de dados no formato de fluxo de rede (netflow), provenientes da Camada 2 da tecnologia TCP/IP. É bem difundida também a utilização de dados neste padrão, provenientes dos desafios de visualização propostos nas conferências VAST, para validação das ferramentas desenvolvidas.

Percebe-se que o cenário leva ao desenvolvimento de uma ferramenta para monitoramento de redes de computadores baseadas no conjunto de protocolos TCP/IP, por ser um padrão mais difundido de rede em uso, com a utilização de técnicas de visualização próprias, desenvolvidas juntamente com a ferramenta, com o objetivo de compreender o comportamento de uma rede e detectar a presença de anomalias (ataques, uso excessivo da rede, intervalos de indisponibilidade e etc.), oferecendo também as funções de detecção de ataques específicos e análise sobre dados históricos. A criação desta ferramenta se daria através de uma linguagem de programação para web, com o auxílio de bibliotecas e *frameworks* para desenvolvimento visual, de modo a facilitar e agilizar o processo de desenvolvimento. A tendência geral seria o desenvolvimento de uma ferramenta que utiliza dados da Camada 2, com dados de fluxo de rede, entretanto, pode-se considerar a utilização de outra camada de rede uma oportunidade na área de pesquisa.

3.5 Considerações Finais do Capítulo

A presente seção do estudo buscou investigar a área de pesquisa da Visualização da Informação aplicada à Segurança de Redes de Computadores por meio da execução de uma revisão sistemática de literatura que foi realizada em diversas bases de dados e que depois das devidas fases de seleção resultou na inclusão de 66 estudos primários neste trabalho.

Para o desenvolvimento de trabalhos futuros, bem como da especificação presente no Capítulo 4, a presente revisão contribuiu mostrando tendências que contribuem no processo de construção, como o uso de linguagens compatíveis com o desenvolvimento web e bibliotecas e *frameworks* visuais, tendências que contribuem com a definição do objetivo da ferramenta, como o foco no estado geral e detecção de anomalias gerais em

redes TCP/IP e a tendência em se desenvolver uma técnica visual própria. Este trabalho contribuiu também mostrando lacunas de pesquisa, como a falta de estudos envolvendo outras camadas de rede além da Camada 2 e a falta de diversidade nas fontes de dados utilizadas.

4 Especificação da Solução

4.1 Considerações Iniciais do Capítulo

O presente capítulo tem como objetivo mostrar o cenário em que o problema está inserido e como as tendências verificadas na revisão de literatura foram aplicadas na solução do problema.

4.2 Cenário

A tecnologia de rede sem fio está presente na maioria das organizações empresariais da atualidade, ela pode ser utilizada para:

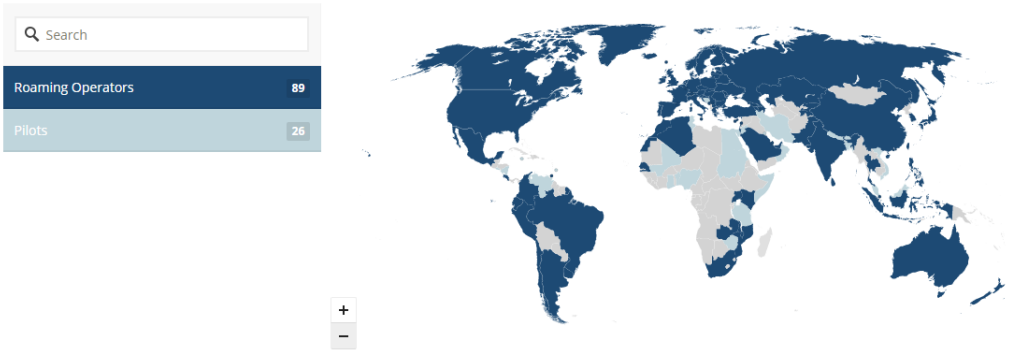
- Operações internas da própria empresa;
- Oferecer acesso à internet para seus visitantes e/ou clientes; e
- Permitir que colaboradores utilizem a internet da empresa em seus equipamentos (celulares, notebooks, etc.).

A Unesp tomou como padrão para sua rede sem fio o serviço Eduroam (*education roaming*), baseado na tecnologia IEEE 802.1X e servidores de *proxy* RADIUS hierárquicos. O objetivo deste serviço é criar uma rede sem fio integrada e transparente entre instituições de ensino e pesquisa. Lançada no Brasil em 2012, essa iniciativa internacional já reúne instituições de aproximadamente 60 países. Além da segurança, o Eduroam tem como benefícios a mobilidade, facilidade de uso e a sua integração à Comunidade Acadêmica Federada (CAFe), uma federação de identidade que reúne instituições de ensino e pesquisa brasileiras gerenciada pela Rede Nacional de Pesquisas (RNP). Na Figura 15 pode-se verificar a cobertura atual do serviço Eduroam.

Para utilização da rede por usuários não vinculados diretamente a comunidade acadêmica da Unesp, foi criada uma rede auxiliar chamada unespVisitante que permite o cadastro por período determinado para qualquer pessoa que necessite de acesso à rede sem fio.

Por meio de estudos realizados sobre a aplicação da Visualização da Informação aplicada à Segurança de Redes de Computadores, propõe-se o desenvolvimento de uma ferramenta para monitoramento de redes, apresentando uma interface no formato de *dashboard*, aplicável a realidade da Unesp e sua estrutura de rede sem fio, buscando identificar possíveis limitações na solução de monitoramento atual.

Figura 15 – Mapa indicando países que são operadores do serviço Eduroam e que possuem pilotos



Fonte — Eduroam. Acessado em 04 de julho de 2018. www.eduroam.org/where.

Desta forma, obteve-se ao final do projeto uma ferramenta para monitoramento de redes que oferece uma visão integrada dos diversos aspectos que compõe a situação de uma rede sem fio, podendo explorá-los de forma interativa, utilizando técnicas de Visualização da Informação.

Através da ferramenta proposta, busca-se:

- Melhorar a gestão da rede sem fio na Unesp, facilitando o acesso aos dados de monitoramento dos equipamentos que a compõe;
- Detectar facilmente problemas na rede, como, por exemplo, gargalos em equipamentos e assim tomar as medidas necessárias para correção destes; e
- Aumentar o conhecimento sobre a estrutura de rede em questão, identificando possíveis ajustes para otimização;

4.3 Detalhamento do Problema

Atualmente, o monitoramento da rede sem fio da Unesp é realizado por meio da ferramenta Zabbix, entretanto, algumas limitações são encontradas, principalmente no que se diz respeito ao acesso às informações dentro da interface do Zabbix, pois os menus possuem diversos níveis e não são intuitivos, demandando um grande esforço para localização da informação desejada.

Devido à complexidade da rede sem fio da Unesp, uma vez que a mesma é composta por 32 unidades, distribuídas em 24 campi, optou-se pelo desenvolvimento inicial de uma ferramenta utilizando o contexto de somente uma unidade, no caso a Faculdade de Medicina de Botucatu (FMB), e depois expansão da ferramenta para as demais unidades, visando assim atingir toda rede sem fio da Unesp.

4.4 Análise de Requisitos

De modo a se obter uma ferramenta de monitoramento baseada em *dashboards* completa, buscou-se identificar, dentro da estrutura da Unesp, os níveis organizacionais e mapear os dados presentes em seus respectivos *dashboards*, conforme visto nos Quadros 2, 3 e 4. Os dados em destaque (negrito) não são coletados e disponibilizados na atual estrutura de monitoramento da rede baseada no software Zabbix.

As medidas relacionadas a tráfegos podem ser detalhadas em categorias baseadas em portas, protocolos, serviços e destino do tráfego, porém, para esse detalhamento é necessário o acesso às informações de um *firewall* ou implementação de um, ou sistema semelhante que forneça essas informações.

As medidas relacionadas a usuários e equipamentos conectados podem ser detalhadas em categorias de equipamentos (notebooks, celulares e etc.) de acordo com a detecção de sistema operacional por parte do servidor *Dynamic Host Configuration Protocol (DHCP)*.

4.5 Obtenção e Organização de Dados

Nas próximas seções é exposta a estrutura atual de coleta de dados e são citados os passos realizados para organização destes dados internamente na ferramenta desenvolvida. Estas informações foram obtidas após reuniões com o GRC.

4.5.1 SNMP

O Simple Network Management Protocol (SNMP), publicado em 1988, foi projetado para prover um padrão de fácil implementação e baixo custo, para o gerenciamento de equipamentos de redes de diferentes fabricantes (STALLINGS, 1998). O protocolo SNMP apresenta diversas características, entre elas (SCHONWALDER, 2003):

- Define um protocolo para troca de informações entre um ou mais sistemas de gerenciamento;
- Fornece uma estrutura para formatar e armazenar as informações de gerenciamento;
- Define um número de variáveis de informação de gerenciamento de propósito geral;
- Minimiza o número e a complexidade das tarefas de monitoramento realizadas pelos agentes;
- É extensível para aceitar aspectos de operação e gerência de rede não previstos;e
- Fornece independência para implantação em servidores e clientes particulares.

Quadro 2 – Proposta de *dashboard* estratégico

Nível:	Estratégico		
Público Alvo:	Reitoria, Assessoria de Informática e Grupo de Redes de Computadores		
Item	Dado Necessário	Fonte	Objetivo
Controladoras	Estado Atual	consulta SNMP na controladora	monitoramento de problemas na controladora
	Pontos de acesso associados	consulta SNMP na controladora	impacto em caso de problemas, balanceamento de cargas
	Carga de uso	consulta SNMP na controladora	monitoramento de problemas na controladora, balanceamento de cargas
	Usuários associados	consulta SNMP na controladora	conhecimento da dimensão do serviço oferecido, impacto em caso de problemas, balanceamento de cargas
	Log	consulta SNMP na controladora	monitoramento de problemas na controladora, detalhamento da situação atual
Tráfego	Valor total da rede sem fio	consulta SNMP nas controladoras	conhecimento da dimensão do serviço oferecido
	Valor agregado por unidade	associação de consultas de SNMP nos pontos de acesso da unidade	conhecimento da dimensão do serviço oferecido a cada unidade
	Valores classificados por segmento (docentes, técnicos admin., alunos, etc.)	**intersecção de dados das controladoras com banco de dados de pessoas**	**conhecimento da utilização do serviço por segmento**
Usuários	Número total ligado à rede sem fio	consulta SNMP nas controladoras	conhecimento da dimensão do serviço oferecido
	Número de usuários provenientes de outras instituições logados na rede da Unesp	**dados das controladoras, filtrando domínio dos usuários autenticados**	**conhecimento da dimensão do serviço oferecido através do *roaming***
	Números de usuários classificados por segmento (docentes, técnicos admin., alunos, etc.)	**intersecção de dados das controladoras com banco de dados de pessoas**	**conhecimento da utilização do serviço por segmento**
	Total de visitantes conectados	**dados das controladoras e do sistema de gestão de visitantes**	**conhecimento da dimensão do serviço oferecido para visitantes**

Fonte: Produzida pelo autor.

Quadro 3 – Proposta de *dashboard* tático

Nível:	Tático		
Público Alvo:	Diretores Técnicos de Informática, Responsáveis por Áreas de Informática em Unidades Auxiliares, Administradores de rede de cada unidade		
Item	Dado Necessário	Fonte	Objetivo
Tráfego	Valor agregado na unidade	associação de consultas de SNMP nos pontos de acesso da unidade	conhecimento da dimensão do serviço oferecido
	Valor agregado por prédio ou departamento	associação de consultas de SNMP nos pontos de acesso do prédio ou departamento	conhecimento da dimensão do serviço oferecido para cada prédio ou departamento e impacto daquele local no valor total
	Parcela da banda da unidade utilizada pela rede sem fio	**associação de consultas de SNMP nos pontos de acesso da unidade e valor de saída de rede da unidade**	**impacto do serviço oferecido na rede da unidade**
Usuários	Total de usuários conectados na unidade	associação de consultas de SNMP nos pontos de acesso da unidade	conhecimento da dimensão do serviço oferecido
	Total de usuários conectados por prédio ou departamento	associação de consultas de SNMP nos pontos de acesso do prédio ou departamento	conhecimento da dimensão do serviço oferecido para cada prédio ou departamento
	Número de usuários de outras instituições e unidades logados na rede da unidade	**dados das controladoras filtrando pontos de acesso da unidade e domínio dos usuários autenticados**	**conhecimento da dimensão do serviço oferecido através do *roaming* e do impacto de usuários não pertencentes àquela unidade**
	Número de usuários visitantes conectados na unidade	**dados das controladoras e do sistema de gestão de visitantes filtrando pontos de acesso da unidade**	**conhecimento da dimensão do serviço oferecido para visitantes**

Fonte: Produzida pelo autor.

Quadro 4 – Proposta de *dashboard* operacional

Nível:	Operacional		
Público Alvo:	Analistas e Assistentes prestadores de serviço nas áreas de rede		
Item	Dado Necessário	Fonte	Objetivo
P. de acesso	Estado atual	consulta SNMP no ponto de acesso	monitoramento de problemas no ponto de acesso
	Carga de uso	consulta SNMP no ponto de acesso	monitoramento de problemas no ponto de acesso, balanceamento de cargas
	Usuários associados	consulta SNMP no ponto de acesso	impacto em caso de problemas, balanceamento de cargas
	Log	consulta SNMP no ponto de acesso	monitoramento de problemas no ponto de acesso, detalhamento da situação atual
	Logins inválidos	consulta SNMP no ponto de acesso	verificação de problemas alegados pelos usuários
Tráfego	Por ponto de acesso	consulta SNMP no ponto de acesso	conhecimento da dimensão do serviço oferecido de forma detalhada, podendo visualizar áreas que sejam grandes consumidoras de banda, balanceamento de cargas
	Por usuário	**consulta de tráfego de um dispositivo conectado ao ponto de acesso e dados da controladora**	**localização de grandes consumidores de banda**

Fonte: Produzida pelo autor.

4.5.2 Zabbix

Zabbix é um software criado em 1998 por Alexei Vladishev, com sua primeira versão alpha lançada em 2001. O software é dividido em 4 módulos: Server, Agents, Frontend e Proxy. O módulo *proxy* atua de maneira a diminuir a carga sobre o módulo *server* e fazer um monitoramento distribuído. Zabbix requer recursos significativos de processamento dependendo da extensão do monitoramento e da base de dados escolhida (Zabbix, 2017).

A *Application Programming Interface* (API) do Zabbix permite, por meio de requisições HTML do tipo POST com conteúdo JSON, a utilização de dados coletados pelo Zabbix e armazenados em seu banco de dados. Os dados fornecidos são também estruturados em JSON, permitindo diversas consultas, entre elas, sobre os *hosts*, os itens pertencentes as eles e o histórico de cada item.

Inicialmente, para testes preliminares, foi realizada uma instalação local do Zabbix na FMB, monitorando parcialmente os dados dos pontos de acesso, de modo a criar uma familiarização acerca da API do Zabbix. Com base nessa instalação foi desenvolvida a primeira versão do protótipo.

Com a validação do primeiro protótipo pela equipe do Grupo de de Redes de Computadores (GRC), o desenvolvimento passou a utilizar da API do Zabbix centralizado, implantado na Reitoria e utilizado por todas as unidades da Unesp.

A atual estrutura de monitoramento do Zabbix centralizado utiliza diversos mecanismos de coleta vinculados ao Zabbix: *Simple Network Management Protocol (SNMP)*, *scripts* executados em um *host* auxiliar *(Dummy Host)*, coleta e tratamento de *logs* através da ferramenta Logstash e descoberta de baixo nível (LLD) do próprio Zabbix. Os dados são reunidos, organizados e armazenados no Zabbix. A Figura 16 demostra essa estrutura de coleta.

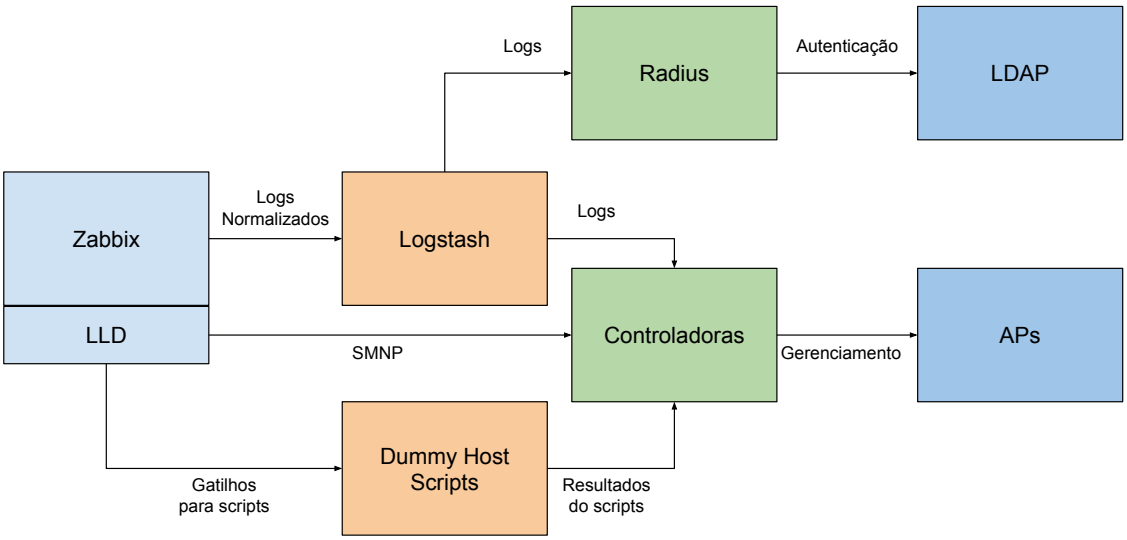
Não foi possível a realização de testes diretamente com consultas SNMP, nem a identificação dos códigos dos objetos Management Information Base (MIB) utilizados, uma vez que a estrutura de coleta de dados já se encontra implementada e não foi fornecido acesso gerencial a ela.

4.5.3 Tratamento dos dados

Os dados obtidos a partir da API do Zabbix são fornecidos no formato JSON, entretanto, esse formato não é compatível com o formato utilizado pela biblioteca D3.js, por conta disso foi criado um tratamento destes dados por meio de um módulo desenvolvido na linguagem PHP.

Os dados são coletados na API do Zabbix de acordo com o período de tempo definido no controle de *slider* adequado, os dados recebidos são constituídos de todas as

Figura 16 – Estrutura da coleta de dados do Zabbix centralizado



Fonte — Produzida pelo autor.

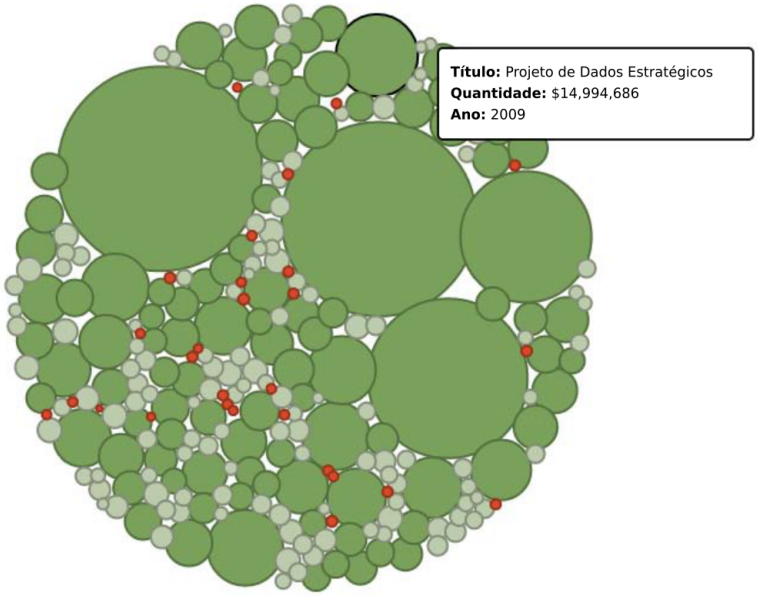
médias por hora realizadas para os itens em questão no período desejado, com estes dados são calculadas as médias de cada item e organizadas de acordo com os pontos de acesso a qual pertencem, com isso estes dados são gravados em um novo arquivo JSON obedecendo ao padrão utilizado pela biblioteca D3.js. O controle de *slider* para controle do período permite variação de 1 hora a 24 horas.

4.6 Representações Visuais

Na presente seção são detalhadas as técnicas visuais selecionadas para construção da ferramenta, todas estas foram utilizadas nas diferentes telas da ferramenta.

Gráfico de bolhas ou gráfico de área proporcional ou gráfico de embalagem de círculo — utilizado para comparação de valores e demostração de proporções, permite uma visão rápida do tamanho relativo dos objetos em comparação ao demais, sem a necessidade de uso de escalas. Possui como desvantagem a dificuldade em estipular o valor representado, desta forma, se mostra útil para comunicação de dados, porém, não tão útil para análises mais detalhadas. Qualquer forma pode ser utilizada na sua construção, desde que a sua área represente o valor da grandeza, porém, as mais comuns são quadrados e círculos. Cada elemento individual representa uma categoria diferente e é dimensionado de acordo com o valor associado. Demais variáveis visuais, como cor e posição, são geralmente adicionadas para melhorar as camadas de significado da exibição, adicionando novos significados (KIRK, 2012). Um exemplo pode ser visto na Figura 17.

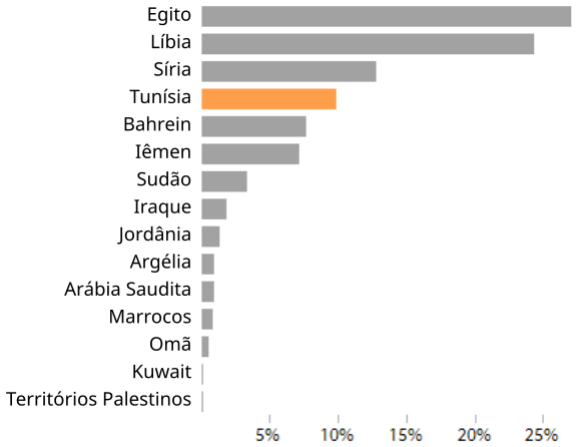
Figura 17 – Exemplo de gráfico de bolhas.



Fonte — Imagem de "Gates Foundation Educational Spending" (http://vallandingham.me/vis/gates/), criada por Jim Vallandingham (KIRK, 2012) Traduzido pelo autor.

Gráfico de barras ou colunas — um dos gráficos considerados mais básicos, permite a comparação facilitada entre diferentes categorias que são representadas próximas, com alinhamento no eixo que representa o valor zero e com a representação dos dados através de sua altura para as colunas e de seu comprimento para as barras. O uso de diferentes cores para destaques ou diferentes categorias pode auxiliar conforme a narrativa desejada (KIRK, 2012). Um exemplo básico deste gráfico está presente na Figura 18.

Figura 18 – Exemplo de gráfico de barras.

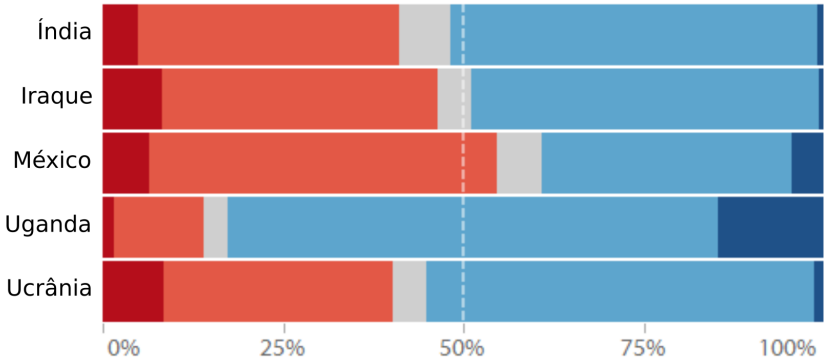


Fonte — (KIRK, 2012) - Traduzido pelo autor.

Gráfico de barras ou colunas empilhadas — utilizado para comparação entre

categorias de dados, entretanto, estas categorias podem ser decompostas em segmentos e comparadas como parte de um todo. Útil para exibição do valor total e de cada parcela que o forma. São bastante autoexplicativas. Cores e posição são utilizadas para diferenciar as categorias de valor. A desvantagem de um gráfico deste tipo é a dificuldade em ser capaz de permitir leitura precisa dos valores, pois, não há uma linha de base comum (KIRK, 2012). Um exemplo deste tipo de gráfico pode ser visto na Figura 19.

Figura 19 – Exemplo de gráfico de barras empilhadas.



Fonte — (KIRK, 2012) - Traduzido pelo autor.

Gráfico de linhas ou séries temporais — exibe informações como uma série de pontos de dados conectados por segmentos de linha reta. É gráfico muito comum, utilizados em muitos campos das ciências. Semelhante a um gráfico de dispersão, exceto que os pontos de medição são ordenados (normalmente pelo seu valor do eixo "x") e unidos com segmentos de linha reta. Comumente utilizados para visualizar tendências em um intervalo de tempo, de maneira cronológica. Os gráficos de linhas são algo com que a maioria das pessoas deve estar familiarizados. Eles são usados para comparar uma variável quantitativa contínua, geralmente o tempo, no eixo "x"e o tamanho dos valores no eixo "y". Os pontos verticais são unidos através de linhas para mostrar a trajetória de deslocamento através dos declives resultantes. Diferente dos gráficos de barras, o eixo "y"não precisa começar do zero (KIRK, 2012). Um exemplo é mostrado na Figura 20.

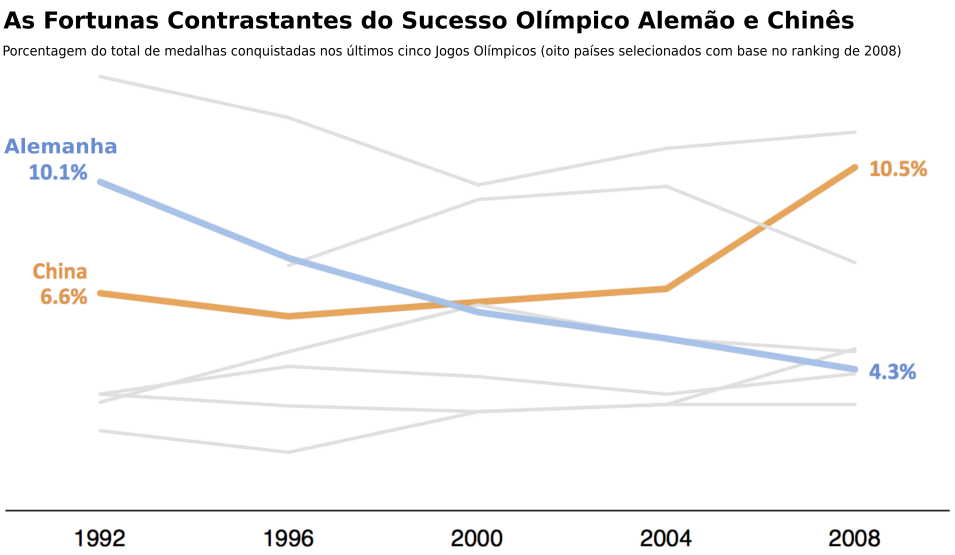
4.7 Tecnologias Escolhidas

Nesta seção serão introduzidas as tecnologias escolhidas para desenvolvimento da ferramenta.

4.7.1 PHP

PHP, um acrônimo recursivo para PHP: Hypertext Preprocessor, é uma linguagem de programação de código aberto, criada e muito utilizada para o desenvolvimento web.

Figura 20 – Exemplo de gráfico de linhas.



Fonte — (KIRK, 2012) - Traduzido pelo autor.

Foi criada no ano de 1994 por Rasmus Lerdorf e disponibilizada ao público no ano seguinte. Atualmente é mantida por uma organização chamada The PHP Group. (The PHP Group, 2018)

O termo PHP significava originalmente *Personal Home Page*, tendo seu significado alterado para o acrônimo recursivo para *Hypertext Preprocessor* com o passar do tempo. A ideia inicial de seu criador era acompanhar o número de visitas a seu site pessoal. Com o passar do tempo e o desenvolvimento de mais *scripts*, aumentando a gama de funcionalidades que as ferramentas do seu site possuíam, ele passou a chamar a tecnologia de PHP Tools.

Após alguns anos, aquele conjunto de ferramentas alcançou sucesso no meio dos desenvolvedores web e seu criador resolveu transformá-lo em uma linguagem de programação. Já em 1998 está linguagem estava presente em boa parte dos *web sites* existentes.

Como uma linguagem *server-side*, o PHP tem seu o código executado no servidor, gerando o HTML que é então enviado para um navegador. O navegador recebe os resultados da execução do código, porém, não sabe qual era o código-fonte.

4.7.2 Javascript

JavaScript (às vezes abreviado para JS) é uma linguagem de programação interpretada, implementada inicialmente como parte dos navegadores web, tem como objetivo permitir que *scripts* pudessem ser executados do lado do cliente (navegador) e interagissem com o usuário sem a necessidade de passar pelo servidor, controlando o navegador, realizando comunicação assíncrona e alterando o conteúdo do documento HTML exibido.

JavaScript foi desenvolvido por Brendan Eich durante seu período trabalhando na Netscape, nessa época a linguagem tinha o nome de Mocha, posteriormente teve seu nome mudado para LiveScript e por fim JavaScript. Em 1995 foi lançada implementada no navegador Netscape versão 2.0.(FLANAGAN, 2006)

4.7.3 D3.js

D3.js é uma biblioteca escrita na linguagem JavaScript para geração de gráficos ou visualizações, manipulando e dando vida a dados por meio das tecnologias HTML, Scalable Vector Graphic (SVG) e Cascading Style Sheets (CSS). Possui ênfase nos padrões atuais da web, de forma a utilizar toda capacidade dos navegadores de internet modernos sem utilização de padrões proprietários. O D3.js é utilizado em centenas de páginas na internet, seus principais usos são para criação de gráficos interativos em sites de notícias, *dashboards* para visualização de dados e produção de mapas para sistemas de informações geográficos.

À primeira vista o D3.js pode ser confundido com um pacote de gráficos, mas ele é muito mais amplo, ele permite a associação de elementos de uma página web com elementos de dados, mapeando atributos de dados para propriedades visuais dos elementos na página web. Para a construção de suas representações, a biblioteca D3.js faz uso extenso das propriedades de desenho presentes na versão 5 da linguagem de marcação para web HTML, em especial da possibilidade de gerar imagens através de código no formato SVG. SVG permite a criação de formas básicas, como retângulos, círculos e linhas e até mesmo elementos mais complexos como polígonos e textos.(CASTILLO, 2014) A combinação destes elementos em SVG dentro dos modelos de visualização disponíveis na galeria de exemplos do D3.js permite ao *designer* de visualização a criação de excelentes visualizações para web de maneira relativamente simples. Os dados podem ser lidos pela biblioteca D3.js a partir de arquivos JSON, CSV, entre outros.

4.7.4 MySQL

MySQL é um sistema de gerenciamento de banco de dados (SGBD) baseado na linguagem *Structured Query Language (SQL)*. Foi desenvolvido por David Axmark, Allan Larsson e o Michael Widenius na Suécia, teve sua primeira versão de teste disponibilizada em 1994. Possui opções de licenciamento gratuitas e comerciais, sendo um software livre. Atualmente se encontra na versão 8. Em 2008 a desenvolvedora MySQL AB, responsável pelo desenvolvimento do MySQL foi adquirida pela Sun Microsystems. Já em 2009, a Sun Microsystems foi adquirida pela Oracle, atual proprietária da ferramenta MySQL. Grandes empresas utilizam o MySQL, entre elas: NASA, Netflix, Youtube, Spotify, Facebook. Apresenta como pontos positivos a flexibilidade na utilização e a escalabilidade, suportando uma grande quantidade de dados (MySQL, 2019).

4.8 Considerações Finais do Capítulo

No presente capítulo foi detalhada a especificação da solução apresentada neste trabalho. O detalhamento passou pelo cenário onde a proposta foi desenvolvida, pelo problema a ser solucionado, a análise de requisitos, o processo de obtenção de dados, a escolha das representações visuais e tecnologias para compor a solução.

5 Comparação com outras ferramentas

5.1 Considerações Iniciais do Capítulo

No presente capítulo são detalhadas ferramentas que podem ser utilizadas para atender às demandas do cenário analisado e avaliadas as vantagens e desvantagens em comparação à especificação apresentada. Após pesquisas realizadas acerca do assunto e consulta a profissionais da área, foram selecionadas as seguintes ferramentas para serem abordadas: Grafana, Kibana, Splunk e Zabdash. Foi realizada uma instalação simples e um breve período de testes, de modo a se obter mais informações sobre cada ferramenta.

5.2 Grafana

Grafana é uma ferramenta gratuita com versão comercial para criação de visualizações em formato de *dashboards* obtendo dados a partir de diversas fontes de dados, entre elas o Zabbix (Grafana Labs, 2018). Uma captura de tela da ferramenta pode ser vista na Figura 21.

A instalação do Grafana para a realização de testes foi realizada no sistema operacional Linux, na distribuição Ubuntu, versão 18.10, através de pacote DEB adicionado ao sistema após download na página do fabricante conforme instruções disponíveis.

- Dependências: Zabbix.
- Preço: Gratuito com opção comercial sem preço informado.
- Limitações: Não possui.
- Licenciamento: Apache 2.0
- Versão: 5.3.4 lançada em 15 de novembro de 2018.
- Pacotes comerciais: Grafana Enterprise: oferece fontes de dados *premium* e *plugins* de autenticação, bem como suporte em tempo integral e treinamento com a equipe central do Grafana. Grafana Cloud: facilita a configuração, operação e dimensionamento do Grafana completamente na nuvem, seguindo o modelo *Software as a Service* (SaaS).
- Sistemas operacionais compatíveis: Windows, Linux e Mac.
- Linguagem de Programação: Não informada.

- Banco de dados: possui Sqlite3 integrado, porém, permite a utilização das opções MySQL e Postgres.
- Gráficos disponíveis: Gráfico de série temporal com linhas, barras e pontos, status simples, tabela de valores, mapas de calor temporais, lista de alertas.

Figura 21 – Tela de simulação de uso do Grafana.

Fonte — Produzida pelo autor.

Grafana é uma ferramenta bem flexível para visualização de dados, possuindo um *plugin* para integração com o Zabbix, se mostrando uma das melhores opções para a visualização de dados de monitoramento de rede. Porém, para o cenário da universidade e em comparação com a especificação deste trabalho, a quantidade de opções de gráficos e as possibilidades de interação com esses gráficos representam limitações em comparação com as possibilidades obtidas através do desenvolvimento de uma nova ferramenta.

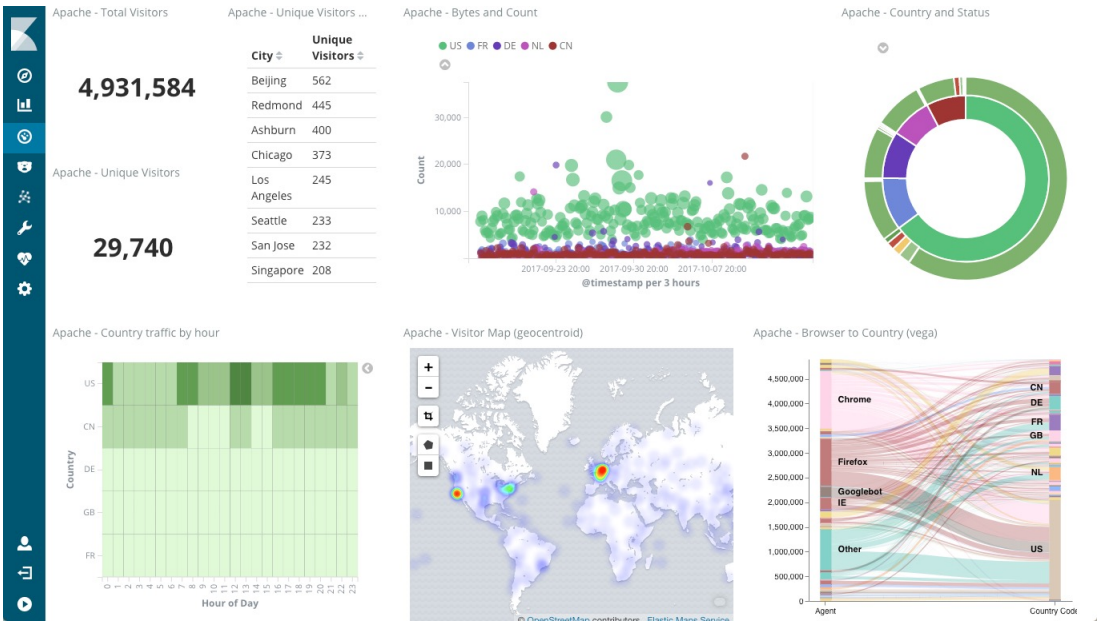
5.3 Kibana

Ferramenta para visualização de dados gratuito que compõe o pacote ou "pilha"de sistemas de software Elastic Stack ou ELK (Elasticsearch, Logstash e Kibana). Serve para geração de visualizações a partir dos dados coletados pela ferramenta Logstash e tratados e manipulados na ferramenta Elasticsearch. Os projetos das três ferramentas foram unidos em junho de 2012, dando origem ao pacote de software como conhecido atualmente (Elastic.co, 2018). Uma captura de tela do Kibana pode ser vista na Figura 22.

Os testes na ferramenta Kibana foram realizados através de uma máquina virtual oferecida pelo grupo Bitnami com o pacote de softwares Elastic Stack (ELK) já implementado.

- Dependências: Compõe pacote Elastic Stack, dependendo do Elasticsearch e do Logstash.
- Preço: Gratuito com opção comercial como serviço em nuvem com preço simulável em site.
- Limitações: Não possui.
- Licenciamento: Apache 2.0
- Versão: 6.5.1 lançada em 20 de novembro de 2018.
- Pacotes comerciais: Elasticsearch Service.
- Sistemas operacionais compatíveis: Windows, Linux e Mac.
- Linguagem de Programação: JavaScript.
- Banco de dados: Não utiliza, atua como extensão do Elasticsearch.
- Gráficos disponíveis: Gráfico de área, mapa de calor, barras horizontais, gráfico de linha, gráfico de torta, barras verticais, tabela de valores, ponteiro, objetivo, métricas simples.

Figura 22 – Tela de exemplo do Kibana.



Fonte — https://www.elastic.co/products/kibana.

A ferramenta Kibana se mostra poderosa para execução de todo tipo de análise de dados, porém, necessita da criação de um cenário elaborado com a utilização do conjunto ELK. Para a necessidade da universidade não é interessante a aplicação de uma solução

de tamanha complexidade, uma vez que já existe uma ferramenta de monitoramento, o Zabbix, implementada. A especificação apresentada se mostra mais vantajosa, pois, trabalha como uma camada desenvolvida sobre o Zabbix.

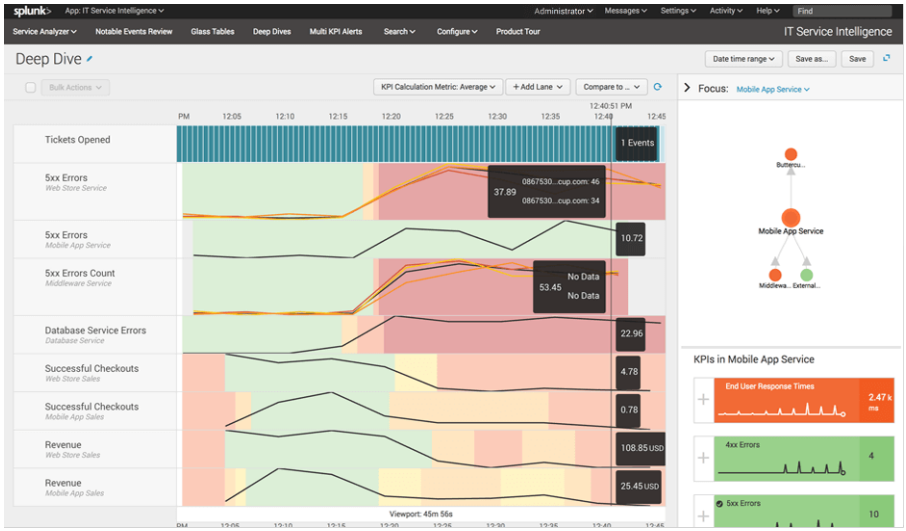
5.4 Splunk

O Splunk é uma ferramenta que captura, indexa e correlaciona dados diversos, entre eles provenientes de equipamentos de rede, em tempo real em um repositório pesquisável, a partir do qual pode gerar gráficos, relatórios, alertas, painéis e visualizações. O Splunk versão 3.0 foi lançado em 6 de agosto de 2007 sendo a primeira versão disponibilizada ao público (Splunk, 2018). Uma captura de tela da ferramenta pode ser vista na Figura 23.

A instalação do Splunk Enterprise Trial para a realização de testes foi realizada no sistema operacional Linux, na distribuição Ubuntu, versão 18.10, através de pacote DEB adicionado ao sistema após download na página do fabricante conforme instruções disponíveis.

- Dependências: Não possui.
- Preço: Gratuito e com versão comercial a partir 150 dólares por mês.
- Limitações: Para a versão gratuita: somente um usuário, trata até 500 MB de dados por dia, busca e análise em tempo real (visualização não) e suporte oferecido pela comunidade.
- Licenciamento: Comercial.
- Versão: 7.2.1 lançada em 02 de outubro de 2018.
- Pacotes comerciais: Splunk Enterprise: sem limitações da versão gratuita. Splunk Cloud: Todos os recursos do Splunk Enterprise oferecido através do padrão SaaS. Splunk Light: opção leve, para organizações menores, oferecido como software ou serviço em nuvem. Possui opções mais completas oferecidas como serviços *premium*.
- Sistemas operacionais compatíveis: Unix e Windows.
- Linguagem de Programação: Não informada.
- Banco de dados: baseado em arquivos.
- Gráficos disponíveis: gráfico de linhas, gráfico de área, gráfico de colunas, gráfico de barras, gráfico de pizza, gráfico de dispersão, gráfico de bolhas, valor simples, ponteiro radial, ponteiro de enchimento, ponteiro de marcadores, mapa de agrupamento, mapa coroplético.

Figura 23 – Tela de exemplo do Splunk.



Fonte — https://www.splunk.com/

O software Splunk se mostrou uma boa opção para análise de dados, inclusive dados de rede, efetuando todas as fases: coleta, tratamento e visualização dos dados. Entretanto, apresenta a desvantagem de ser uma ferramenta comercial, possuindo uma versão gratuita com certas limitações que podem ser inviáveis em certos cenários. A universidade deve priorizar a utilização de ferramentas de software livres e gratuitas, fato esse que em conjunto com as limitações apresentadas na versão gratuita, inviabiliza a utilização do Splunk para o atendimento das necessidades.

5.5 Zabdash

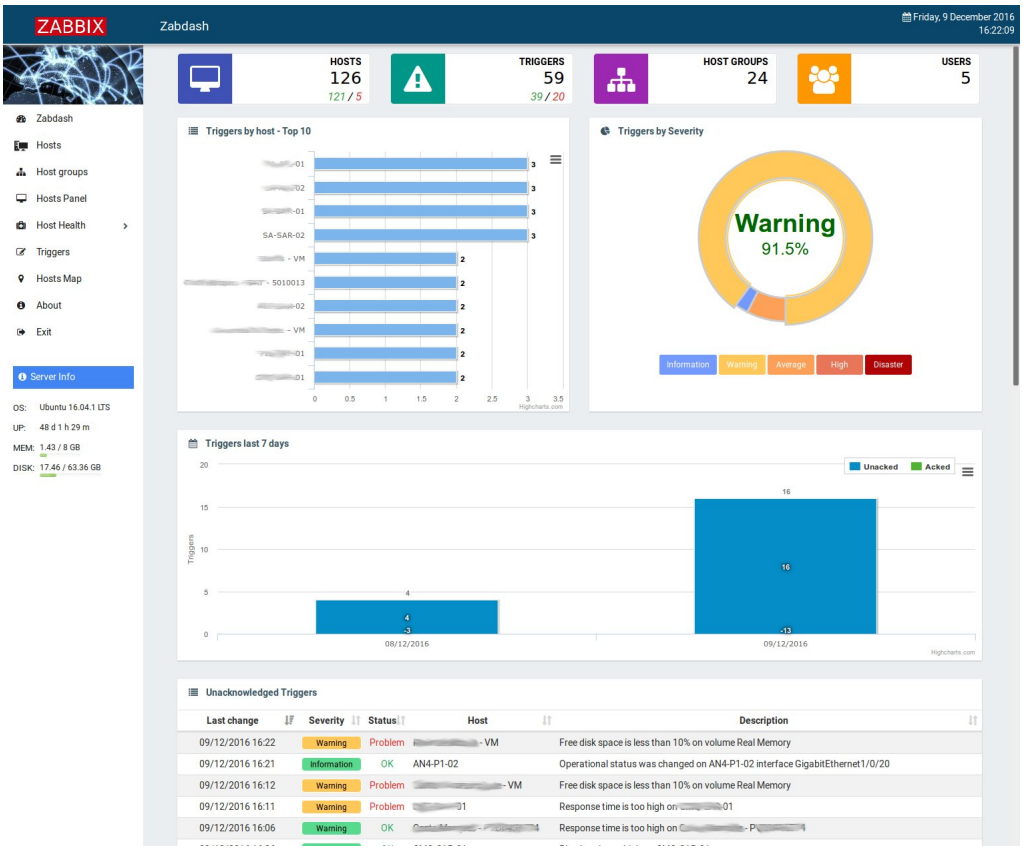
Zabdash é uma extensão para o Zabbix que propõe a adição de uma visualização de *dashboard* gerada a partir dos dados disponibilizados na interface padrão do Zabbix. É fornecida de forma gratuita e aberta através dos repositórios GitHub e SourceForge. Uma captura de tela da ferramenta pode ser vista na Figura 24.

A instalação do Zabdash para a realização de testes foi realizada no sistema operacional Linux, na distribuição Ubuntu, versão 18.04, através da instalação de uma pasta dentro da estrutura do Zabbix previamente instalado através do repositório do sistema operacional.

- Dependências: Zabbix, funciona como extensão.
- Preço: Gratuito.
- Limitações: Não possui.
- Licenciamento: Licença MIT

- Versão: 1.1.2 lançada em 28 de novembro de 2018.
- Pacotes comerciais: Não possui.
- Sistemas operacionais compatíveis: Linux, instalado dentro do Zabbix.
- Linguagem de Programação: PHP.
- Banco de dados: não possui base própria, utiliza a mesma do Zabbix.
- Gráficos disponíveis: Gráfico de série temporal, gráfico de pizza, gráfico de barras.

Figura 24 – Tela de exemplo de uso do Zabdash.



Fonte — https://sourceforge.net/projects/zabdash/.

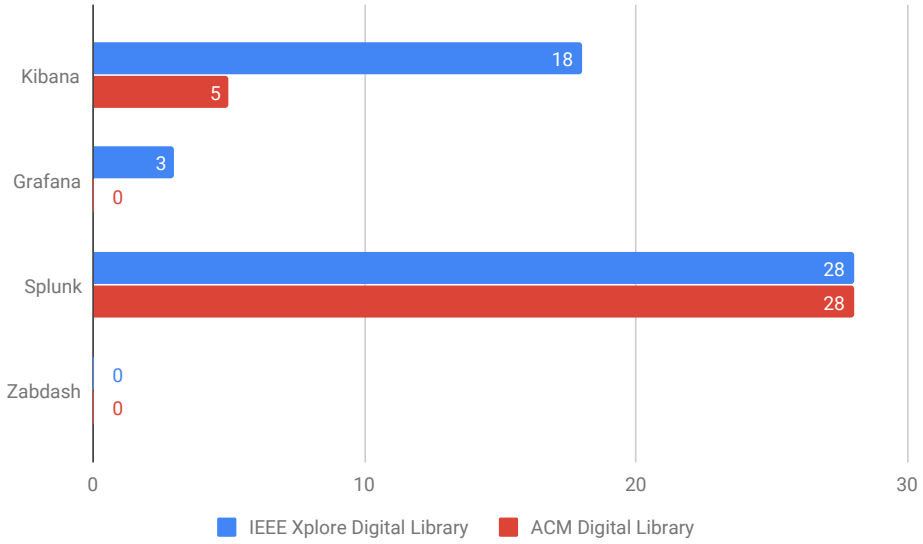
O Zabdash se mostra uma boa opção pela integração grande com o Zabbix e facilidade na instalação, entretanto, possui como limitação a falta de flexibilidade, pois, já possui os gráficos e painéis pré-definidos, sem a possibilidade de customização, se mostrando uma opção pouco viável para o cenário da universidade.

5.6 Trabalhos Relacionados

Foi realizada uma breve busca por estudos relacionados às ferramentas avaliadas nas bases de dados IEEE Xplore Digital Library e ACM Digital Library, utilizando os

termos de busca "Grafana", "Kibana", "Splunk"e "Zabdash". O resultado quantitativo da busca pode ser visto na Figura 25.

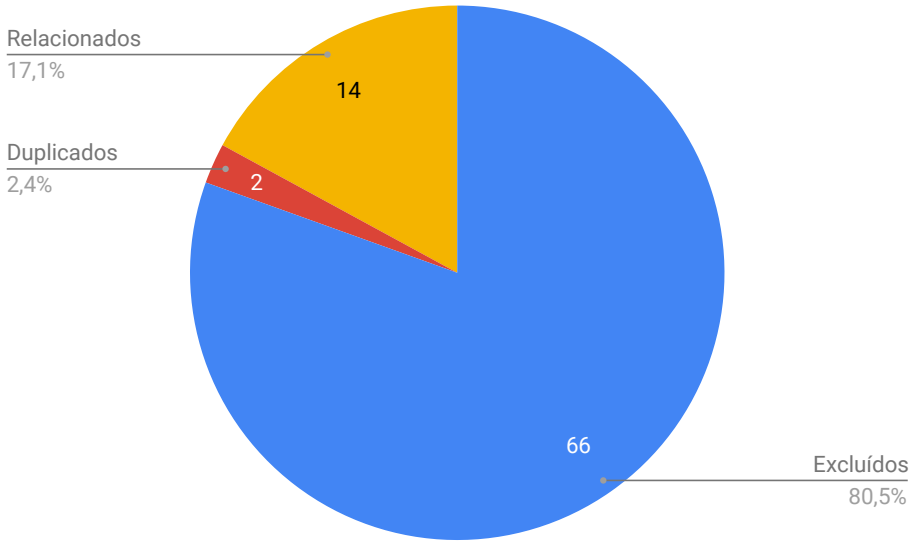
Figura 25 – Resultado quantitativo da busca realizada.



Fonte — Produzida pelo autor.

Após leitura dos resumos e textos completos dos estudos conforme necessidade, foram selecionados 14 estudos, onde o tema Gestão de Redes foi abordado juntamente com uma das ferramentas. A classificação dos estudos pode ser vista na Figura 26.

Figura 26 – Classificação dos Estudos.



Fonte — Produzida pelo autor.

A seguir são descritos brevemente os estudos relacionados:

- (LIU; CHEN, 2010): Detecção de *malwares* com utilização da ferramenta Splunk sobre os dados coletados;
- (PATTON et al., 2011): Ferramenta Splunk agregando e analisando dados de Intrusion detection System (IDS);
- (OZULKU et al., 2014): Criação de ferramenta própria para análise de *logs* e comparação desta ferramenta com Splunk e McAfee Enterprise Log Manager;
- (LAHMADI et al., 2015): Análise com ELK de *logs* e fluxos de rede em aplicações móveis Android;
- (PARK et al., 2015): Utilizando dados de falhas na rede da University of Missouri-Kansas City para análise com Splunk.
- (MOH et al., 2016): Análise de *logs* web de modo a evitar SQL injection, baseado em Bayes Net para aprendizado de máquina e Kibana para reconhecimento de padrões;
- (OKUMURA; FUJIMURA, 2016): Criação e análise de coleção de *logs* com Splunk para a Universidade de Fukuoka;
- (BRATTSTROM; MORREALE, 2017): Sistema de monitoramento baseado em SNMP, com banco Prometheus Time Series e visualizações através de Grafana;
- (CHEN; GURGANUS, 2017): Simulação de ataques e anormalidades em servidores e análise com Splunk;
- (HAMDAN, 2017) Análise de *logs* de servidores web por alunos em curso de Segurança da Informação utilizando Splunk;
- (MCELWEE et al., 2017): Classificador para *logs* com aprendizagem de máquina e uso do Kibana e ELK;
- (VAZHKUDAI et al., 2017): Monitoramento de estrutura de computação de alto desempenho da Oak Leadership Computing Facility com ferramenta Splunk;
- (ALMOHANNADI et al., 2018): Análise de *logs* de *honeypot* com ELK para identificação de padrões de ataque;
- (LV et al., 2018): Monitoramento de rede de alta performance com Kibana e coleta de NetFlow com Filebeat;

5.7 Considerações Finais do Capítulo

Pode-se concluir que as ferramentas analisadas se mostram como opções para a realização da aplicação da Visualização da Informação na gestão e monitoramento de redes, porém, dentro das necessidades levantadas no cenário da universidade, a especificação apresentada neste trabalho se mostra mais adequada. Um resumo da comparação entre as ferramentas pode ser visto no Quadro 5.

A ferramenta apresentada na especificação proposta se mostra mais vantajosa por depender somente do Zabbix, uma solução de monitoramento que já se encontra em uso, por não apresentar custos de aquisição e licenciamento, por poder ser facilmente implantada em um servidor que suporte a hospedagem de páginas na linguagem PHP e por utilizar visualizações projetadas de acordo com as melhores práticas e de forma customizada para o cenário. A necessidade de desenvolvimento pode ser considerada um ponto negativo na comparação, mas a utilização da biblioteca D3.js para acelerar o processo de desenvolvimento e as opções de customização possíveis ajudam a embasar a decisão pelo desenvolvimento. No quadro 6 pode-se verificar as ponderações dos pontos positivos e negativos de cada opção de solução, totalizando a pontuação obtida por cada uma delas, onde pode-se verificar que dentro da avaliação realizada, a solução especificada se mostrou mais vantajosa.

Quadro 5 – Quadro de comparação entre as ferramentas

Item	Grafana	Kibana	Splunk	Zabdash	Solução Especificada
Dependências	Zabbix	Elasticsearch e Logstash	Não possui	Zabbix	Zabbix
Preço	Gratuito com opção comercial sem preço informado	Gratuito com opção comercial em nuvem com preço simulável	Gratuito e com versão comercial a partir 150 dólares por mês	Gratuito	Gratuito
Limitações	Não possui	Não possui	1 usuário, trata até 500 MB/dia, busca e análise em tempo real e suporte pela comunidade	Não possui	Não possui
Sistemas operacionais compatíveis	Windows, Linux e Mac	Windows, Linux e Mac	Unix e Windows	Linux, instalado dentro do Zabbix	Qualquer um que suporte hospedagem PHP
Linguagem de Programação	Não informada	JavaScript	Não informada	PHP	PHP e Javascript
Banco de dados	Sqlite3, MySQL e Postgres	Não utiliza	baseado em arquivos	Não possui base própria, utiliza a mesma do Zabbix	Baseado em arquivos e MySQL para configurações
Gráficos disponíveis	Série temporal com linhas, barras e pontos, status simples, tabela de valores, mapas de calor temporais, lista de alertas	Área, mapa de calor, barras horizontais, linha, torta, barras verticais, tabela de valores, ponteiro, objetivo, métricas simples	Linhas, área, colunas, barras, pizza, dispersão, bolhas, valor simples, ponteiro radial, ponteiro de enchimento, ponteiro de marcadores, mapa de agrupamento, mapa coroplético	Série temporal, pizza, barras.	Área proporcional, barras, colunas, barras empilhadas, séries temporais

Fonte: Fonte — Produzida pelo autor.

Quadro 6 – Quadro de pontuação das ferramentas

Ferramentas	Grafana	Kibana	Splunk	Zabdash	Solução especificada
Dependência	Zabbix	ELK	Não possui	Zabbix	Zabbix
Pontuação	0	-1	1	0	0
Preço	Grátis com opção comercial	Grátis com opção comercial	Grátis limitado com opção comercial	Grátis	Grátis
Pontuação	0	0	-1	1	1
Limitações	Não possui	Não possui	Possui	Não possui	Não possui
Pontuação	1	1	-1	1	1
Customização	Limitada	Limitada	Limitada	Não é possível	Possível
Pontuação	0	0	0	-1	1
Necessidade de desenvolvimento	Não	Não	Não	Não	Sim
Pontuação	1	1	1	1	0
Pontuação Total	2	1	0	2	3

Fonte: Produzida pelo autor.

6 Desenvolvimento

6.1 Considerações Iniciais do Capítulo

No presente capítulo é detalhado o desenvolvimento da ferramenta, já em fase de implantação, são descritos os módulos que compõem a ferramenta, as interações realizadas durante o desenvolvimento e as decisões de design tomadas.

6.2 Módulos

Optou-se pelo desenvolvimento modular da ferramenta, de forma que novas funcionalidades foram acrecidas com a criação de cada módulo. Foram criados os seguintes módulos compondo a ferramenta:

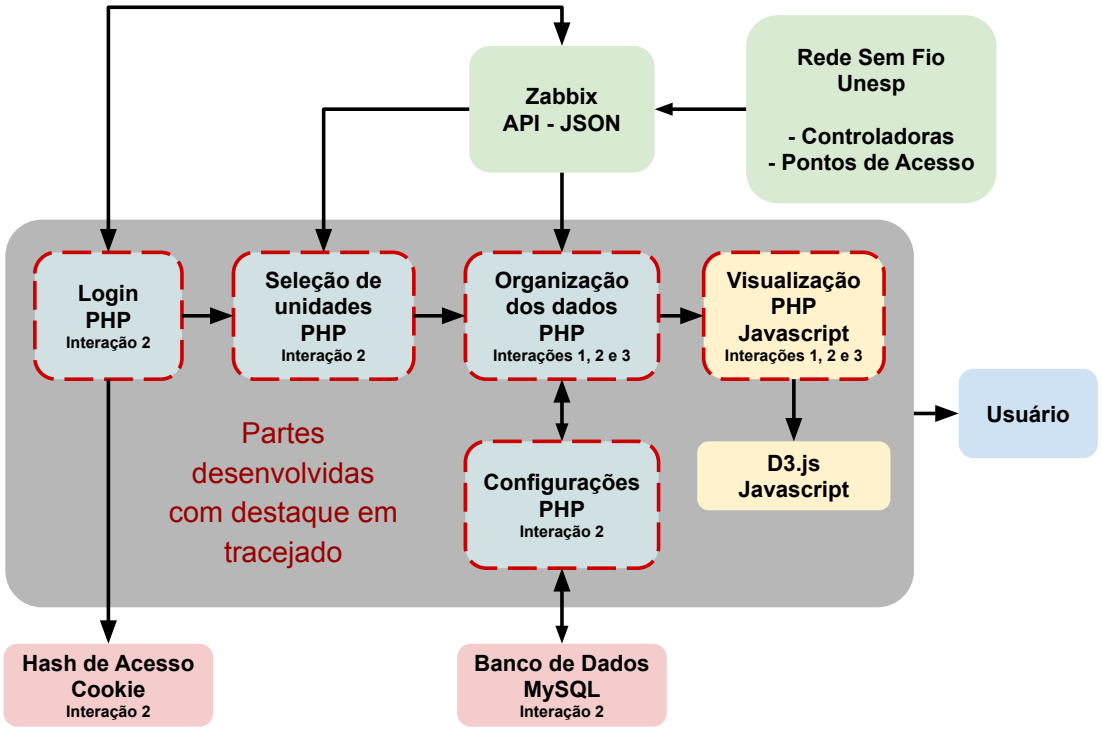
- Login: para gerenciamento dos acessos à ferramenta;
- Seleção de unidades: para escolha da unidade desejada;
- Organização de dados: para tratamento dos dados provenientes do Zabbix;
- Configurações: para customização e armazenamento das configurações; e
- Visualização: para criação e exibição dos gráficos.

Na Figura 27 são mostrados os módulos que compõe a aplicação.

Durante a autenticação, a ferramenta se comunica com o usuário por meio do seu navegador e com o Zabbix para validação das informações de acesso. Durante a seleção da unidade a ferramenta se comunica com o Zabbix e com o banco de dados, obtendo assim as configurações do usuário para aquela unidade. Já no processo de geração das visualizações a comunicação é entre a aplicação e o Zabbix, para criação e fornecimento dos gráficos ao usuário. Desta forma é gerado o fluxo de dados entre os diferentes componentes do sistema que pode ser visto na Figura 28.

O banco de dados implementado por meio do SGBD MySQL é representado no modelo presente na Figura 29. No banco de dados estão presentes duas tabelas: usuários, onde cada utilizador do sistema é registrado e configurações, onde as customizações de configurações feitas por cada usuário, para as diferentes unidades, são armazenadas. A tabela de usuários conta com a chave primária "codUsuario"e a tabela de configurações conta com a chave primária "codConfig"e com a chave estrangeira "codUsuario".

Figura 27 – Diagrama mostrando os módulos que formam a aplicação, em destaque tracejado os que foram desenvolvidos, com a indicação das interações em que foram criados e alterados.



Fonte — Produzida pelo autor.

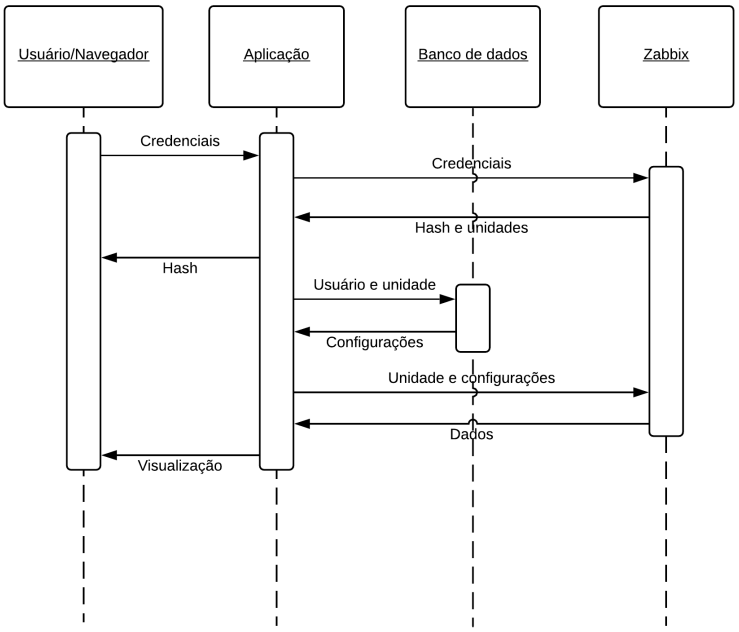
Durante o desenvolvimento da ferramenta, diversos ciclos de interação contemplando as atividades de desenvolvimento, testes e avaliação foram realizados, acrescentando funcionalidades à ferramenta. As próximas seções detalham as interações.

6.3 1ª Interação

A primeira interação estruturou a base da ferramenta, implementando as seguintes funcionalidades:

- Módulo de visualização — módulo utilizado para criação das visualizações com apoio da biblioteca D3.js, realiza a chamada da biblioteca e a geração das visualizações;
- Módulo de organização de dados — módulo para tratamento e organização dos dados, recebe os dados da API do Zabbix, realiza a organização dos dados de forma que sejam aceitos pela biblioteca D3.js e gerem as visualizações;

Figura 28 – Diagrama de sequência mostra o fluxo de dados no sistema da aplicação.



Fonte — Produzida pelo autor.

- Tela principal — a tela principal da aplicação foi desenvolvida priorizando tons de azuis, se baseando na identidade visual da Unesp, cada ponto de acesso possui uma série de informações relacionadas que são exibidas ao se passar o cursor do mouse sobre o respectivo círculo. A construção das telas da aplicação foi realizada considerando como requisito mínimo a tela de um computador de 14 polegadas com resolução de 1366 *pixels* por 768 *pixels*, a opção por essa tela base com resolução e tamanho reduzidos garante o funcionamento da aplicação na maioria dos equipamentos atuais;

- Seleção de intervalos — foi implementado um controle deslizante para ajuste do período utilizado para geração das visualizações, sendo a posição inicial de 1 hora e o intervalo ajustável até 24 horas;

- Lista lateral e busca — para agilizar o processo de localização de um ponto de acesso em específico, foi implementada uma lista lateral exibindo todos os itens e contando com um campo de busca que filtra instantaneamente os pontos de acesso de acordo com a *string* inserida para a busca;

- Estados de atenção — a cor dos círculos se altera de acordo com o estado do ponto de acesso representado, se tornando amarela caso ultrapasse o limite de tráfego ou usuários definido na área lateral e vermelha caso se encontre *offline*;

- Abas superiores — os diferentes equipamentos (pontos de acesso e controladoras) são separados por meio das abas superiores, a aba atualmente exibida se diferencia

Figura 29 – Modelo representando o banco de dados que compõe a aplicação.

Fonte — Produzida pelo autor.

por meio das cores mostradas na aba;

- Animações de carregamento — quando ocorre mudança de parâmetros (intervalo e limite) ou recálculo, a página é recarregada. Durante esse processo a tela exibe uma animação de carregamento. Optou-se pela inserção dessa animação para oferecer ao usuário um *feedback* de que a alteração que ele executou foi aceita e está sendo carregada;

- Tela de visão detalhada — o detalhamento dos dados que compõe a visualização foi realizado por meio de uma tela exibindo um gráfico de série temporal, disponibilizado tanto para os pontos de acesso como para as controladoras. Para exibição de visualizações de detalhamento se utilizou a técnica de *lightbox*, onde a nova página é carregada de maneira sobreposta a anterior, sem a criação de uma nova aba ou janela, escurecendo o conteúdo da janela ao fundo. Essa técnica aumenta a sensação de imersão na aplicação. Nas visualizações de séries temporais foi implementado um destaque ao se passar o mouse sobre a série temporal desejada, aumentando a espessura da linha e um rótulo com o nome da série; e

- Tela de *log* — foi implementada uma tela auxiliar para exibição do *log* de cada ponto

de acesso de forma completa, dentro da tela de detalhamento.

6.4 2ª Interação

A segunda interação estruturou a ferramenta para utilização em múltiplas unidades e buscou resolver problemas de desempenho, implementando as seguintes funcionalidades:

- Módulo de configurações e banco de dados — houve a necessidade de implementação de um banco de dados MySQL para armazenamento das configurações de cada usuário nas diferentes unidades, pois, anteriormente, na primeira interação, as configurações eram armazenadas em um arquivo único para todos os usuários. Foi desenvolvida também uma tela para ajustes das configurações com as opções de importação e exportação por meio de arquivos no formato XML;
- Módulo de seleção de unidades — foi desenvolvida uma tela para seleção da unidade que tem seus dados visualizados, baseada nas permissões disponíveis para aquele determinado usuário no Zabbix;
- Módulo de login — foi elaborado o módulo de login, permitindo a verificação das credenciais de forma *online* no Zabbix, com a gravação da *hash* de acesso no navegador do usuário por meio de *cookie* e o carregamento das configurações para o usuário através do banco de dados; e
- Médias e desempenho — inicialmente foi utilizada a função *history* da API do Zabbix, de modo a se obter todas as medidas coletadas no período para posterior cálculo da média, entretanto, o desempenho da aplicação utilizando esta função não era satisfatório, desta forma, se optou pela utilização da função *trend*, que retorna a médias calculadas a cada período de 1 hora, reduzindo assim a quantidade de dados devolvidos pela API e reduzindo a quantidade de cálculos necessários. Para esta alteração foi necessária a alteração dos períodos selecionados, permitindo somente intervalos fechados, como das 8:00 às 9:00.

6.5 3ª Interação

A terceira interação buscou finalizar o atendimento aos requisitos da especificação e aprimorar a usabilidade, implementando as seguintes funcionalidades:

- Tela de rankings — foi implementada uma nova tela que apresenta a classificação dos pontos de acesso por meio de diversas grandezas, mostrando estado dos equipamentos, maiores consumidores de banda, maior quantidade de clientes conectados e pontos de acesso associados a menos tempo;

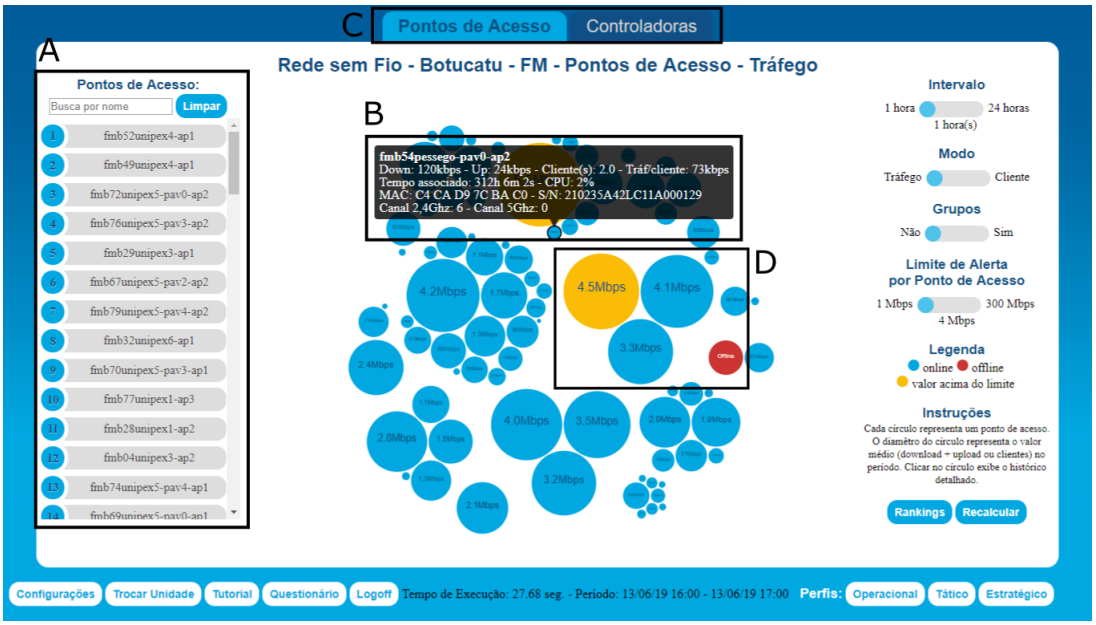
- Seleção de perfis — foram disponibilizados botões que ajustam toda interface para predefinições que atendem os perfis definidos anteriormente na especificação;
- Seleção de modos — a seleção entre a exibição de dados de tráfego e de clientes passou a ser realizada por meio de um controle deslizante na barra lateral;
- Grupos — foi desenvolvida a opção de agrupamentos dos pontos de acesso por meio de um conjunto de palavras pré-cadastradas, possibilitando a separação em grupos referentes aos diferentes prédios e áreas que compõe cada unidade universitária;
- Atualização de dados — para aprimoramento do desempenho foi alterado o comportamento da aplicação, de modo que a consulta a API fosse realizada somente quando necessária, sem a necessidade de se coletar novamente os dados quando não houvesse alteração do período utilizado para a visualização; e
- Opção recalcular — foi incluído um botão para acesso direto à opção de recálculo, onde todos os dados são descartados e a visualização é construída novamente consultando os dados através da API. Está opção foi criada para possibilitar a eliminação de todos os dados armazenados no servidor, de forma que a consulta novamente ao Zabbix seja obrigatória, esta funcionalidade foi implementada para facilitação dos testes.

6.6 Considerações Finais do Capítulo

Neste capítulo foi apresentado o processo de construção da ferramenta, apresentando as funcionalidades e os módulos desenvolvidos a cada interação. Através disso, pode-se compreender melhor o funcionamento e objetivo da aplicação e sua importância dentro do projeto.

Durante o processo de construção da ferramenta, certas decisões foram tomadas acerca do desenho da ferramenta, buscando agregar funcionalidades e melhorar a usabilidade do usuário. Nas Figuras 30, 31 e 32 pode-se visualizar algumas das decisões de design tomadas:

Figura 30 – Decisões de design — O uso das cores da identidade visual da Unesp, detalhe A mostra a lista lateral e o campo de busca, detalhe B mostra o detalhamento dos dados do ponto de acesso, detalhe C mostra as abas superiores e detalhe D mostra os elementos com as cores alteradas.

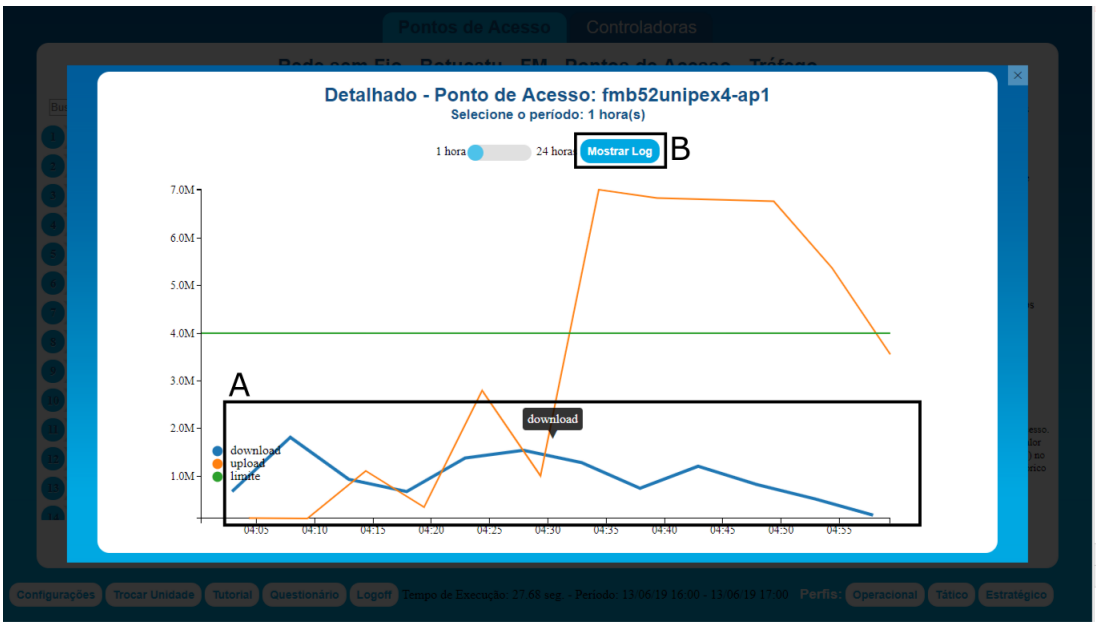


Fonte — Produzida pelo autor.

Figura 31 – Decisões de design — Animação de carregamento.

Fonte — Produzida pelo autor.

Figura 32 – Decisões de design — Gráfico de série temporal sendo mostrado dentro de um *lightbox*, detalhe A mostrando série temporal em destaque e detalhe B mostrando botão para acesso ao *log* do equipamento.



Fonte — Produzida pelo autor.

7 Avaliação

7.1 Considerações Iniciais do Capítulo

Para validação da ferramenta proposta, comprovando a hipótese levantada anteriormente, optou-se pela realização da avaliação de usabilidade da ferramenta com a participação de usuários provenientes de diversas unidades da Unesp. A seguir será exposto todo esse processo de avaliação, desde a escolha do método até a contabilização dos resultados.

7.2 Métodos

As avaliações podem ocorrer em vários locais, como laboratórios, residências, ambientes externos e ambientes de trabalho, além disso, existem diversos métodos de avaliação de interface, qual usar depende dos objetivos da avaliação, Nielsen (1994) classifica esses métodos em três categorias:

- Métodos Analíticos ou de Inspeção: Heurística, Percurso Cognitivo, *Checklist*, etc. Nesta categoria, a avaliação é feita pelos projetistas e por profissionais da área de Interface, sem a participação dos usuários. Esta avaliação é realizada através da aplicação de regras e conceitos já pré-determinados na literatura e dos objetivos previamente definidos no própria especificação e também da simulação do comportamento do usuário.

- Métodos Empíricos ou Teste com Usuários: Teste de Usabilidade e Percurso Pluralístico, etc. Esta categoria inclui instrumentos que permitem a participação dos usuários durante todo processo de desenvolvimento. Nestes métodos é utilizado o sistema implementado ou um protótipo de alta-fidelidade para execução de testes, visando avaliar a facilidade de manipulação e a sequência de telas que compõe o sistema.

- Outras Formas: Modelo Goals, Operators, Methods, Selections Rules (GOMS) e Questionários, etc. Estes métodos contam com a participação parcial dos usuários, ou seja, somente em parte do processo de desenvolvimento. Nesses métodos pode-se avaliar a utilização do sistema através da medição do tempo necessário para execução de tarefas predeterminadas, o que não leva em consideração as diferenças individuais de cada utilizador, e através da aplicação de questionários, identificando as preferências e níveis de satisfação através de perguntas diretas ao utilizador.

7.3 Avaliações Integradas ao Desenvolvimento

Durante o desenvolvimento da ferramenta que compõe a solução, de forma prática, métodos de inspeção, como heurística, percurso cognitivo e inspeção de consistência, foram sendo aplicados através de testes e simulações realizados juntamente com a equipe de informática da FMB, utilizando o conhecimento disponível sobre melhores práticas no desenvolvimento de interfaces.

Na etapa final de desenvolvimento, foram realizados testes de usabilidade com funcionários de outra unidade da Unesp, que pode ser considerada uma amostra do público alvo do sistema, realizando assim um ensaio de interação (DIAS, 2007), avaliando principalmente o funcionamento dos módulos que gerenciam a utilização em múltiplas unidades, coletando a opinião dos usuários envolvidos nos testes, de forma a aprimorar o sistema para a próxima etapa de testes.

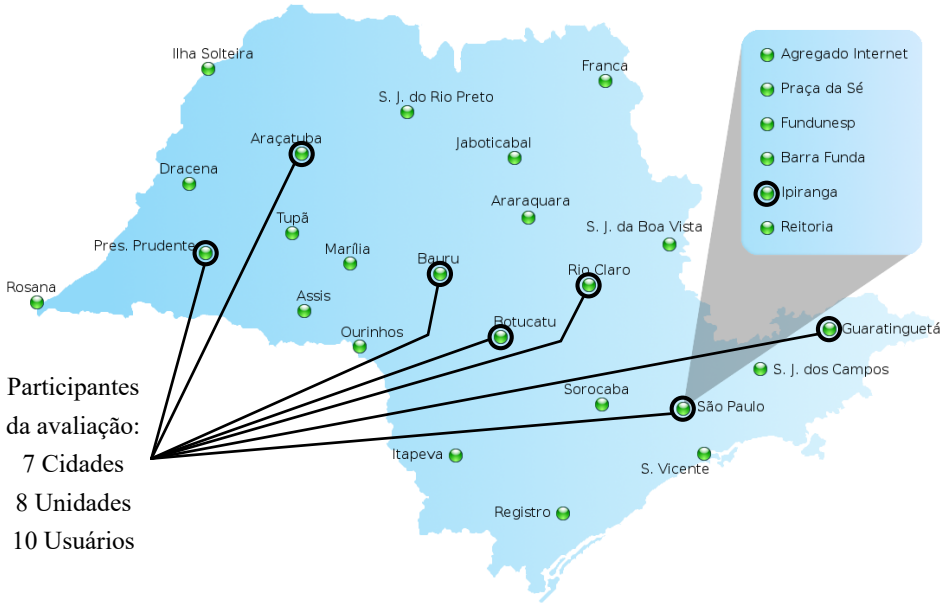
7.4 Questionário

Para aplicação de um questionário, o mesmo deve ser preparado com antecedência, buscando as melhores questões para o contexto desejado. Os questionários podem ser elaborados a partir de questões abertas, de múltipla escolha, etc. Como vantagem pode-se citar que um questionário pode ser aplicado a um número grande de pessoas sem um grande custo. Para a avaliação final da ferramenta desenvolvida optou-se pelo método de questionários.

O questionário desenvolvido se baseou no questionário QUIS, criado em 1987 por um grupo multidisciplinar de estudos do Laboratório de Interação Humano-Computador da Universidade de Maryland, para avaliação de interfaces. O modelo original de avaliação leva em conta 9 fatores, porém, optou-se por simplificar certas questões e omitir seções que não se aplicavam ao contexto de ferramenta. As questões que compõe o questionário QUIS possuem respostas numéricas que variam de "1"como aspecto mais negativo a "9"como aspecto mais positivo, contando também com a opção "Não aplicável".

O público inicial para aplicação do questionário foi definido em 12 unidades da Unesp, selecionando unidades com perfis diversos (menor e maior porte, mais próximas dos interior e na capital) e espalhadas pelo estado de São Paulo. O pedido de avaliação foi enviado ao responsável pela rede em cada unidade. Obteve-se retorno de 10 usuários, pertencentes a 8 unidades distribuídas em 7 cidades, realizando os testes solicitados e respondendo ao questionário. Houve dificuldade na adesão dos profissionais a utilização e avaliação da ferramenta, mesmo após diversos contatos, através de diferentes meios de comunicação (ligações, mensagens de e-mail e mensagens instantâneas). A distribuição destes avaliadores pode ser vista na Figura 33.

Figura 33 – Distribuição dos avaliadores.



Fonte — Produzida pelo autor.

7.5 Tutorial

Para acompanhar e apoiar o processo de avaliação, foi criado um tutorial integrado à ferramenta, utilizando a linguagem HTML e animações GIF, onde são apresentados todos os recursos da ferramenta, de forma a esclarecer o usuário em caso de dúvida. Uma versão deste tutorial está apresentado no Apêndice C.

7.6 Questões e Respostas

A seguir são detalhadas as questões que compõe o questionário e as respostas obtidas. O questionário foi composto por uma etapa de identificação e 8 partes voltadas a diferentes aspectos da interface. Para aplicação do questionário foi utilizada a plataforma de questionários online Google Forms, no Apêndice D todas as perguntas que compõe o questionário são apresentadas de forma textual.

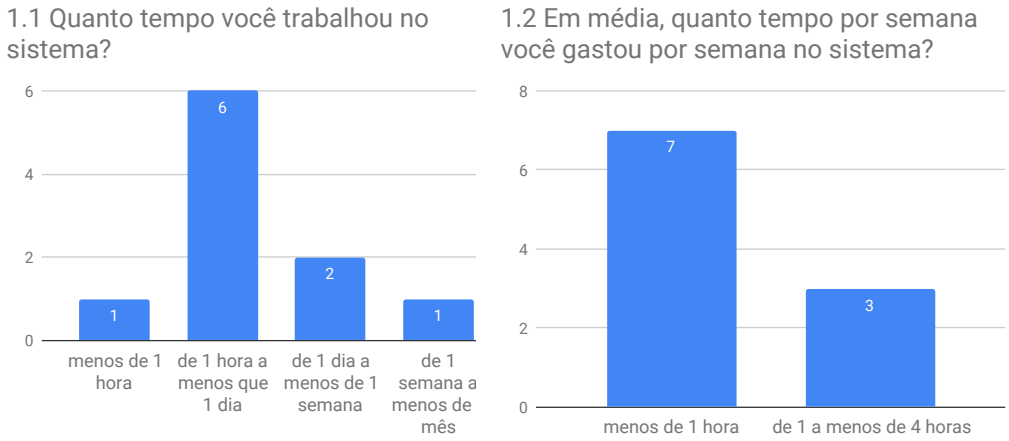
7.6.1 Identificação

Para identificar o avaliador, foram solicitadas as seguintes informações: e-mail (através do login), nome, idade e gênero. A idade dos avaliadores varia entre 30 e 54 anos, todos do gênero masculino.

7.6.2 Parte 1 - Experiência com o sistema

As perguntas que compõem esta parte do questionário e as respostas recebidas podem ser vistas na Figura 34.

Figura 34 – Os gráficos de colunas demonstram o tempo de utilização do sistema pelos avaliadores.



Fonte — Produzida pelo autor.

Verifica-se que os avaliadores utilizaram, em sua maioria, a ferramenta por um período de 1 hora a menos de 1 dia, sendo menos de 1 hora por semana.

7.6.3 Parte 2 - Experiências passadas

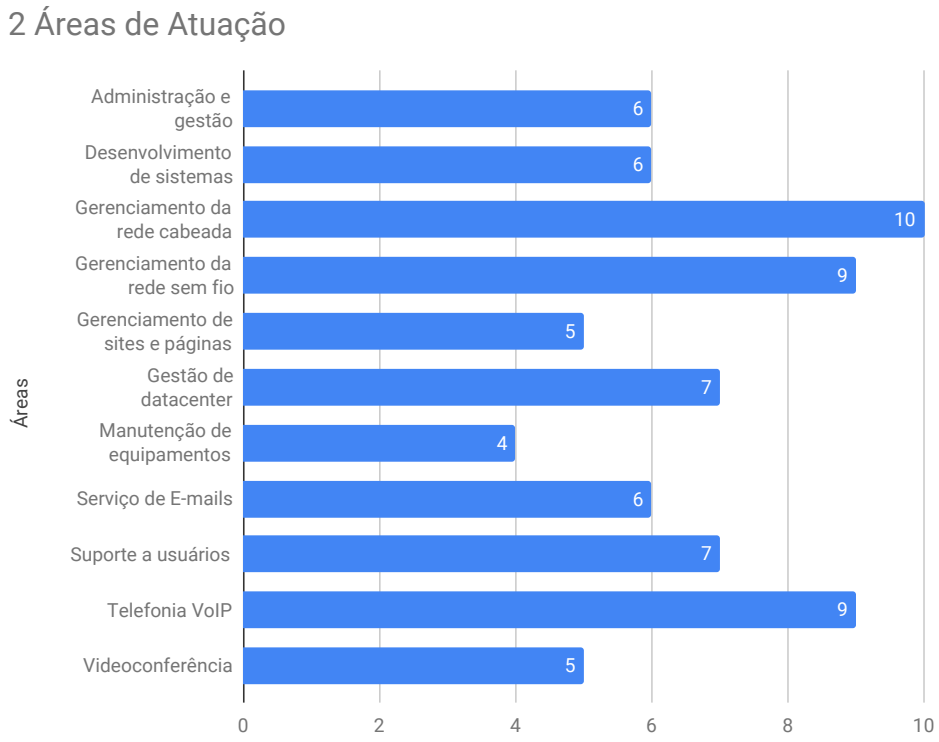
A pergunta que compõe esta parte do questionário e as respostas recebidas podem ser vistas na Figura 35.

Percebe-se que todas as áreas disponíveis no questionário foram escolhidas, com destaque para gerenciamento de redes cabeada e sem fio e telefonia VoIP, com isso pode-se concluir que os avaliadores possuem boa experiência no gerenciamento de redes e infraestrutura de comunicações.

7.6.4 Parte 3 - Reações Gerais do Usuário

As perguntas que compõe esta parte do questionário e as respostas recebidas podem ser vistas na Figura 36.

Figura 35 – O gráfico de barras demonstra as áreas de atuação dos avaliadores.



Fonte — Produzida pelo autor.

Pode-ser observar uma constância nas respostas fornecidas às questões de "3.1"a "3.4", mantendo-se acima do valor 7, demonstrando reações positivas. Entretanto, na questão "3.5 Rígido ou Flexível?"houve uma variação maior, chegando ao valor 4, demonstrando certa insatisfação com relação à flexibilidade apresentada pela ferramenta.

7.6.5 Parte 4 - Telas

As perguntas que compõem esta parte do questionário e as respostas recebidas podem ser vistas na Figura 37.

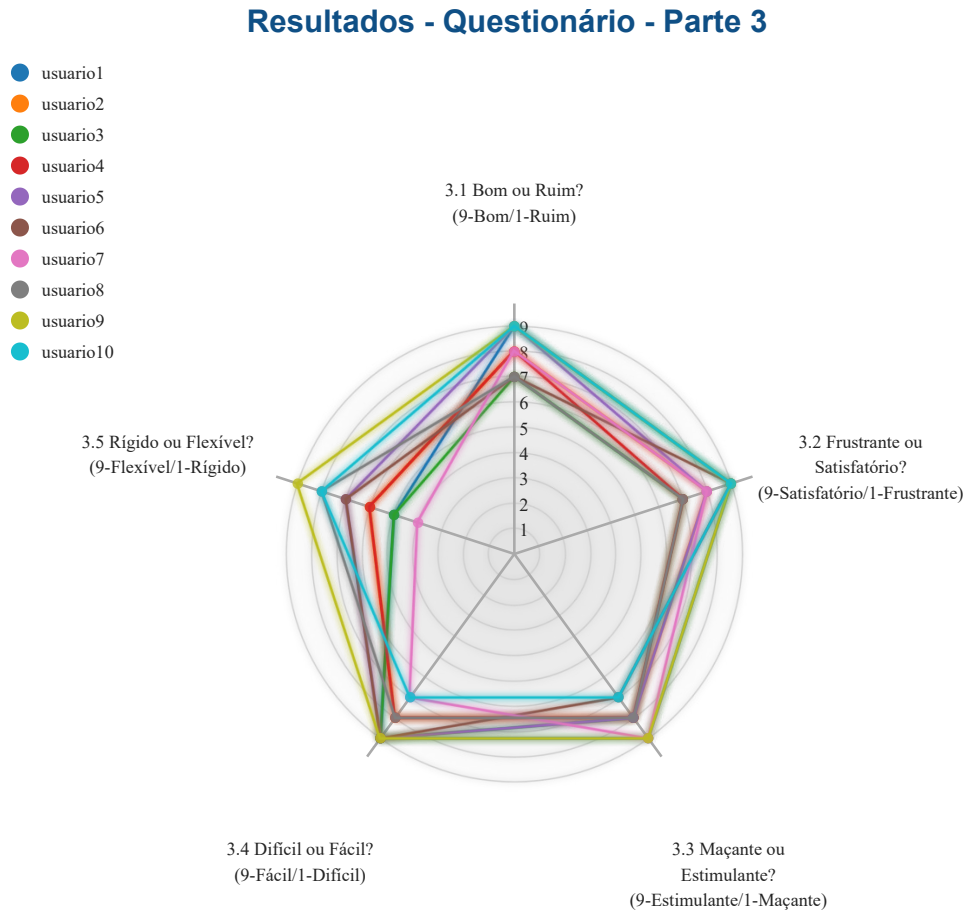
Pode-se observar uma constância nas respostas fornecidas às questões de "4.1"a "4.5", mantendo-se acima do valor 7, demonstrando reações positivas, com destaque a questão "4.2 Destaques na tela", que recebeu somente respostas iguais ou maiores que 8.

7.6.6 Parte 5 - Terminologia e Informações do sistema

As perguntas que compõem esta parte do questionário e as respostas recebidas podem ser vistas na Figura 38.

Pode-ser observar uma constância nas respostas fornecidas às questões de "5.1"a

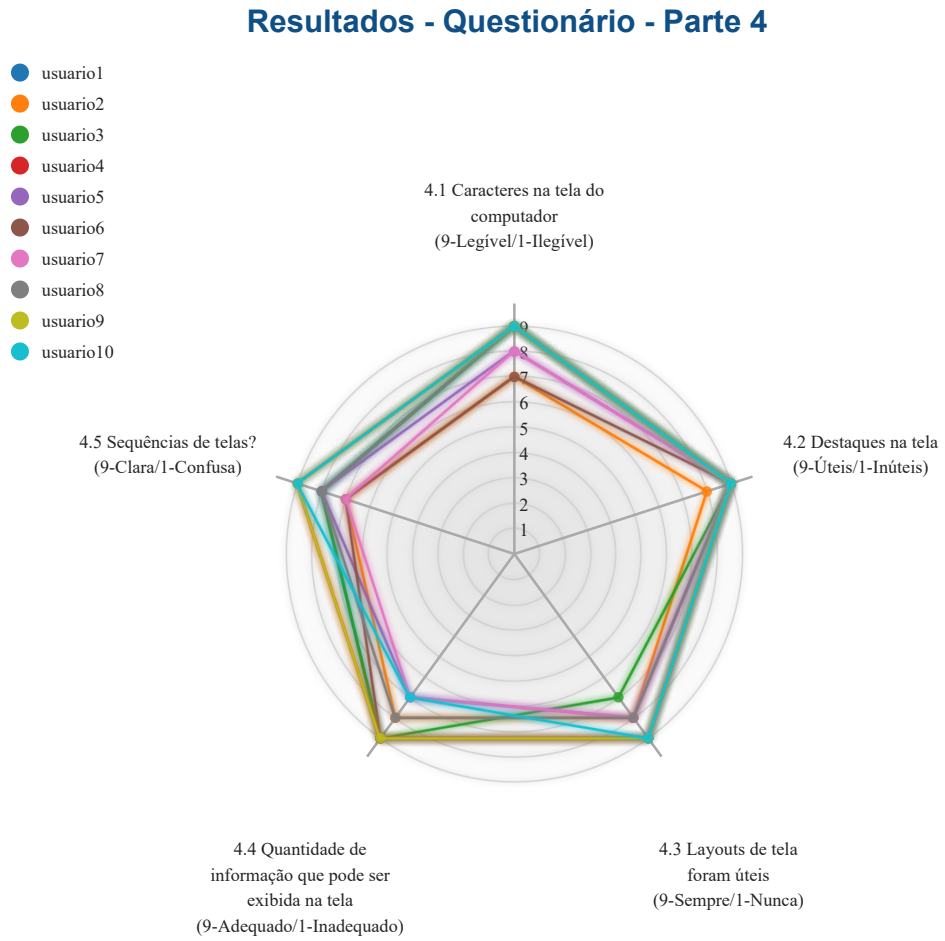
Figura 36 – O gráfico de radar exibe as respostas dadas as questões que compõem a Parte 3 do questionário.



Fonte — Produzida pelo autor.

"5.4"e "5.7", mantendo-se acima do valor 7, demonstrando reações positivas. As questões "5.5 Instruções para corrigir erros"e "5.6 Computador mantém você informado sobre o que está fazendo"receberam respostas com valores menores, mostrando possíveis problemas na comunicação de situações de carregamento e instruções para correção de erros. Dois usuários optaram por responder como não aplicáveis certos aspectos desta parte do questionário.

Figura 37 – O gráfico de radar exibe as respostas dadas as questões que compõem a Parte 4 do questionário.



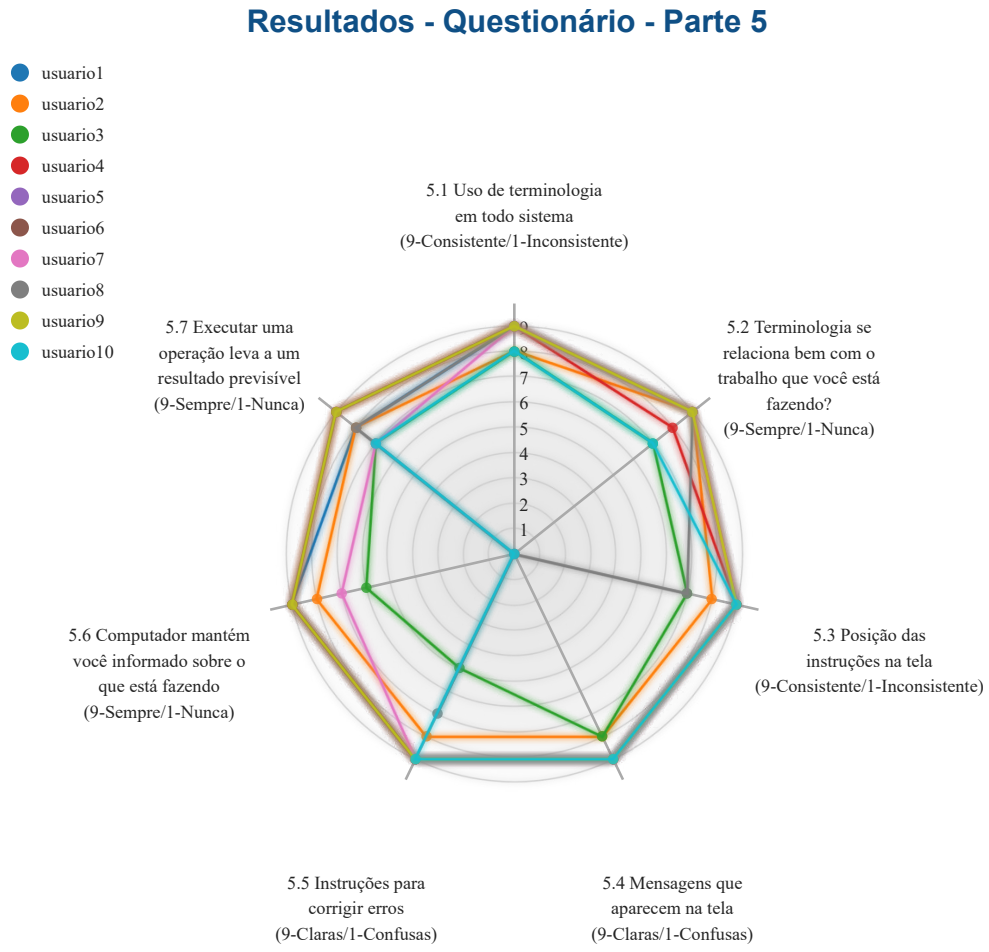
Fonte — Produzida pelo autor.

7.6.7 Parte 6 - Aprendizagem

As perguntas que compõem esta parte do questionário e as respostas recebidas podem ser vistas na Figura 39.

Pode-ser observar uma constância nas respostas fornecidas às questões desta parte do questionário, mantendo-se acima do valor 7, demonstrando reações positivas.

Figura 38 – O gráfico de radar exibe as respostas dadas as questões que compõem a Parte 5 do questionário.



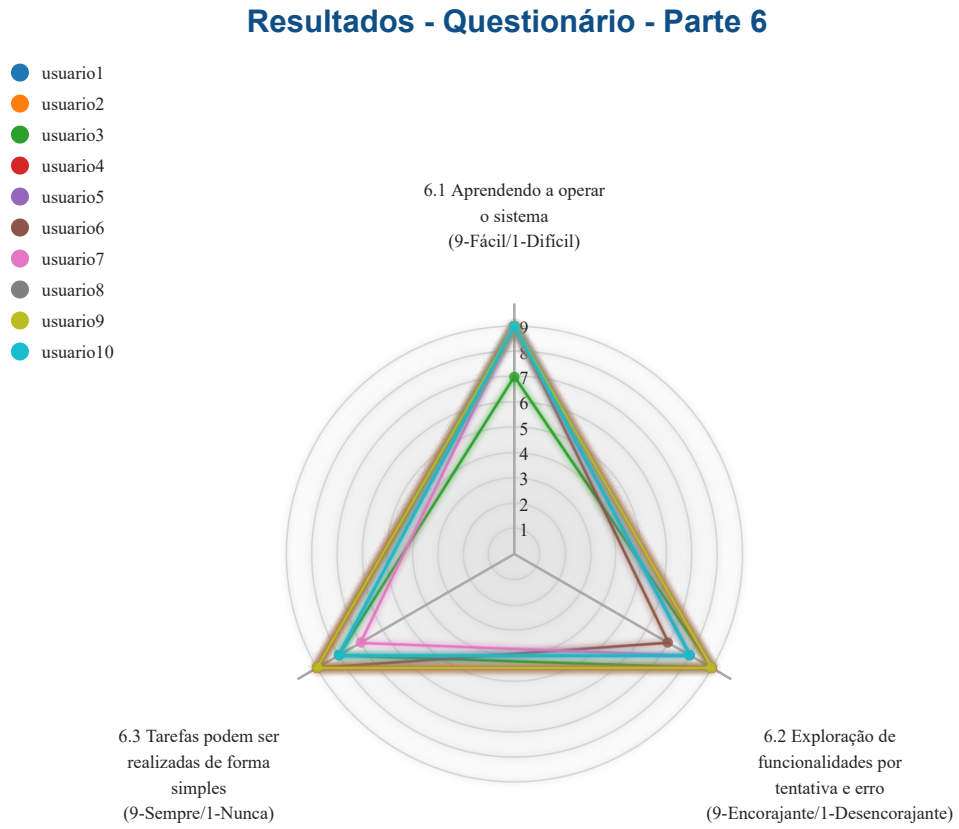
Fonte — Produzida pelo autor.

7.6.8 Parte 7 - Capacidades do Sistema

As perguntas que compõem esta parte do questionário e as respostas recebidas podem ser vistas na Figura 40.

A questão "7.1 Velocidade do sistema"obteve respostas variadas, demonstrando certa instabilidade na velocidade do sistema. A questão "7.2 O sistema é confiável"recebeu diversas respostas entre 8 e 9 e uma única resposta de valor 5, demonstrando que um avaliador teve problemas relacionados à confiabilidade do sistema. As questões "7.3"e "7.4"relacionadas a erros do sistema tiveram somente respostas positivas, iguais ou superiores a 8.

Figura 39 – O gráfico de radar exibe as respostas dadas as questões que compõem a Parte 6 do questionário.



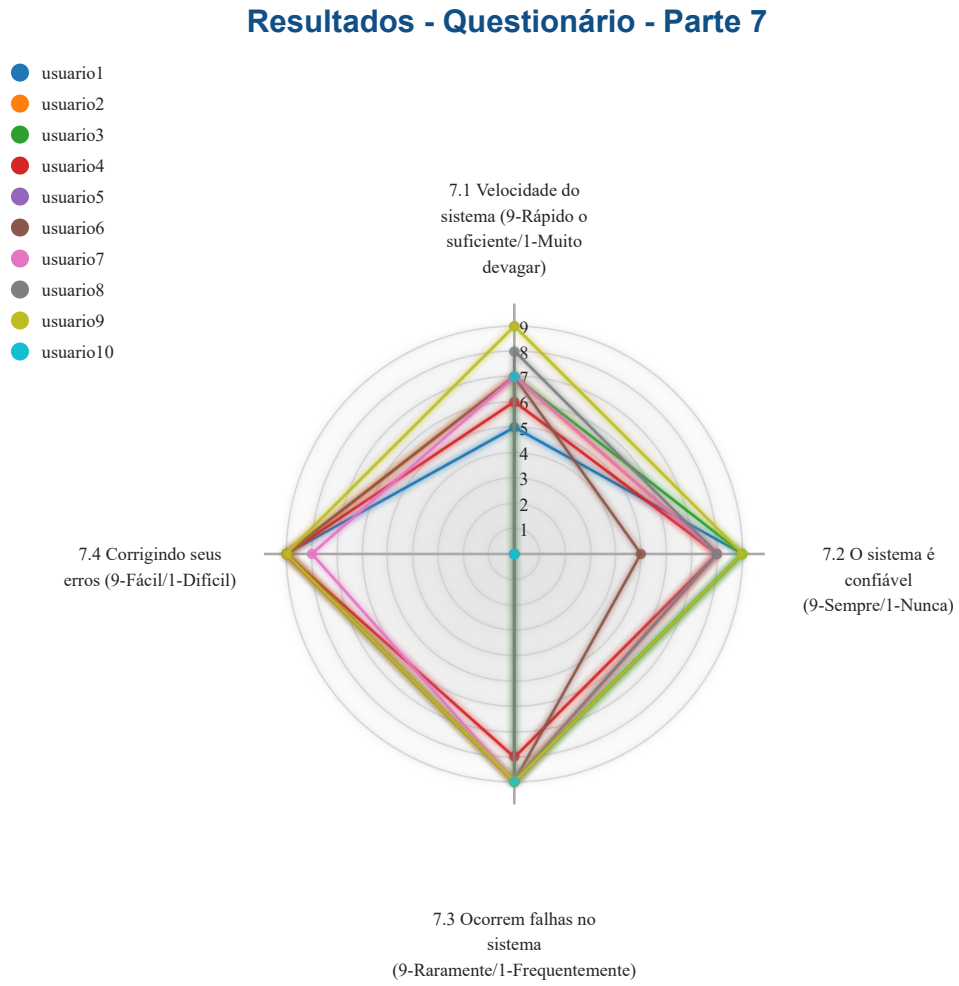
Fonte — Produzida pelo autor.

7.6.9 Parte 8 - Manual de Usuário e Ajuda Online

As perguntas que compõem esta parte do questionário e as respostas recebidas podem ser vistas na Figura 41.

As respostas fornecidas para as questões que compõe a parte 8 do questionário variam de 6 a 9, mostrando certa variação nas opiniões acerca do tutorial disponibilizado com a ferramenta. Ao menos 3 avaliadores deixaram de responder esta parte do questionário, optando pela alternativa "Não Aplicável"em todas as questões, mostrando que estes possivelmente não acessaram o tutorial. Um avaliador respondeu somente 3 das 4 questões,

Figura 40 – O gráfico de radar exibe as respostas dadas as questões que compõem a Parte 7 do questionário.



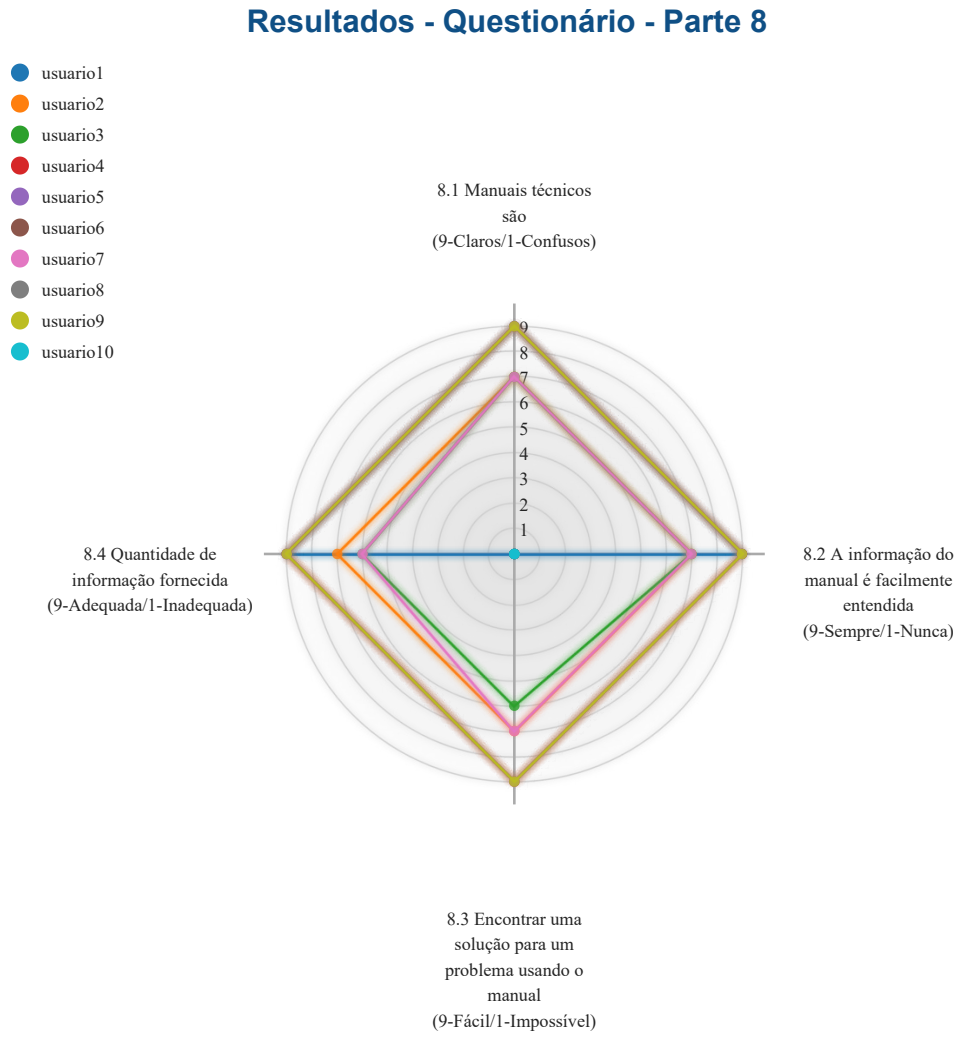
Fonte — Produzida pelo autor.

indicando que não ocorreu uma situação de problema que o levasse a consultar o tutorial.

7.7 Análise e Discussão de Resultados

Pode-se concluir que dentro da amostra selecionada, composta por profissionais do gênero masculino com idade entre 30 e 54 anos, com atuação ligada principalmente à infraestrutura (rede sem fio, rede cabeada, *data centers*, telefonia VoIP), que utilizaram em sua maioria a ferramenta entre uma hora e um dia, sendo no máximo uma hora por semana, a ferramenta agradou em diversos aspectos.

Figura 41 – O gráfico de radar exibe as respostas dadas as questões que compõem a Parte 8 do questionário.



Fonte — Produzida pelo autor.

Como pontos positivos citados podem-se destacar: a facilidade de uso, o processo de aprendizagem com a ferramenta, o design das telas, destaques apresentados, terminologia e mensagens geradas pela ferramenta, simplicidade nas opções de controle, ausência de falhas e erros.

Como pontos negativos pode-se citar: a falta de flexibilidade da ferramenta, lentidão em algumas situações, como, por exemplo, na primeira execução ou com maior período de tempo, falta de instruções para correção de erros, falta de *feedback* do computador durante as operações e a confiabilidade no sistema, com a sugestão de verificação de alguns valores

apresentados.

7.8 Considerações Finais do Capítulo

Pode-se concluir, por meio do processo de avaliação da ferramenta, que a mesma se mostrou útil e de interesse dos profissionais avaliadores, agradando na maioria dos aspectos avaliados, porém, ainda existem melhorias as serem feitas. Para melhorar o processo de avaliação, permitindo uma avaliação mais completa e estatisticamente mais confiável, seria necessário a participação de mais profissionais testando a ferramenta, inclusive com a participação de profissionais externos a universidade.

8 Conclusão

8.1 Considerações Iniciais do Capítulo

Nas seções a seguir são discutidos os aspectos positivos e negativos observados no desenvolvimento da solução.

Como resultado principal se tem a especificação desenvolvida juntamente com a ferramenta, que pode ser visto na Figura 42, tanto a especificação quanto a ferramenta estão de acordo com o direcionamento obtido por meio da revisão sistemática de conteúdo e do levantamento de requisitos realizados previamente. A ferramenta desenvolvida trata de uma estrutura de rede específica por conta da demanda apresentada pelo GRC.

Figura 42 – Imagens mostrando a ferramenta construída.

Fonte — Produzida pelo autor.

A mesma foi construída utilizando linguagens de programação leves e flexíveis, voltadas para web, utilizando biblioteca própria para geração dos gráficos, facilitando e acelerando o desenvolvimento. A ferramenta permite o acompanhamento em tempo real da situação da rede e também a exploração de dados históricos.

O processo de levantamento de requisitos, o acompanhamento do desenvolvimento pelo GRC e a avaliação pelos usuários garantem que o objetivo da ferramenta e o processo de construção das visualizações estejam de acordo com as demandas apresentadas. Buscou se utilizar visualizações adequadas para cada situação e diferentes tipos de dados, de acordo com o apresentado em literatura existente.

8.2 Relevância

A presente ferramenta se mostra relevante principalmente por se tratar de uma aplicação concreta de diversas tecnologias e áreas da Computação, entre elas: Segurança de Redes de Computadores, Gestão de Redes sem Fio, Visualização da Informação e Design de Interfaces. A aplicação obtida durante o desenvolvimento da solução visa ser utilizada em todas as unidades da Unesp, fornecendo informação aos administradores de rede.

Outro ponto relevante é a comparação com o Zabbix e sua interface, pois a ferramenta criada centraliza de maneira mais intuitiva todas as informações de interesse, sem a necessidade da exploração de complexas estruturas de menus e filtros como ocorre com o Zabbix. Entretanto, por se tratar de uma ferramenta que trabalha associada ao Zabbix, pode-se consultar o mesmo sem dificuldades caso seja necessário.

A comparação da ferramenta desenvolvida com as demais opções disponíveis no mercado agrega relevância ao trabalho, buscando mostrar os pontos positivos e negativos de todas as soluções e embasar a decisão de criação de uma nova ferramenta customizada conforme as necessidades.

O processo de desenvolvimento interativo e incremental, finalizado com a avaliação da ferramenta por uma amostra dos futuros usuários, avaliação essa com resultados positivos, conclui todo o projeto comprovando a relevância do mesmo para a universidade, com *feedback* essencialmente positivo.

8.3 Limitações

Como limitação, pode-se citar o problema de desempenho da aplicação, principalmente com intervalos de tempo maiores, como por exemplos 24 horas, isso se deve à necessidade de consultar grandes quantidades de informações históricas sobre os equipamentos, para o cálculo das médias desejadas. Atualmente o Zabbix se encontra implementado na Reitoria da Unesp na cidade de São Paulo e o protótipo implementado na FMB em Botucatu, interior do estado de São Paulo, o tempo necessário para transferência de dados, no mínimo 4 segundos, entre estas duas localidades contribui para a degradação de desempenho. Esta limitação vem sendo amenizada, porém foi identificada como ponto negativo também durante o processo de avaliação da ferramenta.

Outra limitação é a flexibilidade da ferramenta, uma vez que a mesma foi desenvolvida para um cenário específico e para atender uma determinada demanda, não permitindo com facilidade a utilização em outro contexto onde a estrutura de monitoramento e as informações disponibilizadas sejam diferentes, com uma outra configuração do Zabbix ou outra estrutura de rede. O problema de flexibilidade foi também constatado durante o processo de avaliação pelos usuários, pois as visualizações e certos parâmetros que as

compõem já são predefinidos e não permitem grandes customizações.

8.4 Trabalhos Futuros e Continuidade

Serão estudadas soluções para obtenção dos dados que foram previstos nos perfis de uso e que ainda não se encontram disponíveis com a consulta a outras fontes de dados.

Novas possibilidades de visualizações, incluindo visões ligando as controladoras aos pontos de acesso de forma hierárquica, visões dos *logs*, uma visão geral da universidade para utilização do GRC e visões ligadas a dados geográficos estão em estudo.

Melhorias na interface serão implementadas, com a possibilidade de novos filtros e melhora na seleção de intervalo. A atribuição de novos identificadores aos pontos de acesso, facilitando o agrupamento dos mesmos está em estudo.

Existe também a sugestão da expansão das funcionalidades para que a ferramenta passe também a atuar como um detector de anormalidades na rede e com isso possa notificar através de e-mails ou mensagens os incidentes da rede em tempo real.

Inicialmente o projeto contemplou somente a rede sem fio por conta da demanda apresentada pelo GRC, como continuidade pode-se expandir o monitoramento para além da rede sem fio, buscando contemplar a rede cabeada e demais estruturas que compõe a rede da Unesp, agregando novas informações a ferramenta.

8.5 Considerações Finais

A revisão sistemática se mostrou uma ferramenta interessante para investigar a área de pesquisa da Visualização da Informação aplicada à Segurança de Redes de Computadores, sendo realizada a revisão em diversas bases de dados e que, após as devidas fases de seleção, resultou na inclusão de 66 estudos primários neste trabalho.

A revisão contribui também na identificação de lacunas de pesquisa, como a falta de estudos envolvendo outras camadas de rede, além da Camada 2 e a falta de diversidade nas fontes de dados utilizadas. O presente trabalho explorou também o processo de avaliação de uma ferramenta de software e de sua interface, através da realização de testes e aplicação de questionários.

A partir da realização desta revisão se desenvolveu uma especificação com apoio do GRC da Unesp para aplicação da Visualização da Informação à rede sem fio da Unesp, conforme demanda do próprio GRC. Através da revisão sistemática de literatura e do levantamento de requisitos realizado, foi desenvolvida uma especificação de ferramenta para suprir a demanda, considerando no desenvolvimento as melhores práticas de design e aspectos de Segurança de Informação e Visualização da Informação. Esta ferramenta foi

desenvolvida e avaliada por uma parcela dos gestores de rede da Unesp e mostrou-se uma iniciativa válida com avaliações positivas, mesmo apresentando certas limitações a serem superadas.

No presente capítulo buscou-se ter uma visão geral dos resultados apresentados nas diferentes fases do projeto, desde a concepção à avaliação, considerando aspectos positivos e relevantes, e aspectos negativos e limitantes e indicando quais serão as direções a serem tomadas na continuidade do desenvolvimento da ferramenta.

Ao final do estudo se tem registrado todo o processo de pesquisa sobre um determinado tipo de ferramenta, a proposta de implementação deste tipo de ferramenta em uma universidade, o processo de especificação e desenvolvimento desta ferramenta e a avaliação da utilização da mesma em diferentes unidades da universidade. A sequência empregada no desenvolvimento do presente trabalho permitiu que os resultados desejados fossem alcançados, tem como efeito final a disponibilização à universidade de uma ferramenta para monitoramento da rede sem fio para ser utilizada pelos gestores de redes, possibilitando uma melhora na gestão que anteriormente não era possível.

Referências

ABNT, A. B. d. N. T. *ABNT NBR ISO/IEC 17799 - Tecnologia da informação - Técnicas desegurança - Código de prática para agestão da segurança da informação*. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005. 132 p. Citado 2 vezes nas páginas 24 e 25.

ALMOHANNADI, H. et al. Cyber Threat Intelligence from Honeypot Data Using Elasticsearch. In: *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*. [S.l.: s.n.], 2018. p. 900–906. ISSN 2332-5658. Citado na página 73.

ANGELINI, M. et al. The goods, the bads and the uglies: Supporting decisions in malware detection through visual analytics. In: *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2017. p. 1–8. ISBN 978-1-5386-2693-1. Disponível em: <http://ieeexplore.ieee.org/document/8062199/>. Citado 2 vezes nas páginas 20 e 124.

ANGELINI, M. et al. Vulnus: Visual Vulnerability Analysis for Network Security. *IEEE Transactions on Visualization and Computer Graphics*, v. 25, n. 1, p. 183–192, 1 2019. ISSN 1077-2626. Citado na página 128.

ANGELINI, M. et al. Visual Exploration and Analysis of the Italian Cybersecurity Framework. In: *Proceedings of the 2018 International Conference on Advanced Visual Interfaces*. New York, NY, USA: ACM, 2018. (AVI '18), p. 55:1–55:3. ISBN 978-1-4503-5616-9. Disponível em: <http://doi.acm.org/10.1145/3206505.3206579>. Citado na página 126.

ANGELINI, M.; PRIGENT, N.; SANTUCCI, G. PERCIVAL: Proactive and reactive attack and response assessment for cyber incidents using visual analytics. In: *2015 IEEE Symposium on Visualization for Cyber Security, VizSec 2015*. [S.l.]: IEEE, 2015. p. 1–8. ISBN 9781467375993. Citado na página 123.

ANGELINI, M.; SANTUCCI, G. Visual Cyber Situational Awareness for Critical Infrastructures. In: *Proceedings of the 8th International Symposium on Visual Information Communication and Interaction - VINCI '15*. New York, New York, USA: ACM Press, 2015. p. 83–92. ISBN 9781450334822. Disponível em: <http://dl.acm.org/citation.cfm?doid=2801040.2801052>. Citado na página 131.

ANGELINI, M.; SANTUCCI, G. Cyber situational awareness: from geographical alerts to high-level management. *Journal of Visualization*, Springer Berlin Heidelberg, v. 20, n. 3, p. 453–459, 8 2017. ISSN 18758975. Citado na página 118.

BALLORA, M.; HALL, D. L. Do you see what I hear: experiments in multi-channel sound and 3D visualization for network monitoring? In: BUFORD, J. F. et al. (Ed.). *SPIE DEFENSE, SECURITY, AND SENSING*. International Society for Optics and Photonics, 2010. v. 7709, p. 77090J. ISBN 9780819481733. ISSN 0277786X. Disponível em: <http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.850319>. Citado na página 129.

BEAVER, J. M. et al. Visualization techniques for computer network defense. In: CARAPEZZA, E. M. (Ed.). *Proceedings of the SPIE, Volume 8019, id. 801906 (2011).* [S.l.: s.n.], 2011. v. 8019, p. 801906. ISBN 9780819485939. ISSN 0277786X. Citado na página 127.

BERTINI, E.; HERTZOG, P.; LAIANNE, D. SpiralView: Towards security policies assessment through visual correlation of network resources with evolution of alarms. In: *VAST IEEE Symposium on Visual Analytics Science and Technology 2007, Proceedings.* [S.l.]: IEEE, 2007. p. 139–146. ISBN 9781424416592. ISSN 1424416590. Citado na página 124.

BEST, D. M. et al. Atypical behavior identification in large-scale network traffic. In: *1st IEEE Symposium on Large-Scale Data Analysis and Visualization 2011, LDAV 2011 - Proceedings.* [S.l.]: IEEE, 2011. p. 15–22. ISBN 9781467301541. Citado na página 118.

BETHEL, E. W. et al. Accelerating network traffic analytics using query-driven visualization. In: *IEEE Symposium on Visual Analytics Science and Technology 2006, VAST 2006 - Proceedings.* [S.l.]: IEEE, 2006. p. 115–122. ISBN 1424405912. Citado na página 117.

BIERSACK, E. et al. Visual analytics for BGP monitoring and prefix hijacking identification. *IEEE Network*, v. 26, n. 6, p. 33–39, 11 2012. ISSN 08908044. Disponível em: <http://ieeexplore.ieee.org/document/6375891/>. Citado 2 vezes nas páginas 20 e 48.

BIRREL, N. D.; OULD, M. A. *A Practical Handbook for Software Development.* [S.l.]: Cambridge University Press, 1988. 259 p. ISBN 9780521254625. Citado na página 46.

BRATTSTROM, M.; MORREALE, P. Scalable Agentless Cloud Network Monitoring. In: *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud).* [S.l.: s.n.], 2017. p. 171–176. Citado na página 73.

BRERETON, P. et al. Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, Elsevier Science Inc., v. 80, n. 4, p. 571–583, 4 2007. ISSN 01641212. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S016412120600197X>. Citado na página 32.

BURSKÁ, K.; OŠLEJŠEK, R. Visual Analytics for Network Security and Critical Infrastructures. In: *11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2017.* [S.l.]: Springer, Cham, 2017. p. 149–152. Citado na página 131.

CAPPERS, B. C.; WIJK, J. J. V. Understanding the context of network traffic alerts. In: *2016 IEEE Symposium on Visualization for Cyber Security, VizSec 2016.* [S.l.]: IEEE, 2016. p. 1–8. ISBN 9781509016051. Citado na página 125.

CASTILLO, P. N. *Mastering D3. js.* [S.l.]: Packt Publishing Ltd, 2014. Citado na página 64.

CHECHULIN, A.; KOLOMEEC, M.; KOTENKO, I. Visual Analytics for Improving Efficiency of Network Forensics: Account Theft Investigation. *Journal of Physics: Conference Series*, v. 1069, n. 1, p. 12062, 2018. Disponível em: <http://stacks.iop.org/1742-6596/1069/i=1/a=012062>. Citado na página 126.

CHEN, C.; GURGANUS, J. Statistical Anomaly Detection on Metadata Streams via Commodity Software to Protect Company Infrastructure: A Case Study. In: *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*. IEEE, 2017. p. 252–257. ISBN 978-1-5386-3292-5. ISSN 2332-5666. Disponível em: <http://ieeexplore.ieee.org/document/7979825/>. Citado na página 73.

CHEN, S. et al. Oceans. In: *Proceedings of the Eleventh Workshop on Visualization for Cyber Security - VizSec '14*. New York, New York, USA: ACM Press, 2014. p. 1–8. ISBN 9781450328265. Citado 2 vezes nas páginas 20 e 122.

CHEN, V. Y. et al. Multi-aspect visual analytics on large-scale high-dimensional cyber security data. *Information Visualization*, SAGE PublicationsSage UK: London, England, v. 14, n. 1, p. 62–75, 1 2015. ISSN 1473-8716. Disponível em: <http://journals.sagepub.com/doi/10.1177/1473871613488573>. Citado na página 130.

CHEN, X. et al. Correlative Visual Analytics for DNS Traffic with Multiple Views Based on TDRI. *Gongcheng Kexue Yu Jishu/Advanced Engineering Science*, v. 50, n. 4, p. 123–129, 2018. ISSN 20963246. Citado na página 129.

CHEN, Y.; YANG, B.; WANG, W. NetFlowMatrix: a visual approach for analysing large NetFlow data. *International Journal of Security and Networks*, v. 12, n. 4, p. 215, 2017. ISSN 1747-8405. Disponível em: <http://www.inderscience.com/link.php?id=88115>. Citado na página 122.

CHEN, Y. V.; QIAN, Z. C. From when and what to where: Linking spatio-temporal visualizations in visual analytics. In: *IEEE ISI 2013 - 2013 IEEE International Conference on Intelligence and Security Informatics: Big Data, Emergent Threats, and Decision-Making in Security Informatics*. [S.l.]: IEEE, 2013. p. 39–44. ISBN 9781467362115. Citado na página 120.

CHIAVENATO, I. *Introdução à teoria geral da administração*. [S.l.]: Elsevier, 2003. 634 p. ISBN 9788535213485. Citado na página 25.

CHOUDHURY, S. et al. M-Sieve: A visualisation tool for supporting network security analysts: VAST 2012 Mini Challenge 1 award: "Subject matter expert's award". In: *2012 IEEE Conference on Visual Analytics Science and Technology (VAST)*. IEEE, 2012. p. 265–266. ISBN 978-1-4673-4753-2. Disponível em: <http://ieeexplore.ieee.org/document/6400524/>. Citado na página 130.

D'AMICO, A. D. et al. Visual Discovery in Computer Network Defense. *IEEE Computer Graphics and Applications*, v. 27, n. 5, p. 20–27, 9 2007. ISSN 0272-1716. Disponível em: <http://ieeexplore.ieee.org/document/4302579/>. Citado na página 131.

DANG, T. T.; DANG, T. K. Extending Web Application IDS Interface: Visualizing Intrusions in Geographic and Web Space. In: *Proceedings - 2015 International Conference on Advanced Computing and Applications, ACOMP 2015*. [S.l.]: IEEE, 2016. p. 28–34. ISBN 9781467382342. Citado na página 119.

DASGUPTA, A. et al. Human Factors in Streaming Data Analysis: Challenges and Opportunities for Information Visualization. *Computer Graphics Forum*, 9 2017. ISSN 14678659. Disponível em: <http://doi.wiley.com/10.1111/cgf.13264>. Citado 2 vezes nas páginas 20 e 49.

DAVEY, J. et al. Visual analytics: Towards intelligent interactive internet and security solutions. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [S.l.]: Springer, Berlin, Heidelberg, 2012. v. 7281 LNCS, p. 93–104. ISBN 9783642302404. Citado 2 vezes nas páginas 20 e 48.

DIAS, C. C. *Usabilidade na web: criando portais mais acessíveis*. Alta Books, 2007. 296 p. ISBN 8576081407. Disponível em: <https://books.google.com/books?id=CohauAAACAAJ&pgis=1>. Citado na página 86.

Elastic.co. *Kibana User Guide [4.6] | Elastic*. 2018. Disponível em: <https://www.elastic.co/guide/en/kibana/current/index.html>. Citado na página 67.

ERBACHER, R. F.; FORCHT, K. A. Combining Visualization and Interaction for Scalable Detection of Anomalies in Network Data. *Journal of Computer Information Systems*, v. 50, n. 4, p. 117–126, 2010. ISSN 08874417. Citado na página 118.

EROLA, A. et al. RicherPicture: Semi-automated cyber defence using context-aware data analytics. In: *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. [S.l.: s.n.], 2017. p. 1–8. Citado na página 130.

FABBRI, S. et al. Improvements in the StArt tool to better support the systematic review process. In: *Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering - EASE '16*. New York, New York, USA: ACM Press, 2016. p. 1–5. ISBN 9781450336918. Disponível em: <http://dl.acm.org/citation.cfm?doid=2915970.2916013>. Citado na página 37.

FERREIRA, R. E. *Linux Guia do Administrador de Sistemas*. NOVATEC, 2003. ISBN 85-7522-038-17. Disponível em: <https://books.google.com.br/books?id=_WQnghmlubUC>. Citado na página 40.

FEW, S. *Information dashboard design*. [S.l.]: O'Reilly Sebastopol, CA, 2006. Citado na página 27.

FISCHER, A. E.; GRODZINSKY, F. S. *The anatomy of programming languages*. [S.l.]: Prentice Hall, 1993. 557 p. ISBN 0130351555. Citado na página 47.

FISCHER, F. et al. BANKSAFE: Visual analytics for big data in large-scale computer networks. *Information Visualization*, SAGE PublicationsSage UK: London, England, v. 14, n. 1, p. 51–61, 1 2015. ISSN 1473-8716. Citado na página 118.

FISCHER, F. et al. VisTracer. In: *Proceedings of the Ninth International Symposium on Visualization for Cyber Security - VizSec '12*. New York, New York, USA: ACM Press, 2012. p. 80–87. ISBN 9781450314138. Citado na página 125.

FISCHER, F.; KEIM, D. A. NStreamAware. In: *Proceedings of the Eleventh Workshop on Visualization for Cyber Security - VizSec '14*. New York, New York, USA: ACM Press, 2014. p. 65–72. ISBN 9781450328265. Citado na página 122.

FLANAGAN, D. *JavaScript : the definitive guide*. O'Reilly, 2006. 994 p. ISBN 9780596101992. Disponível em: <https://books.google.es/books?hl=es&lr=&id=k0CbAgAAQBAJ&oi=fnd&pg=PT6&dq=javascript&ots=O3nAknjBuZ&sig=4Hzua_-PUGwKcXaZwl-hVxwZhdU#v=onepage&q=javascript&f=false>. Citado na página 64.

GELENBE, E. et al. Security for smart mobile networks: The NEMESYS approach. In: *2013 International Conference on Privacy and Security in Mobile Systems (PRISMS)*. [S.l.]: IEEE, 2013. p. 1–8. ISBN 978-1-4799-0733-5. Citado 2 vezes nas páginas 20 e 123.

GHONIEM, M. et al. VAFLE: visual analytics of firewall log events. In: WONG, P. C. et al. (Ed.). *Visualization and Data Analysis*. [S.l.]: International Society for Optics and Photonics, 2014. v. 9017, p. 901704. ISBN 9780819499349. ISSN 0277786X. Citado na página 125.

GIACOBE, N. A.; XU, S. Geovisual analytics for cyber security: Adopting the GeoViz Toolkit. In: *VAST 2011 - IEEE Conference on Visual Analytics Science and Technology 2011, Proceedings*. [S.l.]: IEEE, 2011. p. 315–316. ISBN 9781467300131. Citado na página 120.

GOODALL, J. R. et al. Situ: Identifying and Explaining Suspicious Behavior in Networks. *IEEE Transactions on Visualization and Computer Graphics*, v. 25, n. 1, p. 204–214, 1 2019. ISSN 1077-2626. Citado na página 124.

GOODALL, J. R.; SOWUL, M. VIAssist: Visual analytics for cyber defense. In: *2009 IEEE Conference on Technologies for Homeland Security*. IEEE, 2009. p. 143–150. ISBN 978-1-4244-4178-5. Disponível em: <http://ieeexplore.ieee.org/document/5168026/>. Citado na página 130.

GOODALL, J. R.; TESONE, D. R. Visual Analytics for Network Flow Analysis. In: *2009 Cybersecurity Applications & Technology Conference for Homeland Security*. [S.l.]: IEEE, 2009. p. 199–204. ISBN 978-0-7695-3568-5. Citado na página 126.

Grafana Labs. *Grafana documentation | Grafana Documentation*. 2018. Disponível em: <http://docs.grafana.org/>. Citado na página 66.

GUERRA, J.; CATANIA, C. A.; VEAS, E. Visual Exploration of Network Hostile Behavior. In: *Proceedings of the 2017 ACM Workshop on Exploratory Search and Interactive Data Analytics - ESIDA '17*. New York, New York, USA: ACM Press, 2017. p. 51–54. ISBN 9781450349031. Citado 2 vezes nas páginas 20 e 127.

GUIMARAES, V. T. et al. A survey on information visualization for network and service management. *IEEE Communications Surveys and Tutorials*, v. 18, n. 1, p. 285–323, 21 2016. ISSN 1553877X. Disponível em: <http://ieeexplore.ieee.org/document/7166305/>. Citado 2 vezes nas páginas 20 e 49.

HAMDAN, B. Teaching Case Study: Introducing Data Analytics in an Advanced Cybersecurty Course. *J. Comput. Sci. Coll.*, Consortium for Computing Sciences in Colleges, USA, v. 33, n. 2, p. 113–120, 2017. ISSN 1937-4771. Disponível em: <http://dl.acm.org/citation.cfm?id=3144645.3144663>. Citado na página 73.

HAN, K. J.; HODGE, M.; ROSS, V. W. Entropy-based heavy tailed distribution transformation and visual analytics for monitoring massive network traffic. In: CARAPEZZA, E. M. (Ed.). *Proceedings of SPIE*. International Society for Optics and Photonics, 2011. v. 8019, n. 1, p. 80190B–80190B–10. ISBN 0277786X (ISSN); 9780819485939 (ISBN). ISSN 0277786X. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=25025087&site=ehost-live>. Citado na página 129.

HAO, L.; HEALEY, C. G.; HUTCHINSON, S. E. Flexible web visualization for alert-based network security analytics. In: *Proceedings of the Tenth Workshop on Visualization for Cyber Security - VizSec '13*. New York, New York, USA: ACM Press, 2013. p. 33–40. ISBN 9781450321730. Citado na página 120.

HARBORT, Z.; LOUTHAN, G.; HALE, J. Techniques for attack graph visualization and interaction. In: *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '11*. New York, New York, USA: ACM Press, 2011. p. 1. ISBN 9781450309455. Disponível em: <http://dl.acm.org/citation.cfm?doid=2179298.2179383>. Citado na página 130.

HARRISON, L. et al. Guiding security analysis through visualization. In: *Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on*. [S.l.]: IEEE, 2011. p. 317–318. ISBN 9781467300131. Citado na página 120.

HE, L. et al. NetflowVis: A temporal visualization system for netflow logs analysis. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [S.l.]: Springer, Cham, 2016. v. 9929 LNCS, p. 202–209. ISBN 9783319467702. Citado na página 122.

HORN, C.; D'AMICO, A. Visual analysis of goal-directed network defense decisions. In: *Proceedings of the 8th International Symposium on Visualization for Cyber Security - VizSec '11*. New York, New York, USA: ACM Press, 2011. p. 1–6. ISBN 9781450306799. Disponível em: <http://dl.acm.org/citation.cfm?doid=2016904.2016909>. Citado na página 131.

HUYNH, N. A. et al. Uncovering periodic network signals of cyber attacks. In: *2016 IEEE Symposium on Visualization for Cyber Security, VizSec 2016*. [S.l.]: IEEE, 2016. p. 1–8. ISBN 9781509016051. Citado na página 124.

IONITA, M.-G.; PATRICIU, V.-V. Cyber Incident Response Aided by Neural Networks and Visual Analytics. In: *2015 20th International Conference on Control Systems and Computer Science*. IEEE, 2015. p. 229–233. ISBN 978-1-4799-1780-8. Disponível em: <http://ieeexplore.ieee.org/document/7168435/>. Citado na página 129.

ISO/IEC, J. S. J. S. . *ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*. Suiça: [s.n.], 2004. Citado na página 25.

JÄCKLE, D. et al. Temporal MDS Plots for Analysis of Multivariate Data. *IEEE Transactions on Visualization and Computer Graphics*, v. 22, n. 1, p. 141–150, 1 2016. ISSN 10772626. Citado na página 124.

JACOBS, J. D. a. *Data-Driven Security : Analysis, Visualization and Dashboards*. [S.l.]: Wiley, 2014. ISBN 1118793722. Citado na página 30.

JACOBS, K. *Data-Driven Security: Analysis, Visualization and Dashboards*. 1st. ed. [S.l.]: Wiley Publishing, 2014. 352 p. ISSN 1098-6596. ISBN 978-1118793725. Citado na página 19.

JEONG, D. H.; JEONG, B.-K.; JI, S.-Y. Designing a hybrid approach with computational analysis and visual analytics to detect network intrusions. In: *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. [S.l.]: IEEE, 2017. p. 1–7. ISBN 978-1-5090-4228-9. Citado na página 119.

KALAMARAS, I. et al. MoVa: A visual analytics tool providing insight in the big mobile network data. In: *IFIP Advances in Information and Communication Technology*. [S.l.]: Springer, Cham, 2015. v. 458, p. 383–396. ISBN 9783319238678. Citado na página 130.

KAO, C.-H. et al. MITC Viz: Visual Analytics for Man-in-the-Cloud Threats Awareness. In: *2016 International Computer Symposium (ICS)*. IEEE, 2016. p. 306–311. ISBN 978-1-5090-3438-3. Disponível em: <http://ieeexplore.ieee.org/document/7858490/>. Citado na página 130.

KARAPISTOLI, E.; ECONOMIDES, A. A. Wireless sensor network security visualization. In: *2012 IV International Congress on Ultra Modern Telecommunications and Control Systems*. IEEE, 2012. p. 850–856. ISBN 978-1-4673-2017-7. Disponível em: <http://ieeexplore.ieee.org/document/6459781/>. Citado na página 131.

KARAPISTOLI, E.; SARIGIANNIDIS, P.; ECONOMIDES, A. A. Visual-Assisted Wormhole Attack Detection for Wireless Sensor Networks. In: *10th International ICST Conference*. [S.l.]: Springer, Cham, 2015. p. 222–238. Citado na página 131.

KEIM, D. A. et al. Monitoring network traffic with radial traffic analyzer. *IEEE Symposium on Visual Analytics Science and Technology 2006, VAST 2006 - Proceedings*, p. 123–128, 2006. Citado na página 121.

KHALILI, A. et al. Impact Modeling and Prediction of Attacks on Cyber Targets. In: BUFORD, J. F. et al. (Ed.). *Cyber Security, Situation Management, and Impact Assessment Ii; and Visual Analytics for Homeland Defense and Security Ii*. International Society for Optics and Photonics, 2010. v. 7709, p. 1–9. ISBN 978-0-8194-8173-3. ISSN 0277-786X. Disponível em: <http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.849755>. Citado na página 129.

KIRK, A. *Data Visualization: A Successful Design Process: A Structured Design Approach To Equip You With The Knowledge Of How To Successfully Accomplish Any Data Visualization Challenge Efficiently And Effectively*. Packt Pub, 2012. 189 p. ISBN 9781849693462 9781849693462. Disponível em: <https://books.google.com.br/books?hl=pt-PT&lr=&id=I4qBVLfD3t4C&oi=fnd&pg=PT6&dq=Data+Visualization:+A+Successful+Design+Process,&ots=b6TGlNbG6s&sig=MIKYZxmgoiqPujxoaQ6qRO6yngQ#v=onepage&q=DataVisualization%3AASuccessfulDesignProcess%2C&f=false>. Citado 4 vezes nas páginas 60, 61, 62 e 63.

KODAGODA, N. et al. Concern level assessment: Building domain knowledge into a visual system to support network-security situation awareness. *Information Visualization*, SAGE PublicationsSage UK: London, England, v. 13, n. 4, p. 346–360, 10 2014. ISSN 1473-8716. Citado na página 118.

KOLOMEETS, M.; CHECHULIN, A.; KOTENKO, I. Visualization Model for Monitoring of Computer Networks Security Based on the Analogue of Voronoi Diagrams. In: *Availability, Reliability, and Security in Information Systems*. [S.l.]: Springer, Cham, 2016. p. 141–157. Citado na página 127.

KOTENKO, I.; NOVIKOVA, E. VisSecAnalyzer: A visual analytics tool for network security assessment. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [S.l.]: Springer, Berlin, Heidelberg, 2013. v. 8128 LNCS, p. 345–360. ISBN 9783642405877. Citado na página 130.

KOTENKO, I.; NOVIKOVA, E. Visualization of security metrics for cyber situation awareness. In: *Proceedings - 9th International Conference on Availability, Reliability and Security, ARES 2014*. [S.l.]: IEEE, 2014. p. 506–513. ISBN 9781479942237. Citado na página 127.

KOVEN, J. et al. Lessons Learned Developing a Visual Analytics Solution for Investigative Analysis of Scamming Activities. *IEEE Transactions on Visualization and Computer Graphics*, v. 25, n. 1, p. 225–234, 1 2018. ISSN 10772626. Citado na página 129.

KUROSE, J. F.; ROSS, K. W. *Computer networking : a top-down approach*. [S.l.]: Pearson, 2013. 862 p. ISBN 0132856204. Citado 2 vezes nas páginas 19 e 24.

LABERGE, L. et al. Enhancing the "think loop process"with consistent interactions. In: *IEEE Conference on Visual Analytics Science and Technology 2012, VAST 2012 - Proceedings*. [S.l.]: IEEE, 2012. p. 275–276. ISBN 9781467347532. Citado na página 119.

LAHMADI, A. et al. A platform for the analysis and visualization of network flow data of android environments. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*. [S.l.: s.n.], 2015. p. 1129–1130. ISBN 9783901882760. ISSN 10636897. Citado na página 73.

LAMAGNA, W. M. An integrated visualization on network events VAST 2011 mini challenge 2 award: Outstanding integrated overview display. In: *VAST 2011 - IEEE Conference on Visual Analytics Science and Technology 2011, Proceedings*. [S.l.]: IEEE, 2011. p. 319–321. ISBN 9781467300131. Citado na página 117.

LANDSTORFER, J. et al. Weaving a carpet from log entries: A network security visualization built with co-creation. In: *2014 IEEE Conference on Visual Analytics Science and Technology, VAST 2014 - Proceedings*. [S.l.]: IEEE, 2014. p. 73–82. ISBN 9781479962273. ISSN 1098-6596. Citado na página 128.

LANGTON, J. T.; NEWEY, B. Evaluation of current visualization tools for cyber security. *Proceedings of SPIE - The International Society for Optical Engineering*, v. 7709, 2010. Citado 2 vezes nas páginas 20 e 48.

LIN, D. A User-Centered Multi-space Collaborative Visual Analysis for Cyber Security. *Chinese Journal of Electronics*, Institution of Engineering and Technology, v. 27, n. 5, p. 910–919, 2018. ISSN 1022-4653. Disponível em: <https://digital-library.theiet.org/content/journals/10.1049/cje.2017.09.021>. Citado na página 117.

LIU, S. T.; CHEN, Y. M. Retrospective detection of malware attacks by cloud computing. In: *Proceedings - 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2010*. [S.l.: s.n.], 2010. p. 510–517. ISBN 9780769542355. ISSN 2042-3217. Citado na página 73.

LOMOTEY, R. K.; PRY, J. C.; CHAI, C. Traceability and visual analytics for the Internet-of-Things (IoT) architecture. *World Wide Web*, Springer US, p. 1–26, 5 2017. ISSN 1386-145X. Disponível em: <http://link.springer.com/10.1007/s11280-017-0461-1>. Citado na página 130.

LU, A. et al. Sybil Attack Detection through Global Topology Pattern Visualization. *Information Visualization*, SAGE PublicationsSage UK: London, England, v. 10, n. 1, p. 32–46, 1 2011. ISSN 1473-8716. Citado 2 vezes nas páginas 20 e 124.

LU, L. F. et al. A new concentric-circle visualization of multi-dimensional data and its application in network security. *Journal of Visual Languages and Computing*, Academic Press, v. 21, n. 4, p. 194–208, 8 2010. ISSN 1045926X. Citado na página 117.

LV, B. et al. Network traffic monitoring system based on big data technology. In: *ACM International Conference Proceeding Series*. New York, NY, USA: ACM, 2018. (ICBDC '18), p. 27–32. ISBN 9781450364263. Disponível em: <http://doi.acm.org/10.1145/3220199.3220221>. Citado na página 73.

MANSMAN, F.; MEIER, L.; KEIM, D. A. Visualization of host behavior for network security. In: *Mathematics and Visualization*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. p. 187–202. ISBN 9783540782421. Citado na página 127.

MANSMANN, F.; VINNIK, S. Interactive exploration of data traffic with hierarchical network maps. *IEEE Transactions on Visualization and Computer Graphics*, v. 12, n. 6, p. 1440–1449, 11 2006. ISSN 10772626. Citado na página 121.

MCELWEE, S. et al. Deep learning for prioritizing and responding to intrusion detection alerts. In: *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*. IEEE, 2017. p. 1–5. ISBN 978-1-5386-0595-0. ISSN 2155-7586. Disponível em: <http://ieeexplore.ieee.org/document/8170757/>. Citado na página 73.

MCKENNA, S. et al. BubbleNet: A Cyber Security Dashboard for Visualizing Patterns. In: *Proceedings of the Eurographics / IEEE VGTC Conference on Visualization*. Goslar Germany, Germany: Eurographics Association, 2016. (EuroVis '16), p. 281–290. Disponível em: <https://doi.org/10.1111/cgf.12904>. Citado 2 vezes nas páginas 20 e 21.

MENDIRATTA, V. B.; THOTTAN, M. Rich Network Anomaly Detection Using Multivariate Data. In: *2017 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. IEEE, 2017. p. 48–51. ISBN 978-1-5386-2387-9. Disponível em: <http://ieeexplore.ieee.org/document/8109248/>. Citado na página 123.

MINARIK, P.; DYMACEK, T. NetFlow data visualization based on graphs. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. v. 5210 LNCS, p. 144–151. ISBN 3540859314. Citado na página 122.

MOH, M. et al. Detecting Web Attacks Using Multi-stage Log Analysis. In: *2016 IEEE 6th International Conference on Advanced Computing (IACC)*. IEEE, 2016. p. 733–738. ISBN 978-1-4673-8286-1. Disponível em: <http://ieeexplore.ieee.org/document/7544930/>. Citado na página 73.

MOUSTAKAS, K. et al. Border gateway protocol graph: detecting and visualising internet routing anomalies. *IET Information Security*, v. 10, n. 3, p. 125–133, 5 2016. ISSN 1751-8709. Citado na página 118.

MUNZNER, T.; MAGUIRE, E. *Visualization analysis & design*. [S.l.: s.n.], 2015. 404 p. ISBN 9781466508934 1466508930 9781498707763 1498707769. Citado 2 vezes nas páginas 27 e 36.

MySQL. 2019. Disponível em: <https://www.mysql.com/>. Citado na página 64.

NEIVA, F.; SILVA, R. *Revisão Sistemática da Literatura em Ciência da Computação - Um Guia Prático*. [S.l.], 2016. Citado 3 vezes nas páginas 34, 35 e 36.

NGUYEN, V. T.; NAMIN, A. S.; DANG, T. MalViz: an interactive visualization tool for tracing malware. In: *Proceedings of the 27th ACM SIGSOFT International Symposium on Software Testing and Analysis - ISSTA 2018*. New York, NY, USA: ACM, 2018. (ISSTA 2018), p. 376–379. ISBN 9781450356992. Disponível em: <http://dl.acm.org/citation.cfm?doid=3213846.3229501>. Citado na página 129.

NIELSEN, J. *Usability Engineering*. Elsevier Science, 1994. (Interactive Technologies). ISBN 9780080520292. Disponível em: <https://books.google.com.br/books?id=DBOowF7LqIQC>. Citado na página 85.

NORMAN, D.; NIELSEN, J. *The Definition of User Experience (UX)*. 2003. Citado na página 31.

OKUMURA, M.; FUJIMURA, S. Constructing a Log Collecting System using Splunk and its Application for Service Support. In: *Proceedings of the 2016 ACM on SIGUCCS Annual Conference - SIGUCCS '16*. New York, NY, USA: ACM, 2016. (SIGUCCS '16), p. 103–106. ISBN 9781450340953. Disponível em: <http://dl.acm.org/citation.cfm?doid=2974927.2974934>. Citado na página 73.

OTHMANE, L. B.; JAATUN, M. G.; WEIPPL, E. *Empirical research for software security: Foundations and experience*. [s.n.], 2017. 1–302 p. ISBN 9781498776424. Disponível em: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85052712295&doi=10.1201%2Fb20962&origin=inward&txGid=77216ec2cd3dc607683d1a5ce58ef751>. Citado na página 131.

OZULKU, O. et al. Anomaly detection system: Towards a framework for enterprise log management of security services. In: *World Congress on Internet Security (WorldCIS-2014)*. IEEE, 2014. p. 97–102. ISBN 978-1-908320-42-1. Disponível em: <http://ieeexplore.ieee.org/document/7028175/>. Citado na página 73.

PARK, H. et al. Understanding university campus network reliability characteristics using a big data analytics tool. In: *2015 11th International Conference on the Design of Reliable Communication Networks (DRCN)*. [S.l.: s.n.], 2015. p. 107–110. Citado na página 73.

PATTON, R. M. et al. Hierarchical clustering and visualization of aggregate cyber data. In: *2011 7th International Wireless Communications and Mobile Computing Conference*. [S.l.: s.n.], 2011. p. 1287–1291. ISSN 2376-6492. Citado na página 73.

PERYT, S. et al. Visualizing a Malware Distribution Network. In: *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2016. p. 1–4. ISBN 978-1-5090-1605-1. Disponível em: <http://ieeexplore.ieee.org/document/7739585/>. Citado na página 131.

PIENTA, R. et al. VIGOR: Interactive Visual Exploration of Graph Query Results. *IEEE Transactions on Visualization and Computer Graphics*, p. 1–1, 2017. ISSN 1077-2626. Disponível em: <http://ieeexplore.ieee.org/document/8019832/>. Citado na página 130.

PREECE, J.; ROGERS, Y.; SHARP, H. *Interaction design : beyond human-computer interaction*. [S.l.: s.n.], 2015. 567 p. ISBN 9781119020752. Citado na página 31.

PROLE, K. et al. Wireless cyber assets discovery visualization. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. v. 5210 LNCS, p. 136–143. ISBN 3540859314. Citado 2 vezes nas páginas 20 e 128.

SAYDAM, T.; MAGEDANZ, T. From Networks and Network Management into Service and Service Management. *Journal of Networks and System Management*, v. 4, n. 4, p. 345–348, 1996. Citado na página 26.

SCHICK, J. et al. Rule Creation in a Knowledge-assisted Visual Analytics Prototype for Malware Analysis. In: . [S.l.: s.n.], 2017. Citado na página 130.

SCHONWALDER, J. On the future of Internet management technologies. *IEEE Communications Magazine*, v. 41, n. October, p. 90–97, 2003. ISSN 0163-6804. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1235600>. Citado na página 55.

SETHI, A.; PACI, F.; WILLS, G. EEVi - framework for evaluating the effectiveness of visualization in cyber-security. In: *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2016. p. 340–345. ISBN 978-1-908320-73-5. Disponível em: <http://ieeexplore.ieee.org/document/7856726/>. Citado na página 129.

SHITTU, R. et al. Visual Analytic Agent-Based Framework for Intrusion Alert Analysis. In: *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. IEEE, 2012. p. 201–207. ISBN 978-1-4673-2624-7. Disponível em: <http://ieeexplore.ieee.org/document/6384968/>. Citado na página 131.

SHITTU, R. et al. Intrusion alert prioritisation and attack detection using post-correlation analysis. *Computers and Security*, v. 50, p. 1–15, 2015. ISSN 01674048. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404814001837>. Citado na página 129.

SHNEIDERMAN, B. The eyes have it: a task by data type taxonomy for information visualizations. In: *Proceedings 1996 IEEE Symposium on Visual Languages*. [S.l.]: IEEE Comput. Soc. Press, 1996. p. 336–343. ISBN 0-8186-7508-X. ISSN 1049-2615. Citado na página 27.

SHURKHOVETSKYY, G.; BAHEY, A.; GHONIEM, M. Visual analytics for network security. In: *2012 IEEE Conference on Visual Analytics Science and Technology (VAST)*. [S.l.]: IEEE, 2012. p. 301–302. ISBN 978-1-4673-4753-2. Citado na página 126.

SINDA, M.; LIAO, Q. Spatial-Temporal Anomaly Detection Using Security Visual Analytics via Entropy Graph and Eigen Matrix. In: *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science*

and Technology Congress(DASC/PiCom/DataCom/CyberSciTech). [S.l.: s.n.], 2017. p. 511–518. Citado na página 130.

Splunk. *Authentication - Splunk Documentation*. 2018. Disponível em: <http://docs.splunk.com/Documentation/CIM/4.11.0/User/Authentication>. Citado na página 69.

STALLINGS, W. SNMP and SNMPv2: The infrastructure for network management. *IEEE Communications Magazine*, v. 36, n. 3, p. 37–43, 1998. ISSN 01636804. Citado na página 55.

STARK, R. F. et al. Visualizing large scale patterns and anomalies in geospatial data. In: *IEEE Conference on Visual Analytics Science and Technology 2012, VAST 2012 - Proceedings*. [S.l.]: IEEE, 2012. p. 271–272. ISBN 9781467347532. ISSN 2325-9442. Citado na página 127.

TABASH, K. A.; HAPPA, J. Insider-threat detection using Gaussian Mixture Models and Sensitivity Profiles. *Computers & Security*, Elsevier Advanced Technology, 3 2018. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404818302487>. Citado 2 vezes nas páginas 20 e 121.

TANENBAUM, A. S.; WETHERALL, D. J. *Computer Networks*. 5th. ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010. ISBN 0132126958, 9780132126953. Citado 2 vezes nas páginas 19 e 24.

TEOH, S. T. et al. Detecting flaws and intruders with visual data analysis. *IEEE Computer Graphics and Applications*, v. 24, n. 5, p. 27–35, 9 2004. ISSN 02721716. Citado na página 119.

The PHP Group. *PHP: O que é o PHP? - Manual*. 2018. Disponível em: <https://secure.php.net/manual/pt_BR/intro-whatis.php>. Citado na página 63.

THERON, R. et al. Network-wide intrusion detection supported by multivariate analysis and interactive visualization. In: *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2017. p. 1–8. ISBN 978-1-5386-2693-1. Disponível em: <http://ieeexplore.ieee.org/document/8062198/>. Citado na página 122.

THONNARD, O.; VERVIER, P.-A.; DACIER, M. Spammers operations: a multifaceted strategic analysis. *Security and Communication Networks*, v. 9, n. 4, p. 336–356, 3 2016. ISSN 19390114. Disponível em: <http://doi.wiley.com/10.1002/sec.640>. Citado na página 130.

VAST. *VAST Challenge 2017*. 2017. Disponível em: <http://www.vacommunity.org/VAST+Challenge+2017>. Citado na página 45.

VAZHKUDAI, S. S. et al. GUIDE: A Scalable Information Directory Service to Collect, Federate, and Analyze Logs for Operational Insights into a Leadership HPC Facility. In: *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*. New York, NY, USA: ACM, 2017. (SC '17), p. 45:1–45:12. ISBN 978-1-4503-5114-0. Disponível em: <http://doi.acm.org/10.1145/3126908.3126946>. Citado na página 73.

VOLODINA, E. et al. Application of Visual Analysis to Detect and Analyze Patterns in VoIP Attack Traffic. In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. [S.l.: s.n.], 2018. p. 260–268. ISSN 2324-9013. Citado na página 118.

WANG, Q. et al. egoPortray: Visual Exploration of Mobile Communication Signature from Egocentric Network Perspective. In: AMSALEG, L. et al. (Ed.). *MultiMedia Modeling*. Cham: Springer International Publishing, 2017. p. 649–661. ISBN 978-3-319-51811-4. Citado na página 129.

WANG, W.; LU, A. Interactive wormhole detection in large scale wireless networks. In: *IEEE Symposium on Visual Analytics Science and Technology 2006, VAST 2006 - Proceedings*. [S.l.]: IEEE, 2006. p. 99–106. ISBN 1424405912. Citado na página 121.

WANG, W.; YANG, B.; CHEN, V. Y. A visual analytics approach to detecting server redirections and data exfiltration. In: *2015 IEEE International Conference on Intelligence and Security Informatics: Securing the World through an Alignment of Technology, Intelligence, Humans and Organizations, ISI 2015*. [S.l.]: IEEE, 2015. p. 13–18. ISBN 9781479998883. Citado 2 vezes nas páginas 20 e 117.

WANG, W.; YANG, B.; CHEN, Y. V. Detecting subtle port scans through characteristics based on interactive visualization. In: *Proceedings of the 3rd annual conference on Research in information technology - RIIT '14*. New York, New York, USA: ACM Press, 2014. p. 33–38. ISBN 9781450327114. Citado na página 119.

WARE, C. *Information Visualization: Perception for Design (Interactive Technologies)*. [S.l.]: Morgan Kaufmann, 2004. 486 p. ISBN 9781558608191. Citado na página 27.

WILLIAMS, F. C. B.; FAITHFULL, W. J.; ROBERTS, J. C. SitaVis - Interactive situation awareness visualization of large datasets. In: *IEEE Conference on Visual Analytics Science and Technology 2012, VAST 2012 - Proceedings*. [S.l.]: IEEE, 2012. p. 273–274. ISBN 9781467347532. Citado na página 123.

XYDAS, I. et al. *Using an Evolutionary Neural Network for Web Intrusion Detection*. [S.l.]: ACTA Press, 2008. Citado na página 125.

YANG, L. Visual Exploration of Frequent Itemsets and Association Rules. In: SIMOFF, S. J.; BOHLEN, M. H.; MAZEIKA, A. (Ed.). *Visual Data Mining*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. p. 60–75. ISBN 978-3-540-71080-6. Citado na página 131.

YOON, Y.; CHOI, Y. On Multilateral Security Monitoring and Analysis With an Abstract Tomogram of Network Flows. *IEEE Access*, v. 6, p. 24118–24127, 2018. ISSN 2169-3536. Disponível em: <https://ieeexplore.ieee.org/document/8347089/>. Citado 2 vezes nas páginas 20 e 122.

YOON, Y.; CHOI, Y.; SHIN, S. Multilateral Context Analysis based on the Novel Visualization of Network Tomography. In: *Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems - DEBS '17*. New York, New York, USA: ACM Press, 2017. p. 343–344. ISBN 9781450350655. Citado na página 123.

YU, H. et al. A visualization analysis tool for DNS amplification attack. In: *Proceedings - 2010 3rd International Conference on Biomedical Engineering and Informatics, BMEI 2010*. [S.l.]: IEEE, 2010. v. 7, p. 2834–2838. ISBN 9781424464968. Citado na página 117.

YUEN, J.; TURNBULL, B.; HERNANDEZ, J. Visual analytics for cyber red teaming. In: *2015 IEEE Symposium on Visualization for Cyber Security, VizSec 2015*. [S.l.]: IEEE, 2015. p. 1–8. ISBN 9781467375993. Citado 2 vezes nas páginas 20 e 125.

Zabbix. *Zabbix Documentation*. 2017. 3–7 p. Disponível em: <https://www.zabbix.com/documentation/2.2/manual/config/notifications/media/sms>. Citado na página 59.

ZHANG, J.; HUANG, M. L. Visual analytics model for intrusion detection in flood attack. In: *Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013*. [S.l.]: IEEE, 2013. p. 277–284. ISBN 9780769550220. Citado na página 126.

ZHANG, Y. et al. A survey of security visualization for computer network logs. *Security and Communication Networks*, John Wiley & Sons, Ltd, v. 5, n. 4, p. 404–421, 4 2012. ISSN 19390122. Disponível em: <http://doi.wiley.com/10.1002/sec.324>. Citado 2 vezes nas páginas 20 e 49.

ZHAO, H. et al. Analysis of Visualization Systems for Cyber Security. In: . [s.n.], 2019. p. 1051–1061. Disponível em: <http://link.springer.com/10.1007/978-981-10-8944-2_122>. Citado na página 49.

ZHAO, Y. et al. MVSec: Multi-perspective and deductive visual analytics on heterogeneous network security data. *Journal of Visualization*, v. 17, n. 3, p. 181–196, 8 2014. ISSN 18758975. Citado na página 121.

ZHAO, Y. et al. IDSRadar: A real-time visualization framework for IDS alerts. *Science China Information Sciences*, Springer Berlin Heidelberg, v. 56, n. 8, p. 1–12, 8 2013. ISSN 1674733X. Citado na página 120.

ZHOU, F. et al. ENTVis: A visual analytic tool for entropy-based network traffic anomaly detection. *IEEE Computer Graphics and Applications*, v. 35, n. 6, p. 42–50, 11 2015. ISSN 02721716. Citado na página 119.

Apêndices

APÊNDICE A – Dados dos estudos incluídos

Neste capítulo são apresentados os dados extraídos dos estudos incluídos na revisão, através da Tabela 9.

Tabela 9 – Estudos incluídos na revisão.

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
A new concentric-circle visualization of multi-dimensional data and its application in network security	Lu et al. (2010)	TCP/IP	coordenadas círculares concêntricas	1	network flow	2	Sim	CCScanViewer	Java
A user-centered multi-space collaborative visual analysis for cyber security	Lin (2018)	TCP/IP	visualização geográfica, nós, séries temporais	1	H3C Intelligent management center (IMC)	1,2	Sim	Não informado	Não informado
A visual analytics approach to detecting server redirections and data exfiltration	Wang, Yang e Chen (2015)	TCP/IP	Gráfico de barras, gráfico de células, gráficos de dispersão, coordenadas paralelas	3	log de firewall, network flow, VAST	1	Sim	Não possui	Javascript
A visualization analysis tool for DNS amplification attack	Yu et al. (2010)	TCP/IP	Gráfico de linhas, gráfico de radar, cilindro ou 3D	3	dados do WinPcap, dados do Snort	2	Sim	Visualization Analysis tool	C#
Accelerating Network Traffic Analytics Using Query-Driven Visualization	Bethel et al. (2006)	TCP/IP	histograma	3	network flow customizado	2	Sim	Fast-Bit	C++
An integrated visualization on network events VAST 2011 Mini Challenge #2 Award: "Outstanding integrated overview display"	Lamagna (2011)	TCP/IP	mapas de calor, coordenadas paralelas	1	dados pcap, log de firewall, log de IDS, VAST	2	Sim	Não possui	Javascript, Processing

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Application of Visual Analysis to Detect and Analyze Patterns in VoIP Attack Traffic	Volodina et al. (2018)	VoIP	diagrama nó-link	3	network flow, log de VoIP	2,3	Não	Gephi	Não se aplica
Atypical behavior identification in large-scale network traffic	Best et al. (2011)	TCP/IP	Sparkline	1	network flow	2	Sim	CLIQUE	Não informado
BANKSAFE: Visual analytics for big data in large-scale computer networks	Fischer et al. (2015)	TCP/IP	treemap, matrix, glifo de relógio circular, linha do tempo visual	1	VAST	2	Sim	BANK-SAFE	Java, Javascript
Border gateway protocol graph: detecting and visualising internet routing anomalies	Moustakas et al. (2016)	BGP	Pontos de dispersão, visualização de gráfico hieráquico	2	dados de transferência de BGP	2	Sim	BGPGraph	Não informado
Combining visualization and interaction for scalable detection of anomalies in network data	Erbacher e Forcht (2010)	TCP/IP	dois eixos de coordenadas paralelas	3	dados de arquivo pcap	2	Sim	Não possui	Java
Concern level assessment: Building domain knowledge into a visual system to support network-security situation awareness	Kodagoda et al. (2014)	TCP/IP	Mapas, histogramas, barras de tempos	2	VAST	2	Sim	M-SIEVE	Não informado
Cyber situational awareness: from geographical alerts to high-level management	Angelini e Santucci (2017)	TCP/IP	Diagrama de voronoi, mapas, nós	2	topologia de redes, dados de negócio	2	Sim	PANOPTE-SEC	Javascript

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Designing a hybrid approach with computational analysis and visual analytics to detect network intrusions	Jeong, Jeong e Ji (2017)	TCP/IP	Coordenadas paralelas	3	network flow	2	Sim	IDViz	Não informado
Detecting flaws and intruders with visual data analysis	Teoh et al. (2004)	BGP	Decomposição de quadtree, visualização de arbustos de eventos, projeção de coordenadas de estrelas	3	diversos	2	Sim	Não possui	Não informado
Detecting Subtle Port Scans Through Characteristics Based on Interactive Visualization	Wang, Yang e Chen (2014)	TCP/IP	Séries temporais, coordenadas paralelas	3	VAST, network flow	2	Sim	Não possui	Não informado
Enhancing the "think loop process"; with consistent interactions: VAST 2012 Mini Challenge 1 award: Honorable mention for good interaction techniques	Laberge et al. (2012)	TCP/IP	Visualização geoespacial, visualização temporal	2	VAST	2	Não	CoMotion	Não se aplica
ENTVis: A Visual Analytic Tool for Entropy-Based Network Traffic Anomaly Detection	Zhou et al. (2015)	TCP/IP	Linha do tempo, visualização radial, visualização de matrix	2	VAST	2	Sim	ENTVis	Java
Extending Web Application IDS Interface: Visualizing Intrusions in Geographic and Web Space	Dang e Dang (2016)	TCP/IP	gráfico bipartido, layout radial de árvore	3	dados de IDS	4	Sim	Não possui	Java

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Flexible Web Visualization for Alert-based Network Security Analytics	Hao, Healey e Hutchinson (2013)	TCP/IP	gráfico de torta, gráfico de barras, gráfico de dispersão, gráfico de Gantt	3	network flow	2	Sim	Não possui	PHP, Javascript
From when and what to where: Linking spatio-temporal visualizations in visual analytics	Chen e Qian (2013)	TCP/IP	Visualizações espaciais-temporais, curvas de séries temporais, visualizações baseadas em pixels	2	VAST	2	Sim	Semantic-Prism's	Não informado
Geovisual analytics for cyber security: Adopting the GeoViz Toolkit	Giacobe e Xu (2011)	TCP/IP	GeoMap, pontos de dispersão, coordenadas paralelas, histogramas	2	VAST	2	Não	GeoViz Toolkit	Não se aplica
Guiding security analysis through visualization	Harrison et al. (2011)	TCP/IP	diagrama nó-link, gráfico de barras	2	informações de negócios,log de firewall, logs de IDS, log do Windows, VAST	2	Sim	Não possui	Perl
IDSRadar: A real-time visualization framework for IDS alerts	Zhao et al. (2013)	TCP/IP	gráfico radial	2	dados do Snort, VAST	2	Sim	IDSRadar	C++

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Interactive Exploration of Data Traffic with Hierarchical Network Maps	Mansmann e Vinnik (2006)	TCP/IP	treemap quadrificado	2	network Flow	2	Sim	Hierarchical Network Maps	Não informado
Insider-threat detection using Gaussian Mixture Models and Sensitivity Profiles	Tabash e Happa (2018)	TCP/IP	Coordenadas paralelas, scatter plot, gráfico de barras, séries temporais	1	CERT Insider-Threat dataset	-	Sim	Insider-Threat Detection System	Python e Javascript
Interactive Wormhole Detection in Large Scale Wireless Networks	Wang e Lu (2006)	Wireless	Espaços 3D	3	dados de topologia	1	Sim	Interactive Visualization of Wormholes (IVoW)	Não informado
Monitoring network traffic with radial traffic analyzer	Keim et al. (2006)	TCP/IP	layout radial hieráquico, treemap	2	dados geográficas, dados de libpcap, dados de WinPcap, dados de JPcap.	2	Sim	Radial Traffic Analyzer	Java
MVSec: Multi-perspective and deductive visual analytics on heterogeneous network security data	Zhao et al. (2014)	TCP/IP	Radial, mapa de calor, matrix de portas, mapa empilhado	1	dados do Packet Sniffer, network flow, log de firewall, log de IDS	2	Sim	MVSec	Processing

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
NetFlow data visualization based on graphs	Minarik e Dymacek (2008)	TCP/IP	grafos	2	network flow, dados de NFDump	2	Sim	NetFlow Visualizer	Java
NetFlowMatrix: A visual approach for analysing large NetFlow data	Chen, Yang e Wang (2017)	TCP/IP	pequenos multiplos, scatter plot, coordenadas paralelas	1	VAST	2	Sim	NetFlowMatrix	Não informado
NetflowVis: A temporal visualization system for netflow logs analysis	He et al. (2016)	TCP/IP	árvore link-nó, ThemeRiver, visão radial	1	network flow	2	Sim	NetflowVis	Não informado
Network-wide intrusion detection supported by multivariate analysis and interactive visualization	Theron et al. (2017)	TCP/IP	série temporal, gráfico de barras, gráfico de radar, MEDA graph	2	network flow	2	Sim	iGPCA	Não informado
NStreamAware: Real-time Visual Analytics for Data Streams to Enhance Situational Awareness	Fischer e Keim (2014)	TCP/IP	word clouds, diagramas nós-link, treemaps, contadores	2	VAST	2	Sim	NStreamAware, NVisAware	Javascript
OCEANS: Online Collaborative Explorative Analysis on Network Security	Chen et al. (2014)	TCP/IP	linha do tempo, gráfico de anel, conexão de rio	1	network flow, log de IPS, log de status de host	2	Sim	OCEANS	PHP, Javascript
On Multilateral Security Monitoring and Analysis With an Abstract Tomogram of Network Flows	Yoon e Choi (2018)	TCP/IP	tomograma de network flows	2	NetInsider DPI	2	Sim	tomogram of network flows	C++ e Javascript

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
PERCIVAL: proactive and reactive attack and response assessment for cyber incidents using visual analytics	Angelini, Prigent e Santucci (2015)	TCP/IP	grafo	2	Não informado	2	Sim	PERCIVAL	Não informado
Poster: Multilateral context analysis based on the novel visualization of network tomography	Yoon, Choi e Shin (2017)	TCP/IP	tomografia de network flows	2	network flow	2,4	Sim	tomography of network flows	Não informado
Rich Network Anomaly Detection Using Multivariate Data	Mendiratta e Thottan (2017)	4G LTE	Gráfico de barras, séries temporais	2	Logs de rede 4G	-	Sim	Não possui	R
Security for smart mobile networks: The NEMESYS approach	Gelenbe et al. (2013)	Mobile: wireless e celular	Visualização multiplas coordenadas	3	honeypots móveis virtualizados, honeyclients	1	Sim	NEMESYS	Android
SitaVis - Interactive situation awareness visualization of large datasets: VAST 2012 Mini Challenge 1 award: Honorable mention for good situational awareness snapshot	Williams, Faithfull e Roberts (2012)	TCP/IP	gráficos de área empilhados, gráficos de pixels densos, representações geográficas dos dados	2	VAST	2	Sim	SitaVis	Java, Processing

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Situ: Identifying and Explaining Suspicious Behavior in Networks	Goodall et al. (2019)	TCP/IP	Histograma temporal, gráficos horizontais, gráfico de barras, gráficos de comunicação de dois saltos	2	network flow, log de firewall e log de web proxy	2	Sim	Situ	Não informado
SpiralView: Towards security policies assessment through visual correlation of network resources with evolution of alarms	Bertini, Hertzog e Laianne (2007)	TCP/IP	gráfico de barras, visão espiral	1	dados de NEXThink	0	Sim	SpiralView	Não informado
Sybil attack detection through global topology pattern visualization	Lu et al. (2011)	wireless	visualização multi-matrix	3	dados de topologia	1	Sim	Não possui	Não informado
Temporal MDS Plots for Analysis of Multivariate Data	Jäckle et al. (2016)	TCP/IP	Temporal Multidimensional Scaling plots	3	network flow, VAST	2	Sim	Temporal Multidimensional Scaling (TMDS)	Não informado
The goods, the bads and the uglies: Supporting decisions in malware detection through visual analytics	Angelini et al. (2017)	TCP/IP	visualização geográfica, radziv	3	AMICO	4	Sim	Visual Analytics Prototype (VAP)	Não informado
Uncovering periodic network signals of cyber attacks	Huynh et al. (2016)	TCP/IP	grafico circular, séries temporais	1	network flow, dados do SplitCap	2	Sim	Não possui	Não informado

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Understanding the context of network traffic alerts	Cappers e Wijk (2016)	TCP/IP	tabela de tempo, mapa de calor, gráfico de linha e mapa de calor	1	dados do WireShark	2	Sim	CoNTA	Não informado
Using an Evolutionary Neural Network for web intrusion detection	Xydas et al. (2008)	TCP/IP	gráficos 3D	2	dados de tcpdump, log do Web IIS	4	Sim	Evolutionary Artificial Neural Network (EANN)	DOT language
VAFLE: Visual analytics of firewall log events	Ghoniem et al. (2014)	TCP/IP	mapa de calor	1	VAST	2	Sim	VAFLE	Java
VisTracer: A Visual Analytics Tool to Investigate Routing Anomalies in Traceroutes	Fischer et al. (2012)	BGP	Baseada em mapas, baseada em glifos	2	dados do Spamtracer	2	Sim	VisTracer	Java
Visual analytics for cyber red teaming	Yuen, Turnbull e Hernandez (2015)	TCP/IP	grafo de forças direcionado multifoco, árvore Reingold-Tilford, cordenadas paralelas	3	dados da topologia	4	Sim	Trogdor	Javascript

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Visual Analytics for Improving Efficiency of Network Forensics: Account Theft Investigation	Chechulin, Kolomeec e Kotenko (2018)	TCP/IP	gráfico de barras, coordenadas paralelas, gráfico de dispersão, grafico circular, treemap, diagrama de voronoi, diagrama de cordas, coordenadas triangulares	1	dados do Wireshark	1,2	Sim	Não informado	Não informado
Visual Analytics for Network Flow Analysis	Goodall e Tesone (2009)	TCP/IP	Gráficos de dispersão	2	dados do SiLK	2	Sim	VIAssist	Não informado
Visual analytics for network security	Shurkhovetskyy, Bahey e Ghoniem (2012)	TCP/IP	Mapa de calor, séries temporais, coordenadas paralelas	2	log de firewall, log de IDS	2	Não	InfoVis Toolkit	Não se aplica
Visual Analytics Model for Intrusion Detection in Flood Attack	Zhang e Huang (2013)	TCP/IP	grafos clássicos não direcionados	3	network flow, ISCX2012	2,3	Sim	Density-Workload	Não informado
Visual exploration and analysis of the Italian cybersecurity framework	Angelini et al. (2018)	TCP/IP	gráfico de barras	2	Italian Adaptation of the Cyber Security Framework (IACSF)		Sim	CRUMBS	Não informado

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Visual Exploration of Network Hostile Behavior	Guerra, Catania e Veas (2017)	TCP/IP	mapa de calor, gráfico de barras	2	dados do Stratosphere IPS	2	Sim	RiskID	Javascript
Visualization model for monitoring of computer networks security based on the analogue of Voronoi diagrams	Kolomeets, Chechulin e Kotenko (2016)	TCP/IP	Diagramas análogos ao diagrama de Voronoi	2	paramêtros de hosts, dados de link entre hosts	2	Sim	Não possuí	Não informado
Visualization of host behavior for network security	Mansman, Meier e Keim (2008)	TCP/IP	grafos de força direcionados, visão hierárquica	2	dados do SNORT	4	Sim	HNMap tool	Não informado
Visualization of Security Metrics for Cyber Situation Awareness	Kotenko e Novikova (2014)	TCP/IP	Treemaps Pictograma baseado em círculo	2	network flow, meta-data	2	Sim	VisSecA-nalyzes	Java
Visualization techniques for computer network defense	Beaver et al. (2011)	TCP/IP	diagrama Sunburst, diagrama de partículas, gráfico de dispersão, gráfico de pizza	3	dados de IDS, logs diversos, dados de Splunk	2	Sim	ORCA	Java
Visualizing large scale patterns and anomalies in geospatial data: VAST 2012 Mini Challenge #1 award: Honorable mention for good visual design	Stark et al. (2012)	TCP/IP	Visualização Geospatial	2	VAST	2	Sim	Charles River Analytics solution	Java

(continuação)

Título	Autor (Ano)	Tipos de rede	Técnicas de visualização	Objetivo das visualizações (Categoria)	Fonte de dados	Camada de Rede	Houve desenvolvimento	Nome da ferramenta	Linguagens utilizadas
Vulnus: Visual Vulnerability Analysis for Network Security	Angelini et al. (2019)	TCP/IP	treemap modificado, painéis coordenados	1	CVSS, dados de OpenVas, dados do Nessus e dados do LanGuard	4	Sim	VULNUS	Não informado
Weaving a carpet from log entries: A network security visualization built with co-creation	Landstorfer et al. (2014)	TCP/IP	mapa de pixels	1	log de acesso do Apache	4	Sim	Pixel Carpet	Não informado
Wireless cyber assets discovery visualization	Prole et al. (2008)	wireless	árvores, grafos, histogramas, visualizações geográficas	2	dados do Kismet	1	Sim	MeerCAT	Java

Fonte - Produzida pelo autor.

APÊNDICE B – Estudos excluídos

Os seguintes estudos foram excluídos durante a etapa de extração:

- Correlative Visual Analytics for DNS Traffic with Multiple Views Based on TDRI (CHEN et al., 2018) Motivo da exclusão: Estudo não está disponível completo no idioma inglês.
- Cyber incident response aided by neural networks and visual analytics (IONITA; PATRICIU, 2015) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Do you see what I hear: Experiments in multi-channel sound and 3D visualization for network monitoring? (BALLORA; HALL, 2010) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- EEVi - framework for evaluating the effectiveness of visualization in cyber-security (SETHI; PACI; WILLS, 2016) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Egoportray: Visual exploration of mobile communication signature from egocentric network perspective (WANG et al., 2017) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Entropy-based heavy tailed distribution transformation and visual analytics for monitoring massive network traffic(HAN; HODGE; ROSS, 2011) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Impact modeling and prediction of attacks on cyber targets (KHALILI et al., 2010) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Intrusion alert prioritisation and attack detection using post-correlation analysis (SHITTU et al., 2015) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Lessons Learned Developing a Visual Analytics Solution for Investigative Analysis of Scamming Activities (KOVEN et al., 2018) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- MalViz: An Interactive Visualization Tool for Tracing Malware (NGUYEN; NAMIN; DANG, 2018) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.

- MITC Viz: Visual Analytics for Man-in-the-Cloud Threats Awareness (KAO et al., 2016) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- MoVa: A visual analytics tool providing insight in the big mobile network data (KALAMARAS et al., 2015) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Multi-aspect visual analytics on largescale high-dimensional cyber security data (CHEN et al., 2015) Motivo da exclusão: Trata de ferramenta já analisada.
- M-Sieve: A visualisation tool for supporting network security analysts: VAST 2012 Mini Challenge 1 award: "Subject matter expert's award"(CHOUDHURY et al., 2012) Motivo da exclusão: Trata de ferramenta já analisada.
- RicherPicture: Semi-automated cyber defence using context-aware data analytics (EROLA et al., 2017) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Rule creation in a knowledge-assisted visual analytics prototype for malware analysis (SCHICK et al., 2017) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Spammers operations: A multifaceted strategic analysis (THONNARD; VERVIER; DACIER, 2016) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Spatial-Temporal Anomaly Detection Using Security Visual Analytics via Entropy Graph and Eigen Matrix (SINDA; LIAO, 2017) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Techniques for Attack Graph Visualization and Interaction (HARBORT; LOUTHAN; HALE, 2011) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Traceability and visual analytics for the Internet-of-Things (IoT) architecture (LOMOTEY; PRY; CHAI, 2017) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- VIAssist: Visual analytics for cyber defense (GOODALL; SOWUL, 2009) Motivo da exclusão: Trata de ferramenta já analisada.
- VIGOR: Interactive Visual Exploration of Graph Query Results (PIENTA et al., 2017) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- VisSecAnalyzer: A visual analytics tool for network security assessment (KOTENKO; NOVIKOVA, 2013) Motivo da exclusão: Trata de ferramenta já analisada.

- Visual Analysis of Goal-directed Network Defense Decisions (HORN; D'AMICO, 2011) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Visual Analytic Agent-Based Framework for Intrusion Alert Analysis (SHITTU et al., 2012) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Visual analytics for network security and critical infrastructures (BURSKÁ; OŠLEJŠEK, 2017) Motivo da exclusão: Não é um artigo.
- Visual analytics: Foundations and experiences in malware analysis (OTHMANE; JAATUN; WEIPPL, 2017) Motivo da exclusão: Não é um artigo.
- Visual Cyber Situational Awareness for Critical Infrastructures (ANGELINI; SANTUCCI, 2015) Motivo da exclusão: Trata de ferramenta já analisada.
- Visual Discovery in Computer Network Defense(D'AMICO et al., 2007) Motivo da exclusão: Trata de ferramenta já analisada.
- Visual exploration of frequent itemsets and association rules (YANG, 2008) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Visual-assisted wormhole attack detection for wireless sensor networks (KARAPISTOLI; SARIGIANNIDIS; ECONOMIDES, 2015) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Visualizing a Malware Distribution Network (PERYT et al., 2016) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.
- Wireless sensor network security visualization (KARAPISTOLI; ECONOMIDES, 2012) Motivo da exclusão: Falta de afinidade do estudo com os temas desejados.

APÊNDICE C – Tutorial de utilização da ferramenta

Rede sem Fio - Tutorial

1 - Login

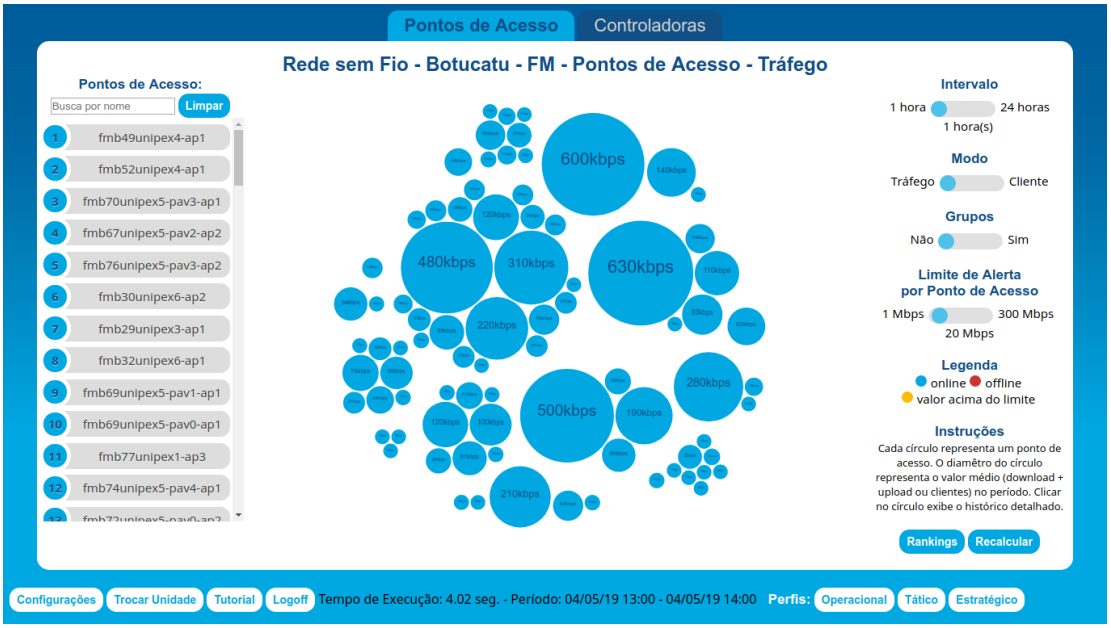
O início da utilização da ferramenta se dá pela tela da login, ela deve ser preenchida com as credenciais da Central de Acessos Unesp (com ou sem "@unesp.br"), com um usuário que tenha acesso à ferramenta de monitoramento Zabbix. O campo "Servidor" já vem preenchido com o servidor da Unesp, não havendo necessidade de alteração, porém, existe a possibilidade para alteração futura. Caso as credenciais sejam inválidas, o sistema notificará.

2 - Seleção de Unidades

O passo seguinte é a seleção da unidade na lista apresentada, após a escolha, clique em "Selecionar" para continuar ou em "Logoff" para sair da ferramenta.

3 - Visão geral

A ferramenta apresenta a seguinte tela principal.



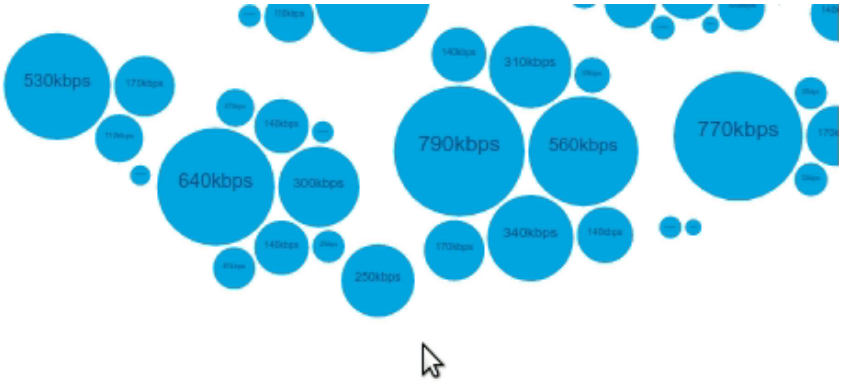
Na parte superior temos as opções de visualizar as abas referentes a "Pontos de Acesso" e "Controladoras", estas abas permanecem constantes, independente de qual estiver ativa.

Na parte inferior temos as opções de visualizar os perfis predefinidos: "Operacional", "Tático" e "Estratégico", ajustando os parâmetros automaticamente de acordo com o foco desejado.

4 - Aba Pontos de Acesso

Na lateral esquerda, a ferramenta apresenta uma lista de pontos de acesso, onde é possível realizar a busca textual dentro da lista.

O posicionamento do ponteiro do mouse sobre um círculo ou sobre seu nome na lista lateral gera destaque sobre o item.



Na lateral direita estão as opções para ajustar a visualização:

1 - É possível alterar o intervalo de medições que compõe os valores da visualização, variando de 1 a 24 horas.

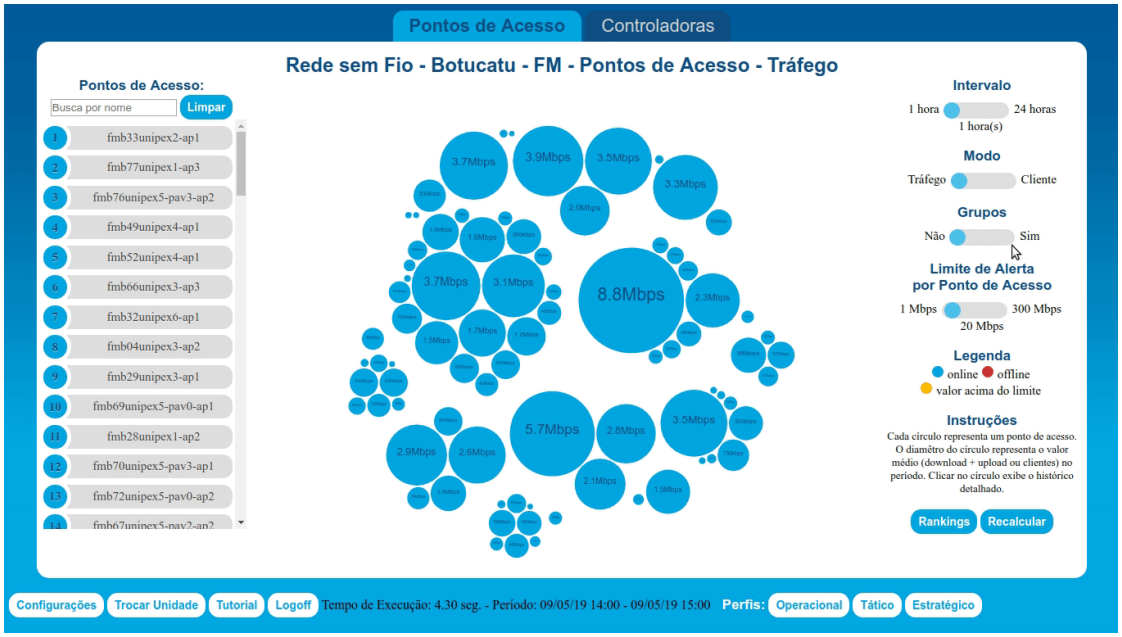
2 - É possível alterar a grandeza utilizada para criação da visualização: valor de tráfego ou número de clientes conectados

3 - É possível habilitar o agrupamento dos pontos de acesso de acordo com palavras pré-cadastras (configuração mostrada no item 6 - Configurações), essa opção possibilita o agrupamento de prédios ou departamentos por exemplo.

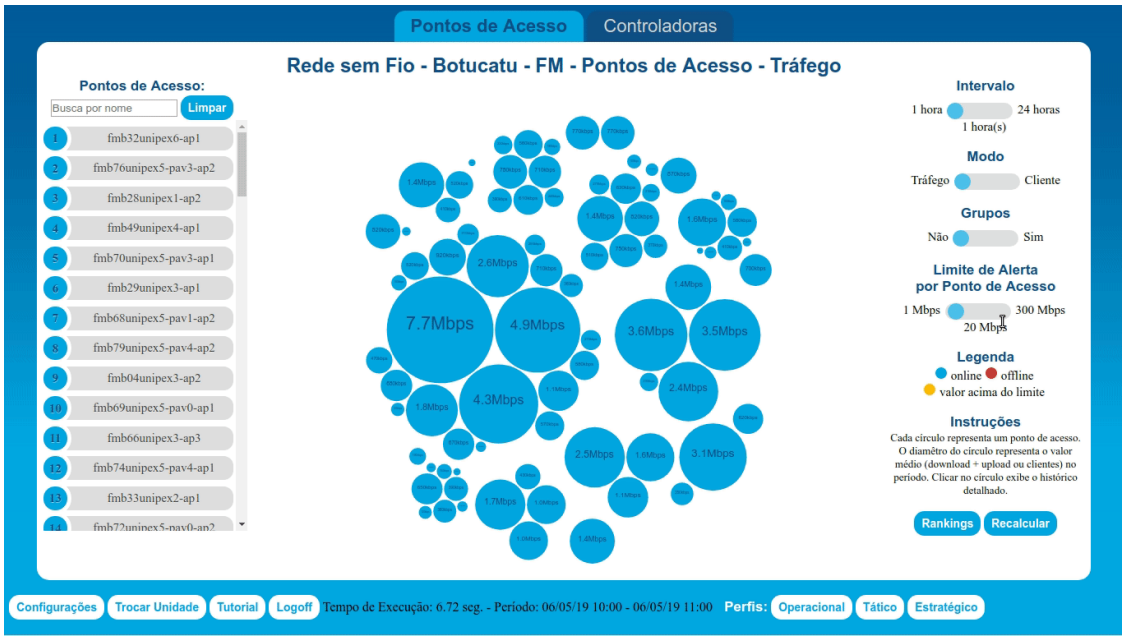
4 - Valor de alerta é um valor que quando ultrapassado por um ponto de acesso causa a alteração da cor desse ponto de acesso. Pode-se customizar os valores de alertas, sejam eles de tráfego ou de clientes. A variação de tráfego é de 1Mbps a 300Mbps, para clientes é de 1 a 100 clientes.

5 - Através do botão "Rankings" é possível acessar novas visualizações dos dados. O botão "Recalcular" força a atualização de todos os dados que formam as visualizações.

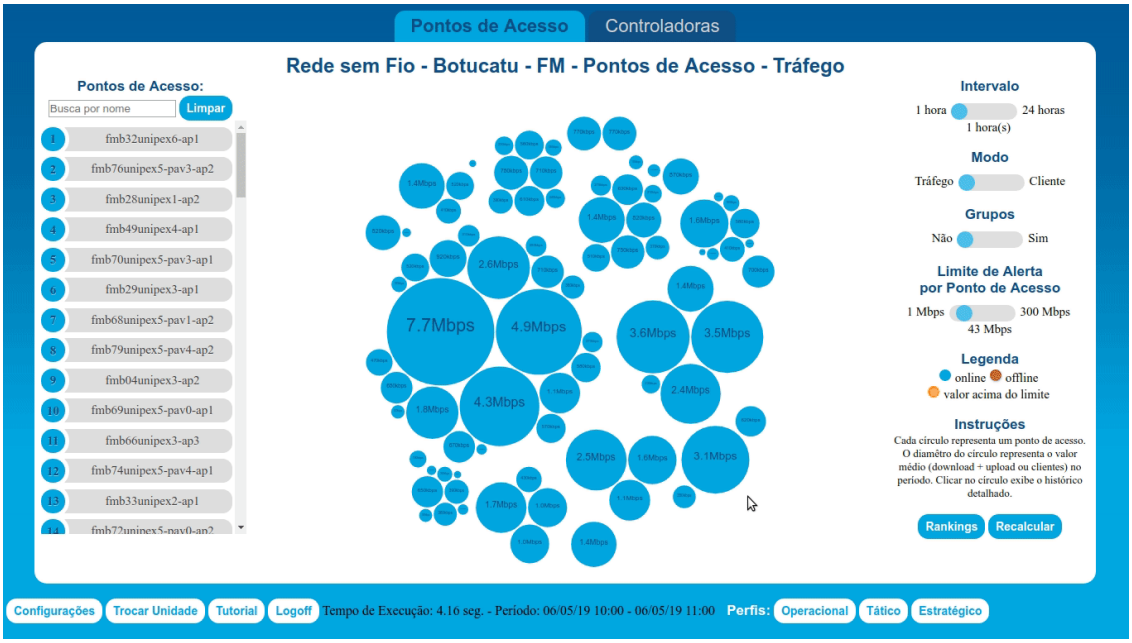
Observe a opção de grupos sendo ativada e a ação de zoom em um grupo:



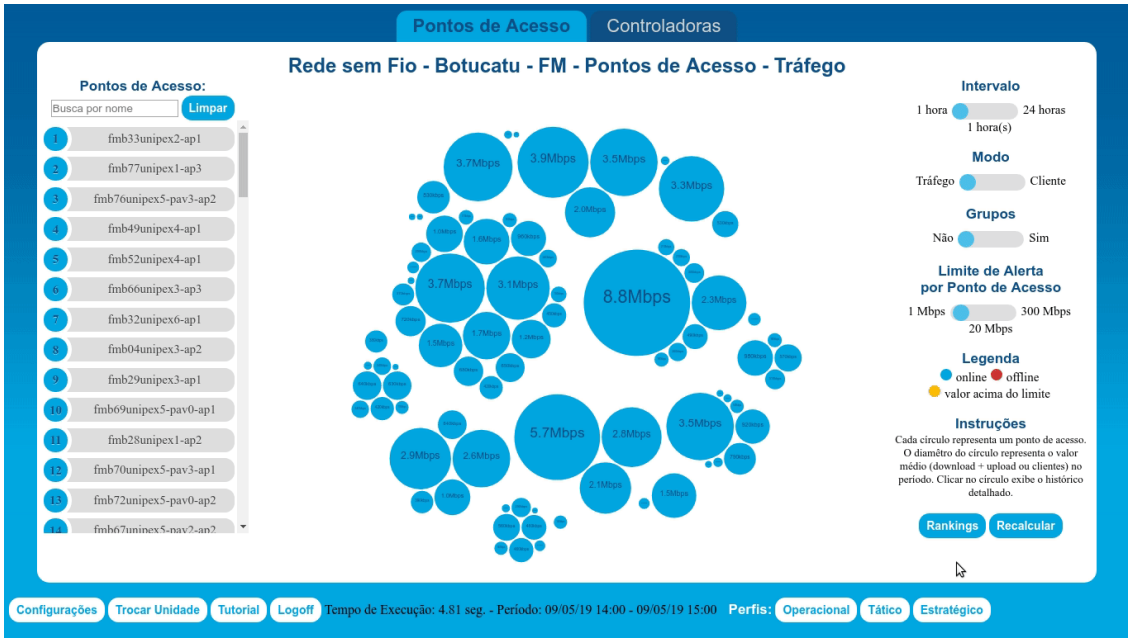
Observe também a opção de alertas sendo ativada:



Clicar em um dos círculos dá acesso à visualização com os dados detalhados no período. O período pode ser customizado dentro desta nova janela, além de ser possível também o acesso aos dados de log daquele ponto de acesso.

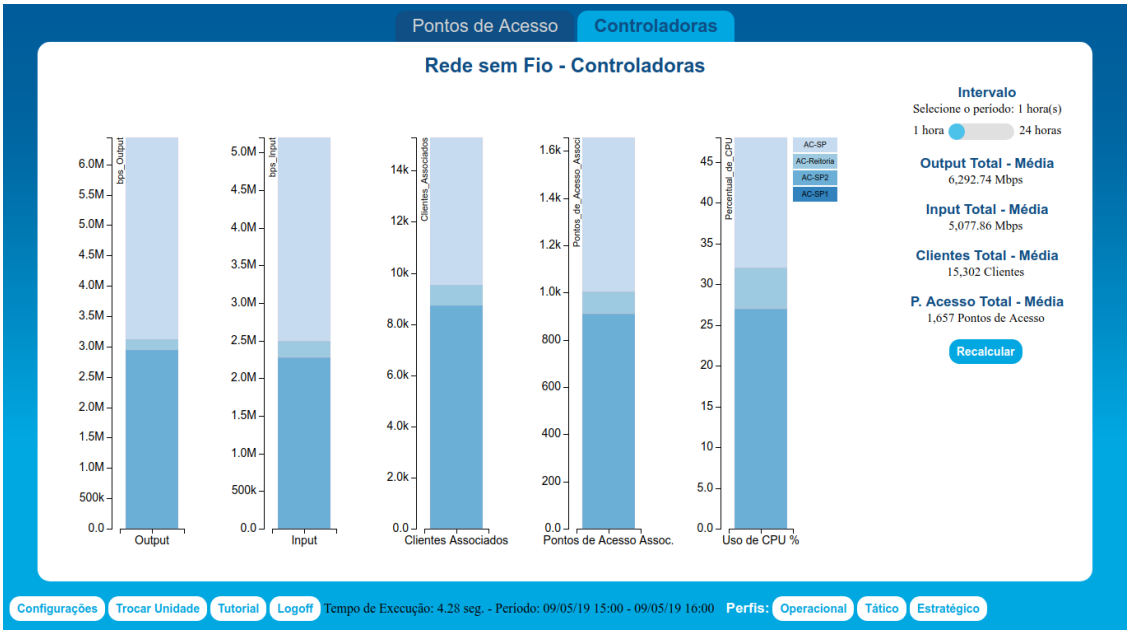


Clicar no botão "Rankings" permite o acesso a mais visualizações referentes aos dados dos pontos de acesso.

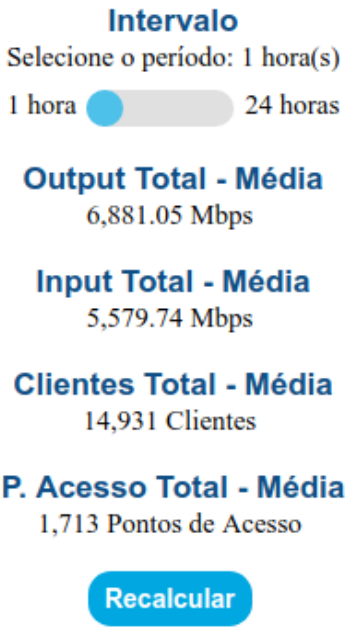


5 - Aba Controladoras

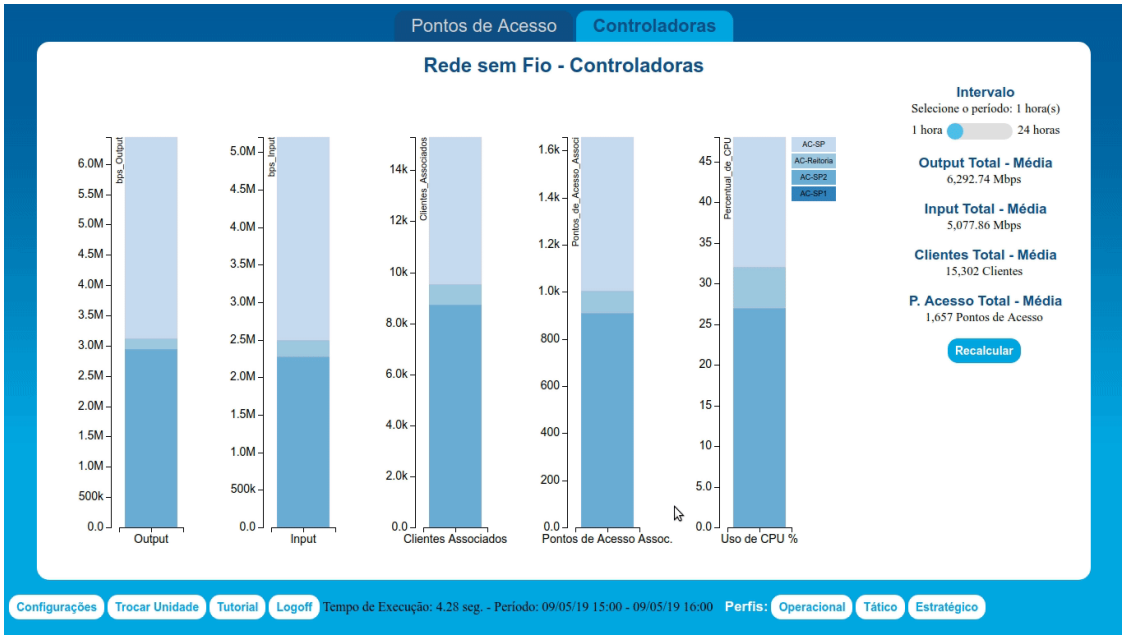
Além da aba Pontos de Acesso, temos também disponível a aba Controladoras, exibindo dados dos equipamentos instalados na Reitoria.



Na lateral direita temos o controle para ajuste do período, os dados totalizados de todas as controladoras e o botão "Recalcular".

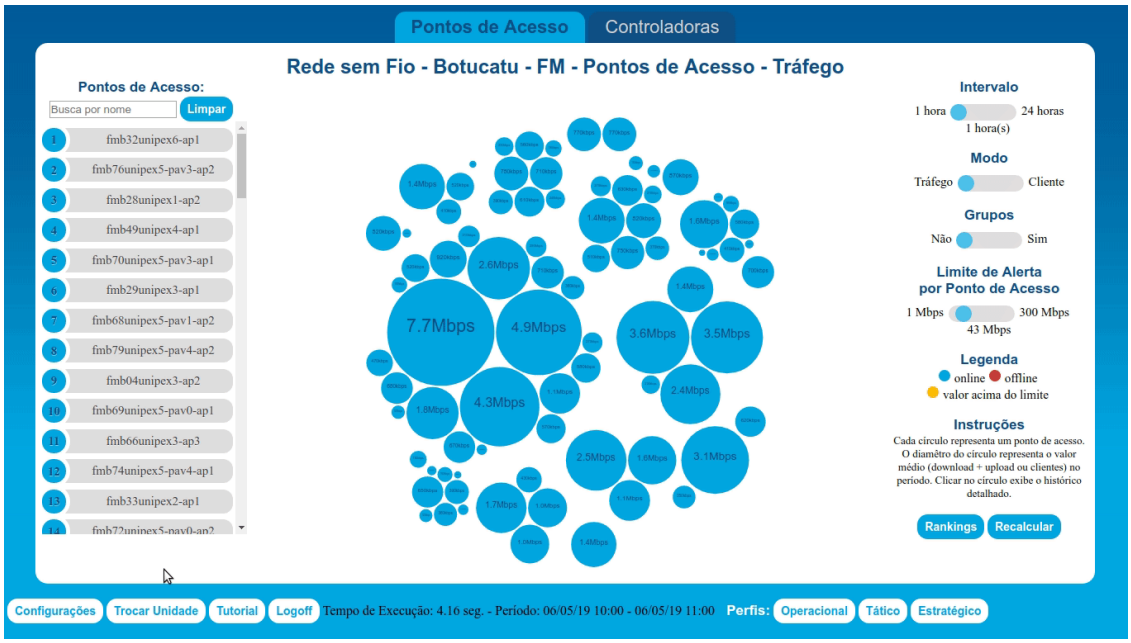


Ao apontar o cursor e clicar em uma das barras empilhadas, a barra ganha destaque e uma janela exibindo a visualização com o detalhamento dos dados no período é exibida.



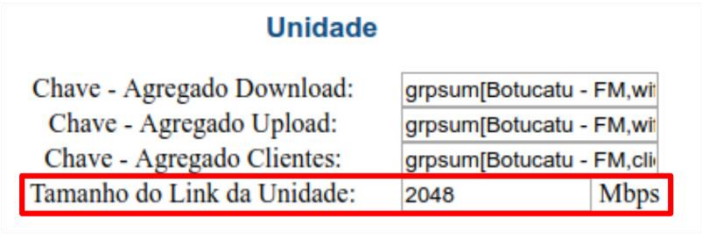
6 - Configurações

As configurações podem ser acessadas através do botão disponível na parte inferior.

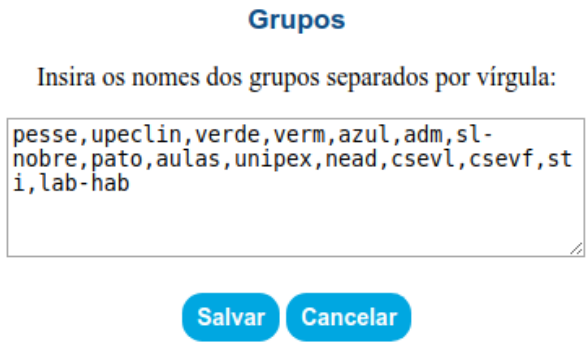


A maioria dos campos já vem configurados com os valores para utilização com o Zabbix disponibilizado pela Reitoria, as configurações a serem alteradas são:

Tamanho do link: pode ser customizada de acordo com o link disponibilizado para a unidade/campus.



Grupos: podem ser cadastradas as palavras para agrupamentos, separadas por vírgula.



Dentro do menu de Configurações ainda é possível fazer o Download e o Upload das configurações da ferramenta no formato XML.

APÊNDICE D – Questionário de avaliação da ferramenta

Avaliação de Ferramenta para Monitoramento da Rede sem Fio - Unesp

Pedimos que este formulário seja respondido após um período de utilização da ferramenta para monitoramento da Rede sem Fio da Unesp, desenvolvida pelo servidor/aluno Luiz Felipe de Camargo, dentro do seu projeto de mestrado, sob orientação do prof. Remo e com colaboração do GRC.

Seu endereço de e-mail (**luiz.felipe@unesp.br**) será registrado quando você enviar este formulário.
Não é **luiz.felipe**? Sair
*Obrigatório

1. **Nome** *

_____

2. **Idade** *

_____

3. **Gênero** *
Marcar apenas uma oval.

- ◯ Feminino
- ◯ Masculino
- ◯ Outro: _____

Parte 1 - Experiência com o sistema

4. **1.1 Quanto tempo você trabalhou no sistema?** *
Marcar apenas uma oval.

- ◯ menos de 1 hora
- ◯ de 1 hora a menos que 1 dia
- ◯ de 1 dia a menos de 1 semana
- ◯ de 1 semana a menos de 1 mês

5. **1.2 Em média, quanto tempo por semana você gastou por semana no sistema?** *
Marcar apenas uma oval.

- ◯ menos de 1 hora
- ◯ de 1 a menos de 4 horas
- ◯ de 4 a menos de 10 horas
- ◯ mais que 10 horas

Parte 2 - Experiências passadas

6. **2 Áreas de Atuação** *

Marque todas que se aplicam.

- [ ] Administração e gestão
- [ ] Desenvolvimento de sistemas
- [ ] Gerenciamento da rede cabeada
- [ ] Gerenciamento da rede sem fio
- [ ] Gerenciamento de sites e páginas
- [ ] Gestão de datacenter
- [ ] Manutenção de equipamentos
- [ ] Serviço de E-mails
- [ ] Suporte a usuários
- [ ] Videoconferência
- [ ] Telefonia VoIP
- [ ] Outro: _____

Parte 3 - Reações Gerais do Usuário

Por favor selecione os números que refletem mais apropriadamente suas impressões sobre o uso desse sistema computacional.

7. **3.1 Bom ou Ruim?** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Ruim
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Bom

8. **3.2 Frustrante ou Satisfatório?** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Frustrante
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Satisfatório

9. **3.3 Maçante ou Estimulante?** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Maçante
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Estimulante

10. **3.4 Difícil ou Fácil?** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Difícil
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Fácil

11. **3.5 Rígido ou Flexível?** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Rígido
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Flexível

Parte 4 - Telas

Por favor selecione os números que refletem mais apropriadamente suas impressões sobre o uso desse sistema computacional.

12. **4.1 Caracteres na tela do computador** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Ilegível
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Legível

13. **4.2 Destaques na tela** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Inúteis
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Úteis

14. **4.3 Layouts de tela foram úteis** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Nunca
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Sempre

15. **4.4 Quantidade de informação que pode ser exibida na tela** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Inadequado
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Adequado

16. **4.5 Sequências de telas** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Confusa
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Clara

17. **Por favor, escreva seus comentários sobre as telas aqui:**

_____

_____

_____

_____

_____

Parte 5 - Terminologia e Informações do sistema

Por favor selecione os números que refletem mais apropriadamente suas impressões sobre o uso desse sistema computacional.

18. **5.1 Uso de terminologia em todo sistema** *

Marcar apenas uma oval.

- Não aplicável
- 1 - Inconsistente
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9 - Consistente

19. **5.2 Terminologia se relaciona bem com o trabalho que você está fazendo?** *

Marcar apenas uma oval.

- Não aplicável
- 1 - Nunca
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9 - Sempre

20. **5.3 Posição das instruções na tela** *

Marcar apenas uma oval.

- Não aplicável
- 1 - Inconsistente
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9 - Consistente

21. **5.4 Mensagens que aparecem na tela** *

Marcar apenas uma oval.

- Não aplicável
- 1 - Confusas
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9 - Claras

22. **5.5 Instruções para corrigir erros** *

Marcar apenas uma oval.

- Não aplicável
- 1 - Confusas
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9 - Claras

23. **5.6 Computador mantém você informado sobre o que está fazendo** *

Marcar apenas uma oval.

- Não aplicável
- 1 - Nunca
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9 - Sempre

24. **5.7 Executar uma operação leva a um resultado previsível** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Nunca
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Sempre

25. **Por favor, escreva seus comentários sobre a terminologia e as informações do sistema aqui:**

_____

_____

_____

_____

_____

Parte 6 - Aprendizagem

Por favor selecione os números que refletem mais apropriadamente suas impressões sobre o uso desse sistema computacional.

26. **6.1 Aprendendo a operar o sistema** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Difícil
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Fácil

27. **6.2 Exploração de funcionalidades por tentativa e erro** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Desencorajante
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Encorajante

28. **6.3 Tarefas podem ser realizadas de forma simples** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Nunca
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Sempre

29. **Por favor, escreva seus comentários sobre a aprendizagem aqui:**

_____

_____

_____

_____

_____

Parte 7 - Capacidades do Sistema

Por favor selecione os números que refletem mais apropriadamente suas impressões sobre o uso desse sistema computacional.

30. **7.1 Velocidade do sistema** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Muito devagar
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Rápido o suficiente

31. **7.2 O sistema é confiável** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Nunca
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Sempre

32. **7.3 Ocorrem falhas no sistema** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Frequentemente
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Raramente

33. **7.4 Corrigindo seus erros** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Difícil
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Fácil

34. **Por favor, escreva seus comentários sobre as capacidades do sistema aqui:**

_____

_____

_____

_____

_____

Parte 8 - Manual de Usuário e Ajuda On-line

35. **8.1 Manuais técnicos são** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Confusos
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Claros

36. **8.2 A informação do manual é facilmente entendida** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Nunca
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Sempre

37. **8.3 Encontrar uma solução para um problema usando o manual** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Impossível
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Fácil

38. **8.4 Quantidade de informação fornecida** *

Marcar apenas uma oval.

- ◯ Não aplicável
- ◯ 1 - Inadequada
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9 - Adequada

Por favor, escreva seus comentários sobre manuais técnicos e ajuda on-line aqui: