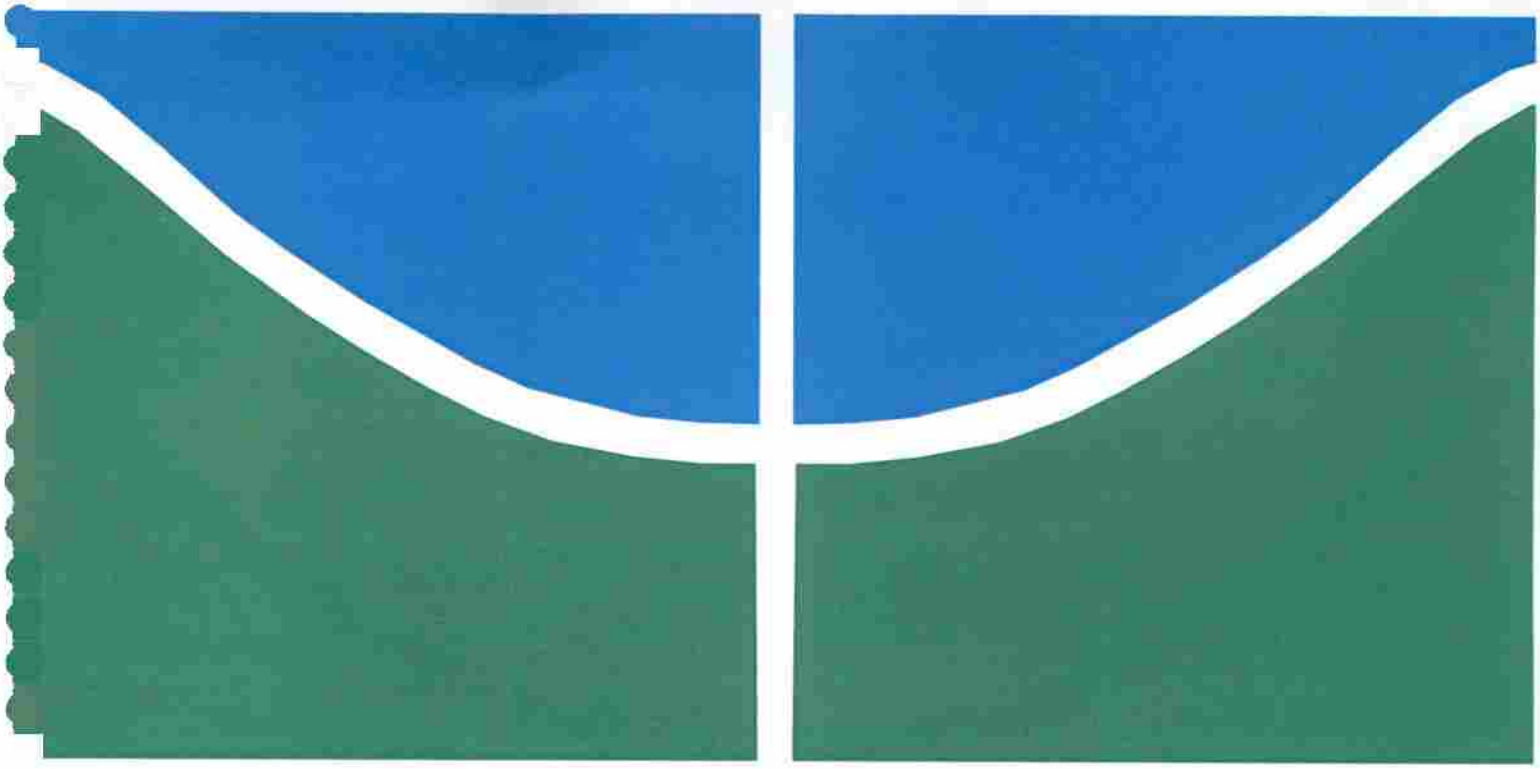


MONITORAMENTO DE SISTEMAS: MÉTRICAS PARA APLICAÇÕES LEGADAS NA UNIVERSIDADE DE BRASÍLIA

MARCOS VINÍCIUS LINHARES CASTRO

MONOGRAFIA DE ESPECIALIZAÇÃO
GESTÃO EM SEGURANÇA DA INFORMAÇÃO

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MONITORAMENTO DE SISTEMAS: MÉTRICAS PARA APLICAÇÕES LEGADAS NA UNIVERSIDADE DE BRASÍLIA

MARCOS VINÍCIUS LINHARES CASTRO

ORIENTADORA: PROFESSORA DRA. EDNA DIAS CANEDO

MONOGRAFIA DE ESPECIALIZAÇÃO – GESTÃO EM SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: UnBLabRedes.MFE.026/2017

BRASÍLIA, DF: 24 AGOSTO / 2017.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MONITORAMENTO DE SISTEMAS: MÉTRICAS PARA APLICAÇÕES LEGADAS NA UNIVERSIDADE DE BRASÍLIA

MARCOS VINÍCIUS LINHARES CASTRO

MONOGRAFIA SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA EM SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

EDNA DIAS CANEDO, ORIENTADORA
DOUTORA, FGA/UNB

_____

RAFAEL TIMOTEO DE SOUSA JUNIOR
DOUTOR, ENE/UNB (EXAMINADOR INTERNO)

_____

ELIANE CARNEIRO SOARES
MESTRE, SEEDF (EXAMINADOR EXTERNO)

BRASÍLIA, DF, 24 DE AGOSTO DE 2017.

FICHA CATALOGRÁFICA

Castro, Marcos Vinícius Linhares.

Monitoramento de Sistemas: Métricas Para Aplicações Legadas na Universidade de Brasília[Distrito Federal], 2017.

UnBLabRedes.MFE.026/2017 210 x 297mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2017).

Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia.

1. CPD
2. Métricas
3. Monitoramento
4. Nagios
5. UnB

I. ENE/FT/UnB
II. Título (série)

Departamento de Engenharia Elétrica.

REFERÊNCIA BIBLIOGRÁFICA

Castro, Marcos Vinícius Linhares. (2017). Monitoramento de Sistemas: Métricas Para Aplicações Legadas na Universidade de Brasília. Monografia de Especialização, Publicação UnBLabRedes.MFE.026/2017, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 88p.

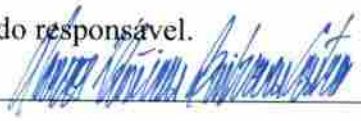
CESSÃO DE DIREITOS

AUTOR: Marcos Vinícius Linhares Castro

TITULO DA MONOGRAFIA: Monitoramento de Sistemas: Métricas Para Aplicações Legadas na Universidade de Brasília.

GRAU / ANO: Especialista / 2017

É concedida à Universidade de Brasília permissão para reproduzir cópias deste Trabalho de Conclusão de Curso de especialização e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte desse Trabalho de Conclusão de Curso pode ser reproduzido sem autorização por escrito do responsável.



Marcos Vinícius Linhares Castro
QSD 37 Lote 14 Vila Matias – Taguatinga
CEP: 72.020-370 - Brasília - DF
Tel. 55 – 61 – 98143-3953 / mvlcastro@unb.br

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, pela oportunidade de me conceder o dom da vida.

Em seguida agradeço à minha família, meus pais e irmãos, e minha esposa e filhos, por suportarem a minha ausência durante o curso e a preparação deste trabalho, e pela ajuda nos momentos mais difíceis.

A minha orientadora, Professora Doutora Edna Dias Canedo, pela paciência e pela oportunidade de trabalho.

Aos colegas de trabalho, em especial a Reinaldo Baldoino, Reginaldo Ramos, Rister, Halley e outros, agradeço pelas contribuições para a elaboração deste trabalho, sem esquecer dos demais colegas do CPD que responderam aos questionários e prestaram de forma solícita todos os esclarecimentos necessários.

A todos os colegas da turma do curso de Gestão em Segurança da Informação, pelos momentos partilhados e pela valiosa troca de experiências, e também aos professores do curso e a equipe da secretaria (LabRedes).

E à Universidade de Brasília, por ter concedido a oportunidade de crescimento acadêmico e profissional.

Dedico este trabalho à minha família, em especial a minha esposa Marybel Alves Camargo, pelo apoio ao longo de todos os anos.

"Feliz o homem que encontrou a sabedoria, o homem que alcançou o entendimento"

A Bíblia, livro de Provérbios 3:13

RESUMO

MONITORAMENTO DE SISTEMAS: MÉTRICAS PARA APLICAÇÕES LEGADAS NA UNIVERSIDADE DE BRASÍLIA

Autor: Marcos Vinícius Linhares Castro
Orientador: Professora Dra. Edna Dias Canedo
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 24 de agosto de 2017.

Ferramentas de monitoramento proporcionam aos administradores de rede um diagnóstico mais facilitado de falhas e comportamentos anormais e consequentemente sua solução mais rápida. Além do auxílio na detecção de anomalias tais aplicações podem apontar tendências e comportamentos que auxiliam uma detecção antecipada de irregularidades diversas, facilitando as atividades de manutenção preventiva. Este estudo tem como objetivo propor a adoção de métricas para monitorar os sistemas da Universidade de Brasília (UnB), verificar o monitoramento de sistemas do Centro de Informática (CPD) feito atualmente através do software Nagios, elaborar um levantamento das métricas em uso bem como elaborar uma proposta para adoção de métricas apropriadas. Para tanto foram utilizados como métodos de coleta de dados a pesquisa bibliográfica, o levantamento de informações no servidor de monitoramento e a aplicação de questionário aos colaboradores do CPD. A partir da análise de dados das respostas do questionário foi possível constatar a percepção sobre a disponibilidade dos serviços e a importância do monitoramento de sistemas para o CPD. Por sua vez, o levantamento de métricas proporcionou a obtenção de informações a respeito do monitoramento dos sistemas em produção. Por meio dos estudos, da pesquisa e dos levantamentos realizados foi possível definir um painel da situação atual do monitoramento de sistemas no CPD da Universidade.

Palavras-chave: CPD, Métricas, Monitoramento, Nagios, UnB

ABSTRACT

SYSTEM MONITORING: METRICS FOR LEGACY APPLICATIONS IN UNIVERSITY OF BRASILIA - BRAZIL
Author: Marcos Vinícius Linhares Castro
Supervisor: Professora Dra. Edna Dias Canedo
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 24 de agosto de 2017

Monitoring tools provide network administrators with easier diagnostics of faults and abnormal behavior and consequently their faster solution. Besides the aid in the detection of anomalies such applications can point out tendencies and behaviors that help the early detection of diverse irregularities, facilitating the preventive maintenance activities. . This study aims at proposing the adoption of metrics to monitor the systems of the University of Brasília (UnB), to verify the monitoring of systems of the Center of Informatics (CPD) done through the Nagios software, to elaborate a survey of the metrics in use as well as Prepare a proposal for the adoption of appropriate metrics. For this purpose, the bibliographic research, the collection of information on the monitoring server and the application of a questionnaire to the CPD collaborators were used as methods of data collection. From the data analysis of the questionnaire responses it was possible to verify the perception about the availability of the services and the importance of the monitoring of systems for the CPD. On the other hand, the metric survey provided information about the monitoring of the systems in production. Through the studies, research and surveys carried out, it was possible to define a panel of the current situation of systems monitoring in the University's CPD.
Keywords: CPD, Metrics, Monitoring, Nagios, UnB

SUMÁRIO

1 INTRODUÇÃO **1**

1.1 MOTIVAÇÃO 2

1.2 OBJETIVO DO TRABALHO 3

1.2.1 Objetivo Geral *3*

1.2.2 Objetivos Específicos *3*

1.3 METODOLOGIA DE PESQUISA 3

1.4 CONTRIBUIÇÕES DO TRABALHO 3

1.5 ORGANIZAÇÃO DO TRABALHO 4

2 EMBASAMENTO TEÓRICO **5**

2.1 OS AVANÇOS E OS DESAFIOS PARA A GESTÃO DE REDES 5

2.2 A SEGURANÇA DA INFORMAÇÃO, AS NORMAS, A DISPONIBILIDADE E O MONITORAMENTO 5

2.3 CONCEITOS DE REDES 8

2.3.1 Conceito de Redes e Seus Benefícios, Motivos de Utilização e Aspectos Técnicos *8*

2.3.2 Redes LAN, MAN, WAN e Inter-Redes *10*

2.3.3 Arquitetura de Redes, Padrões e Protocolos *11*

2.3.4 O Modelo TCP/IP *13*

2.3.5 O Protocolo ICMP *16*

2.4 GERENCIAMENTO DE REDES 18

2.4.1 O Protocolo SNMP *23*

2.5 OS REQUISITOS PARA UM SISTEMA DE MONITORAMENTO 25

2.6 PARÂMETROS PARA MONITORAMENTO 27

2.7 O NAGIOS COMO FERRAMENTA DE MONITORAMENTO 29

3 APLICAÇÃO PRÁTICA – ESTUDO DE CASO E RESULTADOS **34**

3.1 PESQUISA DE OPINIÃO 34

3.1.1 Perguntas Sobre o Perfil dos Entrevistados *34*

3.1.2 Perguntas Sobre a Opinião dos Entrevistados - Indisponibilidade *37*

3.1.3 Perguntas Sobre a Opinião dos Entrevistados - Monitoramento *43*

3.2 LEVANTAMENTO DE PARÂMETROS PARA MONITORAMENTO 52

3.3 PROPOSTA – PARÂMETROS ADICIONAIS E MELHORIAS PARA O MONITORAMENTO 58

3.3.1 Métricas ou Parâmetros Para Monitoramento *58*

3.3.2 Ajustes no Servidor de Monitoramento *60*

3.3.3 Ajustes Relacionados à Interface e à Solução *60*

4 CONCLUSÃO **61**

4.1 TRABALHOS FUTUROS 62

REFERÊNCIAS BIBLIOGRÁFICAS **64**

APÊNDICES **68**

APÊNDICE A – QUESTIONÁRIO DA PESQUISA **69**

PESQUISA ACADÊMICA: A PERCEPÇÃO DOS USUÁRIOS SOBRE A IMPORTÂNCIA DO MONITORAMENTO DE SISTEMAS NO CPD DA UNB **69**

LISTA DE TABELAS

Tabela 1 – Mensagens de erro ICMP (Tanenbaum, 2003) (Forouzan, 2008) 16
Tabela 2 – Mensagens de consulta ICMP (Forouzan, 2008) 17
Tabela 3 – Questão 1 – Grau de Escolaridade (Do Autor, 2017) 34
Tabela 4 – Questão 2 – Vínculo com a Instituição (Do Autor, 2017) 35
Tabela 5 – Questão 3 – Área de Atuação (Do Autor, 2017) 36
Tabela 6 – Questão 4 – Cargos de Chefia (Do Autor, 2017) 37
Tabela 7 – Questão 5 – Ciência de Eventos de Indisponibilidade (Do Autor, 2017) 38
Tabela 8 – Questão 6 – Frequência de Eventos (Do Autor, 2017) 39
Tabela 9 – Questão 7 – Meios de Ciência de Eventos (Do Autor, 2017) 39
Tabela 10 – Questão 8 – Causa de Eventos (Do Autor, 2017) 40
Tabela 11 – Questão 9 e 10 – Comunicado e Resposta (Do Autor, 2017) 41
Tabela 12 – Questão 11 – Impacto dos Eventos (Do Autor, 2017) 42
Tabela 13 – Questões 12 a 14 – Conhecimento x Uso x Importância (Do Autor, 2017) 44
Tabela 14 – Questão 16 – Utilização do Monitoramento (Do Autor, 2017) 45
Tabela 15 – Questão 17 – Tempo de Utilização Monitoramento (Do Autor, 2017) 46
Tabela 16 – Questão 18 – Recursos Monitorados (Do Autor, 2017) 47
Tabela 17 – Questão 19 – Intenção de Ampliação (Do Autor, 2017) 48
Tabela 18 – Questões 21 e 22 – Intenção de Implantar x Tempo (Do Autor, 2017) 50
Tabela 19 – Itens Monitorados – Geral (Do Autor, 2017) 52
Tabela 20 – Itens Monitorados – Adicionais (Do Autor, 2017) 53
Tabela 21 – Itens Monitorados – Servidores Homologação Web (Do Autor, 2017) 54
Tabela 22 – Itens Monitorados – Servidores Produção e Aplicação (Do Autor, 2017) 55
Tabela 23 – Monitoramento – Servidores Produção Aplicações Web (Do Autor, 2017) ... 56
Tabela 24 – Monitoramento – Servidores de Banco de Dados (Do Autor, 2017) 57
Tabela 25 – Itens Exclusivos – Servidor Banco de Dados – Produção (Do Autor, 2017) .. 57

LISTA DE FIGURAS

Figura 1 – Rede de 5 camadas (Soares, Souza Filho e Colcher, 1995) 12
Figura 2 – Comparação OSI x TCP/IP (Tanembaum, 2003) 14
Figura 3 – Arquitetura de Sistema de Gerenciamento (Stallings, 1999) 19
Figura 4 – Estrutura de Identificação de Objetos (Forouzan, 2008) 22
Figura 5 – Relacionamento Gerente e Agente (Douglas e Schmidt, 2005) 23
Figura 6 – Relacionamento Entre *Plug-in* e NAGIOS (Nagios P., 2017) 31
Figura 7 – Exemplo de *Dashboard* de NAGIOS (Nagios B., 2017) 33
Figura 8 – Questão 1 – Grau de Escolaridade (Do Autor, 2017) 35
Figura 9 – Questão 2 – Vínculo com a Instituição (Do Autor, 2017) 35
Figura 10 – Questão 3 – Área de Atuação (Do Autor, 2017) 36
Figura 11 – Questão 4 – Cargos de Chefia (Do Autor, 2017) 37
Figura 12 – Questão 5 – Ciência de Eventos de Indisponibilidade (Do Autor, 2017) 38
Figura 13 – Questão 6 – Frequência de Eventos (Do Autor, 2017) 39
Figura 14 – Questão 7 – Meios de Ciência de Eventos (Do Autor, 2017) 40
Figura 15 – Questão 8 – Causa de Eventos (Do Autor, 2017) 41
Figura 16 – Questão 9 e 10 – Comunicado e Resposta (Do Autor, 2017) 42
Figura 17 – Questão 11 – Impacto dos Eventos (Do Autor, 2017) 43
Figura 18 – Questões 12 a 14 – Conhecimento x Uso x Importância (Do Autor, 2017) 44
Figura 19 – Questão 15 – Importância do Monitoramento para o CPD (Do Autor, 2017). 45
Figura 20 – Questão 16 – Utilização do Monitoramento (Do Autor, 2017) 46
Figura 21 – Questão 17 – Tempo de Utilização Monitoramento (Do Autor, 2017) 47
Figura 22 – Questão 18 – Recursos Monitorados (Do Autor, 2017) 48
Figura 23 – Questão 19 – Intenção de Ampliação (Do Autor, 2017) 49
Figura 24 – Questão 20 – Sugestões de Melhoria (Do Autor, 2017) 49
Figura 25 – Questões 21 e 22 – Intenção de Implantar x Tempo (Do Autor, 2017) 51

LISTA DE ACRÔNIMOS

ARP	*Address Resolution Protocol*
CPU	*Central Processing Unit*
ASN.1	*Abstract Syntax Notation One*
DNS	*Domain Name System*
FTP	*File Transfer Protocol*
HTTP	*HyperText Transfer Protocol*
IEC	*International Electrotechnical Commission*
ICMP	*Internet Control Message Protocol*
IGMP	*Internet Group Message Protocol*
IMAP	*Internet Message Access Protocol*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
LAN	*Local Area Network*
MAN	*Metropolitan Area Network*
MIB	*Management Information Base*
NMA	*Network Management Application*
NME	*Network Management Entity*
NOC	*Network Operations Center*
OID	*Object Identifier*
OSI	*Open Systems Interconnection*
POP3	*Post Office Protocol*
RARP	*Reverse Address Resolution Protocol*
SCTP	*Stream Control Transmission Protocol*
SGBD	Sistema Gerenciador de Banco de Dados
SLA	*Service Level Agreement*
SMI	*Structure of Management Information*
SMTP	*Simple Mail Transfer Protocol*
SMS	*Short Messages Service*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*

TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
UDP	*User Datagram Protocol*
WAN	*Wide Area Network*
WMI	*Windows Management Instrumentation*

1 INTRODUÇÃO

As organizações brasileiras vêm desde as últimas duas décadas se beneficiando das vantagens da tecnologia da informação. Segundo Forouzan (2008) as comunicações de dados e as redes estão mudando de fazer negócios e o modo de viver, com as decisões de negócio tomadas de modo cada vez mais rápido. A utilização dos recursos de Tecnologia da Informação e Comunicação (TIC), demanda a otimização dos investimentos, visando a continuidade das operações e qualidade na prestação de serviços.

Para o atendimento destes dois propósitos é necessário a adoção de técnicas e recursos gerenciais com o objetivo de alinhar os investimentos e operações de TI ao negócio. Nos últimos anos surgiram diversos *frameworks* para gerenciamento de Tecnologia da Informação, sendo a biblioteca ITIL (*Information Technology Infrastructure Library*) um dos mais conhecidos e utilizados: "É um agrupamento das melhores práticas utilizadas para o gerenciamento de serviços de tecnologia de informação de alta qualidade (Fernandes; Abreu, 2008). As práticas do modelo foram organizadas em cinco processos, correspondentes aos respectivos estágios do ciclo de vida dos serviços em uma organização.

De acordo com o *framework* ITIL em alguns estágios estão processos relacionados a desempenho, disponibilidade e continuidade, bem como evento, incidente e problemas devem ser gerenciados. O devido gerenciamento destes indicadores permitem aos técnicos e gestores avaliar a disponibilidade dos serviços sempre que necessário e serem notificados por meio de alarmes, registros de falhas e notificações em tela ou mensagens, tornando possível a tomada de medidas proativas para garantir a continuidade dos serviços disponíveis. É possível, ainda, acompanhado de um planejamento adequado, implementar melhorias e aplicar modificações minimizando eventuais impactos.

Como aspectos técnicos da monitoração de sistemas, existem diversos aplicativos para monitoramento no mercado, sendo um dos mais conhecidos para essa finalidade o NAGIOS. Trata-se de uma solução *Open Source*, ou código aberto, o que permite que seja alterado pelos administradores e respectiva comunidades de usuários. Tais grupos são responsáveis também pelo desenvolvimento e melhoria da ferramenta, o que tem proporcionado constantes atualizações.

A Universidade de Brasília vem utilizando o NAGIOS desde 2007, mas a consolidação do seu uso se deu entre dois e cinco anos mais tarde. Hoje o NAGIOS está

configurado para a monitoria de equipamentos servidores, serviços e ativos de rede instalados no CPD do campus e nas demais instalações administrativas e acadêmicas.

1.1 MOTIVAÇÃO

A utilização do NAGIOS na Universidade de Brasília está atualmente em um estado "consolidado", desempenhando a monitoração de boa parte dos ativos de rede, servidores e serviços, sendo grande parte das aplicações administrativas e acadêmicas compostas de soluções legadas, com mais de quinze anos de uso desde a implantação. Tais aplicações possibilitam o apoio às atividades meio (gestão orçamentária e execução financeira, controle de patrimônio e transporte) e também atividades fim (sistemas de gestão acadêmica dos cursos de graduação, pós-graduação e extensão). Alguns desses programas são levados a termo em ambiente Windows e programados em Visual Basic versão VB 6, com outras executadas em Linux e codificadas em JAVA. Todos os sistemas utilizam base de dados de produção em ambiente Windows e SGBD Microsoft SQL Server 2008 R2. Uma vez que as aplicações descritas acima são consideradas de "missão crítica" para a universidade, com atenção especial àquelas de gestão acadêmica, se torna essencial para as equipes de sustentação de sistemas monitorar o seu funcionamento com vistas a minimizar impactos causados por eventuais falhas de continuidade destes serviços.

O sistema de monitoração existente vem contribuindo de forma positiva, porém ainda existem dificuldades em acompanhar o funcionamento das aplicações legadas. Em muitos casos a equipe de suporte se depara com falhas de indisponibilidade reportadas pelos próprios usuários, apesar dos operadores não serem notificados pelos recursos de monitoramento. Assim, a dificuldade em monitorar o funcionamento dos sistemas legados da universidade poderia ser resolvida com a aplicação e o ajuste de métricas adequadas para o monitoramento dos recursos por parte dos operadores de sistema e demais profissionais envolvidos. Portanto, buscou-se reunir os dados e informações com o propósito de responder ao seguinte problema de pesquisa: como a aplicação de métricas adequadas de monitoramento pode refletir ou contribuir para a monitoria de sistemas?

Com base nas questões expostas acima, devido à dificuldade em acompanhar o funcionamento dos sistemas legados a pesquisa se justifica através da necessidade de levantamento de métricas adequadas para melhorar a qualidade da monitoria dos sistemas em produção

1.2 OBJETIVO DO TRABALHO

1.2.1 Objetivo Geral

O objetivo geral deste trabalho é propor a adoção de métricas apropriadas para monitorar de forma objetiva os sistemas legados da Universidade de Brasília (UnB), visando a continuidade dos serviços prestados e fornecer subsídios para ações corretivas ou preventivas por parte das equipes de sustentação, manutenção e desenvolvimento dos sistemas.

1.2.2 Objetivos Específicos

Para atingir o objetivo geral, foram definidos os seguintes objetivos específicos:

a. Verificar como é feito o monitoramento de sistemas na Universidade de Brasília (UnB);
b. Efetuar um levantamento das métricas em uso atualmente para a monitoria de sistemas legados na UnB;
c. Identificar as métricas que sejam relevantes para o desempenho dos sistemas;
d. Elaborar proposta para adoção de métricas apropriadas para o monitoramento de sistemas;
e. Propor a adoção de novas métricas para monitoramento dos sistemas.

1.3 METODOLOGIA DE PESQUISA

A metodologia de pesquisa proposta está dividida em duas fases descritas em seguida. Tal divisão tem por finalidade facilitar o trabalho com a pesquisa de informações e suas aplicações no campo prático.

Fase 1: Pesquisa bibliográfica, identificando, classificando e catalogando livros, manuais, artigos e textos que apresentem relevância no tema da monografia.

Fase 2: Levantamento de informações sobre os sistemas em produção incluindo as configurações da solução de monitoramento utilizadas. Nesta etapa será feita a aplicação de questionário aos usuários e também a pesquisa de levantamento das métricas a serem propostas.

1.4 CONTRIBUIÇÕES DO TRABALHO

Sistemas de monitoramento de código aberto como NAGIOS requerem que seus administradores façam customizações, adaptações e ajustes para que possam ter seu funcionamento otimizado. Este trabalho tem como objetivo as seguintes contribuições:

- Apresentação dos resultados da pesquisa efetuada com os usuários;
- Apresentação das métricas usadas no monitoramento de sistemas;
- Apresentação de proposta de parâmetros adicionais e medidas a aplicar no monitoramento de sistemas legados;

1.5 ORGANIZAÇÃO DO TRABALHO

Para facilitar o entendimento deste trabalho a organização do mesmo é apresentada a seguir:

O capítulo 2 trata da revisão de conceitos técnicos envolvidos, com os capítulos 2.1 e 2.2 tratando de aspectos como os desafios para a gestão de redes, a segurança da informação e o monitoramento de sistemas. Em seguida apresentam-se conceitos de redes, os benefícios de sua utilização e alguns aspectos técnicos como redes locais e de longa distância. Para melhor compreensão do tema, no item 2.3.1 e seguintes são apresentados o modelo TCP/IP e o protocolo ICMP. A parte de gerência de redes é apresentada no item 2.4, e devido ao relacionamento direto com o tema, o protocolo SNMP é apresentado no item 2.4.1.Os requisitos para um sistema de monitoramento, os parâmetros e a ferramenta Nagios são apresentados nos itens 2.5, 2.6 e 2.7 respectivamente.

O capítulo 3 trata dos aspectos práticos da pesquisa, como resultado da pesquisa de opinião, o levantamento de métricas para o estudo de caso e a proposta de novas métricas e melhorias no sistema de monitoramento do CPD da UnB.

O capítulo 4 apresenta o encerramento expondo os resultados obtidos e também aspectos que poderão ser abordados em uma eventual sequência para pesquisas futuras.

2 EMBASAMENTO TEÓRICO

2.1 OS AVANÇOS E OS DESAFIOS PARA A GESTÃO DE REDES

Os últimos anos foram marcados por mudanças intensas no que diz respeito a gestão dos recursos de informação e comunicação. Com os benefícios das técnicas e recursos surgidos nos últimos 70 anos, a sociedade e também as empresas podem usufruir das inovações no que diz respeito ao processamento e difusão das informações.

Conforme Prado Filho (2015):

> Através dos anos, as tecnologias da informação e comunicação (TIC) tornaram-se uma parte integrante de muitas atividades fundamentais para suportar a infraestrutura crítica em organizações de todos os setores, sejam públicas, privadas ou voluntárias. A proliferação da internet e de outros serviços de comunicação digital, somada à capacidade dos sistemas e aplicações utilizados hoje, resultaram em um cenário onde as organizações tornaram-se mais dependentes de uma infraestrutura de TIC confiável e segura.

Os dois atributos citados - confiabilidade e segurança - demandam por uma atuação ainda mais ágil das equipes de TIC, uma vez que ocorrências relacionadas à segurança tais como falhas de equipamentos e quedas de links de comunicação causam impacto na continuidade do negócio e também em suas operações.

Isto pode ser confirmado por Prado Filho (2015) ao afirmar que as funções críticas de negócio nas quais se apresentem os requisitos de continuidade são dependentes da TIC, e neste contexto a pró atividade de suas equipes é indispensável para a manutenção dos negócios e segurança da informação. A presteza e a tempestividade das equipes fazem a diferença em instantes de adversidades que possam colocar em risco a continuidade dos negócios e a capacidade de operação das instituições.

2.2 A SEGURANÇA DA INFORMAÇÃO, AS NORMAS, A DISPONIBILIDADE E O MONITORAMENTO

A crescente adoção e uso intensivo dos recursos tecnológicos de comunicação e processamento de dados vem proporcionando a difusão das informações de forma acelerada e disseminada, o que traz benefícios e também desvantagens, sendo as últimas potenciais causadoras de forte impacto negativo para as entidades, sejam pessoas ou organizações.

Segundo Osiro (2006):

> Na sociedade da informação, ao mesmo tempo que as informações são consideradas os principais patrimônios de uma organização, estão também sob constante risco, como nunca estiveram antes. A sua perda ou roubo constitui um prejuízo para a organização e é um fator decisivo na sua sobrevivência ou descontinuidade. [...] O que aconteceria se uma empresa perdesse todas as informações relativas aos seus clientes, fornecedores ou mesmo sobre os registros funcionais dos seus empregados? Poderia ter sérios prejuízos ou mesmo descontinuar sua atividade.

O autor destaca a característica da informação como item de valor elevado para a organização e como tal deve ser protegida, sentença bastante difundida entre os profissionais de TIC e também com os gestores das empresas. A necessidade de resguardar os dados leva ao conceito de Segurança da Informação.

Para o termo Segurança da Informação, em diversas publicações e autores são apresentadas definições semelhantes. Para uma definição mais formal toma-se como exemplo os termos descritos na família ou grupo de normas ISO/IEC (*International Organization for Standardization/International Electrotechnical Commission*), mais precisamente a norma ISO/IEC 27000, a qual apresenta uma visão geral, introdutória e com diversas definições. Dessa forma, o conceito de segurança da informação, segundo ISO/IEC 27000 (2016, tradução nossa), consiste na "preservação da confidencialidade, integridade e disponibilidade da informação. " .

A definição acima apresenta um aspecto mais técnico e resumido, embora o termo se apresente de forma mais ampla na realidade. Existe atualmente uma visão mais abrangente do termo, uma vez que a segurança dos dados e informações é algo essencial para a sobrevivência de uma organização.

Para Sêmola (2014) "podemos definir segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". A definição acima carece, ainda, de melhor compreensão, de tal forma que o mesmo autor complementa que, "de forma mais ampla, podemos também considerá-la como a prática de gestão de riscos incidentes que impliquem o comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. " (Sêmola, 2014).

A partir deste ponto, dispondo de uma definição mais abrangente e direcionada à gestão, cabe discutir de forma breve as características básicas da Segurança da Informação.

Voltando à norma ISO/IEC 27000 (2016, tradução nossa), os princípios básicos são:

> Disponibilidade como a propriedade de ser acessível e utilizável a pedido por uma entidade autorizada;

> Confidencialidade como a propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados;
> Integridade como a propriedade de exatidão e completude.

Além dos três princípios citados acima existem outros tópicos mencionados por Sêmola (2016) como autenticação e conformidade, bem como outros itens como auditoria, autenticidade, autorização, criticidade, irretratabilidade (conhecida como não repúdio), relevância do ativo e dos processos de negócio e severidade. Todos os princípios citados são importantes para a Gestão da Segurança da Informação, porém fogem ao escopo deste trabalho. Desta forma, será tratado a seguir o princípio básico disponibilidade.

Em uma definição formal conforme o Dicionário Aulete (2017) disponibilidade é a "qualidade ou condição daquilo que se encontra disponível", ao passo que a norma ISO/IEC 27000 (2016) estabelece como critério o fato do recurso estar acessível e em condições de uso por um solicitante autorizado, sendo esse requerente um usuário de um sistema, aplicação ou ainda outro sistema automatizado. O oposto dessa situação – a indisponibilidade – é causadora em potencial de impactos negativos à segurança da informação.

A indisponibilidade pode ser oriunda de diversas causas diretas ou indiretas das ameaças a que um sistema de informação pode estar sujeito, tais como carência de suprimentos e insumos de qualquer natureza (falhas no fornecimento de energia elétrica), fenômenos físicos (inundações, incêndios ou vendavais) ou ainda por meio de ações humanas acidentais (negligência, imprudência ou imperícia) ou intencionais (propagação e disseminação de vírus ou ataques e invasões). Com a intenção de minimizar as ocorrências de indisponibilidade ao máximo possível, os gestores devem considerar aspectos de planejamento que levem em consideração a gestão e o monitoramento dos recursos de TIC.

Levando em consideração também que os *datacenters* atuais apresentam plataformas de *hardware*, *software* e redes complexas e heterogêneas, o desafio para o contingente de TIC é conseguir acompanhar o andamento das operações de forma preventiva, tendo em mente a manutenção da disponibilidade, um dos pilares da segurança da informação. E para facilitar o acompanhamento das operações os gestores e profissionais dispõem do monitoramento de serviços.

Entende-se por monitorar o ato de, conforme o Dicionário Aulete (2017) "acompanhar, vigiar e simultaneamente avaliar (alguém, atividade, desempenho, funcionamento etc.) com ou sem o uso de aparelhos ".

Através de aplicações de monitoramento, a equipe de TI pode acompanhar o estado de servidores quanto à memória, uso de processador e ocupação de discos, situação de equipamentos ativos de rede tais como modems, roteadores, switches e pontos de acesso sem fio. É possível acompanhar também a disponibilidade de serviços tais como web, http, ftp e bancos de dados. Além de indicar o estado presente dos recursos, os eventos são armazenados em base de dados para consultas e geração de relatórios e acompanhamento de históricos. As comunicações entre o servidor rodando a aplicação e os elementos monitorados da rede funcionam baseadas sobretudo no protocolo SNMP, cujo funcionamento será detalhado mais adiante neste trabalho.

2.3 CONCEITOS DE REDES

Para apresentação do tema monitoramento e suas definições relacionadas cabe a exposição prévia de conceitos de rede e também alguns modelos e convenções relacionados.

2.3.1 Conceito de Redes e Seus Benefícios, Motivos de Utilização e Aspectos Técnicos

Os computadores surgiram no século XX, mais precisamente na segunda metade de década de 1940. Para Tanenbaum (2003), "durante as duas primeiras décadas de sua existência, os sistemas computacionais eram altamente centralizados, em geral instalados em uma em uma grande sala com paredes de vidro". Eram equipamentos que trabalhavam isolados e com o funcionamento restrito ao local ao qual estavam instalados.

Com o passar do tempo o desenvolvimento das tecnologias de comunicação beneficiou também os computadores e a sua organização atual. Ainda de acordo com Tanenbaum (2003):

> O velho modelo de um único computador atendendo a todas as necessidades computacionais da organização foi substituído pelas chamadas **redes de computadores**, nas quais os trabalhos são realizados por um grande número de computadores separados, mas interconectados. (Grifo do autor)

A citação anterior remete ao termo redes de computadores, para o qual existem diversas definições por vários autores. O primeiro exemplo é como um agrupamento de computadores independentes interligados por um meio comum, e de forma complementar,

que "dois computadores estão interconectados quando podem trocar informações" (Tanenbaum, 2003).

Outra definição relevante é apresentada por Forouzan (2008) na qual se define uma rede por "um conjunto de dispositivos (normalmente conhecidos como nós) conectados por links de comunicação. Um nó pode ser um computador, uma impressora ou outro dispositivo de envio e/ou recepção de dados, que estejam conectados a outros nós da rede. ".

Para o estudo das redes de computadores cabe destacar seu principal benefício, os motivos de sua utilização e os requisitos técnicos mais relevantes.

Tanenbaum (1997) descreve como exemplo uma empresa com muitas fábricas em diversas localidades e computadores funcionando de forma autônoma, e em um dado momento a gestão decidiu interligá-los para obter informações centralizadas para toda a organização.

O exemplo descreve a funcionalidade de compartilhamento de recursos, sobre o qual se observa que a utilização das redes proporciona aumento de produtividade aos usuários e suas instituições.

Por sua vez, como características de elementos motivadores para a adoção das redes, (Tanenbaum, 1997) cita ainda:

- Confiabilidade: A disponibilidade de meios alternativos visando a contingência para a provisão de recursos;
- Economia de recursos: A adoção de ambientes descentralizados possui custos mais reduzidos, comparados aos mainframes (arquitetura cliente/servidor);
- Escalabilidade: Ao contrário dos mainframes, é possível prover aumento de recursos em função da demanda de serviços;
- Comunicação: sem relação direta com a tecnologia, recursos de comunicação via rede viabilizam o aumento de produtividade independente de sua localização geográfica.

Tais elementos demonstram que a adoção das redes pelas instituições pode trazer inúmeras vantagens para a redução de custos operacionais.

Visando aspectos técnicos, Forouzan (2008) afirma que uma rede deve atender a certa quantidade de conceitos, e enumera os mais importantes:

- Desempenho: medidos pelo tempo de trânsito e tempo de resposta; depende de vários fatores; avaliado por métricas como capacidade de vazão (*throughput*) e atraso (*delay*);

- Confiabilidade: mensurada pela frequência de falhas, tempo de recuperação a partir da ocorrência de uma falha e robustez da rede em caso de incidentes;
- Segurança: a proteção dos dados contra acesso não autorizado, danos e o desenvolvimento e implementação de políticas e procedimentos para recuperação de violações e perda de dados;

De acordo com o autor, os conceitos acima são requisitos técnicos relevantes para o funcionamento de uma rede, e para cada condição são citados alguns critérios de medida. Os parâmetros para aferição do desempenho são diversos e alguns deles também são aplicados ao monitoramento de sistemas, razão pela qual serão citados neste trabalho mais adiante.

Em seguida aos conceitos de redes cabe discutir também alguns aspectos de classificação, modelos e gerenciamento.

2.3.2 Redes LAN, MAN, WAN e Inter-Redes

Uma forma de classificação de redes utiliza o critério da extensão geográfica, o qual relaciona três tipos: Redes Locais ou LAN (*Local Area Network*), Redes de Abrangência Metropolitana ou MAN (*Metropolitan Area Network*) e Rede de Ampla Abrangência ou WAN (*Wide Area Network*). Tal raciocínio leva em consideração o alcance e a distância máxima entre os pontos dessa rede.

De acordo com Forouzan (2008) "uma LAN normalmente cobre uma área geográfica menor que 3 km; uma WAN pode ter uma cobertura mundial. As redes de tamanho intermediário a esses são, em geral, conhecidas como redes de abrangência metropolitana (MAN) e abrangem uma cobertura de dezenas de quilômetros".

As redes locais ou LAN, portanto, são redes limitadas a um escritório, uma edificação ou uma área um pouco maior como um campus. Uma MAN ou rede metropolitana pode cobrir bairros e cidades ao passo que uma WAN tem abrangência nacional, internacional ou até mesmo mundial. Atualmente conta-se com a onipresença das redes de tal forma que, "hoje, é muito raro vermos uma LAN, MAN ou WAN isoladas; elas estão conectadas entre si. " (Forouzan, 2008).

Uma abordagem técnica é necessária para detalhar as características dos três tipos de rede. Tanenbaum (2003) menciona particularidades para as redes LAN, como restrição de tamanho, tecnologias de transmissão e topologia, sendo que tais aspectos influem na adoção

de tecnologias que seriam inviáveis em outras situações como as WANs, que lançam mão de recursos como linhas de transmissão e elementos de comutação.

Embora os conceitos expostos acima sejam consenso entre os dois autores, cabem ainda algumas observações a respeito. Forouzan (2008) afirma que "Quando duas ou mais redes estiverem conectadas, elas se tornam uma *internetwork* ou internet. ", conceito também apresentado por Tanenbaum (2003) quando afirma que "um conjunto de redes interconectadas é chamado **inter-rede** ou **internet** (grifo do autor) ". A opinião do primeiro autor vai ao encontro do pensamento do segundo quando dizem que os termos *internetwork*, inter-rede ou internet servem para definir o conceito apresentado, e também apontam a Internet mundial (com letra "I" maiúscula) como exemplo de uma inter rede específica.

As redes podem, portanto, ser classificadas como LAN, MAN e WAN, a depender de sua abrangência geográfica, e possuem características próprias, com as LANs dispondo de diversas topologias e recursos técnicos e as WANs se baseando em linhas de transmissão e elementos de comutação de pacotes.

2.3.3 Arquitetura de Redes, Padrões e Protocolos

As redes de computadores atualmente estão interligadas por diversos meios e recursos, somando-se a isto a diversidade de soluções apresentadas por fabricantes. A interconexão destas redes pode apresentar desafios de natureza técnica devido às questões de compatibilidade entre os inúmeros padrões existentes.

Ao longo dos primeiros anos do surgimento das redes de computadores, o projeto tinha o hardware em evidência em detrimento do software (Tanenbaum, 2003). Devido a este enfoque surgiram questões relacionadas à integração entre padrões que dificultava a comunicação entre plataformas diferentes. De acordo com Soares, Souza Filho e Colcher (1995) "Tornou-se necessário definir uma arquitetura única, e para garantir que nenhum fabricante levasse vantagem em relação aos outros a arquitetura teria que ser aberta e pública. ". Nesse ensejo se desenvolveram modelos, padrões e protocolos com a intenção de possibilitar o funcionamento dos sistemas de comunicação de forma independente dos fornecedores envolvidos.

Para facilitar o projeto de redes, conforme Tanenbaum (2003) elas são estruturadas como "uma pilha de **camadas** ou **níveis,** colocadas umas sobre as outras" (grifo do autor). O mesmo autor (Idem, 2003) informa também que "as entidades que ocupam as camadas

correspondentes em diferentes máquinas são chamadas **pares** (**peers**). " (grifos do autor). Pares podem ser processos, dispositivos de hardware ou mesmo pessoas. A Figura 1 apresenta uma rede de 7 camadas.

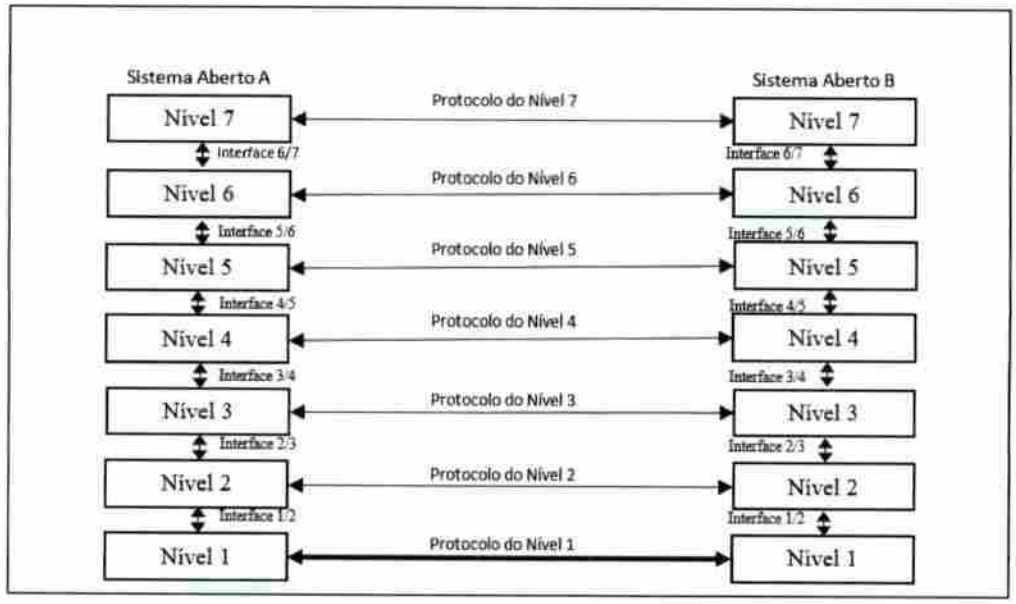


Figura 1 – Rede de 5 camadas (Soares, Souza Filho e Colcher, 1995)

Com base na figura acima é possível detalhar melhor o funcionamento da estrutura. Cada camada ou nível "deve ser pensada como um programa ou processo, implementada por hardware e software que se comunica com o processo correspondente na outra máquina. " (Soares, Souza Filho e Colcher, 1995).

Cabe ainda explicar que entre duas entidades de mesmo nível, os dados não são enviados diretamente ou de forma horizontal ao respectivo nível de destino, mas sim de forma vertical, através dos níveis descendentes até o nível 1 (o qual é o único ponto de comunicação horizontal entre máquinas); ao chegar ao nível 1 do sistema de destino percorrem em ordem ascendente de níveis até a camada de mesmo número da entidade de origem.

A comunicação através de uma dada camada de uma máquina a outra é viável graças aos protocolos. Segundo Tanenbaum (2003) "protocolo é um conjunto de regras que controla o formato e o significado dos pacotes ou mensagens que são trocadas pelas entidades pares, contidas em uma camada. " Complementando com as palavras de Forouzan (2008) um protocolo define o que, como e quando deve ser comunicado.

Cabe aqui destacar a diferença entre serviço e protocolo. O último diz respeito aos pacotes enviados entre entidades pares de máquinas diferentes, enquanto o primeiro está

relacionado às interfaces entre camadas. Tanenbaum (2003) adverte sobre a necessidade de não se confundir os dois conceitos.

A diversidade de fabricantes de equipamentos de telecomunicações e redes levou à criação de padrões por iniciativas de entidades internacionais. Segundo Forouzan (2008) os padrões são imprescindíveis para uma competição saudável entre os fabricantes de equipamentos e garantir interconectividade entre os diversos agentes de mercado (governo, consumidores e indústria).

Para o estabelecimento de padrões diversas entidades estão envolvidas, como ISO, IEC, IEEE, IETF e outras. Existem inúmeros padrões atualmente, mas os mais conhecidos são o modelo de referência OSI e o TCP/IP. O segundo padrão será abordado neste trabalho mais adiante.

Ainda sobre os dois padrões citados, cabe fazer uma observação sobre eles: Soares, Souza Filho e Colcher (1995) afirma que a adoção do TCP/IP como solução não-proprietária para a interconexão de sistemas fez dela um padrão *de facto*, devido à sua adoção pelo mercado. Já o modelo OSI da ISO, embora não desfrute da mesma aceitação por parte do mercado se trata de um padrão *de jure*, isto é, elaborado por uma instituição legalmente constituída para tal fim.

2.3.4 O Modelo TCP/IP

Desde a primeira metade da década de 1970 um modelo de redes já estava estabelecido e em funcionamento. Inicialmente foi empregado na ARPANET, uma rede de pesquisas patrocinada pelo Departamento de Defesa Norte-Americano (DoD) e surgiu com a interligação de poucos nós entre universidades e repartições públicas. Chamado TCP/IP (*Transmission Control Protocol/Internet Protocol*), permitiu às universidades e repartições públicas que se conectassem por meio de linhas telefônicas dedicadas. Posteriormente surgiram questões sobre as conexões com os protocolos utilizados à época, o que provocou o surgimento de requisitos de conexão às várias redes de maneira uniforme. Os dois principais protocolos empregados na arquitetura, o TCP e o IP foram criados por Vint Cerf e Robert Kahn em 1974, e o modelo de referência passou a ter o nome de Modelo de Referência TCP/IP (Tanenbaum, 2003).

Conforme explicado acima, o modelo é baseado nos seus dois protocolos principais, o TCP (*Transmission Control Protocol*) e o IP (*Internetworking Protocol*). Além desses

existem outros protocolos envolvidos, o que pode causar confusão quando se referem à pilha de protocolos propriamente dita e os protocolos TCP e IP, com características diferentes (Poleto Filho, 2011). Como exemplo, o protocolo TCP é um protocolo que atua na camada de transporte, e o IP atua na camada inter-rede.

A Figura 2 apresenta uma comparação do modelo OSI com o TCP/IP, em relação às camadas dos dois paradigmas.

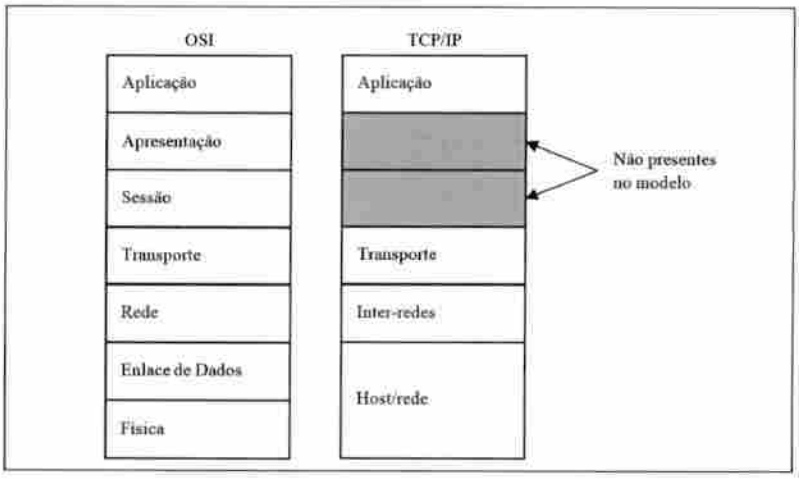


Figura 2 – Comparação OSI x TCP/IP (Tanembaum, 2003)

Tomando por base a figura acima, vale destacar a equivalência entre camadas:

> O conjunto de protocolos TCP IP foi definido como tendo quatro camadas: Host-rede, internet, transporte e aplicação. Entretanto, quando o TCP/IP é comparado ao modelo OSI podemos dizer que a camada host-rede é equivalente à combinação das camadas física e enlace de dados. A camada internet equivale à camada de rede e a camada de aplicação realiza, a grosso modo, as funções das camadas de sessão, de apresentação e de aplicação com a camada de transporte no TCP/IP cuidando também de parte das tarefas da camada de sessão (Forouzan, 2008).

Tomando por base a informação acima em relação ao modelo TCP/IP, entende-se que, além de se apresentar de um modo mais simplificado, o modelo TCP/IP possui camadas que assumem funções análogas às do modelo OSI. Temos, por exemplo, o caso da camada de transporte que é semelhante nos dois modelos. Já as camadas física e de enlace de dados do modelo OSI são equivalentes à camada host-rede do modelo TCP/IP, o qual por sua vez não apresenta as camadas de sessão e apresentação presentes no modelo desenvolvido pela ISO.

Baseado nas citações dos autores acima, pode-se constatar que eles concordam nos aspectos do protocolo TCP/IP com quatro camadas, pois se referem aos nomes de cada camada e também na quantidade de camadas empregadas no modelo. Mesmo assim, alguns

autores empregam um modelo diferente com cinco camadas, como afirma Tanenbaum (2003), que divide a camada host-rede em duas, a camada física e camada de enlace de dados. O autor deixa claro que tal modelo, denominado híbrido, é usado para fins de estudo em seu livro. Uma abordagem semelhante é utilizada por Comer (2007), embora neste caso a camada host-rede é dividida entre camada física e interface de rede. Neste trabalho, entretanto, será adotado o modelo de 4 camadas. A seguir apresenta-se a função das quatro camadas e alguns de seus protocolos mais conhecidos.

A primeira camada em nível mais baixo é a camada host-rede. Uma vez que "os livros e a documentação que tratam do modelo TCP/IP raramente descrevem este protocolo" (Tanenbaum, 2003), sabe-se que tal camada é responsável pelo envio e recebimento de pacotes IP. Já Forouzan (2008) afirma que essa camada não define protocolo, mas suporta protocolos-padrão e proprietários.

A camada superior à camada de host-rede é a camada de rede, inter-redes, ou internet, e é responsável pela integração de toda a arquitetura, e também por possibilitar que os hosts apresentem os pacotes em qualquer rede e garantir que eles possam seguir de maneira independente até o destino, inclusive em redes diferentes (Tanenbaum, 2003). Neste nível funciona, com função principal, o IP (*Internetworking Protocol*), um protocolo sem conexão e não confiável. De acordo com Forouzan (2008), os dados são agrupados em pacotes denominados datagramas, os quais podem trafegar por diferentes rotas até o destino, podendo ainda chegar fora de sequência ou mesmo duplicados.

Esta camada tem outras duas atribuições importantes. Tanenbaum (2003) complementa que elas são o roteamento de pacotes e o controle de congestionamento, o que faz esta camada semelhante à camada de redes do modelo OSI. Outros protocolos de rede que atuam nesta camada são o ARP (*Address Resolution Protocol*), RARP (*Reverse Address Resolution Protocol*), ICMP (*Internet Control Message Protocol*) e IGMP (*Internet Group Message Protocol*).

A camada seguinte é a camada de transporte e tem a função de estabelecer comunicação entre dois hosts de modo semelhante à camada de mesmo nome do modelo OSI (Tanenbaum, 2003). Atua nesta camada o TCP (*Transmission Control Protocol*), um protocolo confiável (que permite a entrega sem erros) e orientado a conexão (que estabelece uma conexão entre as duas pontas de uma transmissão). Ainda sobre o TCP, ele divide o fluxo em unidades menores e com números sequenciados chamados segmentos, o que permite uma reorganização no host de destino (Forouzan, 2008).

Ainda sobre esta camada, outros dois protocolos importantes são o UDP (*User Datagram Protocol*) e o SCTP (*Stream Control Transmission Protocol*). O primeiro consiste em um protocolo sem conexão e não confiável, utilizado quando a velocidade de entrega é prioritária, como transmissão de dados de áudio ou vídeo (Tanenbaum, 2003). Já o segundo "provê suporte para as aplicações mais recentes, como voz sobre IP. Trata-se um protocolo de camada de transporte que combina o que há de melhor no UDP e no TCP" (Forouzan, 2008).

A camada seguinte e de nível mais alto é a camada de aplicação. É importante lembrar que o modelo TCP/IP não possui as camadas de sessão e apresentação, disponíveis no modelo OSI, uma vez que não foi percebida a mesma necessidade no TCP/IP; na prática isto foi confirmado pois são usadas muito pouco nas aplicações (Tanenbaum, 2003).

Nesta camada atuam muitos protocolos, como o Protocolo de Transferência de arquivos ou FTP (*File Transfer Protocol*), o Protocolo Simples de Transferência de Mensagens ou SMTP (*Simple Mail Transfer Protocol*), o Sistema de Nomes de Domínio ou DNS (*Domain Name System*) para resolução de nomes e o Protocolo de Transferência de Hipertexto ou HTTP (*HyperText Transfer Protocol*) para acesso à web.

2.3.5 O Protocolo ICMP

No modelo TCP/IP o protocolo mais utilizado durante o funcionamento da rede, na transmissão dos dados até o seu destino é o IP. Como explicado em capítulos anteriores se trata de um protocolo sem conexão e não confiável. Entretanto existe um meio de controle de erros, de tal forma que o "IP tenta evitar erros e relatar problemas quando eles acontecem" (Comer 2006). Para as notificações de erro é utilizado o Protocolo Internet de Controle de Mensagens ou ICMP (*Internet Control Message Protocol*).

O ICMP funciona como um protocolo de auxílio ao protocolo IP. No momento da detecção de erros ele encaminha notificações ao transmissor da mensagem, deixando a correção a cargo de outros protocolos de nível mais alto. O protocolo usa o endereço IP de origem para enviar a mensagem de erro para a origem (transmissor) do datagrama (Forouzan 2008). Está previsto o tratamento de cinco tipos de erros, mostrados na Tabela 1:

Tabela 1 – Mensagens de erro ICMP (Tanenbaum, 2003) (Forouzan, 2008)

Tipo	Mensagem	Descrição
3	Destination Unreachable	Destino inalcançável
4	Source Quench	Notificação para ajuste de taxa de transmissão
5	Redirect	Orientação de rota para roteadores

Tipo	Mensagem	Descrição
11	Time Exceeded	Tempo expirado (campo TIME TO LIVE)
12	Parameter Problem	Parâmetro (cabeçalho) inválido

De acordo com a tabela acima, pode-se tomar como exemplo um envio de mensagem do tipo 02 (*Destination Unreachable*) a um host originador da mensagem que enviou um datagrama, para auxílio na detecção de algum tipo de erro que esteja impedindo a chegada dos dados no destino.

Além das mensagens de notificação de erros existem também as mensagens de consulta, estas em pares (solicitação e resposta) com as quais administradores ou hosts podem obter informações de um outro host ou roteador. Estas mensagens, úteis para a resolução de problemas, podem ser utilizadas como ferramentas auxiliares de diagnóstico pelos administradores da rede (Forouzan, 2008). A Tabela 2 apresenta os quatro tipos de requisição:

Tabela 2 – Mensagens de consulta ICMP (Forouzan, 2008)

Tipo	Mensagem	Descrição
0	Echo Reply	Resposta da mensagem de requisição
8	Echo Request	Mensagem de requisição
9	Router Advertisement	Anúncio de roteadores
10	Router Solicitation	Solicitação de roteadores
13	Timestamp	Solicitação de carimbo de tempo
14	Timestamp Reply	Resposta de carimbo de tempo
17	Address Mask Request	Solicitação de máscara de endereço
18	Address Mask Reply	Resposta de máscara de endereço

A partir das duas tabelas mostradas anteriores, pode-se tomar como exemplo o uso de dois aplicativos utilizados como ferramentas de debug: o ping e o traceroute. O primeiro utiliza as mensagens do tipo 8 e 0 (*Echo Request* e *Echo Reply*) para verificar se um host está ativo. Já o segundo, traceroute, se utiliza de mensagens do tipo 11 (*Time Exceeded*), 3 (*Destination Unreachable*) ou ainda solicitações do tipo 8 e 0 (a depender da implementação) para construir uma lista de roteadores envolvidos da origem a um dado destino (Comer 2006).

O protocolo ICMP também é utilizado em softwares de monitoramento para acompanhar o funcionamento de hosts, roteadores e equipamentos de rede.

2.4 GERENCIAMENTO DE REDES

As redes atuais são compostas por muitos componentes de hardware e software interconectados. Mesmo com a universalização dos padrões de conectividade como TCP/IP e OSI, o gerenciamento de redes heterogêneas se apresenta como um desafio para as equipes de administração.

A dificuldade de administração de uma rede se apresenta por dois motivos: heterogeneidade e extensão. O primeiro motivo pela quantidade e diversidade de componentes e seus fornecedores, e a segunda razão pelo alcance geográfico das redes, uma vez que envolve equipamentos instalados de forma remota (Comer, 2007).

O mesmo autor fornece também dois exemplos de problemas de redes:

> Por exemplo, uma falha intermitente pode não ser percebida porque o TCP automaticamente retransmite os dados danificados no tráfego. [...] A retransmissão de pacotes usa largura de banda que poderia ser usada para enviar novos dados. Similarmente, uma falha de hardware que permanece despercebida se torna pior com o passar do tempo, conforme o hardware se deteriora [...]. Como as retransmissões baixam o throughput e aumentam o atraso, o desempenho global da rede diminui gradualmente. (Comer, 2007).

Os motivos e exemplos acima ilustram a importância do gerenciamento de redes. Falhas de rede que ocorrem de forma discreta podem se agravar com o passar do tempo até a completa indisponibilidade do sistema. Quando a falha não se manifesta de imediato pode provocar quedas no desempenho de modo imperceptível, o que pode incorrer em consumo de tráfego, tempo de processamento e consumo de recursos.

Para o controle das operações de uma rede em níveis satisfatórios de qualidade os seus administradores precisam manter a operação dos recursos com níveis baixos de indisponibilidade de serviços, o que demanda a identificação tempestiva de problemas, anomalias e falhas. E para facilitar a operação os profissionais envolvidos podem contar com o gerenciamento de redes, o qual pode ser definido como o monitoramento, teste, configuração e diagnóstico dos itens de uma rede para atender a sua operação de modo estável, eficiente e com níveis de serviços em consonância ao acordado com seus usuários, utilizando para isto de um sistema que envolva hardware, software e pessoas (Forouzan 2008).

Um sistema de gerenciamento de redes, conforme Stallings (1999), apresenta um conjunto de ferramentas de monitoramento e controle integradas da seguinte maneira:

- Uma única interface de operador com um poderoso e amigável conjunto de comandos para execução de todas ou quase todas as atividades de gerenciamento;

- Uma quantidade mínima de equipamentos separados, de tal forma que a maior parte de hardware e software necessários para o gerenciamento da rede sejam incorporados nos equipamentos de usuários existentes.

O software usado nas atividades de monitoramento é executado nos computadores hospedeiros e nos equipamentos de suporte à comunicação (switches e roteadores) e servidores de aplicação, web, correio eletrônico e outros. Por meio dos softwares de gerência de redes os gerentes podem efetuar consultas aos dispositivos como hosts, roteadores e switches para obter informações de funcionamento e dados estatísticos sobre as redes com as quais estão interligados, bem como efetuar controle e configuração de dispositivos. Os softwares de gerência de rede são utilizados em centrais de operações conhecidas como NOC (*Network Operations Center*) e são aplicações de auxílio aos administradores no monitoramento, administração e controle de uma rede. (Comer, 2007), (Kurose, 2010). A Figura 3 apresenta um modelo de arquitetura de gerenciamento:

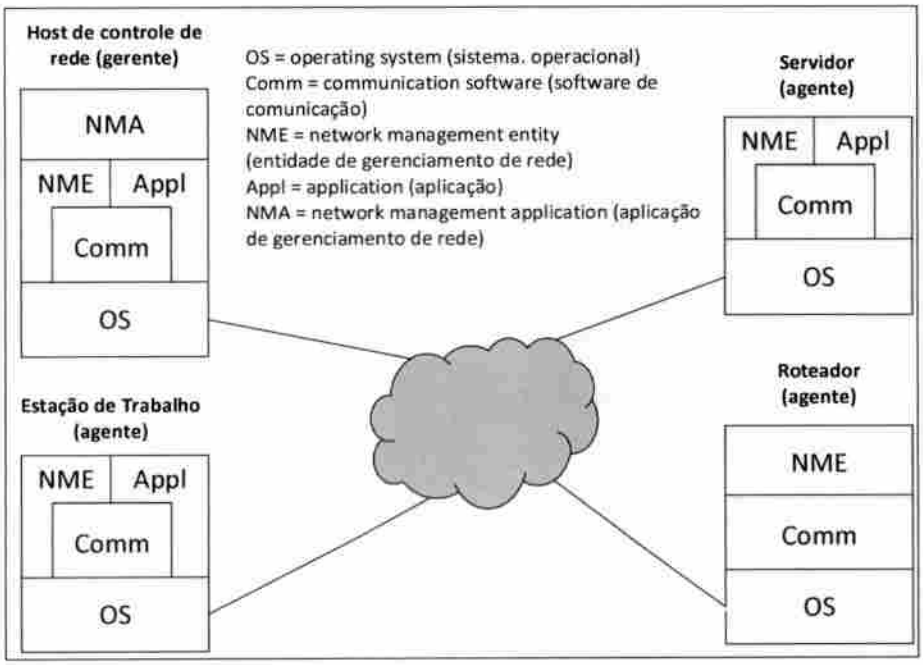


Figura 3 – Arquitetura de Sistema de Gerenciamento (Stallings, 1999)

De acordo com Stallings (1999), na figura acima cada nó de rede contém um conjunto de software dedicado ao gerenciamento de rede e descrita na figura como Entidade de Gerenciamento de Rede ou NME (*Network Management Entity*). Cada entidade de gerenciamento executa as seguintes tarefas:

- Coletar estatísticas a respeito das atividades relacionadas a rede;
- Armazenar as estatísticas localmente;
- Responder a comandos do Centro de Controle, entre os quais:

1. Transmitir estatísticas ao Centro de Controle;
2. Alterar parâmetros (por exemplo um timer usado em um protocolo de transporte)
3. Fornecer informações de status (por exemplo valores de parâmetros diversos, links ativos)
4. Gerar tráfico artificial para executar testes;

- Enviar mensagens ao centro de controle quando de mudanças significativas

Ainda sobre a figura, pelo menos um host é destinado a ser o host de controle, ou gerente. Este ainda possui um conjunto de software chamado Aplicação de gerenciamento de rede, ou NMA (*Network Management Application*), que conta com uma interface para acesso ao usuário que irá operar o sistema. O NMA responde aos comandos do usuário para exibir informações e também pode enviar comandos às demais entidades envolvidas

Para apresentação de um exemplo toma-se um programa aplicativo de gerência que desempenha o papel de cliente enquanto um software aplicativo instalado no dispositivo funciona como servidor. A comunicação se dá por meio de protocolos TCP ou UDP, com o cliente enviando solicitações e o servidor respondendo.

Com o intuito de se evitar equívocos entre as aplicações acionadas por usuários e as aplicações envolvidas no gerenciamento de redes, utilizam-se os termos gerente e agente. O programa cliente executado no equipamento é chamado gerente, e a aplicação executada no dispositivo é chamada de agente. (Comer, 2007).

Voltando à arquitetura de gerenciamento, Stallings (1999) afirma também que o software em uma arquitetura de gerenciamento pode ser dividido em três categorias:

- Software de apresentação de usuário
- Software de gerenciamento de rede
- Software de comunicações e suporte à base de dados

A primeira categoria diz respeito a interação entre o sistema de gerência e o usuário. Deve apresentar uma interface unificada de tal forma que permita a utilização ao operador da forma mais facilitada possível. Outro aspecto importante diz respeito à quantidade de informação apresentada em tela, para evitar sobrecarga de informações aos operadores.

A segunda categoria trata das aplicações envolvidas no fornecimento de serviços de interesse aos usuários no que diz respeito ao gerenciamento de rede. Também envolve a apresentação das informações aos usuários, um protocolo de gerenciamento de rede para troca de informações de gerenciamento entre gerentes e agentes e o acesso às bases de dados.

A terceira categoria é responsável pelo suporte às bases de dados locais e também pela comunicação entre outros nós. A Base de Informações de Gerenciamento ou MIB

(*Management Information Base*) diz respeito às informações de características e comportamentos do nó que devem ser monitoradas. Já a comunicação consiste entre as trocas de informações entre os nós gerente/agente por meio de uma pilha de protocolos. Ainda sobre o software de monitoramento, cabe destacar que o mesmo opera na camada de aplicação, conforme a norma de gerenciamento de redes da ISO (ISO/IEC 7498-4, 1989).

Ainda sobre o suporte à base de dados, para fins de definição da estrutura das informações de gerenciamento a serem armazenadas foi definido um padrão internacional denominado Estrutura de Informações de Gerenciamento ou SMI (*Structure of Management Information*). Tal protocolo "define precisamente como os objetos são nomeados e especifica seus tipos de dados associados. " (Mauro e Schmidt, 2011). A intenção foi criar um padrão simples e extensível dentro de uma base, de tal modo que existem apenas dois tipos de dados simples (escalares e dois vetores bidimensionais de escalares), não existindo suporte para a criação e recuperação de dados complexos (Stallings, 1999). Como forma de possibilitar um meio de representação padronizada, a SMI deve:

- Fornecer um meio técnico de padronização para definir a estrutura de determinada base de gerenciamento;
- Fornecer um meio padronizado para definição de objetos individuais incluindo a sintaxe e valor de cada objeto;
- Fornecer técnica padronizada para codificar valores de objeto.

Sobre suas restrições do SMI, vale mencionar Forouzan (2008) quando afirma que "O SMI não define o número de objetos que uma entidade pode gerenciar, não dá nomes aos objetos a serem gerenciados nem define a associação entre os objetos e seus valores. " Para suprir as limitações deste protocolo existe um outro padrão, a MIB.

A MIB ou Base de Informações de Gerenciamento é um outro padrão que define a criação de um conjunto de objetos para cada uma das entidades. Apresenta semelhança a um banco de dados usando metadados. (Forouzan, 2008). Os objetos incluídos em uma MIB são definidos de maneira formal, de tal modo que as definições especifiquem os tipos de dados de um objeto, como podem ser permitidos e intervalos de valores e também seus relacionamentos com outros objetos dentro da MIB. Para a definição de tais objetos é utilizada a Notação de Sintaxe Abstrata 1 ASN.1 (*Abstract Syntax Notation*), a qual também serve para definir a inteira estrutura da MIB. Para manter a mesma diretriz de simplicidade adotada no protocolo SMI somente um subconjunto restrito dos elementos e recursos da ASN.1 são utilizados. (Stallings, 1999).

Para atender a uma determinação da SMI cada objeto gerenciado (um servidor, uma variável em um servidor ou um valor) tenha um nome exclusivo. Assim, cada nome recebe um identificador hierárquico dentro de uma estrutura em forma de árvore. A Figura 4 apresenta uma representação simplificada da referida estrutura.

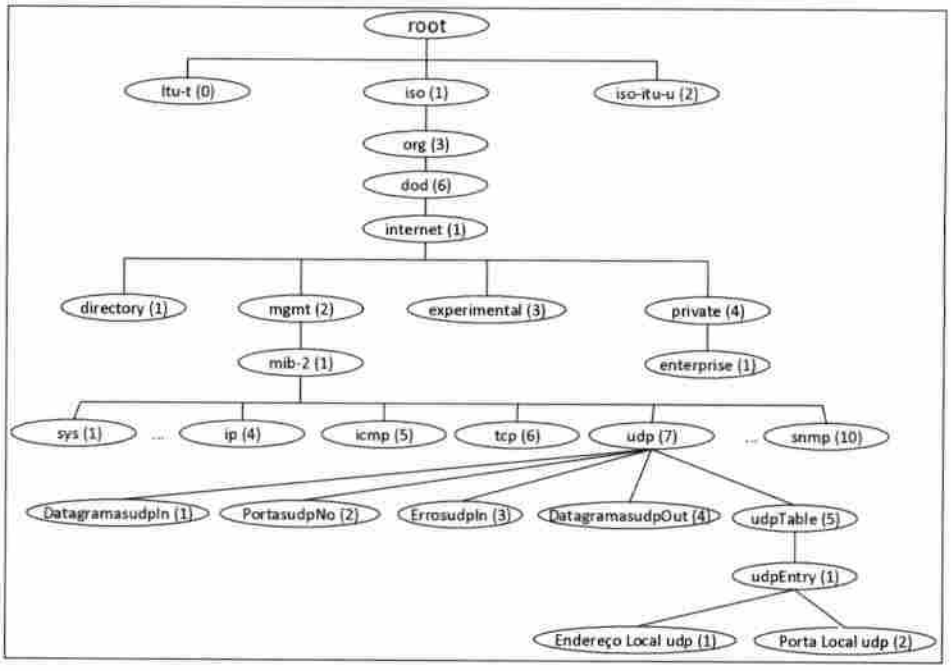


Figura 4 – Estrutura de Identificação de Objetos (Forouzan, 2008)

De acordo com a Figura 4 o nome de um objeto ou OID (Object Identifier) é obtido através da sequência de inteiros separados por pontos, a cada nó. Um objeto pode também ser definido pela sequência de nomes em texto, também separados por pontos. Assim, as duas formas de identificação com notações distintas são válidas:

iso.org.dod.internet.mgmt.mib-2 1.3.6.1.2.1

O exemplo acima serve para o protocolo SNMP. Uma vez que o SNMP opera na mib-2, o identificador de objeto sempre será iniciado com 1.3.6.1.2.1.

O segundo exemplo serve para demonstrar o acesso ao objeto udp, o qual acessa informações relativas ao protocolo UDP, como número de portas e pacotes enviados e recebidos. Para acessar as variáveis usa-se o id do grupo (1.3.6.1.2.1.7) seguida do id da variável. Uma vez que os identificadores acessam somente a variável, para acessar a instancia respectiva deve-se adicionar o número 0:

udpInDatagrams.0 1.3.6.12.1.7.1.0

udpNoPorts.0	1.3.6.12.1.7.2.0
udpInErrors.0	1.3.6.12.1.7.3.0
udpOutDatagrams.0	1.3.6.12.1.7.4.0

Com o esquema de notação descrito acima é possível referenciar qualquer objeto em uma MIB utilizando-se os nomes de objetos e seus atributos.

Os protocolos SMI e MIB em conjunto com a notação ASN.1 tornam possível a padronização dos sistemas de gerenciamento e são utilizados pelo protocolo SMTP, tema do próximo tópico.

2.4.1 O Protocolo SNMP

Na Seção 2.4 foi apresentada a gerência de redes e seus principais componentes. Foi explicado que uma estrutura de gerenciamento padrão é constituída de definições dos objetos de gerenciamento (MIB), linguagem de definição de dados (SMI) e um protocolo. As duas primeiras foram tratadas no tópico anterior, restando o detalhamento do último. O Protocolo de Gerenciamento de Rede Simples ou SNMP (*Simple Network Management Protocol*) funciona de forma simplificada e modularizada, com a linguagem de definição de dados e a MIB independentes do protocolo, que por sua vez é independente do MIB. A integração entre os componentes foi bem-sucedida, de tal forma que Forouzan (2008) define o SNMP como um *framework* para gerenciamento de dispositivos em rede com o uso de protocolos TCP/IP.

O SNMP utiliza o conceito de gerente e agente, onde uma estação de gerencia roda o programa cliente, e uma estação gerenciada de nome agente roda um programa servidor SNMP. A Figura 5 apresenta o relacionamento entre o gerente e o agente.

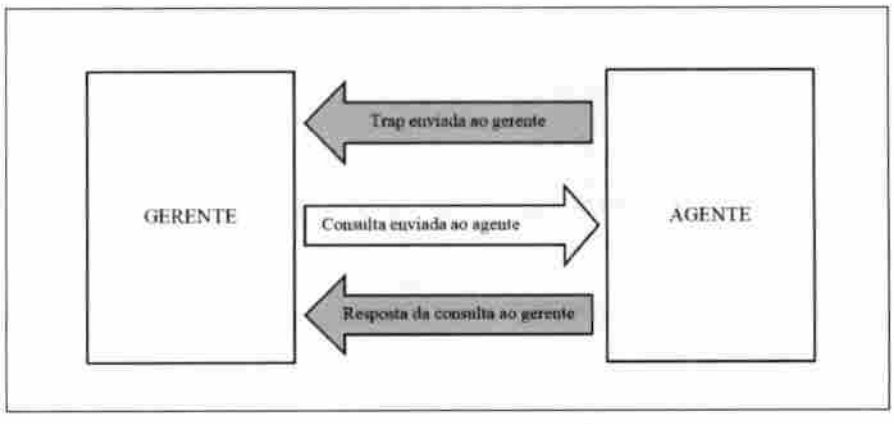


Figura 5 – Relacionamento Gerente e Agente (Douglas e Schmidt, 2005)

De acordo com a Figura a comunicação entre gerente e agente ocorre de duas formas. Uma delas é uma forma interativa de comunicação baseada em consulta e resposta, e a outra consiste em uma notificação do agente ao gerente (*trap*) enviada em virtude de alguma ocorrência (Mauro e Schmidt, 2005).

O funcionamento acima é descrito de forma mais detalhada por Stallings (1999) ao afirmar que as informações entre agentes e gerentes são repassadas por meio de duas técnicas: *polling* (consulta, apuração ou pesquisa) e *event-reporting* (relatório de evento). A primeira é uma consulta, pesquisa ou apuração (*poll*) do tipo *request-response* com as respostas contendo um ou mais dados. A segunda técnica consiste em uma iniciativa do agente, quando este envia ao gerente informações de forma periódica ou baseada em critérios específicos, com tais critérios estabelecidos pelo gerente. Agentes também podem enviar relatórios na ocorrência de eventos significativos, tais como uma alteração de estado ou ocorrência de falhas.

O programa agente pode ser executado em roteadores, *switches*, impressoras ou mesmo servidores de arquivos, de páginas web, ou outros. O referido programa mantém as informações de gerência em um banco de dados cujas informações são armazenadas pelo gerente (Forouzan, 2008). Através dos dados lidos o gerente confere as variáveis de desempenho para avaliar anomalias como congestionamentos ou outros tipos de falhas na rede.

Kaushik (2010) complementa que os dados podem ser coletados de diversas formas através das operações do protocolo como *GetRequest*, *SetRequest*, *GetNextRequest*, *ResponseTrap* e outras, sendo que o gerente de monitoramento pode efetuar uma solicitação do tipo *get* ou ainda ajustar um critério ou limiares (*threshold*) para o envio de uma informação do tipo *trap* para o gerente.

O protocolo SNMP usa serviços do protocolo UDP com as portas 161 e 162, sendo a porta 161 usada pelo servidor ou agente, e a porta 161 pelo cliente ou gerente. Os aplicativos cliente e servidor ficam rodando indefinidamente, para que as mensagens de solicitação e também as do tipo *trap* possam ser trocadas (Forouzan, 2008).

O padrão em estudo foi escolhido inicialmente como solução provisória, uma vez que havia outro protocolo de gerenciamento desenvolvido pela ISO que concorria para ser adotado. Uma vez que o SNMP se consagrou como o padrão de fato, houveram revisões posteriores para melhorias (Kurose, 2010). A versão mais atual é a SNMP v3, com o SNMP original conhecido como SMNPv1.

Uma vez que as versões anteriores tinham como ponto fraco a segurança, na versão mais recente esta característica recebeu reforços com a utilização de recursos como autenticação de mensagens, privacidade e autorização do gerente. A compatibilidade com versões anteriores foi mantida para o suporte a todas as operações definidas anteriormente, com a norma sendo reescrita para tornar a interpretação dos tipos de dados mais precisa (Forouzan, 2008) (Douglas e Schmidt, 2002).

O protocolo SNMP é utilizado atualmente em todas as aplicações de monitoramento de redes, em versões comerciais e livres (Kaushik 2010). Por meio dele diversas informações previstas na MIB podem ser recuperadas, como taxas de transmissão, erros, estados de interfaces, consumo de memória e processamento, dentre outras. Para tal é necessário que existam os dados previstos na MIB, para que sejam recuperadas pelo agente.

2.5 OS REQUISITOS PARA UM SISTEMA DE MONITORAMENTO

Um dos requisitos para a disponibilidade dos serviços é que os sistemas de informação estejam sob constante monitoramento. A indisponibilidade de um recurso pode trazer transtornos para os negócios, além de prejuízos e danos à imagem das empresas (Pedreira, 2015). Diante desse cenário, as instituições investem em sistemas de monitoramento, sejam versões comerciais ou livres.

Uma solução atual de monitoramento deve ser capaz de atender aos requisitos dos ambientes computacionais mais modernos, que requerem rapidez na identificação e solução de falhas e comportamentos anormais, bem como elucidar questões de desempenho. Segundo Prigge (2015) a monitoração é um dos aspectos mais críticos da infraestrutura e no entanto um dos mais negligenciados. Assim, uma avaliação adequada para a escolha da solução pode ser um fator diferencial para momentos posteriores, como a operação, manutenção e retorno ao negócio de uma solução.

Existem diversas soluções atualmente no mercado, e vários critérios podem ser utilizados para a adoção de uma solução. Hernantes, Gallardo e Serrano (2015) definem vários fatores para a decisão, sendo o primeiro deles as funcionalidades que tenham afinidade com os aspectos técnicos e do negócio; o segundo, critérios de implantação e manutenção que estejam em alinhamento com os recursos e capacidade para a equipe de TI; por fim, é necessário ter a noção do impacto positivo da ferramenta para a organização.

Por sua vez, Prigge (2015) menciona 5 aspectos que uma solução de monitoramento deve apresentar:

- Vários colecionadores redundantes: o software para fazer o levantamento de dados ou a sondagem deve ser capaz de ser instalado em vários locais, pela capacidade de redundância e também para possibilitar mais de uma visão de um mesmo elemento;
- Capacidade gráfica: o sistema de monitoramento deve ter um processamento gráfico excelente, capaz de visualizar múltiplos gráficos de forma simultânea, uma vez que isto facilita a correlação de eventos diversos;
- Supressão de eventos facilitada: a solução deve possibilitar a eliminação de eventos conhecidos ou esperados, para evitar que a equipe venha a perder o foco com problemas de falsos positivos ou alarmes causados por eventos de manutenção;
- Múltiplos métodos de coleta de dados: todos as aplicações possuem suporte ao SNMP, ICMP e WMI, mas é desejável também compatibilidade com outras interfaces mais modernas. Outro aspecto importante é a capacidade de consultas SQL;
- Facilidade de Integração e extensão: uma suíte de monitoramento deve apresentar compatibilidade com outras soluções ou ainda possibilitar a integração ou o desenvolvimento de funcionalidades adicionais.

As características descritas se apresentam como premissas essenciais para soluções de monitoramento, mas podem ser complementadas com mais requisitos. Hernantes, Gallardo e Serrano (2015) apresentam também outros aspectos que vão ao encontro dos fundamentos descritos acima:

- Funcionalidade: a ferramenta deve ser capaz de atender a necessidade de diferentes usuários, do nível gerencial ao técnico, como exemplo, a um gerente interessa um relatório de acordo de nível de serviço enquanto a um técnico é mais importante um relatório de falhas de desempenho;
- Interfaces de usuário: embora já bem amadurecidas, a interface gráfica merece atenção, uma vez que os usuários podem demandar funcionalidades mais atuais. É necessário encontrar uma interface web que funcione com diversos clientes, ou ainda capaz de operar em dispositivos móveis caso isto seja necessário pela equipe de TI;
- Alertas, integração com help desk e automação: o objetivo de ferramentas de monitoramento é a resposta aos problemas o mais rápido possível, o que demanda sistemas de alertas por Envio de Mensagens curtas ou SMS (*Short Messages Service*), e-mail, e integração com o sistema de *HelpDesk*;

- Instalação e Manutenção: o processo de instalação deve estar alinhado com políticas corporativas, e a ferramenta deve ser compatível com todos os aspectos do departamento de TI, para que este se utilize de métodos adequados para coletar medidas e dados que apresentem uma avaliação perspicaz;
- Custos: aspectos como custo de implantação e também o custo total de propriedade deve ser considerado.

Os autores citados acima apresentam fundamentos para uma escolha adequada de ferramentas de monitoramento tendo em consideração diversos aspectos. O primeiro apresenta as facilidades como critério de escolha, ao passo que os segundos elegem alguns pontos relacionados à gestão, como custo total de propriedade e atenção a alguns processos de instalação e manutenção. Em ambos os casos, a opção por uma determinada solução deve ser tomada com racionalidade e critérios de retorno sobre o ativo.

A afirmação acima pode ser corroborada por Kaushik (2010), ao afirmar que as indústrias estão investindo um capital considerável para monitorar seus servidores, aplicações e redes, com tal investimento sendo um tratamento proativo para tomar conhecimento dos problemas antes de um incidente e também facilitar o tratamento de eventos de indisponibilidade. Uma vez que monitorar os diversos elementos de uma rede pode tomar tempo considerável dos usuários, as ferramentas de monitoramento podem representar um investimento decisivo para a operação da TI de uma instituição.

2.6 PARÂMETROS PARA MONITORAMENTO

Um software de monitoramento funciona baseado em coleta de dados em rede e em seguida utilizando de tais dados para emissão de alertas ou alguma ação. Tais critérios precisam ser ajustados pelos administradores para um acompanhamento adequado dos serviços.

Em uma rede corporativa os gerentes e administradores devem alinhar o desempenho da rede às necessidades de negócios e garantir a manutenção dos níveis de serviços adequados (Poleto Filho, 2011). Assim, um dos principais critérios para estabelecimento de padrões deve ser baseado nos níveis de serviço estabelecidos. Como exemplo um determinado serviço considerado como de operação crítica deve contar com critérios mais rígidos de avaliação e monitoramento.

Para a definição de parâmetros são estabelecidos valores de limiares ou *thresholds*. Conforme Mohr (2012) a escolha de tais critérios deve ser feita de forma cuidadosa, sob

pena de situações de falso positivo, quando o software poderá concluir que existe um problema sem que ele realmente exista, ou falso negativo, quando o problema é ignorado apesar de realmente existir.

Para a monitoria de serviços, estes têm os indicadores de desempenho e disponibilidade acompanhados pelas equipes de TI. De acordo com Forouzan (2008) um servidor é um "programa capaz de fornecer serviços a outros programas, chamados clientes". Por extensão, os computadores que executam tais programas são chamados servidores.

Conforme Poleto Filho (2011) e Zibiani (2011), para o acompanhamento de desempenho, disponibilidade e continuidade de serviços em servidores são observados os seguintes elementos:

- CPU: Responsável pelo processamento, tem dentre alguns aspectos mais importantes o tempo do processador, comprimento da fila, tempo de usuário e de interrupção;
- Memória: Responsável pelo armazenamento de dados para execução de aplicativos pelo processador, dentre os itens mais importantes estão a memória física disponível, uso de memória virtual e uso de tabelas de paginação;
- Disco: Responsável pelo armazenamento de grandes quantidades de dados, requer para acompanhamento itens como espaço livre, tempo de ociosidade e tempos médios para leitura e gravação;
- Processos: Processos são os programas em execução pelo sistema operacional do equipamento, e tem como principais aspectos o número de identificadores, contagem de threads e processos por byte alocados de forma exclusiva;
- Rede: Responsável pela transmissão e recepção de dados, tem como principais identificadores a quantidade total de bytes por segundo, taxa de erros e comprimento da fila de saída.

Além dos itens citados acima existe também a possibilidade de monitorar as aplicações que rodam no servidor além do sistema operacional. Pode ser acompanhado o consumo de memória de determinado processo, o tempo de processamento, fluxo de entrada e saída de dados, dentre outras informações.

Em sistemas operacionais Windows as informações descritas acima podem ser coletadas através de agentes. Para ampliar as possibilidades de acesso a informações existe também a possibilidade de utilização da Instrumentação para Gerenciamento do Windows ou WMI (Windows Management Instrumentation).

WMI consiste em uma estrutura para o gerenciamento dos dados e operações em ambiente Windows. Baseado em classes e entidades, os diversos objetos previstos podem ser consultados para obter informações detalhadas sobre o hardware ou software instalado no equipamento, sendo o acesso local ou remoto. Através do WMI é possível o desenvolvimento de scripts ou aplicações com o uso da linguagem C++, Microsoft Visual Basic Application ou scripts para coleta de informações de gerenciamento e envio periódico aos servidores (MSDN, 2012).

De acordo com Mohr (2012), uma limitação do WMI será notada caso for necessário o monitoramento de algum atributo que não possua uma classe configurada pela Microsoft.

2.7 O NAGIOS COMO FERRAMENTA DE MONITORAMENTO

Existem no mercado diversas ferramentas para monitoramento no mercado. Todas apresentam diversas funcionalidades e características diversas quando comparadas entre si, o que pode demandar do administrador um trabalho de escolha para escolher a ferramenta mais adequada.

A ferramenta de monitoramento mais popular é o NAGIOS. Trata-se de uma solução de código livre *open source* capaz de monitorar serviços de rede, permitindo às organizações identificar e resolver problemas de infraestrutura de TI em tempo hábil, impedindo que os incidentes venham afetar os processos de negócio. Em caso de falhas Nagios pode alertar as equipes responsáveis pelo serviço de TI (Kaushik, 2010), (Nagios, B., 2017). A funcionalidade de envio de alertas pode contribuir com a gestão proativa dos recursos de rede, servidores e seus serviços e telecomunicações.

Nagios é uma solução disponível há muitos anos no mercado. Em 1999 o administrador de redes Ethan Galstad criou o aplicativo que permite às equipes acompanhar o funcionamento das redes e seus diversos componentes. No início a ferramenta se chamava *NetSaint*, e vem se desenvolvendo até a atualidade com a colaboração da comunidade de software livre se desenvolveu até os dias atuais (Oliveira 2014).

Atualmente Nagios está disponível em duas versões, Nagios Core e Nagios XI, sendo a primeira a versão gratuita e a outra a comercial, com custos para aquisição. A opção Nagios Core não conta com diversos recursos da opção XI, a qual dispõe de uma interface gráfica melhorada em comparação com a primeira, mais pobre. Outras diferenças dizem respeito aos recursos de configuração e customização, escalabilidade e extensibilidade, além dos

contratos de suporte em favor da opção comercial (Hernantes; Gallardo; Serrano, 2015), (Nagios, X., 2017). A interface gráfica limitada do Nagios Core pode ser melhorada com a instalação de plug-ins, uma vez que se trata de solução do tipo *open source*, onde os usuários podem customizar e desenvolver suas soluções.

A alternativa comercial apresenta duas opções, Nagios XI Standard e Nagios XI Enterprise, com diferenças baseadas principalmente no oferecimento de recursos de configuração em larga escala, capacidade de planejamento (*capacity planning*), previsões e relatórios agendados por parte da última versão. Existe, ainda, uma opção gratuita e sem restrição de monitoração de serviços, porém limitada a sete hosts (nós). (Nagios, X., 2017). As diversas modalidades apresentadas permitem às empresas escolher aquela que se adapta melhor a sua capacidade, além de poder optar pela versão gratuita.

Sobre as versões de Nagios e suas referências, no Centro de Informática da Universidade de Brasília está em utilização a versão Nagios Core. Assim, para fins de referência neste trabalho sempre que se utilizar o termo Nagios este estará se referindo ao Nagios Core.

A solução é desenvolvida em linguagem C e tem como característica a instalação facilitada, embora os ajustes dos arquivos de configuração para testes e execução apresentem uma curva de aprendizagem íngreme por parte das equipes de implantação. Tais dificuldades podem ser superadas pela ampla e ativa comunidade de apoio, o que facilita o suporte para implantação e a solução de problemas, bem como o desenvolvimento e aperfeiçoamento de *plug-ins*. (Kaushik, 2010), (Hernantes; Gallardo; Serrano 2015).

Os *plug-ins* podem ser utilizados para resolver algumas limitações da ferramenta, como dificuldades de configuração e proporcionam também melhoramentos na interface gráfica deficiente (Hernantes; Gallardo; Serrano 2015). Existem muitos *plug-ins* desenvolvidos pela comunidade.

Ainda sobre os *plug-ins*, conforme a página oficial de Nagios, cabe uma explicação adicional:

> Ao contrário de muitas outras ferramentas de monitoramento, Nagios não inclui nenhum mecanismo interno para checagem do status de hosts e serviços na rede, ao invés disso, Nagios se baseia em programas externos (chamados plug-ins) para fazer todo o trabalho sujo. (Nagios, P., 2017, tradução nossa).

Conforme a citação acima, Nagios funciona baseado em *plug-ins*, os quais são programas compilados executáveis ou *scripts* em *Perl*, *Shell Scripts* ou outros, que fazem a tarefa de checar o estado de um *host* ou serviço, e com as saídas ou informações originadas ele pode avaliar a situação dos elementos monitorados na rede. A Figura 6 mostra o relacionamento do *plug-in* com o Nagios:

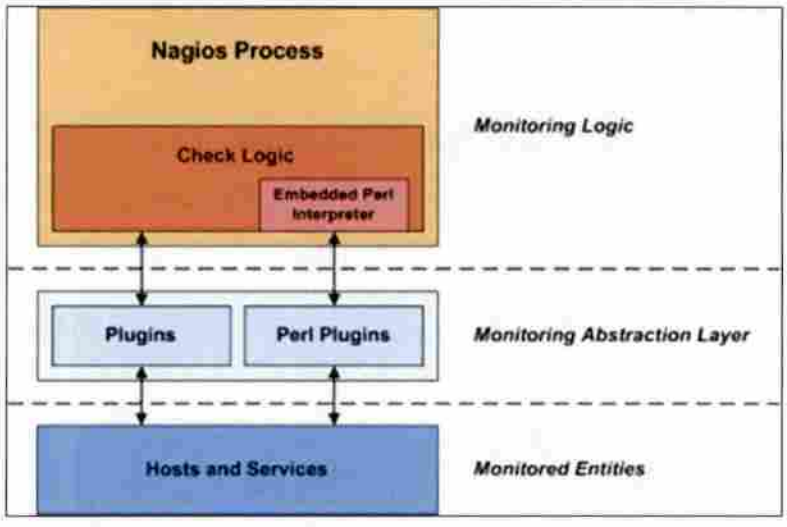


Figura 6 – Relacionamento Entre *Plug-in* e NAGIOS (Nagios P., 2017)

De acordo com a Figura, o plug-in se apresenta como uma camada de abstração (*Monitoring Abstraction Layer*) entre a lógica de monitoramento (*Monitoring Logic*) que está presente no *daemon* Nagios e os serviços e hosts que estão sendo monitorados, ou entidades monitoradas (*Monitored Entities*). (Nagios, P., 2017). Dessa forma, torna-se possível desenvolver plug-ins customizados para monitorar o que for necessário. Como exemplo pode-se acompanhar estatísticas de tráfego de redes, taxas de erros, a temperatura de uma sala em um datacenter, a voltagem de uma CPU e outros parâmetros.

Existem plug-ins disponíveis atualmente para monitorar serviços como HTTP, FTP, Carga de uso de CPU, uso de disco e de memória. Estão disponíveis em diversas plataformas como Unix, Linux, Windows e Netware, além de dispositivos como roteadores e switches. Os plug-ins podem ser obtidos na página oficial ou ainda na internet, por meio das comunidades de suporte ao Nagios.

Outra utilização de plug-ins é a possibilidade de personalizar as notificações para os usuários quando da ocorrência de eventos. Tais notificações podem ser enviadas na forma de e-mails, mensagens de SMS, alarmes sonoros etc. (Pessoa, 2010)

De acordo com Pedreira (2015) a ferramenta pode fazer a monitoria de serviços públicos ou privados. Os primeiros consistem em aplicações baseadas em protocolos que são acessados através da rede diretamente pelo Nagios. Como exemplo temos o Ping, SSH, POP3, IMAP e outros. O monitoramento pode ser feito sem precisar de recursos especiais, apenas com a configuração dos plug-ins apropriados. Para o segundo caso, de serviços privados, é necessária a utilização de agentes.

Agentes são programas instalados no equipamento a ser monitorado com a função de coletar informações específicas do equipamento como carga da CPU, uso de memória, disco, dentre outras informações. Existem agentes disponíveis para Windows e Unix/Linux.

NAGIOS pode reagir a alterações de estado dos itens monitorados de acordo com parâmetros configurados previamente. Tais parâmetros são chamados limiares de alerta ou thresholds, e são utilizados para comparação de valores ao longo do tempo. A escolha de tais valores deve ser feira com critérios objetivos com a intenção de se evitar avaliações indevidas (Mohr, 2012). Com base em um determinado threshold a aplicação reage enviando mensagens de e-mail ou SMS, desabilitando interfaces ou ainda efetuando notificações em tela.

Para complementar o funcionamento da ferramenta existe uma interface chamada *Dashboard*. Consiste em um painel para acompanhamento em tela dos elementos monitorados e a gestão dos alertas recebidos. É necessário também que exista uma separação dos elementos em estado normal ou não, para possibilitar clareza no acompanhamento dos recursos e consequente facilidade na tomada de decisões. (Mohr, 2012). A Figura 7 apresenta um exemplo de *Dashboard*:

Figura 7 – Exemplo de *Dashboard* de NAGIOS (Nagios B., 2017)

A Figura 7 apresenta o *Dashboard* de Nagios com a opção de exibir em tela os serviços classificados por host. Similar a ela outros ajustes podem ser configurados pelo usuário como classificação por serviços, agrupamentos de determinadas categorias de equipamentos e um grande número de configurações disponíveis.

3 APLICAÇÃO PRÁTICA – ESTUDO DE CASO E RESULTADOS

3.1 PESQUISA DE OPINIÃO

Com a intenção de sondar as opiniões dos integrantes do CPD sobre a importância do tema monitoramento de sistemas foi realizado uma pesquisa entre os colaboradores.

A pesquisa do tipo qualitativa e quantitativa consistiu em um questionário de 22 perguntas, sendo as quatro primeiras questões sobre o perfil dos entrevistados (questões 01 a 04) e as demais relacionadas ao tema indisponibilidade de serviços (questões 05 a 11) e monitoramento de sistemas (questões 12 a 22). Foram utilizadas questões fechadas do tipo binárias (sim ou não) e múltipla escolha, além de questões abertas. Não foram utilizadas questões com preenchimento de resposta obrigatório.

A pesquisa foi realizada por meio de questionário elaborado pela aplicação Google Formulários (*Google Forms*). O link para as perguntas foi enviado por e-mail aos participantes totalizando 126 convites enviados. Desses, 55 responderam à pesquisa, em um total de 43,65%.

A seguir são apresentadas as tabulações dos dados.

3.1.1 Perguntas Sobre o Perfil dos Entrevistados

As quatro primeiras perguntas foram feitas com a intenção de se obter informações sobre o perfil dos entrevistados: foi perguntado sobre a escolaridade, o vínculo profissional com a instituição, a área de atuação no CPD e se exerciam algum cargo de chefia, coordenação ou liderança.

Para a questão 1, foi perguntado aos participantes sobre o grau de escolaridade:

Tabela 3 – Questão 1 – Grau de Escolaridade (Do Autor, 2017)

Grau de Escolaridade	**Quantidade**	**%**
Doutorado	1	1,82%
Ensino Superior	16	29,09%
Especialização	29	52,73%
Mestrado	9	16,36%
Total Geral	**55**	**100,00%**

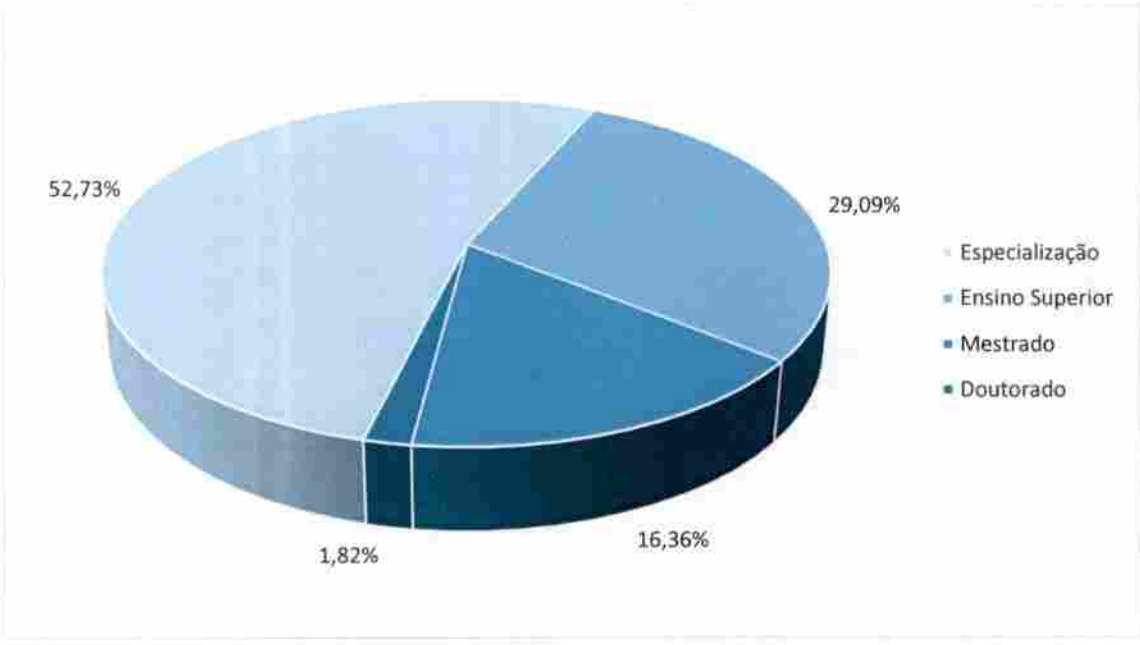


Figura 8 – Questão 1 – Grau de Escolaridade (Do Autor, 2017)

Para a questão 2, foi perguntado aos participantes o vínculo com a instituição.

Tabela 4 – Questão 2 – Vínculo com a Instituição (Do Autor, 2017)

Vínculo Institucional	**Quantidade**	**%**
Estagiário	1	1,82%
Terceirizado	2	3,64%
Servidor	52	94,55%
Total Geral	**55**	**100,00%**

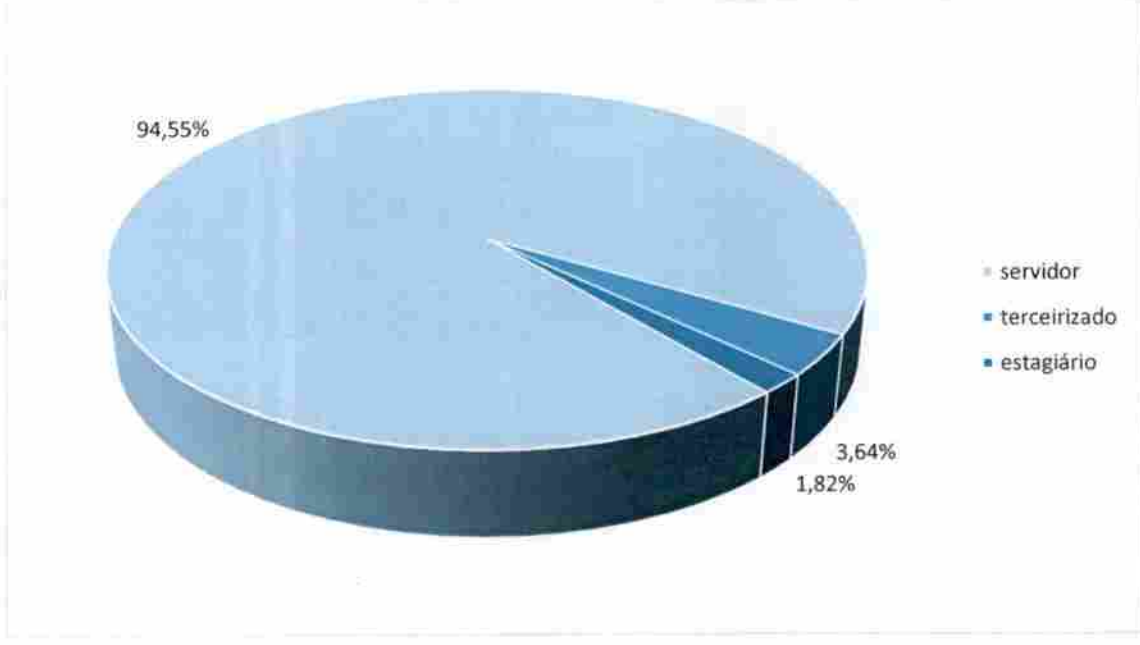


Figura 9 – Questão 2 – Vínculo com a Instituição (Do Autor, 2017)

Para a questão 3, foi perguntado aos participantes a área de atuação no CPD

Tabela 5 – Questão 3 – Área de Atuação (Do Autor, 2017)

Área de Atuação	**Área**	**%**
Apoio à Governança	1	1,82%
Administração	10	18,18%
Banco de Dados	3	5,45%
Desenvolvimento	13	23,64%
HelpDesk	2	3,64%
Infraestrutura de Redes	4	7,27%
NOC	1	1,82%
Operação de Sistemas	1	1,82%
Redes	7	12,73%
Segurança	7	12,73%
Serviço Redes e Suporte	1	1,82%
Suporte Avançado	5	9,09%
Total Geral	**55**	**100,00%**

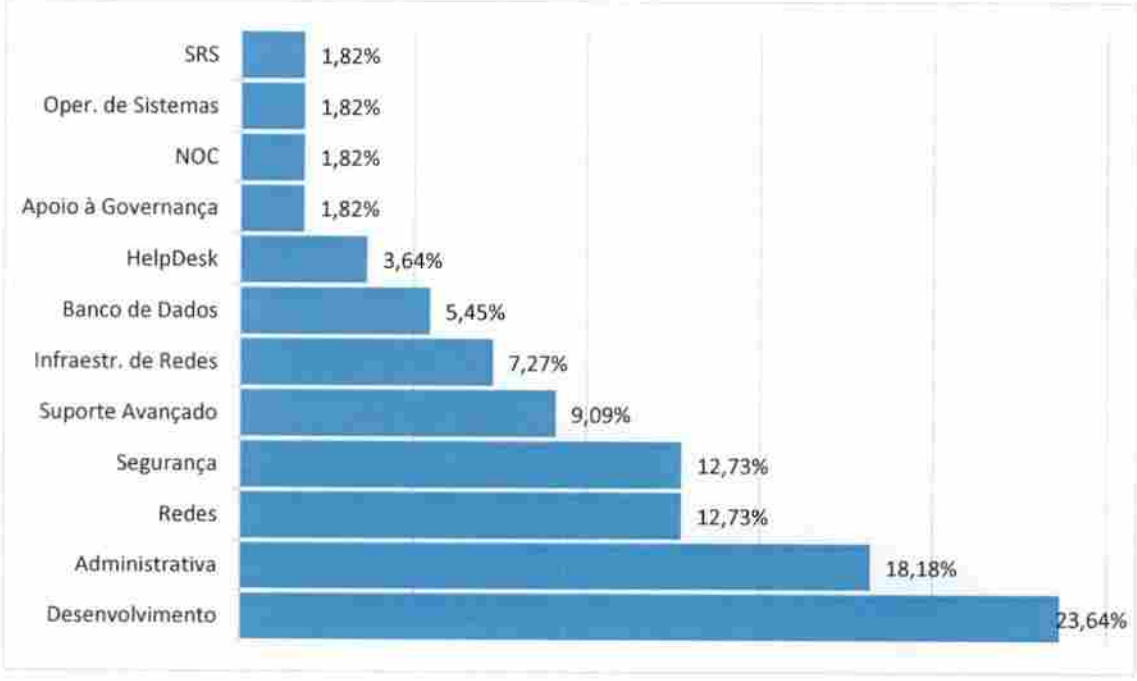


Figura 10 – Questão 3 – Área de Atuação (Do Autor, 2017)

Para a questão 4, foi perguntado aos participantes se exerciam algum cargo de chefia ou liderança:

Tabela 6 – Questão 4 – Cargos de Chefia (Do Autor, 2017)

Cargos de Chefia	Quantidade	%
Não	48	87,27%
Sim	7	12,73%
Total Geral	**55**	**100,00%**

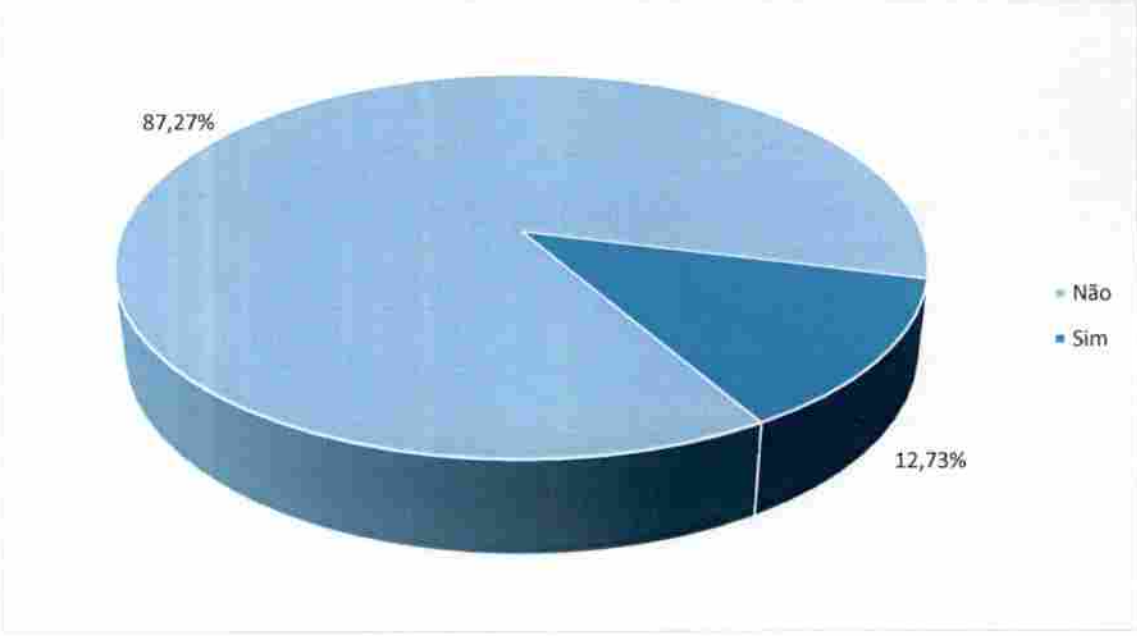


Figura 11 – Questão 4 – Cargos de Chefia (Do Autor, 2017)

A partir dos gráficos mostrados nas Figuras 8 a 11, pode-se obter um perfil dos entrevistados. De acordo com a Figura 8 pode-se constatar que a maior parte deles possui especialização, em 52,73%, seguidos de colaboradores com graduação, em 29,09%, mestrado com 16,36% e doutorado com 1,82%. Em relação a Figura 9, a maior parte dos entrevistados ocupa cargo de servidor com 94,55%, sendo 3,64% terceirizados e 1,82% estagiários. A distribuição por área de atuação é mostrada na Figura 10 com a maior parte dos entrevistados na área de desenvolvimento, com 23,64%, seguida da área administrativa com 18,18% e áreas de redes e segurança com 12,73% cada. Por fim, a Figura 11 aponta que 12,73% dos entrevistados possui cargo de chefia ou liderança, sendo os demais 82,72% colaboradores sem função administrativa.

3.1.2 Perguntas Sobre a Opinião dos Entrevistados - Indisponibilidade

As demais perguntas foram feitas para se obter perguntas sobre a opinião do entrevistado sobre a disponibilidade e sobre o monitoramento de sistemas.

Foi apresentado aos usuários uma definição do termo indisponibilidade seguida das perguntas relacionadas. A intenção foi obter informações da percepção dos usuários sobre os eventos, frequência, como eles tomam ciência de tais acontecimentos, a comunicação dos responsáveis a respeito da situação e o nível de impacto causado nas atividades do usuário.

Para a questão 5, foi perguntado aos usuários se eles têm conhecimento de eventos de indisponibilidade nos sistemas da UnB

Tabela 7 – Questão 5 – Ciência de Eventos de Indisponibilidade (Do Autor, 2017)

Ciência de Eventos de Indisponibilidade	**Quantidade**	**%**
Sim	48	87,27%
Não	7	12,73%
Total Geral	**55**	**100,00%**

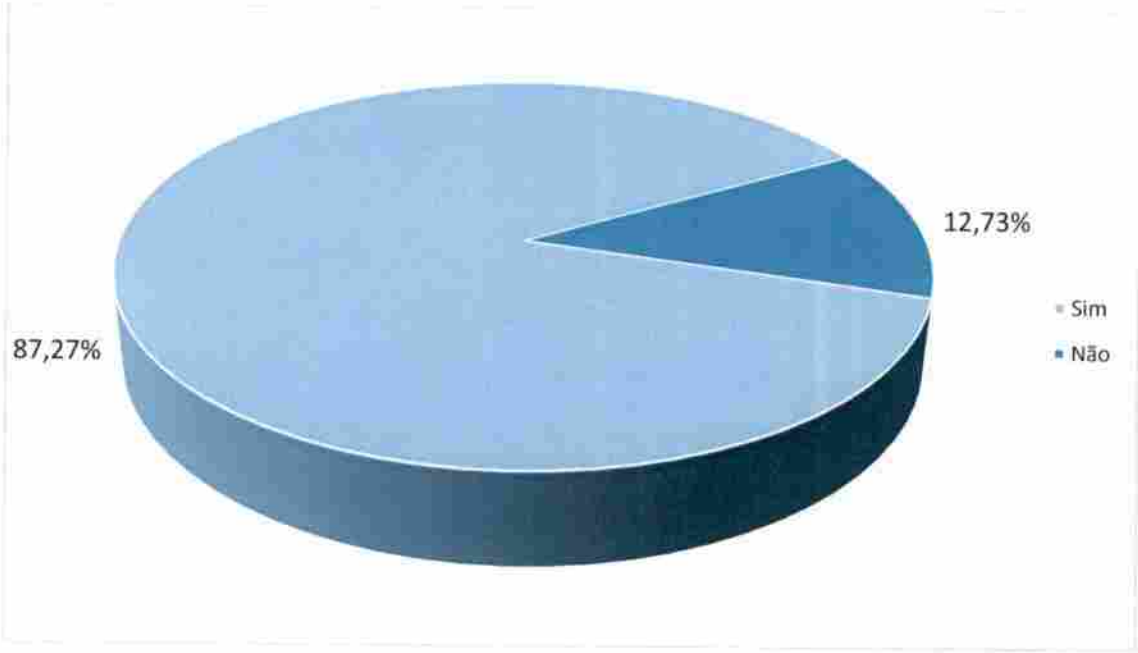


Figura 12 – Questão 5 – Ciência de Eventos de Indisponibilidade (Do Autor, 2017)

Conforme a Figura 12, 87,27% dos entrevistados tem conhecimento da ocorrência de eventos de indisponibilidade no centro.

Para a pergunta 6, foi perguntado aos participantes a frequência dos eventos percebidos:

Tabela 8 – Questão 6 – Frequência de Eventos (Do Autor, 2017)

Frequência	Diária	Mensal	Quinzenal	Semanal	**Total**
Quantidade	6	18	9	15	**48**
%	12,50%	37,50%	18,75%	31,25%	**100,00%**

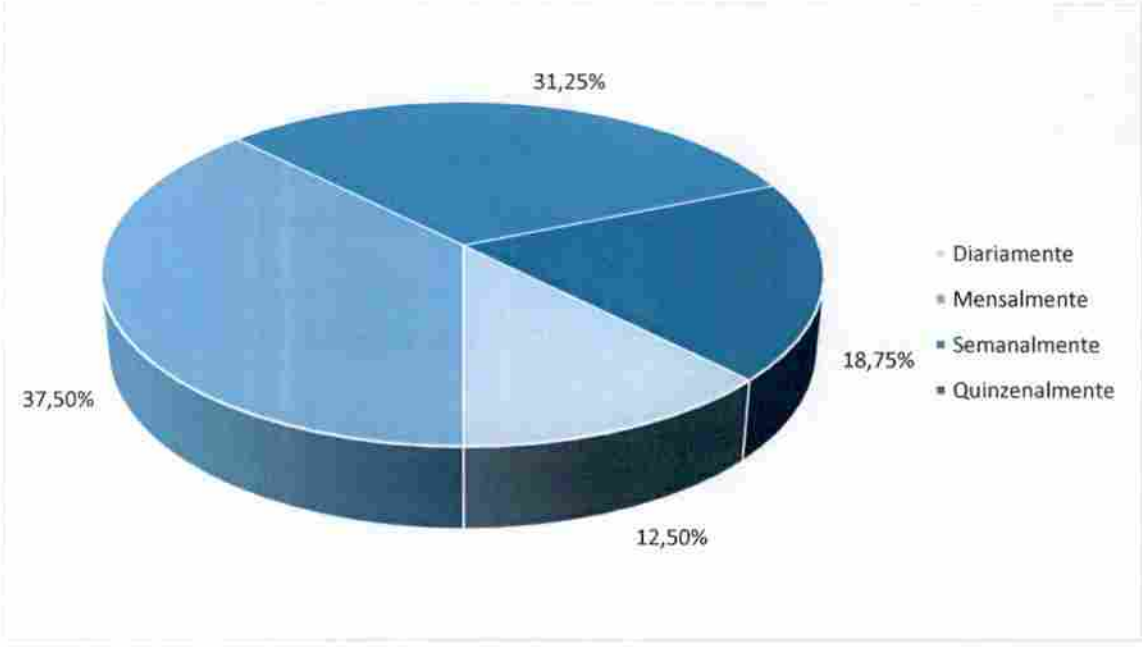


Figura 13 – Questão 6 – Frequência de Eventos (Do Autor, 2017)

De acordo com a Figura 13, 37,5% informou que os eventos de indisponibilidade ocorrem mensalmente, 31.25% afirmou ocorrerem semanalmente, 18,75% afirmaram a ocorrência quinzenal, e 12,5% afirmaram que os eventos ocorrem com frequência diária.

Para a pergunta 7 os participantes foram questionados por quais meios eles tomam ciência dos eventos:

Tabela 9 – Questão 7 – Meios de Ciência de Eventos (Do Autor, 2017)

Meios	**Próprios**	**Por Alguém**	**Comunicados**	**Outros**	**Total**
Quantidade	13	12	17	6	48
%	27,08%	25,00%	35,42%	12,50%	100,00%

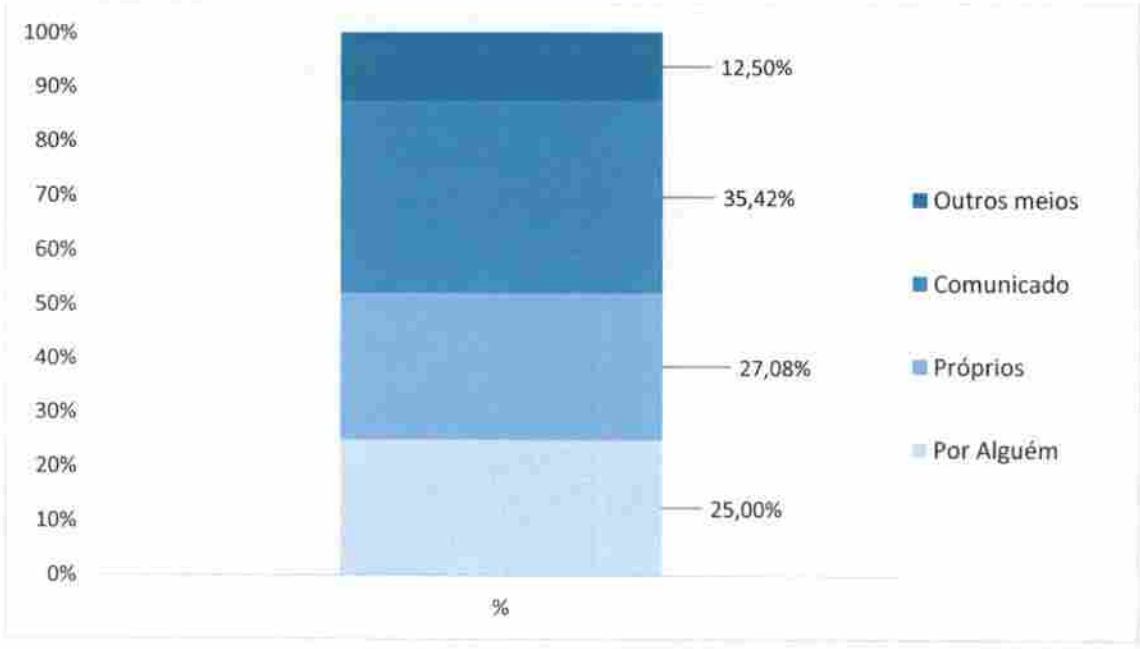


Figura 14 – Questão 7 – Meios de Ciência de Eventos (Do Autor, 2017)

De acordo com a Figura 14, 35,42% informam que tomam ciência dos eventos de indisponibilidade por meio de comunicados, 27,08% toma conhecimento das ocorrências por meios próprios, 25% por meio de outras pessoas e 12,50% por outros meios.

Para a pergunta 8 foi perguntado se o usuário tinha ciência da causa dos eventos. Nesta questão o entrevistado pode escolher mais de uma opção.

Tabela 10 – Questão 8 – Causa de Eventos (Do Autor, 2017)

Causas	**Quantidade**
Falhas de Energia	44
Falhas nos servidores	8
Falhas de Telecomunicação	6
Eventos de Manutenção	33
Outros	4

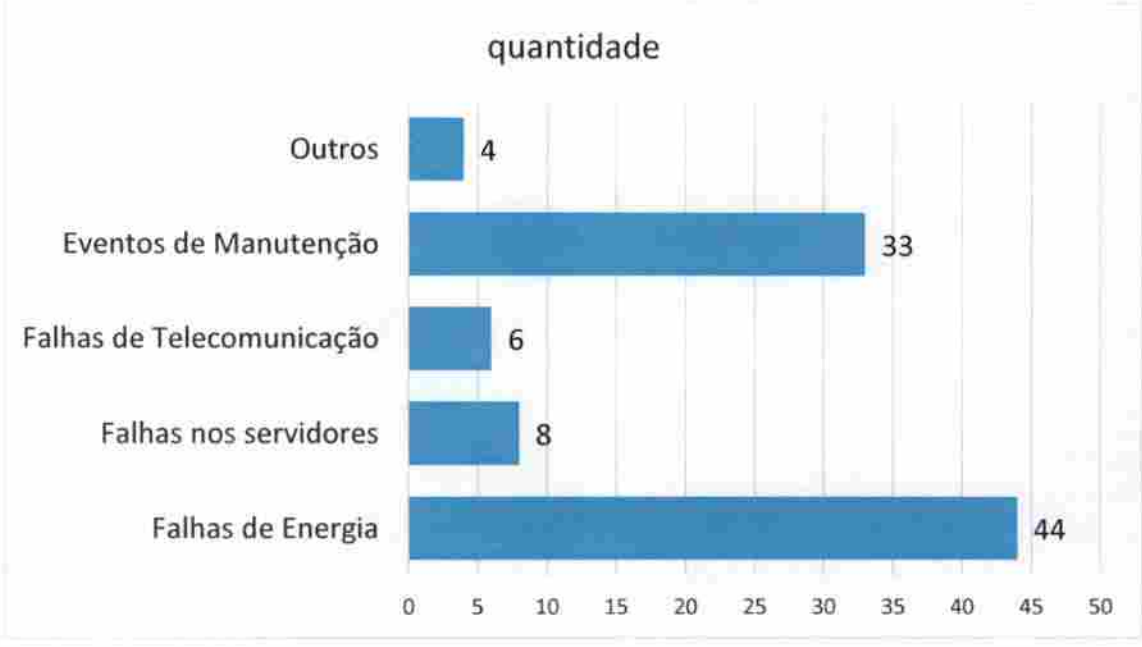


Figura 15 – Questão 8 – Causa de Eventos (Do Autor, 2017)

Conforme a Figura 15, as falhas de energia foram assinaladas com a maior causa dos eventos, com 44 pontos, seguida de eventos de manutenção, com 33 pontos, falhas nos servidores com 8 pontos, falhas de telecomunicação com 6 pontos, e outros com 4 pontos.

Para a questão 9 os usuários foram perguntados se algum comunicado era recebido das equipes de suporte durante a ocorrência dos eventos. Para a questão 10, os usuários entrevistados foram perguntados se as equipes de suporte forneciam uma previsão para o retorno dos sistemas ou resolução do problema. As duas perguntas foram tabuladas de forma a detalhar a resposta:

Tabela 11 – Questão 9 e 10 – Comunicado e Resposta (Do Autor, 2017)

Tipo de comunicado	**Quant.**	**%**	**Quant.**	**%**
NÃO RECEBO	10	20,83%		
Com previsão			2	4,17%
Sem previsão			8	16,67%
SIM, DE FORMA VERBAL	14	29,17%		
Com previsão			11	22,92%
Sem previsão			3	6,25%
SIM, VIA E-MAIL	24	50,00%		
Com previsão			20	41,67%
Sem previsão			4	8,33%
Total Geral	**48**	**100,00%**	**48**	**100,00%**

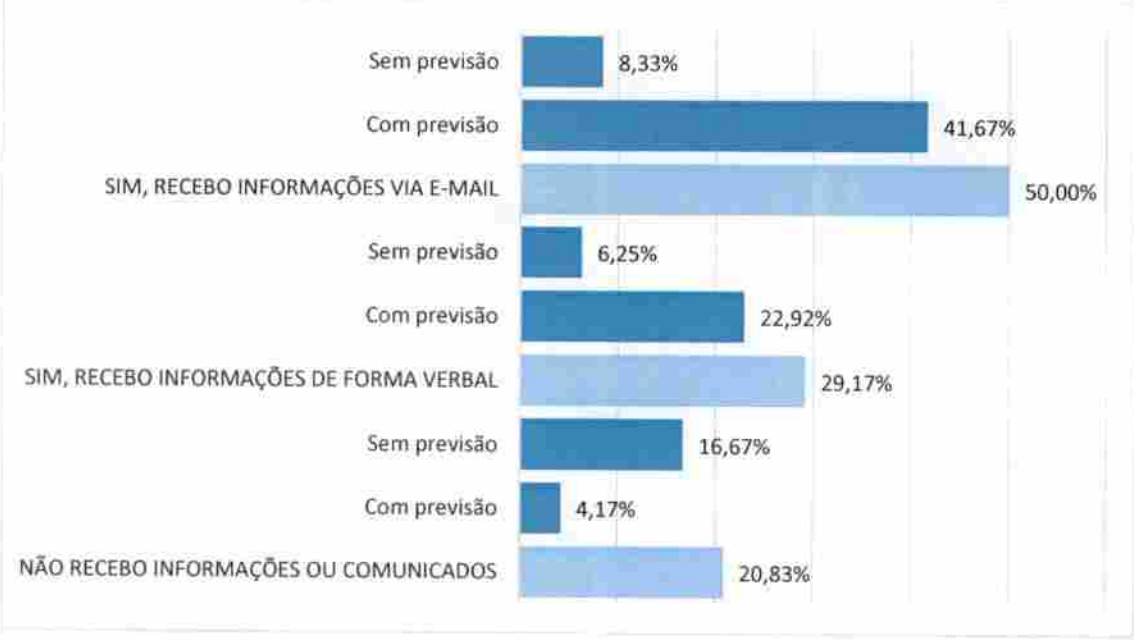


Figura 16 – Questão 9 e 10 – Comunicado e Resposta (Do Autor, 2017)

Pela Figura 16, a maior parte dos comunicados de indisponibilidade são recebidos por E-mail, com 50%, seguidos dos comunicados de forma verbal, com 29,17%, enquanto 20,83 dos entrevistados que responderam não recebem comunicados. Aqueles que recebem os informes via e-mail recebem uma previsão de retorno dos serviços em 41,67% dos comunicados. Ainda em respeito a este aspecto, os comunicados verbais ou não sempre informam uma estimativa de restabelecimento.

Um dado que merece atenção é associado à resposta não, uma vez que 4,17% dos entrevistados que responderam à pergunta informaram receber previsões de retorno, mesmo sem receber comunicados.

A pergunta 11 perguntou aos entrevistados se os eventos causavam impacto na unidade de trabalho correspondente:

Tabela 12 – Questão 11 – Impacto dos Eventos (Do Autor, 2017)

Impacto	**Quantidade**	**%**
Muito Baixo	0	0,00%
Baixo	8	16,67%
Moderado	21	43,75%
Alto	15	31,25%
Muito Alto	4	8,33%
Total	**48**	**100,00%**

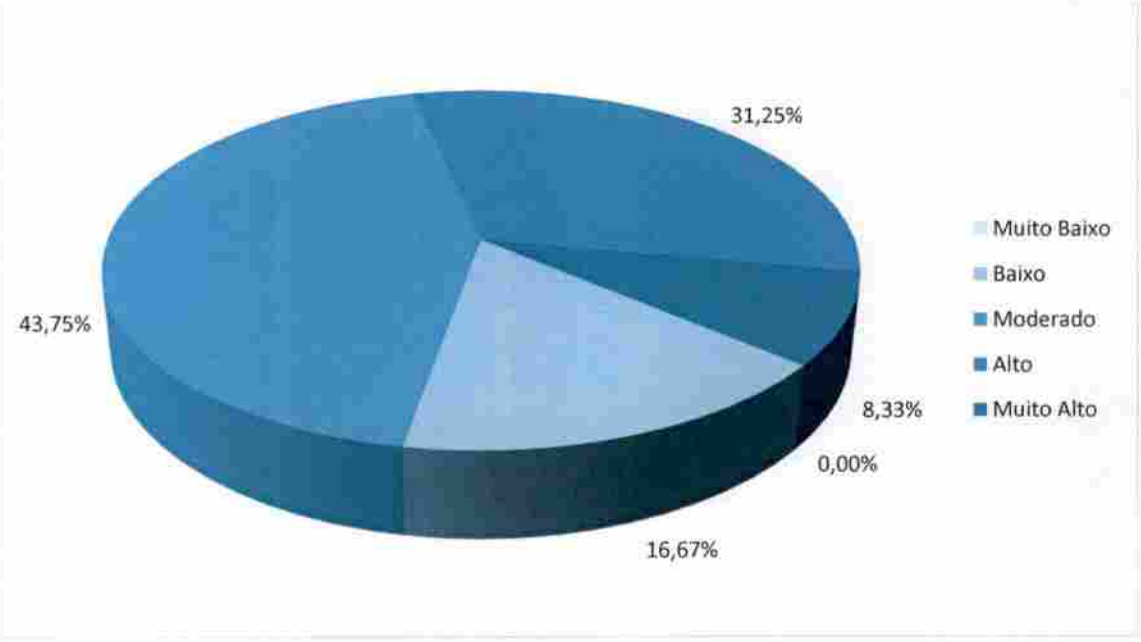


Figura 17 – Questão 11 – Impacto dos Eventos (Do Autor, 2017)

De acordo com a Figura 17 é observado que 43,75% dos entrevistados classificam o impacto causado pelos eventos de indisponibilidade como moderado, seguido das classificações alta e baixa com 31,25% e 16,67% respectivamente. Somente 8,33% dos usuários classificam os impactos como muito alto.

3.1.3 Perguntas Sobre a Opinião dos Entrevistados - Monitoramento

A terceira parte do questionário sondou as opiniões dos usuários sobre o monitoramento de sistemas. Foi apresentado um conceito para o termo seguido das perguntas relacionadas.

A pergunta 12 indagou aos entrevistados se tinham noção ou conhecimento sobre o monitoramento de sistemas. A questão 13 perguntou se eles tinham ciência de algum serviço, sistema ou ferramenta de monitoramento utilizada no CPD. A questão 14 perguntou ainda se eles consideravam o monitoramento de sistemas importante para a sua unidade de trabalho:

Tabela 13 – Questões 12 a 14 – Conhecimento x Uso x Importância (Do Autor, 2017)

Perguntas	**Conhecimento S. Monitoramento**		**Uso no CPD**		**Importância Para a Unidade**	
Sim	40	72,73%	38	69,09%	53	96,36%
Não	15	27,27%	17	30,91%	2	3,64%
Total	**55**	**100,00%**	**55**	**100,00%**	**55**	**100,00%**

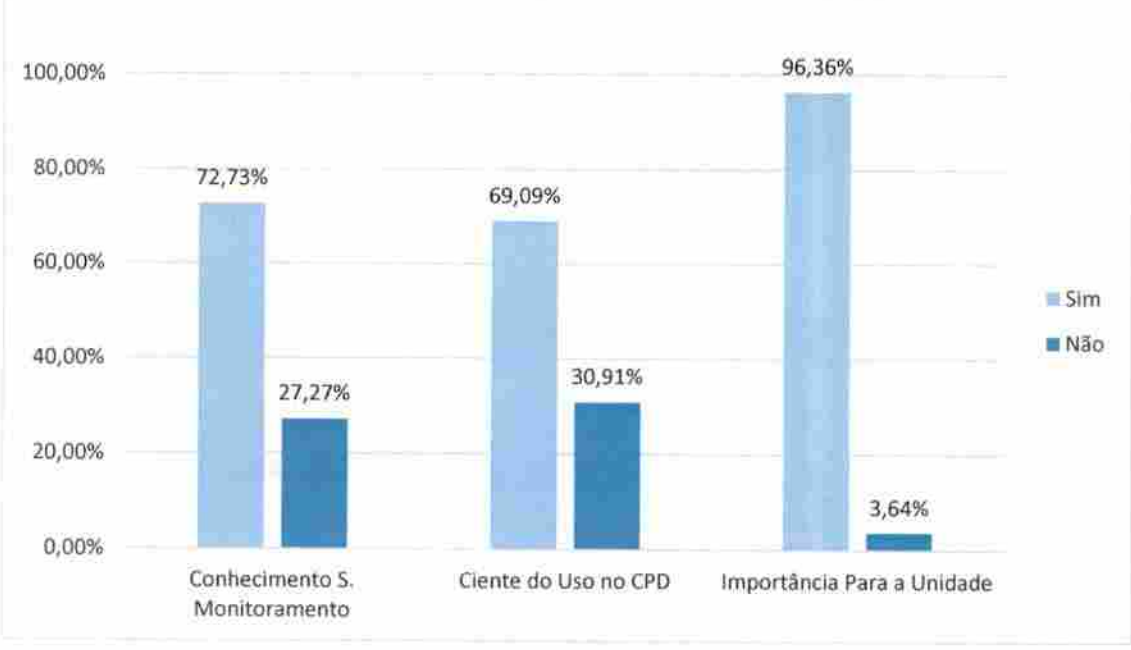


Figura 18 – Questões 12 a 14 – Conhecimento x Uso x Importância (Do Autor, 2017)

Conforme mostra a Figura 18, 72,73% dos entrevistados possuem ciência do monitoramento de sistemas, 69,09% são cientes de seu uso no CPD e 96,36% reconhecem a importância do monitoramento de sistemas para as atividades de sua unidade.

Para a questão 15 foi perguntado aos usuários se o monitoramento de sistemas é importante para as atividades do CPD, e pediu-se também uma justificativa. Esta pergunta foi aberta e contou com 43 respostas dos entrevistados.

Para análise da resposta foi utilizado o *Google Word Cloud Generator*, capaz de criar uma nuvem de palavras a partir de um texto de entrada, onde as palavras com maior relevância surgem em destaque. O resultado das 43 respostas é apresentado na Figura 19:

Figura 19 – Questão 15 – Importância do Monitoramento para o CPD (Do Autor, 2017)

De acordo com a Figura 19, a opinião dos usuários é que o monitoramento é importante para as atividades do CPD. Outras palavras identificadas na imagem complementam a assertiva, como os substantivos dados, disponibilidade, falhas, monitoramento e problemas, e os adjetivos importante e essencial.

Na questão 16 foi perguntado aos usuários se eles se utilizavam de algum serviço de monitoramento em suas unidades de trabalho:

Tabela 14 – Questão 16 – Utilização do Monitoramento (Do Autor, 2017)

Utilização do Serviço de Monitoramento	**Quantidade**	**%**
Não	25	45,45%
Sim	30	54,55%
Total Geral	**55**	**100,00%**

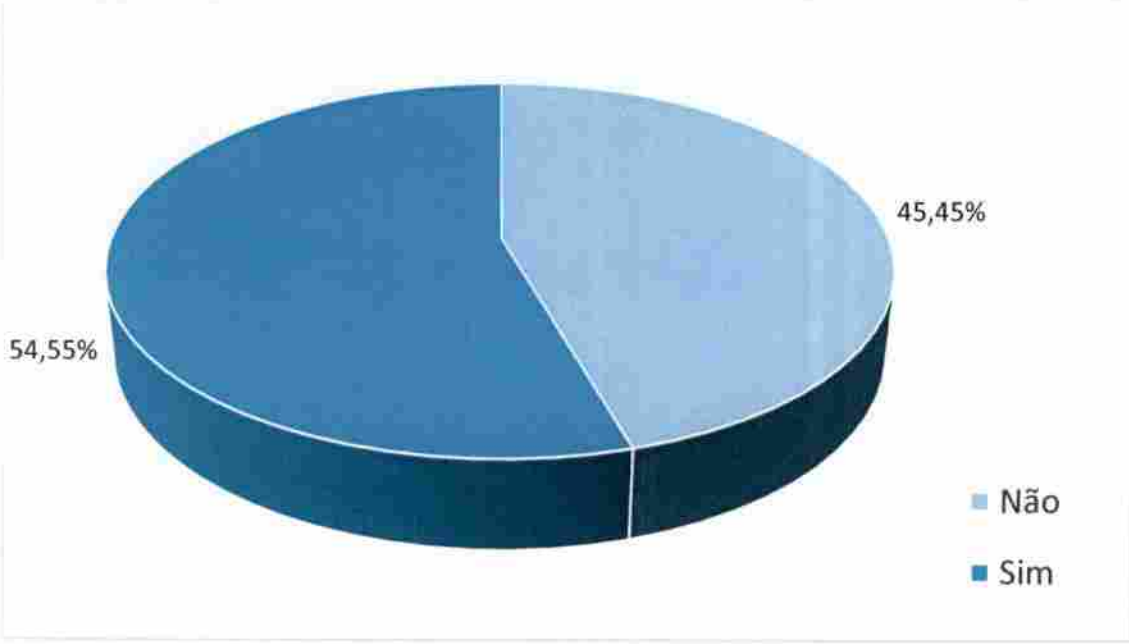


Figura 20 – Questão 16 – Utilização do Monitoramento (Do Autor, 2017)

Conforme a Figura 20 54,55% dos entrevistados utilizam algum tipo de serviço de monitoramento em suas unidades de trabalho.

Na questão 17 foi perguntado aos entrevistados há quanto tempo a unidade utiliza os serviços de monitoramento:

Tabela 15 – Questão 17 – Tempo de Utilização Monitoramento (Do Autor, 2017)

Tempo	**Quantidade**	**%**
Há menos de um mês	1	3,33%
Há menos de três meses	2	6,67%
Há mais de seis meses	0	0,00%
Há mais de um ano	6	20,00%
Há mais de cinco anos	21	70,00%
Total Geral	**30**	**100,00%**

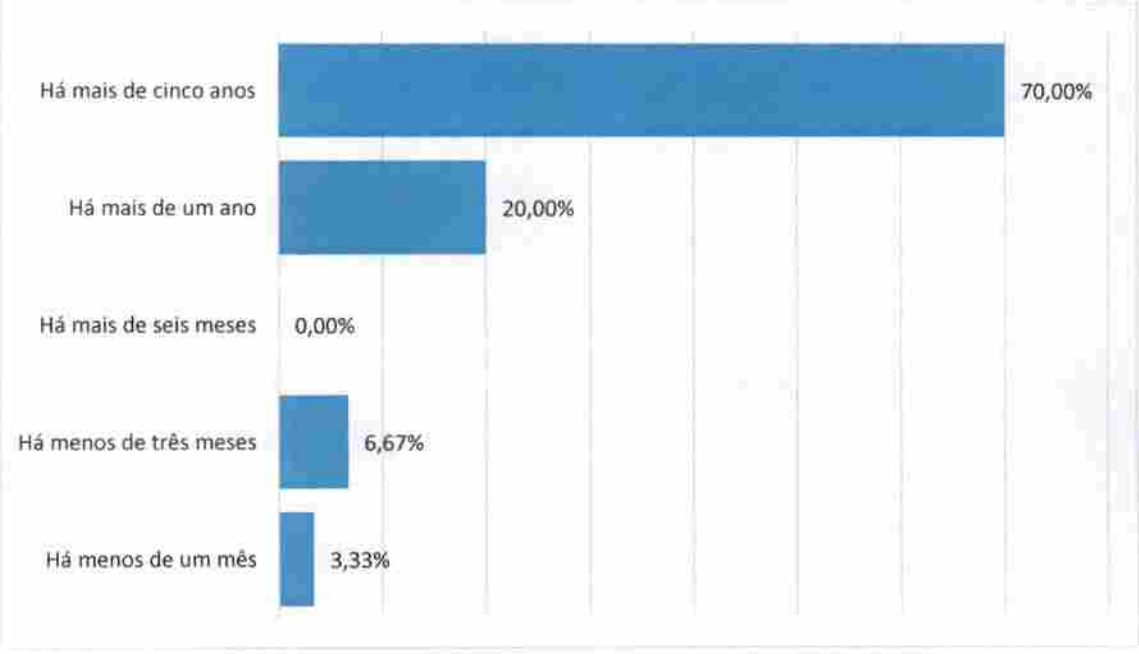


Figura 21 – Questão 17 – Tempo de Utilização Monitoramento (Do Autor, 2017)

De acordo com a Figura 21, dos entrevistados que responderam a esta pergunta 70% utilizam algum serviço de monitoramento em suas unidades há mais de cinco anos, 20% utilizam há mais de um ano, 6,67% Há menos de três meses e 3,33% há menos de um mês.

A questão 18 perguntou aos usuários quais os tipos de recursos são monitorados. Nesta questão, de múltipla escolha, os usuários puderam indicar mais de uma opção:

Tabela 16 – Questão 18 – Recursos Monitorados (Do Autor, 2017)

Recursos	**Quantidade**
Atividade dos Servidores	20
Resposta dos Servidores	16
Infra de Redes	24
Serviços (DLL)	9
Servidores (Aplicação)	17
Servidores (BD)	20
Servidores (e-mail)	18
Servidores infraestrutura (DNS)	17
Servidores WEB	16

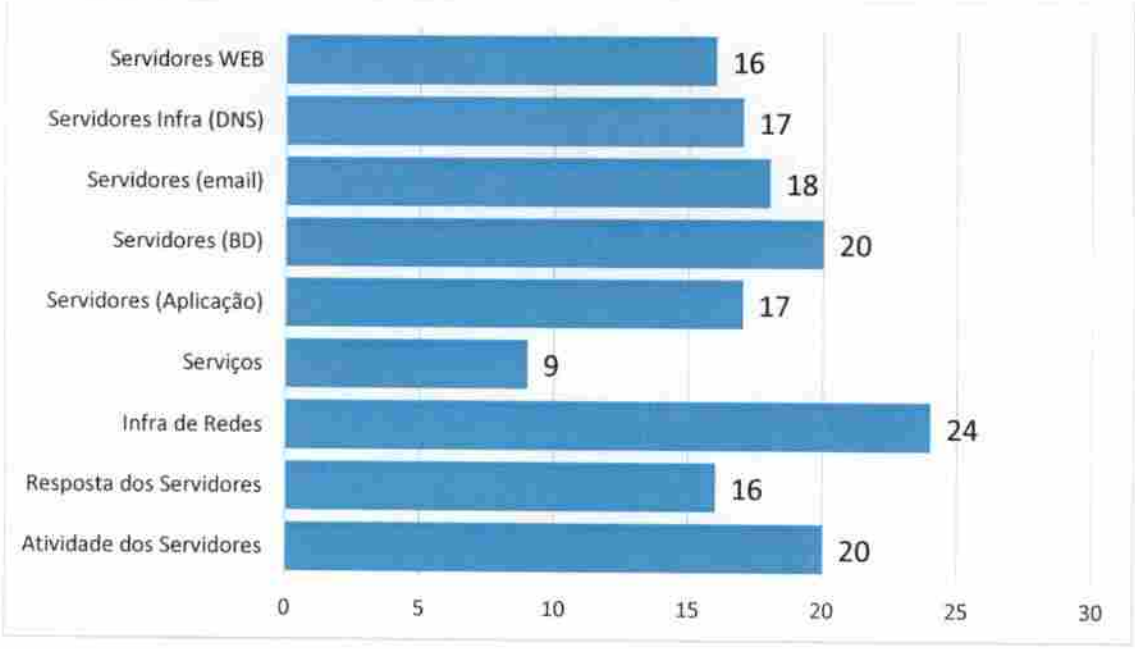


Figura 22 – Questão 18 – Recursos Monitorados (Do Autor, 2017)

Conforme a figura 22, as respostas indicaram que a infraestrutura de redes, servidores de banco de dados e servidores são os itens que mais se utilizam dos recursos de monitoramento, e o monitoramento de serviços em separado a menor utilização. Os servidores Web e de aplicação ficaram em uma classificação intermediária.

A questão 19 perguntou aos entrevistados se havia a intenção de se ampliar o uso dos sistemas de monitoramento em suas unidades:

Tabela 17 – Questão 19 – Intenção de Ampliação (Do Autor, 2017)

Intenção de ampliação	**Quantidade**	**%**
Não	8	27,59%
Sim, em alguns meses	12	41,38%
Sim, em um ano	9	31,03%
Total Geral	**29**	**100,00%**

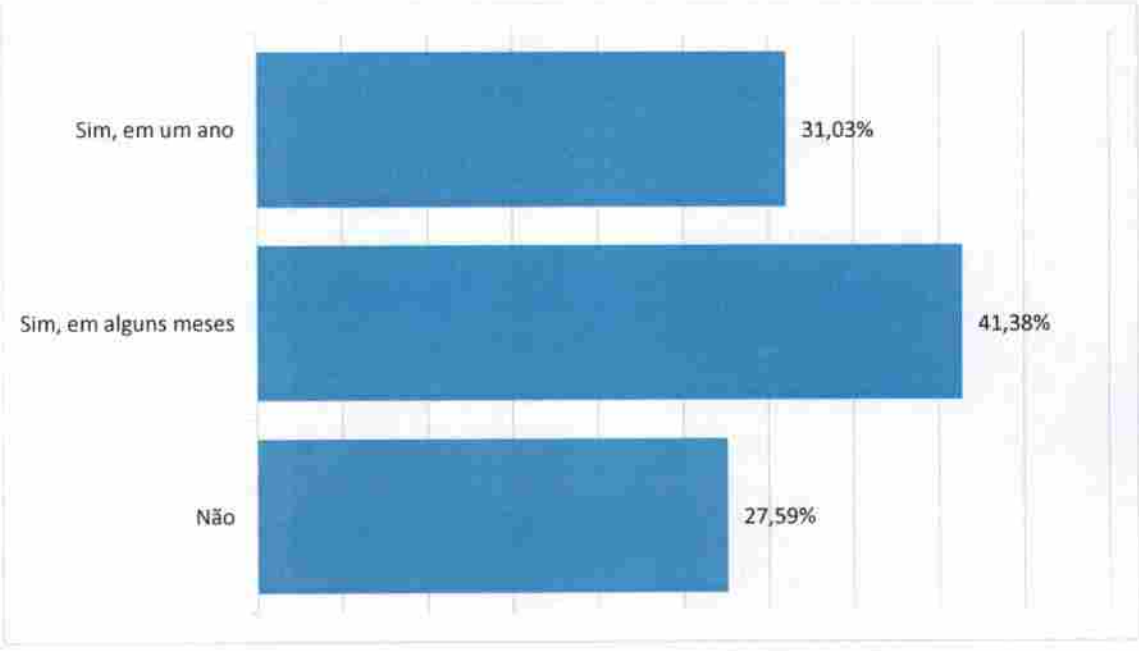


Figura 23 – Questão 19 – Intenção de Ampliação (Do Autor, 2017)

De acordo com a Figura 23, a ampliação de uso dos sistemas de monitoramento é desejada por 41,38% e pretendem fazê-lo em alguns meses, enquanto 31.03% pretendem fazê-lo em um ano.

A questão 20 perguntou aos entrevistados o que deveria ser melhorado no serviço de monitoramento. Foi feita uma pergunta aberta e que obteve respostas de 23 entrevistados

Assim como na questão 15 foi usado o *Google Word Cloud Generator*, que gerou uma imagem a partir das 23 respostas fornecidas, e cujo resultado é mostrado na Figura 24:

Figura 24 – Questão 20 – Sugestões de Melhoria (Do Autor, 2017)

Conforme a Figura 24, a principal palavra é monitoramento, seguida da palavra servidores e ferramentas. Baseado nas respostas do questionário (Apêndice A) e a nuvem de palavras observa-se que os usuários sugerem ampliação para mais servidores e serviços, aquisição de ferramentas mais modernas, treinamento de servidores, envio de avisos para equipes responsáveis, melhorias nos alarmes e alertas, parâmetros e métricas de monitoramento, dentre outras sugestões.

As questões 21 e 22 foram respondidas por 25 entrevistados, uma vez que somente responderam a estas perguntas aqueles que responderam não à questão de número 16 (utilização de serviços de monitoramento).

A questão 21 perguntou aos entrevistados se, mesmo não se utilizando de algum serviço de monitoramento em sua unidade, achavam importante a sua adoção nos processos e rotinas de trabalho. A questão 22 perguntou ainda se, caso pretendesse adotar o monitoramento em sua unidade, em quanto tempo pretendia fazê-lo. As duas perguntas foram tabuladas de forma a detalhar melhor a resposta:

Tabela 18 – Questões 21 e 22 – Intenção de Implantar x Tempo (Do Autor, 2017)

INTENÇÃO EM IMPLANTAR	**Importância**		**Tempo**	
	Quantidade	%	Quantidade	%
NÃO	1	4,00%		
Não			1	4,00%
SIM	18	72,00%		
Dentro de alguns meses			3	12,00%
Dentro de um ano			7	28,00%
Não			8	32,00%
TALVEZ	6	24,00%		
Dentro de alguns meses			1	4,00%
Dentro de um ano			1	4,00%
Não			4	16,00%
TOTAL	**25**	**100,00%**	**25**	**100,00%**

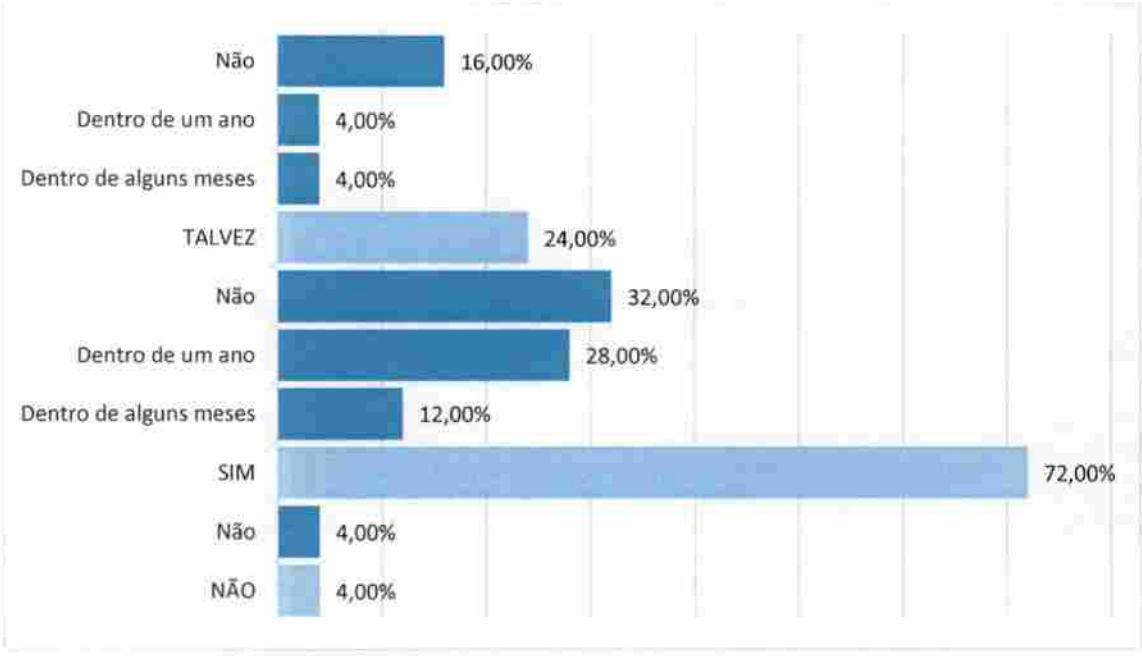


Figura 25 – Questões 21 e 22 – Intenção de Implantar x Tempo (Do Autor, 2017)

De acordo com a figura 25, grande parte dos entrevistados que responderam à pergunta têm interesse em adotar recursos de monitoramento, em um indicativo de 72%. Desses, 28% pretendem adotar dentro de um ano, e 12% dentro de alguns meses.

A pesquisa permitiu conhecer a opinião dos entrevistados em diversos aspectos. Além do perfil dos participantes, foi demonstrado pela opinião da maioria sobre o conhecimento dos recursos de monitoramento, a utilização deles e a sua importância para as unidades e o próprio CPD. A pesquisa mostra também que os usuários pretendem ampliar o uso do monitoramento, e daqueles que não utilizam tem interesse em adotar os recursos a curto prazo. Outro aspecto que se revelou com a pesquisa é a percepção de eventos de indisponibilidade entre os participantes, que apontaram a falta de energia como a maior causa desses eventos. Tal dado talvez não tenha muita correlação com o tema monitoramento, porém pode ensejar algumas medidas ou estudos para explorar a questão.

3.2 LEVANTAMENTO DE PARÂMETROS PARA MONITORAMENTO

Esta parte do trabalho apresenta o levantamento dos recursos monitorados pelo Nagios referentes aos servidores Windows de aplicações instalados no CPD da Universidade de Brasília – UnB, no mês de julho de 2017.

Nos equipamentos vistoriados para o levantamento são mantidas aplicações do tipo web e cliente-servidor para suporte das atividades administrativas e acadêmicas da instituição. Algumas das aplicações são o SIPES (Sistema de Pessoal), SIGRA (Sistema de apoio à Graduação) e outras, inclusive os equipamentos destinados ao atendimento da aplicação MatriculaWeb. Tais sistemas rodam em servidores Windows e tem acesso a um servidor de banco de dados com o Microsoft SQL Server. Todos os servidores estão funcionando como máquinas virtuais com exceção do servidor de banco de dados de produção, que é instalado em uma máquina física.

Para todos os servidores são acompanhados diversos pontos de monitoramento como processador, memória, disco, interface de rede e outros. A Tabela 19 mostra a lista de itens monitorados para todos os servidores do levantamento e o significado de cada item:

Tabela 19 – Itens Monitorados – Geral (Do Autor, 2017)

Parâmetros	Descrição
Check_MK	Funcionamento do agente de verificação instalado nos hosts
Uptime	Tempo de atividade de servidor desde a inicialização
System Time	Conferencia de tempo entre o agente e o gerente
Services Summary	Serviços de inicialização automática parados
CPU Utilization	Utilizaçao da CPU
Memory and Pagefile	Dados de uso de memória e paginação
Disk IO Summary	Taxa de throughput de disco (s)
Network Interfaces	Estado e tráfego das interfaces de rede
Disk Space	Espaço livre em disco

A Tabela 19 apresenta os itens monitorados em servidores Windows. Os tópicos dispostos se apresentam de duas formas diferentes na interface de monitoramento (*Dashboard*): As informações *check_mk*, *uptime*, *system time*, *services summary* e *Disk IO Summary* são informativas, isto é, que apresentam o estado do recurso (disponível ou não) ou seus dados de forma resumida; As demais itens como *CPU Utilization*, *Memory and Pagefile*, *Disk IO Summary*, *Network Interfaces* e *Disk Space* são apresentadas com os valores correspondentes e também apresentam em tela mensagens de advertência (*warning*)

ou críticas (*critical*), a depender dos níveis definidos pelos administradores da rede, conhecidos por *thresholds* ou limiares. Tais critérios são apresentados no presente levantamento.

Os outros itens monitorados não são observados em todos os servidores, e tratam de acompanhamento de logs, processos do Serviço de Informação para Internet ou IIS (Internet Information Service) e monitoramento de alguns tipos de serviço web, sendo do tipo informativo ou baseados em thresholds. A Tabela 20 apresenta os itens adicionais:

Tabela 20 – Itens Monitorados – Adicionais (Do Autor, 2017)

Parâmetros	Descrição
LOG Internet Explorer	Atividades do Internet Explorer
LOG MS-Win_Fwd/Oper.	Encaminhador de logs de eventos de Windows
LOG Security	Log de eventos de segurança
LOG Windows PowerShell	Log de atividades do *PowerShell*
proc_W3SVC.exe	Processo relacionado ao Microsoft IIS
proc_w3wp.exe	Processo relacionado ao Microsoft IIS
TCP Port 80	Monitoramento de porta 80 de servidor
MatriculaWeb Seguro	Monitoramento de https do site MatriculaWeb
MatriculaWeb	Monitoramento de http do site MatriculaWeb
UnBDoc	Monitoramento de http do site UnBDOC

Baseados na Tabela 20 e sobre os parâmetros de monitoramento pode-se informar que alguns pontos são apenas informativos e outros baseados em thresholds, com seus limiares baseados em unidades por milissegundos, segundos, horas ou unidades por segundo.

Todas as máquinas monitoradas que estão descritas neste levantamento são servidores Windows rodando em ambientes de desenvolvimento, homologação e produção. Existe mais de uma máquina para um mesmo grupo de atuação, como banco de dados, aplicações e servidores web. Os nomes reais dos equipamentos foram descaracterizados por razões de segurança e seus nomes são apresentados com a seguinte notação:

SRVXYZ

Onde as primeiras letras (SRV) representam a palavra servidor, a quarta letra (X) corresponde à função nos três ambientes de trabalho representadas (Desenvolvimento, Homologação e Produção respectivamente), a quinta o tipo de servidor (Web, Aplicação ou Banco de Dados), seguida de um número sequencial, que diferencia máquinas semelhantes.

As próximas tabelas apresentam os servidores, suas configurações respectivas de hardware e também os itens que são monitorados. As tabelas começam pelos servidores de homologação Web, seguidos dos equipamentos de aplicação, servidores Web de produção e os bancos de dados.

A Tabela 21 apresenta os itens monitorados nos servidores de homologação para aplicações web:

Tabela 21 – Itens Monitorados – Servidores Homologação Web (Do Autor, 2017)

		SRVHW1 a SRVHW3		
	TIPO	MONIT.	Thresholds	
ITENS MONITORADOS - GERAL			WARN.	CRIT.
Check_MK	Estado	SIM	-	-
Services Summary	Estado	SIM	-	-
Uptime	Estado	SIM	-	-
System Time	Estado	SIM	-	-
CPU Utilization	Percentual	SIM	80	90
Memory and Pagefile	Percentual	SIM	90	95
Network Interfaces	Percentual	SIM	99,95	99,999
Disk IO Summary	MB/s	SIM	-	-
Disk Space	Ocupação	SIM	80	90
ITENS MONITORADOS - LOGs				
LOG Internet Explorer	Estado	NÃO	-	-
LOG MS-Win_Fwd/Oper.	Estado	NÃO	-	-
LOG Security	Estado	NÃO	-	-
LOG Windows PowerShell	Estado	NÃO	-	-
ITENS MONITORADOS - PROCESSOS				
proc_W3SVC.exe	Unidades	SIM	100000	100000
proc_w3wp.exe	Unidades	SIM	100000	100000
TCP Port 80	Estado	SIM	-	-
ITENS MONITORADOS - SITES				
MatriculaWeb Seguro	Estado	SIM	-	-
MatriculaWeb	Estado	NÃO	-	-
UnBDoc	Estado	NÃO	-	-

A Tabela 22 apresenta os itens monitorados nos dois servidores de produção, para aplicações cliente servidor. Em tais servidores rodam as aplicações legadas que apresentam a característica de necessidade de instalação em máquinas cliente.

Tabela 22 – Itens Monitorados – Servidores Produção e Aplicação (Do Autor, 2017)

		SRVPA1 e SRVPA2		
			Thresholds	
ITENS MONITORADOS - GERAL	TIPO	MONIT.	WARN.	CRIT.
Check_MK	Estado	SIM	-	-
Services Summary	Estado	SIM	-	-
Uptime	Estado	SIM	-	-
System Time	Estado	SIM	-	-
CPU Utilization	Percentual	SIM	80	90
Memory and Pagefile	Percentual	SIM	90	95
Network Interfaces	Percentual	SIM	99,95	99,999
Disk IO Summary	MB/s	SIM	-	-
Disk Space	Ocupação	SIM	80	90
ITENS MONITORADOS - LOGs				
LOG Internet Explorer	Estado	NÃO	-	-
LOG MS-Win_Fwd/Oper.	Estado	NÃO	-	-
LOG Security	Estado	NÃO	-	-
LOG Windows PowerShell	Estado	NÃO	-	-
ITENS MONITORADOS - PROCESSOS				
proc_W3SVC.exe	Unidades	NÃO	-	-
proc_w3wp.exe	Unidades	SIM	100000	100000
TCP Port 80	Estado	SIM	-	-
ITENS MONITORADOS - SITES				
MatriculaWeb Seguro	Estado	NÃO	-	-
MatriculaWeb	Estado	NÃO	-	-
UnBDoc	Estado	NÃO	-	-

É necessário lembrar também que alguns dos servidores de produção, em especial os responsáveis pelo MatriculaWeb estão funcionando com um arranjo de cluster, onde a quantidade dos mesmos pode ser adicionada ou reduzida com o objetivo de ajustar a performance conforme a necessidade. Tais máquinas apresentam configurações idênticas e são todas virtualizadas.

Uma vez que a aplicação MatriculaWeb é uma solução cujo funcionamento é essencial para a universidade, foram disponibilizadas soluções de redundância para se criar um ambiente com o máximo de disponibilidade possível. Assim, tais servidores demandam uma necessidade muito forte de robustez e serem capazes de tratar altas demandas de utilização, o que se dá nos períodos de matrículas.

A Tabela 23 apresenta os itens monitorados nos seis servidores de produção WEB:

Tabela 23 – Monitoramento – Servidores Produção Aplicações Web (Do Autor, 2017)

		SRVPW1 a SRVPW6		
			Thresholds	
ITENS MONITORADOS - GERAL	TIPO	MONIT.	WARN.	CRIT.
Check_MK	Estado	SIM	-	-
Services Summary	Estado	SIM	-	-
Uptime	Estado	SIM	-	-
System Time	Estado	SIM	-	-
CPU Utilization	Percentual	SIM	80	90
Memory and Pagefile	Percentual	SIM	90	95
Network Interfaces	Percentual	SIM	99,95	99,999
Disk IO Summary	MB/s	SIM	-	-
Disk Space	Ocupação	SIM	80	90
ITENS MONITORADOS - LOGs				
LOG Internet Explorer	Estado	SIM	-	-
LOG MS-Win_Fwd/Oper.	Estado	SIM	-	-
LOG Security	Estado	SIM	-	-
LOG Windows PowerShell	Estado	SIM	-	-
ITENS MONITORADOS - PROCESSOS				
proc_W3SVC.exe	Unidades	NÃO	-	-
proc_w3wp.exe	Unidades	SIM	100000	100000
TCP Port 80	Estado	SIM	-	-
ITENS MONITORADOS - SITES				
MatriculaWeb Seguro	Estado	SIM	-	-
MatriculaWeb	Estado	SIM	-	-
UnBDoc	Estado	SIM	-	-

Em comparação com os demais servidores cliente-servidor e web, alguns itens não são monitorados nos equipamentos mencionados a seguir, portanto apresentam uma configuração mais simples comparada aos demais servidores, com a monitoração disposta em poucos itens. Nestes equipamentos rodam as aplicações de banco de dados e sem os servidores Web, o que torna dispensável a monitoração desses itens. Servidores de Banco de Dados apresentam requisitos diferentes de monitoramento para as suas funções.

A Tabela 24 apresenta os itens monitorados em todos os servidores de Banco de Dados (Desenvolvimento, Homologação e Produção):

Tabela 24 – Monitoramento – Servidores de Banco de Dados (Do Autor, 2017)

	SRVDBD1, SRVHBD1 e SRVPBD1			
	TIPO	MONIT.	Thresholds	
ITENS MONITORADOS - GERAL			WARN.	CRIT.
Check_MK	Estado	SIM	-	-
Services Summary	Estado	SIM	-	-
Uptime	Estado	SIM	-	-
System Time	Estado	SIM	-	-
CPU Utilization	Percentual	SIM	80	90
Memory and Pagefile	Percentual	SIM	90	95
Network Interfaces	Percentual	SIM	99,95	99,999
Disk IO Summary	MB/s	SIM	-	-
Disk Space	Ocupação	SIM	80	90

A exceção difere apenas no servidor de produção, com acompanhamento de alguns itens relacionados a desempenho e funcionamento do MS-SQL. A Tabela 25 apresenta os itens exclusivos para acompanhamento no servidor de banco de dados de produção:

Tabela 25 – Itens Exclusivos – Servidor Banco de Dados – Produção (Do Autor, 2017)

Parâmetros	**Critério**	**THRESHOLD WARNING**	**THRESHOLD CRITICAL**
Full-scans	Unidades/s	900	1000
Batch-requests	Unidades/s	1800	1900
Connected-users	Unidades/s	1500	2000
Connection-time	Unidades/s	1	5
Database-datafile-auto-growths	Ativo/inativo	-	-
Database-file-auto-growths	Ativo/inativo	-	-
Database-logbackup-age	Tempo (h)	48	72
Database-logfile-auto-growths	Informativo	-	-
Database-online	Informativo	-	-
Failed-jobs	Unidades	120	300
Latches-wait-time	Tempo	1ms	5ms
Latches-waits	Unidades/s	3000-5000	5000-8000
Locks-deadlocks	Unitário	1	5
Locks-timeouts	Unidades/s	3	5
Locks-waits	Unidades/s	100	500
mem-pool-data-buffer-hit-radio	Tempo (min)	90	80
MS-SQL	Informativo	-	-
Page-file-expectancy	Tempo (s)	300	180
Proc_MSSQLSERVER	Percentual	90	98
SQL-recompilations	Unidades	9	10

Sobre os bancos de dados, estes não desempenham funções de desenvolvimento de sistemas, porém os recursos de desenvolvimento, homologação e produção acessam as bases armazenadas em seus respectivos repositórios. Para este tipo de recurso, um evento de indisponibilidade pode apresentar alto impacto para as atividades da instituição. Por essa razão os servidores de banco de dados também foram incluídos neste levantamento.

Buscando um enfoque mais global para o monitoramento dos servidores, em uma observação mais detalhada dos itens monitorados nota-se que os parâmetros são semelhantes entres si, independentemente do tipo de atividade do equipamento e serviços ativos. Para adequar melhor as métricas aos servidores de diferentes modalidades são necessárias uma revisão e configuração dos equipamentos, tema da proposta do próximo tópico.

3.3 PROPOSTA – PARÂMETROS ADICIONAIS E MELHORIAS PARA O MONITORAMENTO

Um sistema de monitoramento ajustado conforme as necessidades da instituição pode ser um recurso importante para as atividades de gerencia e operação executadas pela equipe de TI. Sob esse ponto de vista, é necessário que a ferramenta adotada seja adequadamente configurada de tal forma que atenda aos requisitos dos seus usuários.

A presente proposta tem por objetivo expor aos gestores sugestões de melhoria com a intenção de tornar o serviço de monitoramento no CPD da Universidade mais proativo, abrangente e com menor tempo de resposta a falhas.

As sugestões apresentadas poderão ser tomadas em três frentes de atuação, classificadas conforme as atividades relacionadas ao serviço de monitoramento:

- Ações relacionadas às métricas ou parâmetros de monitoramento;
- Ajustes no servidor de monitoramento;
- Ajustes relacionados à interface e à solução;

Todas as sugestões apresentadas nesta proposta podem ser aplicadas em separado e independente de ordem.

3.3.1 Métricas ou Parâmetros Para Monitoramento

O monitoramento trata de coletar informações periodicamente, e tomar determinadas ações baseadas em limiares ou *thresholds* previamente estabelecidos. Os limites devem ser estabelecidos de forma cuidadosa com a intenção de se evitar uma avaliação do tipo falso

negativo ou falso positivo, o que torna o monitoramento impreciso e dificulta o trabalho das equipes. As ações se baseiam nas seguintes diretrizes:

- Personalização de *thresholds* e intervalos de coleta;
- Uso de recursos complementares como WMI;
- Exploração da MIB privada da Microsoft;
- Registro de DLLs de Windows para monitoramento;

As ações acima têm a intenção de ampliar os itens observados melhorando a qualidade do monitoramento dos sistemas, e são descritas com mais detalhes a seguir.

O levantamento realizado indicou que os equipamentos possuem thresholds semelhantes entre eles, independentemente do tipo de trabalho realizado. Servidores de aplicação cliente-servidor, servidores Web e de banco de dados possuem características diferentes em relação ao tipo de trabalho realizado. Assim, é necessário personalizar os thresholds e os intervalos de coleta de informações para cada categoria de serviço conforme o tipo e a criticidade da aplicação. Isto pode proporcionar às equipes um tempo de reação menor para os serviços mais críticos.

Outro aspecto percebido se refere aos servidores Windows. A solução de monitoramento possui a capacidade de monitorar o funcionamento básico da máquina além de alguns serviços. Para coletar algumas informações mais específicas dos servidores é necessário a customização de agentes utilizando recursos de Windows como a Instrumentação para Gerenciamento de Windows ou WMI (*Windows Management Instrumentation*), que pode possibilitar a coleta de dados de funcionamento do sistema operacional e das aplicações instaladas para avaliação pelo Nagios.

Ainda em relação a solução de monitoramento, existe uma Base de Informações de Gerenciamento ou MIB (*Management Information Base*) privada da Microsoft. Assim, estudos adicionais podem ser feitos para uma possível aplicação das facilidades desta base.

Os desenvolvedores Windows criam e registram diversas Bibliotecas de Vínculo Dinâmico ou DLL (*Dynamic Link Library*) para as aplicações executadas no servidor. Uma vez que é possível o registro de DLLs como serviços, existe a possibilidade de se utilizar desse recurso para facilitar o monitoramento pelo Nagios uma vez que ele monitora serviços de Windows. Esta medida, no entanto, precisa ser testada antes de colocada em produção, para evitar que os sistemas legados possam apresentar algum comportamento imprevisto.

3.3.2 Ajustes no Servidor de Monitoramento

A melhoria do serviço de monitoramento não pode ser feita sem a implementação de ajustes no servidor correspondente para proporcionar mais segurança para a sua operação. As medidas passam pela avaliação de cópias de segurança (*backup* e restauração) com as equipes correspondentes e a elaboração de um plano de recuperação de desastres para o servidor, complementadas por medidas de médio prazo com a configuração de recursos de redundância.

3.3.3 Ajustes Relacionados à Interface e à Solução

Grande parte das atividades de monitoramento pode ser executada por meio da interface da solução envolvida. Assim, as melhorias no envio de alarmes e notificações contribuem com a qualidade do serviço prestado.

Um recurso disponível no Nagios é o envio de alertas e notificações, seja na tela da interface, por e-mail ou SMS. Por meio de plug-ins desenvolvidos pela comunidade tais recursos podem ser implementados com dificuldade baixa ou moderada.

Uma opção que pode despertar interesse para as equipes de gestão e plantonistas é o envio por meio de SMS, por ser uma solução de fácil implantação. O envio por SMS funciona baseado em um modem conectado à porta USB do servidor ou através de serviços de *gateway* na internet, com a cobranças de taxas telefônicas. Assim os alertas podem ser enviados aos membros da equipe de suporte e notificar eventuais anomalias.

O serviço de monitoramento não precisa ficar restrito às equipes do Centro de Operações de Redes ou NOC (*Network Operations Center*). Uma vez que a interface gráfica (*Dashboard*) é baseada em Web, podem ser desenvolvidas visões personalizadas para as diversas unidades do CPD, inclusive banco de dados e desenvolvimento de aplicações. Por meio dessas interfaces os interessados poderão acessar e participar do acompanhamento de servidores e serviços de seus respectivos interesses, utilizando os serviços de monitoramento. As áreas gerenciais também poderão ser beneficiadas com os recursos de relatórios relacionados a Acordos de Nível de Serviço.

As medidas descritas acima irão contribuir não somente com os sistemas legados, mas também com todos os sistemas e serviços prestados atualmente no CPD com o objetivo final de aumentar a qualidade do monitoramento de serviços e sistemas como um todo.

4 CONCLUSÃO

O uso de ferramentas de monitoramento é atualmente um item indispensável para a operação dos datacenters atuais. Suas facilidades e recursos possibilitam aos operadores a rápida identificação de falhas e comportamentos anormais, facilitam aos administradores de redes identificação mais rápida dos problemas e sua devida correção e também proporcionam aos gestores a manutenção dos acordos de nível de serviço em graus de conformidade adequados.

A elaboração deste trabalho possibilitou analisar o funcionamento de protocolos usados para gerencia de redes, compreender as expectativas dos usuários a respeito do serviço de monitoramento, analisar o funcionamento do software de monitoramento Nagios e avaliar as métricas e parâmetros utilizados para monitoramento dos servidores instalados no CPD da Universidade de Brasília.

Foi elaborada a fundamentação teórica, e dentro do estudo de caso foi feita a aplicação de um questionário, um levantamento de métricas utilizadas e uma proposta com sugestão de melhorias.

A preparação da fundamentação teórica possibilitou a análise e compreensão do funcionamento de protocolos utilizados no gerenciamento de redes e os fundamentos envolvidos. Para o estudo de caso o questionário teve a intenção de sondar as opiniões dos usuários sobre os temas disponibilidade de serviços e monitoramento, um levantamento dos parâmetros e métricas de monitoramento utilizados atualmente para monitoria dos servidores web, de aplicação e de bancos de dados do CPD. Ainda dentro do estudo de caso foi elaborada também uma proposta sobre parâmetros adicionais e melhorias para o serviço de monitoramento. Com base nas ações desenvolvidas é possível concluir que os objetivos do trabalho foram atingidos.

Durante a elaboração da fundamentação teórica por meio de pesquisa bibliográfica foram revisados os conhecimentos relacionados aos protocolos do modelo TCP/IP como o ICMP e SNMP, protocolos utilizados para troca de informações entre os softwares gerentes e agentes. Além dos protocolos, foram estudados os conceitos envolvidos no gerenciamento de redes como os protocolos SMI, MIB e a notação ASN.1, os requisitos para um sistema de monitoramento e os parâmetros comumente utilizados. Também foram feitos estudos sobre a ferramenta Nagios. O estudo teórico possibilitou a compreensão do tema e uma visão mais abrangente do gerenciamento de redes.

O estudo de caso consistiu em três atividades: aplicação de questionário, o levantamento de métricas utilizadas e uma proposta. Por meio do questionário foi possível sondar as opiniões dos usuários, onde se constatou que ocorrem muitos eventos de indisponibilidade no CPD, que o serviço de monitoramento é importante para a maioria dos entrevistados, que boa parte deles usufrui do monitoramento oferecido pelo Centro e tem a intenção de ampliar o uso dos serviços.

De forma complementar ao questionário o levantamento das métricas utilizadas mostrou que os equipamentos utilizam as mesmas métricas, independentemente de sua natureza de utilização. Uma vez que as aplicações dos servidores podem ser diferentes, constatou-se a necessidade de customização dos parâmetros utilizados.

Com base nas informações sondadas na pesquisa e no levantamento foi possível elaborar a proposta com as sugestões de melhoria para o serviço. Esta parte do trabalho apresentou recomendações voltadas para as métricas a empregar, ajustes de customização nos servidores, na interface gráfica e outras observações para a solução como um todo.

4.1 TRABALHOS FUTUROS

O tema monitoramento se revelou mais amplo que o inicialmente suposto, sobretudo quanto aos aspectos de levantamento de informações por parte dos agentes. Baseado neste contexto, a exploração de tais recursos se apresenta como possibilidade para estudos.

Um aspecto não muito utilizado pelos administradores do Nagios é a coleta de informações em servidores Windows utilizando recursos WMI. Uma vez que na Universidade de Brasília são usados sistemas da Microsoft, um trabalho de pesquisa pode ser desenvolvido para explorar as facilidades e obter informações que não estão disponíveis a partir de configurações básicas do software de monitoramento. Outro ponto semelhante é a exploração das capacidades da base MIB privada da Microsoft, a qual pode ser considerada como outro tema para os estudos.

É possível citar além das sugestões acima a personalização e o desenvolvimento de plug-ins para Nagios, uma vez que ele possui uma comunidade grande e com bastante documentação disponível, sendo outra frente para estudos que pode ser aproveitada para trabalhos acadêmicos.

No contexto apresentado, a otimização dos recursos de monitoramento através de métricas apropriadas permite aos gerentes de rede uma melhor administração dos servidores e seus respectivos serviços, facilitando o reconhecimento de situações anormais

e viabilizando uma intervenção tempestiva para a solução do problema. Face à importância do monitoramento para o Centro de Informática da UnB, e tendo como base a amplitude do tema, este trabalho não esgota o assunto, motivo pelo qual as sugestões apresentadas acima podem contribuir com o enriquecimento da matéria.

REFERÊNCIAS BIBLIOGRÁFICAS

"DISPONIBILIDADE" In: Dicionário Aulete Digital. 2008. Desenvolvido por Lexikon Editora Digital Ltda. Disponível em: <http://www.aulete.com.br/disponibilidade>. Acesso em: 14 abr. 2017.

"MONITORAR" In: - Dicionário Aulete Digital. 2008. Desenvolvido por Lexikon Editora Digital Ltda.. Disponível em: <http://www.aulete.com.br/monitorar>. Acesso em: 14 abr. 2017.

COMER, Douglas Earl. Internetworking With TCP/IP Volume I: Principles, Protocols and Architecture. 5. ed. Upper Saddle River: Pearson Prentice Hall, 2006.

COMER, Douglas Earl. Redes de Computadores e Internet. 4. ed. Porto Alegre: Bookman, 2007. 640 p. Tradução Álvaro Strube de Lima.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. Implantando a governança de TI: da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.

FOROUZAN, Behrouz. Comunicação de Dados e Redes de Computadores. 4. ed. São Paulo: McGraw-Hill, 2008. 1134 p. Tradução Ariovaldo Griesi.

FOROUZAN, Behrouz; MOSHARRAF, Firouz. Redes de Computadores: Uma Abordagem Top-Down. Porto Alegre: Bookman McGraw-Hill, 2013. 928 p. Tradução de Marcos A. Simplício Jr. e Charles Christian Miers.

HERNANTES, Josune; GALLARDO, Gorka; SERRANO, Nicolas. IT Infrastructure-Monitoring Tools. IEEE Software, [s.l.], v. 32, n. 4, p.88-93, jul. 2015. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/ms.2015.96. Disponível em: <http://ieeexplore.ieee.org.ez54.periodicos.capes.gov.br/stamp/stamp.jsp?arnumber=7140697>. Acesso em: 10 maio 2017.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 7498-4:1989: Information processing system - Open Systems Interconnection - Basic Reference Model - Part 4: Management framework. 4 ed. Genebra: ISO/IEC, 1989. 16 p. Disponível em: <http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989(E).zip>. Acesso em: 22 abr. 2017.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000-4:2016: Information technology — Security techniques — Information security management systems — Overview and vocabulary. 4 ed. Genebra: ISO/IEC, 2016. 42 p. Disponível em: <http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip>. Acesso em: 02 maio 2017.

KAUSHIK, Anshul. Use of Open Source Technologies For Enterprise Server Monitoring Using SNMP. International Journal On Computer Science And Engineering. Chennai, p. 2246-2252. 01 out. 2010. Disponível em: <http://www.enggjournals.com/ijcse/doc/IJCSE10-02-07-32.pdf>. Acesso em: 11 maio 2017.

KUROSE, James F.; ROSS, Keith W.. Redes de Computadores e a Internet: Uma Abordagem Top-Down. 5. ed. São Paulo: Pearson Education, 2010. Tradução Opportunity Translations.

MAURO, Douglas; SCHMIDT, Kevin James. Essential SNMP. 2. ed. Sebastopol: O'Reilly, 2011. 442 p.

MOHR, Rodrigo Fraga. Análise de Ferramentas de Monitoração de Código Aberto. 2012. 70 f. TCC (Graduação) - Curso de Ciência da Computação, Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2012. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/66105/000870983.pdf>. Acesso em: 12 abr. 2017.

MSDN: Windows Management Instrumentation. 2017. Elaborada por Microsoft Developer Network. Disponível em: <https://msdn.microsoft.com/en-us/library/aa394582(v=vs.85).aspx>. Acesso em: 20 jul. 2017.

NAGIOS Brazillian Community Site. 2017. Disponível em: <http://nagios-br.com/nagios-core>. Acesso em: 18 jul. 2017.

NAGIOS Plugins. Nagios Core Documentation. Disponível em: <https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/plugins.html>. Acesso em: 21 jul. 2017.

NAGIOS XI FAQs. Disponível em: <https://www.nagios.com/products/nagios-xi/#faqs>. Acesso em: 21 jul. 2017.

OLIVEIRA, Marcos Henrique de. Nagios Monitorando Redes Corporativas. Rio de Janeiro: Editora Ciência Moderna, 2014.

OSIRO, Kendy Aparecido. Estudo de Segurança da Informação com enfoque nas Normas ABNT NBR ISO/IEC 17799:2005 e NBR ISO/IEC 27001:2006, para aplicação no Senado Federal. 2006. 114 f. Monografia (Especialização) - Curso de Especialização em Gestão em Tecnologia da Informação, Departamento de Engenharia Elétrica, Universidade do Legislativo Brasileiro (UNILEGIS) e Universidade de Brasília (UnB), Brasília, DF, 2006. Disponível em: <http://www2.senado.leg.br/bdsf/handle/id/70462>. Acesso em: 01 maio 2017.

PEDREIRA, Paulo Ricardo Tobias. Gerenciamento de Redes com o Nagios. 2015. Disponível em: <https://pt.linkedin.com/pulse/gerenciamento-de-redes-com-o-nagios-paulo-ricardo-tobias-pedreira>. Acesso em: 24 maio 2017.

PESSOA, Márcio. Pra que serve o Nagios? 2010. Disponível em: <https://pessoa.eti.br/main/2010/10/11/pra-que-serve-o-nagios/>. Acesso em: 10 jul. 2017.

POLETO FILHO, Olavo. Gerenciamento e monitoramento de redes: análise de desempenho. 2011. 94 f. Monografia (Especialização) - Curso de Engenharia de Redes e Sistemas de Telecomunicações, Instituto Nacional de Telecomunicações, Santa Rita do Sapucaí, 2011.

PRADO FILHO, Hayrton Rodrigues do. Continuidade dos negócios e segurança da informação. 04/03/2015. Blog Qualidade Online. Disponível em: <https://qualidadeonline.wordpress.com/2015/03/04/continuidade-dos-negocios-e-seguranca-da-informacao>. Acesso em: 14 abr. 2017.

PRIGGE, Matt. 5 recursos que todo sistema de monitoramento deveria ter. Computerworld, São Paulo, v. 1, n. 1, p.001-001, 16 fev. 2015. Disponível em: <http://computerworld.com.br/tecnologia/2015/02/16/5-recursos-que-todo-sistema-de-monitoramento-deveria-ter>. Acesso em: 10 abr. 2017.

ROCHOL, Juergen. Comunicação de Dados - Vol. 22: Série Livros Didáticos Informática UFRGS. Porto Alegre: Bookman, 2012.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SOARES, Luiz Fernando Gomes; SOUZA FILHO, Guido Lemos de; COLCHER, Sérgio. Redes de Computadores: Das LANs, MANs e WANs às redes ATM. 7. ed. Rio de Janeiro: Campus, 1995.

STALLINGS, William. SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. 3. ed. New York: Addison-Wesley, 1999.

TANENBAUM, Andrew Stuart. Redes de Computadores. 3. ed. Rio de Janeiro: Campus, 1997.

TANENBAUM, Andrew Stuart. Redes de Computadores. 4. ed. Rio de Janeiro: Elsevier, 2003. Tradução Vanderberg D. de Souza.

ZIBIANI, Fabio Augusto. Avaliando o desempenho do seu servidor. 2011. BLOG Fabio Augusto. Disponível em: <https://fabiozibiani.wordpress.com/2011/01/04/avaliando-o-desempenho-do-seu-servidor/>. Acesso em: 20 jul. 2017.

APÊNDICES

APÊNDICE A – QUESTIONÁRIO DA PESQUISA

PESQUISA ACADÊMICA: A PERCEPÇÃO DOS USUÁRIOS SOBRE A IMPORTÂNCIA DO MONITORAMENTO DE SISTEMAS NO CPD DA UNB

APRESENTAÇÃO

Olá,

Este questionário faz parte da elaboração de trabalho de conclusão de curso de Especialização em Gestão de Segurança da Informação da Faculdade de Tecnologia da UNB, turma 2016/2017. Ele tem por objetivo analisar a percepção por parte dos usuários e gestores da importância do monitoramento de sistemas no âmbito do CPD da Universidade de Brasília. Ao responder as perguntas você estará colaborando com um trabalho acadêmico e também com a gestão de TI da Universidade.

ORIENTAÇÕES QUANTO AO PREENCHIMENTO:

O presente questionário de baseia em questões do tipo múltipla escolha e resposta a perguntas.
A primeira parte apresenta questões sobre a qualificação dos usuários;
A segunda parte dispõe de perguntas sobre a disponibilidade dos sistemas;
A terceira parte trata sobre o monitoramento de sistemas.

TERMO DE CONFIDENCIALIDADE E ACESSO AOS RESULTADOS

O pesquisador do projeto assume o compromisso de:

1. Preservar o sigilo e a privacidade dos sujeitos e das unidades cujos dados serão estudados;
2. Assegurar que as informações serão utilizadas única e exclusivamente para a execução do projeto em questão;
3. Assegurar que os resultados da pesquisa somente serão divulgados de forma anônima, não sendo usadas iniciais ou quaisquer outras indicações que possam identificar o sujeito da pesquisa.

4. Caso houver interesse, os entrevistados poderão ter acesso aos resultados e formulários da pesquisa entrando em contato com pesquisador, por meio de endereço de e-mail. Os resultados estarão disponíveis após a finalização da pesquisa.

QUESTÕES SOBRE O PERFIL DO ENTREVISTADO

PRIMEIRA PARTE: SOBRE A SUA ATIVIDADE

Forneça informações sobre escolaridade e outras informações sobre a sua atuação no CPD

1 Por favor, informe o seu grau de escolaridade

Ensino Fundamental

Ensino Médio

Ensino Superior

Especialização

Mestrado

Doutorado

2 Informe o seu vínculo com a Instituição

Sou servidor da universidade (docente ou técnico administrativo)

Sou funcionário de empresa terceirizada

Sou estagiário ou bolsista

Outro:

3 Informe a sua área de atuação no CPD

Área Administrativa (Direção, Administração e Secretaria)

Banco de Dados

Desenvolvimento

HelpDesk (atendimento ao usuário)

Infraestrutura de Redes

Operação de Sistemas

Redes

Suporte Avançado

Segurança

Outro:

4 Você exerce cargo de chefia, coordenação ou liderança?

Sim, exerço cargo de chefia, coordenação ou liderança

Não, exerço cargo técnico administrativo ou colaborador

QUESTÕES SOBRE A OPINIÃO DO ENTREVISTADO

SEGUNDA PARTE: SOBRE A DISPONIBILIDADE DOS SISTEMAS

A indisponibilidade é um evento no qual as informações deixam de estar disponíveis aos usuários por causas diversas. Sobre isto responda às próximas questões:

5 Você tem conhecimento de eventos de indisponibilidade nos sistemas da UnB?
Sim
Não

6 Qual a frequência desses eventos?
Diariamente
A cada dois dias
Semanalmente
Quinzenalmente
Mensalmente

7 Como você toma ciência de tais eventos?
Alguém comenta que o sistema está fora do ar
Eu mesmo (a) percebo durante a utilização do sistema
Recebo avisos por email ou outra forma de comunicação do CPD
Outro:

8 Você tem ciência da causa de tais eventos? Escolha as principais:
Falhas no fornecimento de energia
Sobrecarga de trabalho nos servidores
Sobrecarga de capacidade dos recursos de comunicação
Eventos de manutenção
Outro:

9 Quando esses eventos ocorrem, você recebe alguma informação ou comunicado das equipes de suporte?
Sim, recebo informações por e-mail
Sim, recebo informações de forma verbal
Não recebo informações ou comunicados

QUESTÕES SOBRE A OPINIÃO DO ENTREVISTADO

SEGUNDA PARTE: SOBRE A DISPONIBILIDADE DOS SISTEMAS – CONTINUAÇÃO

10 Ainda sobre esses eventos, você recebe alguma informação das equipes sobre a previsão para retorno do sistema ou resolução do problema?
Sim
Não

Eventos de indisponibilidade podem causar impacto negativo aos usuários. Sobre isto responda:

11 Estes eventos causam impacto na sua atividade?
Muito baixo ou nulo
Baixo
Moderado
Alto
Muito Alto

TERCEIRA PARTE: MONITORAMENTO DE SISTEMAS

O monitoramento de sistemas consiste no uso de equipamentos, aplicações e processos de trabalho para informar as equipes de suporte sobre os eventos que ocorrem na rede. Sobre isto responda às próximas questões:

12 Você tem noção ou conhecimento sobre o monitoramento de sistemas?
Sim
Não

13 Você tem ciência de algum serviço, sistema ou ferramenta de monitoramento utilizada pelas equipes de suporte do CPD?
Sim
Não

14 Você acha que o monitoramento de sistemas é importante para o trabalho de sua unidade?
Sim
Não

QUESTÕES SOBRE A OPINIÃO DO ENTREVISTADO

TERCEIRA PARTE: MONITORAMENTO DE SISTEMAS - CONTINUAÇÃO

15 Você acha que o monitoramento de sistemas é importante para as atividades do CPD? Porque?

Sua resposta

As questões seguintes dizem respeito ao monitoramento de sistemas na sua unidade de trabalho:

16 Em sua unidade você se utiliza de algum serviço de monitoramento?

Sim

Não

17 Há quanto tempo sua unidade está utilizando os serviços de monitoramento?

Há menos de um mês

Há menos de três meses

Há mais de seis meses

Há mais de um ano

Há mais de cinco anos

18 Quais os tipos de recursos são monitorados?

Recursos de Infraestrutura de Redes (Switches, Roteadores etc)

Servidores de Banco de Dados

Servidores de Aplicação

Servidores WEB

Servidores de Infraestrutura (Exemplo : DNS)

Servidores de email

Serviços executados em servidores (Bibliotecas DLL, Filas de Impressão)

Atividade dos servidores (PING)

Atividade dos servidores (CPU, Memória, Disco, Rede)

19 Pretende ampliar a utilização dos sistemas de monitoramento em sua unidade?

Sim, dentro de alguns meses

Sim, dentro de um ano

Não

20 Quanto ao serviço de monitoramento, o que você acha que deve ser melhorado?

Resposta:

QUESTÕES SOBRE A OPINIÃO DO ENTREVISTADO

TERCEIRA PARTE: MONITORAMENTO DE SISTEMAS - CONTINUAÇÃO

21 Mesmo sem utilizar algum serviço de monitoramento em sua unidade, você acha importante e/ou necessário a sua adoção nos seus processos e rotinas de trabalho?

Sim

Não

Talvez, ainda não foi decidido

22 Caso pretenda adotar a utilização dos serviços de monitoramento em sua unidade, em quanto tempo pretende fazê-lo?

Não

Dentro de alguns meses

Dentro de um ano

Encerramento

Agradecemos a sua gentileza em dispor de seu tempo para a realização desta pesquisa. Caso tenha interesse nos resultados, ou ainda para mais esclarecimentos, por favor entre em contato pelo endereço de email pesquisa.gsi.unb.2017@gmail.com.