UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ – UTFPR
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
ESPECIALIZAÇÃO EM TELEINFORMÁTICA E REDES DE COMPUTADORES

GIULIANO SUCKOW

GERÊNCIA DE ATIVOS DE TI NAS ORGANIZAÇÕES PÚBLICAS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2011

GIULIANO SUCKOW

GERÊNCIA DE ATIVOS DE TI NAS ORGANIZAÇÕES PÚBLICAS

Monografia apresentada como requisito parcial para a obtenção do título de Especialista em Teleinformática e Redes de Computadores da Universidade Tecnológica Federal do Paraná, UTFPR.

Orientador: Prof. Dr. Armando Rech Filho

CURITIBA

2011

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação do *Campus* Curitiba
Departamento Acadêmico de Eletrônica
Especialização em Teleinformática e Redes de Computadores

TERMO DE APROVAÇÃO

GERÊNCIA DE ATIVOS DE TI NAS ORGANIZAÇÕES PÚBLICAS

por

GIULIANO SUCKOW

Esta monografia foi apresentada às 15:00h do dia 08 de fevereiro de 2012 como requisito parcial para a obtenção do título de ESPECIALISTA EM TELEINFORMÁTICA E REDES DE COMPUTADORES, Universidade Tecnológica Federal do Paraná. O candidato foi argüido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado com a nota 10,0 (DEZ INTEIROS)

Prof. Dr. Armando Rech Filho
(UTFPR)

Prof. Dr. Walter Godoy Júnior
(UTFPR)

Visto da Coordenação

Prof. Dr. Walter Godoy Júnior
Coordenador do Curso

AGRADECIMENTOS

A Deus, por me conceder a vida, saúde e inteligência. Itens fundamentais para o desenvolvimento intelectual de qualquer ser humano.

A minha Mãe, por ter me educado no caminho certo, ter me dado muito carinho e grandes exemplos de força, companheirismo e dedicação, características sempre nela presentes nos momentos mais difíceis que a vida nos proporciona.

Ao meu Pai, que sempre me orientou e se manteve firme na minha educação, tomou atitudes certas nos momentos certos, visando sempre o meu bem. Hoje, depois de adulto e também pai, compreendo e tomo como exemplo algumas de suas decisões.

A minha amada esposa, que me permitiu realizar um grande sonho: O de ter uma linda família. Sempre se mostrando companheira, e que me incentivou a continuar estudando.

Ao meu filho, que completa minha vida e me enche de alegrias.

RESUMO

SUCKOW, Giuliano. **Gerência de ativos de TI nas organizações públicas**. 2011. 62 f. Monografia (Especialização em Teleinformática e Redes de Computadores) – Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

A constante demanda por gerenciamento dos ativos de TI atualmente atinge qualquer organização, principalmente as de médio e grande porte. Neste trabalho é abordada a demanda que o setor público federal tem por melhor gerência de seus ativos de TI, demonstrando quais os problemas enfrentados pelos gerentes de TI em implementar um ambiente que seja eficientemente gerenciável, quais as conseqüências em não se ter um ambiente gerenciável, quais os mecanismos e ferramentas disponíveis atualmente no mercado capazes de melhorar a gerência dos ativos. Demonstra também que não custa caro implementar ferramentas de gerência de TI e por fim descreve um ambiente real de uma organização pública federal pertencente ao poder Executivo, a Superintendência Regional de Polícia Federal no Paraná, onde recentemente foram implementadas ferramentas e metodologias para tornar o ambiente de TI gerenciável, demonstrando na prática as vantagens e benefícios obtidos.

Palavras-chave: Gerência de TI, Organizações Públicas, Ferramentas para Tecnologia da Informação, Ferramentas.

ABSTRACT

SUCKOW, Giuliano. **IT asset management in public organizations**. 2011. 62 f. Monografia (Especialização em Teleinformática e Redes de Computadores) – Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

The continuous demand for management of equipment, software and computer systems is present in any organization, especially those of medium and large size.
In this work is demonstrated that the federal public sector requires better management of its computer equipment, software's and information systems, and the problems faced by managers in implementing technological environments efficiently manageable. Also discusses the consequences of not having a manageable environment and the methods and tools available today that can improve computer equipment management and information systems, demonstrating that isn't expensive to implement those management tools in the computers environments. And finally, describes a real environment of an organization of brazilian federal executive branch, the Regional Superintendence of Federal Police in the state of Paraná, that has recently implemented tools and methodologies to make manageable the computer environment, demonstrating practical advantages and benefits.

Keywords: IT Management, Public Organizations, Tools for Information Technology, Tools.

LISTA DE FIGURAS

LISTA DE SIGLAS E ACRÔNIMOS

AD	*Active Directory*
DTMF	*Distributed Management Task Force*
GNU	*General Public License*
HTML	*HyperText Markup Language*
IETF	*Internet Engineering Task Force*
ITIL	*Information Technology Infrastructure Library*
MAC	*Media Access Control*
MIB	*Management Information Base*
MRTG	*Multi Router Traffic Grapher*
RFC	*Request for Comments*
SARG	*SQUID Analysis Report Generator*
SLA	*Service Level Agreement*
SNMP	*Simple Network Management Protocol*
SQL	*Structured Query Language*
TI	Tecnologia da Informação
UDP	*User Datagram Protocol*
WBEM	*Web Based Enterprise Management*
WMI	*Windows Management Instrumentation*
WWW	*World Wide WEB*

SUMÁRIO

1 INTRODUÇÃO

> O Gerenciamento de Ativos de TI (Tecnologia da Informação) pode ser interpretado como o caminho entre as forças de finanças (que envolve dinheiro e conformidades) e de Serviços (que envolve mudanças e melhorias). O Gerenciamento de Ativos de TI representa ou compreende todos os sistemas, processos e controles para medir e gerenciar os ativos de TI e seu ciclo de vida em uma organização. (NATAL, 2010, p.1).

Fagundes (2004, p.1) salienta que atualmente qualquer organização seja ela pública ou privada de médio e grande porte obrigatoriamente necessita que seu parque de equipamentos e sistemas esteja inserido em um ambiente gerenciável. Essa demanda é relativamente nova, nos últimos 10 (dez) anos a concorrência no mercado em qualquer setor aumentou significativamente obrigando as pessoas do mais alto escalão de uma organização a pensarem em maneiras de diminuir custos para se manterem competitivos no mercado.

Ortolani (2008, p.2) destaca que “a tendência natural é tentar medir o valor da informação pelo quanto adicional ela traz, entretanto, o conceito mais amplo e correto é o custo de oportunidade - quanto custa não tê-la. Neste sentido, medir o valor da informação passa a ser um processo semelhante ao de um seguro ou propaganda - quanto custa não ter".

Essa abordagem é amplamente utilizada, a informação muitas vezes é tratada como um simples recurso, possuindo assim um custo e valor, taxa de retorno, custo de possibilidade de não se ter a informação.

Ortolani (2008, p.2) destaca ainda que independente do tipo de organização, seja ela pública ou privada, espera-se que o administrador oriente suas decisões de investimentos adotando o princípio da racionalidade econômica, para tentar obter o máximo resultado com um dado montante de recursos ou minimizar este montante para obtenção de um determinado resultado.

O avanço da tecnologia revolucionou a estratégia de negócios das organizações privadas e públicas. Os gestores de TI assumiram responsabilidades e tarefas indispensáveis para o bom andamento dos trabalhos. O acesso a equipamentos de ponta, softwares e hardwares cada vez mais complexos e a heterogeneidade de fabricantes, aliado ao grande número de equipamentos, trouxe problemas que antes nem eram imagináveis.

Quando se fala em gestão de TI, logo vem o pensamento de que o assunto é caro, complexo e inviável. A falta de conhecimento, vontade de aprender e muitas vezes de reconhecimento dos superiores hierárquicos da organização que a TI hoje é fundamental para o sucesso do negócio, acabam mistificando negativamente a gerência de TI.

Uma das mais importantes ações para que uma organização seja competitiva no mercado é a diminuição dos custos e melhorias na qualidade do serviço prestado ou produto final. E isso só é satisfatoriamente possível se o ambiente de TI da organização for gerenciável.

Especificamente no setor público há uma enorme demanda em tornar o ambiente de TI, incluindo os equipamentos ativos e sistemas de informação, gerenciável. Para tanto é necessário adaptar os ativos já existentes utilizando de ferramentas e metodologias que já estão consolidadas no mercado e aperfeiçoar a especificação técnica dos equipamentos que certamente terão que ser substituídos futuramente por modelos mais modernos, garantindo que o vencedor da licitação entregue equipamentos capazes de atender as características de gerenciamento desejadas.

Os gestores de TI das organizações públicas enfrentam no seu dia a dia inúmeros problemas para implementar um ambiente gerenciável. Muitos desses gestores não atualizam seus conhecimentos no dinâmico mercado de soluções para a área, muitas vezes não por culpa deles, e sim por conta de uma instituição com visão ainda retrograda de que a TI, por não se tratar da atividade fim da instituição, não é importante concentrar investimentos em desenvolvimento, mas apenas na manutenção do que já existe. Outro problema existente, que é específico do setor público, é que além dos conhecimentos em tecnologia necessários para se fazer uma boa gestão o gestor necessita de conhecimentos sobre a legalidade dos processos de compra de uma organização pública e conhecer a fundo como se deve especificar um equipamento para que no final da licitação de aquisição seja fornecido um equipamento que realmente irá atender o esperado.

As conseqüências de um ambiente de TI não gerenciável afetam diretamente os gestores e indiretamente os outros servidores da instituição, prejudicando o desenvolvimento e resultados da área fim da instituição. Conseqüentemente, todos nós como integrantes de uma sociedade, seremos

prejudicados por não termos à disposição um serviço público ágil de qualidade e compatível com os altos impostos cobrados pelo governo.

Com as inúmeras ferramentas hoje disponíveis que são gratuitas, é possível implementar um ambiente com um bom nível de gerência sem a necessidade de altos investimentos em softwares proprietários, bastando possuir conhecimentos na área e disponibilidade de tempo, preparando o terreno para até mesmo a implementação de um sistema padronizado de governança da Tecnologia da Informação como o ITIL (*Information Technology Infrastructure Library)*.

É possível demonstrar, tomando como base um ambiente verídico de uma instituição pública pertencente ao poder Executivo, a Superintendência Regional de Polícia Federal no Paraná, que em um passado próximo não possuía nenhuma ferramenta de gerência, quais as principais ferramentas disponíveis implementadas que transformaram esse cenário em um ambiente mais confiável, seguro e consolidado, produzindo assim uma melhoria nos serviços disponíveis para todos os servidores e conseqüentemente uma melhoria significativa dos serviços prestados à sociedade.

O objetivo deste trabalho é demonstrar quais são as dificuldades encontradas pelos gestores de TI de uma organização pública em implementar ambientes gerenciáveis e quais as ações que pode-se tomar para minimizar essas dificuldades.

São objetivos específicos:

- Conhecer a demanda por gerência dos ativos de TI nas organizações públicas;

- Demonstrar as vantagens de se ter um ambiente de TI gerenciável e as dificuldades para sua implementação;

- Analisar algumas ferramentas e metodologias atualmente existentes no mercado;

- Demonstrar um estudo de caso de implementação de ambiente de TI gerenciado na Superintendência Regional de Polícia Federal no Paraná.

Para atender esses objetivos, o capítulo 2 aborda inicialmente a demanda por gerência dos ativos de TI nas organizações públicas, sendo feito um levantamento do histórico da TI no setor, como é feita a gestão de TI nas organizações e quais as perspectivas e diretrizes do governo federal em relação ao

desenvolvimento do assunto e a importância da TI no contexto das organizações públicas federais.

Em seguida, o capítulo 3 demonstra as principais vantagens de se ter um ambiente de TI gerenciável em um contexto geral, e no contexto específico das organizações públicas.

No capítulo 4 demonstram-se quais são as dificuldades de se implementar um ambiente gerenciável no contexto geral e específico do governo federal.

O capítulo 5 analisa quais as ferramentas e metodologias disponíveis hoje para se implementar ambientes de TI gerenciáveis e seus custos de implementação.

E por fim, o capítulo 6 demonstra um estudo de caso real de uma instituição publica federal do poder Executivo, a Superintendência Regional de Polícia Federal no Paraná, comprovando na pratica as melhorias e vantagens apontadas no desenvolvimento do trabalho.

A fonte de informações para desenvolver este trabalho, de natureza exploratória, é basicamente secundária e consiste em: pesquisas de diretivas do governo em relação à área de TI das organizações públicas, busca nos periódicos e livros de autores consagrados na área de TI informações sobre metodologias e ferramentas disponíveis, pesquisa de desenvolvedores de ferramentas livres de gerenciamento de TI buscando quais os benefícios práticos de cada uma delas e analisar os benefícios obtidos em um ambiente real onde foram implementadas as ferramentas e metodologias estudadas. Os conhecimentos adquiridos na pesquisa justificam e subsidiam a apresentação de um estudo de caso de implantação.

2 DEMANDA POR GERÊNCIA DOS ATIVOS DE TI

2.1 HISTÓRICO

Natal (2010, p.1) explana que por volta dos anos 70 as organizações de médio e grande porte possuíam equipamentos de grande porte físico para processamento centralizado de informações, e algumas unidades sem inteligência ou capacidade de processamento utilizados apenas para consulta. Tais ambientes eram quase sempre homogêneos em termos de fabricantes e fornecedores, o que tornava a resolução de problemas ou de interrupções mais fácil.

No final dos anos 80, houve mudanças muito significativas no cenário de TI, cresceu exponencialmente o número de unidades com processamento embarcado e o volume de equipamentos e informação, tornando suas interconexões bastante complexas. O ambiente passou a ser heterogêneo em termos de fabricantes e fornecedores, distribuído e com um alto grau de complexidade.

Quanto mais complexo o cenário mais suscetível a erros, problemas e interrupções ele se torna, e como o mercado passou a ficar cada vez mais dependente de recursos de TI, estava criada a demanda para se ter um ambiente gerenciável. Imediatamente diversos fabricantes e fornecedores surgiram com ferramentas que prometiam verdadeiros milagres, e então surgiu um novo problema, como integrar esse ambiente completamente heterogêneo com as diferentes ferramentas de diferentes fabricantes?

2.2 GESTÃO DA TI NO SETOR PÚBLICO

Com o avanço da TI no setor público, houve uma divisão histórica que demarcou uma era. O que anteriormente era moroso, burocrático e de difícil controle hoje se tornou fácil, rápido e confiável. Tudo isso graças à informatização dos processos. A desburocratização do setor público por conseqüência da TI gera incontestavelmente maior eficácia nas ações governamentais.

> Na gestão pública, a TI tem a mesma função das grandes organizações privadas, em algumas há consenso dos gestores que a TI deva ser centralizada, e em outras há consenso que deve ser descentralizada,

> dependendo das características de seus projetos e atividades. (CUNHA; MARQUES; MEIRELLES, 2002).

Segundo Bahiense e Nogueira (2002) na gestão de TI as instituições públicas podem ser segmentadas em três conglomerados de diferentes perfis, conforme sintetizado no Quadro 1:

PERFIL	CARACTERÍSTICA
Inovação	Baixa influência política, motivação, política de recursos humanos consistente, participação da TI no planejamento estratégico e da alta administração no planejamento de TI, maior ênfase na efetividade do que na eficiência dos processos, visão da TI como alavancadora de progresso e maior oferta de serviços eletrônicos.
Ação Burocrática	A burocracia é usada como escudo contra interferências políticas, ausência de planejamento de longo prazo, atitudes pró-ativas com relação política a recursos humanos, visão da TI como avanço e inovação, TI não é considerada estratégica e menor oferta de serviços digitais.
Inação	Apresenta distância de aspectos relevantes na construção de bases sólidas para avançar nos processo de gestão.

Quadro 1 - Perfis da TI nas Instituições Públicas
Fonte: Bahiense e Nogueira (2002, p. 13).

> Observa-se que os três segmentos não apresentam questões importantes para gestão de TI como gestão de custos, gestão de mudanças, recrutamento e conservação do capital intelectual e o papel de TI no redesenho de processos. No entanto, o segmento Ação Burocrática é o que apresenta maiores possibilidades de saltos qualitativos. (BAHIENSE; NOGUEIRA,, 2002).

Segundo Cunha, Marques e Meirelles (2002), na percepção dos executivos de TI da administração pública a política de TI na área pública deve ser alinhada ao plano de governo, obedecendo os critérios: formalização; estabelecimento de mecanismos de controle; acompanhamento e avaliação de custos e de seus projetos; busca da melhora da visão da TI para os gestores públicos; focar em resultados; construir e manter a infra- estrutura de TI do governo; formalizar a política de segurança física das informações e estabelecer uma política de recursos humanos, visando capacitar e reter os profissionais especializados.

2.3 IMPORTÂNCIA DA TI NAS ORGANIZAÇÕES PÚBLICAS

“A criação e a manutenção de uma infraestrutura de TI requerem investimentos que muitas vezes são questionados pela alta administração da empresa” (VIEIRA, 2005, p. 27).

Toda organização, seja ela pública ou privada, possui um consumidor final para o qual trabalha produzindo bens ou serviços. Nas organizações privadas este público é o consumidor, enquanto nas organizações públicas é o cidadão.

O recurso administrado nos dois casos é a informação. O uso da TI pelas organizações privadas visa explorar ao máximo os benefícios que a tecnologia pode oferecer para obter mais vantagem em relação à concorrência. Justificando assim os altos investimentos na área de TI. Os gestores de TI têm o papel de provar para os investidores que os gastos com TI não são gastos, e sim investimentos que no futuro se convertem em mais lucro.

Nas organizações públicas o ganho de competitividade não é vital para a sua continuidade, portanto a TI ganha um novo papel para elas. As organizações públicas dependem hoje da TI para a perpetuação de seus serviços. A TI melhorou e melhora a eficiência organizacional agilizando os processos, estrutura, a comunicação e eliminando grande parte da burocracia. O uso estratégico da TI nas organizações públicas pode e deve melhorar o atendimento da população e serviços prestados à sociedade.

Se o Estado não executar o seu papel em prestar serviços públicos de qualidade, certamente surgirão grupos organizados que trarão alternativas para prover a população de maneira mais eficiente, e conseqüentemente passando a ter forte domínio sobre a mesma, influenciando seus interesses. O que não é interessante para o governo.

Portanto, os gestores de TI das organizações públicas, devem focar não apenas o contexto interno da organização a que pertencem, mas também o contexto externo, que diferencia a qualidade dos serviços prestados à sociedade e assim contribuir para a atuação eficaz do poder público. Justificando assim os altos impostos que os cidadãos são obrigados a pagar.

Percebendo que os sistemas informatizados facilitam todo o processo, diminuindo o tempo de conclusão e aumentando a qualidade final, as organizações

públicas puderam, assim como as privadas, aumentar a produtividade e até mesmo suas competências, pois com a integração da informação hoje é possível oferecer mais serviços do que antigamente utilizando os mesmos recursos humanos.

Um exemplo prático disso é a emissão de documentos de passaporte. Hoje o processo de emissão de passaportes no Brasil é inteiro informatizado. Tal medida possibilitou aumentar a segurança quanto a fraudes e documentos falsificados, aumentar o controle de emissão destes documentos e principalmente possibilitou que fossem emitidos muito mais documentos com a mesma estrutura de pessoal.

Devido a essa grande dependência que o setor público tem hoje dos sistemas informatizados, o governo está preocupado em estabelecer diretrizes e normas para serem aplicadas nas organizações. Um exemplo disso é o portal de Governo Eletrônico (BRASIL, 2011), o qual tem como principio a utilização das modernas tecnologias de informação e comunicação para democratizar o acesso à informação, ampliar discussões e dinamizar a prestação dos serviços públicos como foco na eficiência e efetividade das funções governamentais.

Segundo o mesmo portal, a política de Governo Eletrônico segue um conjunto de diretrizes que atuam em três frentes fundamentais: junto ao cidadão; na melhoria da sua própria gestão interna; e na integração com parceiros e fornecedores.

O que o governo pretende com as políticas do Programa de Governo Eletrônico é: transformar as relações do Governo com os cidadãos, empresas e também entre os órgãos do próprio governo de forma a aprimorar a qualidade dos serviços prestados; promover a interação com empresas e indústrias; e fortalecer a participação cidadã por meio do acesso a informação e a uma administração mais eficiente.

3 VANTAGENS DE UM AMBIENTE DE TI GERENCIÁVEL

Existem diversas disciplinas para gerenciamento de TI disponíveis nas várias metodologias encontradas no mercado. Este trabalho elenca algumas delas que são tratadas na sequência como subsídio para o estudo de caso.

3.1 GERENCIAMENTO DE PROBLEMAS

> O gerenciamento de problemas busca identificar a causa raíz, propondo soluções para os problemas, eliminando problemas repetidos, acelerando o tempo de solução e gerando um banco de soluções. Os objetivos do Gerenciamento de Problemas incluem aumentar a qualidade da infra-estrutura de TI pela investigação das causas dos incidentes ou de potenciais incidentes, removendo-as de forma permanente e prevenindo pró ativamente novos incidentes. Uma vez que a causa de um problema é identificada e uma solução é estabelecida, um problema passa a ser denominado como um erro conhecido. (LEITE et al, 2005, p. 91).

Qualquer ambiente que depende de pessoas e máquinas pode apresentar problemas, pois são comuns erros de configuração dos sistemas, ataques de vírus na rede, equipamentos que apresentam defeito e reclamações dos usuários em relação ao desempenho dos sistemas. Grande parte desses problemas é de fácil solução, não demandam tempo ou conhecimentos específicos para solucioná-los, mas o que é difícil e requer conhecimento específico é identificar o problema.

Saber identificar onde está a origem de um problema é o primeiro e mais importante passo para solucioná-lo. Portanto, para que a TI atenda as necessidades da organização de maneira eficiente, é fundamental que o gestor de TI invista em métodos que diminuam o tempo de detecção e localização da origem dos problemas.

Uma grande vantagem que um ambiente de TI gerenciável proporciona é a capacidade de dispor ao gestor uma grande quantidade de informações como indicativos sobre o status, velocidade, configuração, etc dos equipamentos inseridos na rede. Tais informações se forem sabiamente interpretadas são de fundamental ajuda para a detecção precoce dos problemas e a origem deles.

3.2 GERENCIAMENTO DA CONTINUIDADE

> Em TI, a gerência da continuidade visa gerenciar o desastre, mantendo planos de contingência e de recuperação de desastres, sobrevivência do negócio, riscos e vulnerabilidades. Trata também das interrupções inesperadas nos serviços de TI, preparando e planejando medidas de recuperação e restauração dos serviços. (LEITE et al, 2005, p. 92).

Em uma situação critica, onde os serviços estão completamente parados e a pressão para que tudo se normalize é muito grande, cabe ao gestor manter a calma e se organizar de maneira que a solução do caos seja implementada o mais rapidamente possível. Para tanto é necessário um bom gerenciamento da situação, poder implementar possíveis soluções e rapidamente analisar os efeitos dela, o que só é possível em um ambiente de TI gerenciável.

3.3 GERENCIAMENTO DE LIBERAÇÃO

> O gerenciamento de liberação consiste em controlar a distribuição e o controle de liberação de software, de hardware e atualizações. Controlar todo o software e hardware existente na infra-estrutura de TI em produção e organiza a distribuição nos ambientes operacionais. Apenas software e hardware verificados, testados e aprovados pelo Gerenciamento de Liberações são distribuídos, garantido que as versões originais possam ser retomadas em caso de falhas. (LEITE et al, 2005, p. 92).

Em um ambiente de TI gerenciável é possível realizar auditorias nos equipamentos sem a necessidade de se deslocar a até eles, concentrando todas as informações em um único local, podendo assim verificar quais os softwares instalados nas estações, versões de softwares e licenças de uso. Podendo gerar eventos que destaquem ao gestor as situações atípicas ao esperado para que possam ser rapidamente corrigidas.

3.4 GERENCIAMENTO DE DISPONIBILIDADE

> O gerenciamento de disponibilidade gerência o presente, otimiza a cadeia de prestação de serviço e acompanha o negócio. Identifica, define e prepara

> as medidas necessárias para garantir a disponibilidade requerida pelos serviços, monitorando a confiabilidade e a disponibilidade nas falhas e interrupções e recomenda mudanças para prevenir futuras perdas na qualidade dos serviços. (LEITE et al, 2005, p. 92).

Em um ambiente gerenciável é possível auditar quais, quando e onde foram os eventos que causaram indisponibilidade dos serviços, é possível controlar se os serviços fornecidos por uma determinada operadora de telecomunicações estão de acordo com o contratado, podendo o gestor dispor de dados técnicos confiáveis para argumentar com os fornecedores em casos de não conformidades.

3.5 GERENCIAMENTO FINANCEIRO

> O gerenciamento financeiro gerência os custos efetivos, a alocação dos recursos financeiros e o retorno do investimento. Realiza a correta provisão orçamentária dos serviços de TI, fazendo uma consideração entre custos envolvidos e possíveis benefícios nos investimentos, em especial nas tomadas de decisões a respeito de mudanças no ambiente. (LEITE et al, 2005, p. 92).

Uma das grandes dificuldades em um ambiente de TI é o correto dimensionamento dos serviços e capacidades dos equipamentos. Como atualmente esses parâmetros são os principais para a definição do custo envolvido é fundamental que sejam bem especificados, para que não gerem custos desnecessários e comprometam todo o negócio ou não fiquem aquém do que realmente se necessita.

É comum em organizações públicas ouvir reclamações que a velocidade dos sistemas não está boa, que é necessário aumentar a banda de comunicação entre as localidades ou que há congestionamento no canal de comunicação de dados com a Internet. Fatos todos que são facilmente verificados em um ambiente gerenciável, disponibilizando dados estatísticos precisos em relação à taxa de ocupação de um canal de comunicação, seja externo ou interno. Indicando onde realmente estão ocorrendo congestionamentos das informações possibilitando ao gestor tomar a decisão mais eficiente e econômica.

4 DIFICULDADES EM SE TER UM AMBIENTE DE TI GERENCIÁVEL EM ORGÃOS PÚBLICOS

> Em algum momento no passado a TI perdeu a importância no governo federal, ficou sem técnicos ou com técnicos antigos e desatualizados, equipamentos obsoletos, sistemas antigos e rede de comunicação de dados ultrapassada; ficou sem planejamento estratégico e sem cumprir com o dever com as obrigações perante os usuários. Ou seja, perdeu o respeito. (PINTO, 2009 p. 1.)

Pinto (2009, p. 1) ainda destaca que por volta de 1997, atitudes do próprio governo federal desencadearam na desintegração da TI, na época o presidente Fernando Henrique Cardoso publicou o decreto n° 2.271, artigo1°, parágrafo 1°, que as atividades de “limpeza [...], transportes, informática, copeiragem, recepção, telecomunicações e manutenção predial [...] serão, de preferência, objeto de execução indireta”. Ou seja, a TI erroneamente se enquadrou em algo entre dirigir um carro e servir um cafezinho.

Vários órgãos do poder executivo implementaram as recomendações do decreto ao pé da letra, e transferiram áreas inteiras (pessoal, equipamentos, sistema e gerência) para empresas terceirizadas.

Somente em 2009 o governo se deu conta que algo precisava ser feito urgente para tentar reverter a situação. O Tribunal de Contas da União então publicou a Instrução Normativa n°4. Em 11 páginas ela instrui os serviços de TI de acordo com o planejamento estratégico do órgão, obrigando cada instituição a elaborar seu planejamento. Entre outras obrigações estão a constituição de uma comissão de TI que é responsável por analisar a viabilidade dos contratos, estabelecer planos de transferência do conhecimento dos contratados para os técnicos internos, analisar os riscos e gerenciar os contratos.

Os executivos de TI começaram então a tomar providências para se adaptarem à instrução normativa n°4, uns mais devagar outros mais depressa. Diante da realidade que a maioria, cerca de 60%, dos servidores da área de TI não possuía formação na área, eram apenas servidores públicos que passaram no concurso há anos e não se atualizaram, passou-se a contratar novos servidores específicos para a área de TI, exigindo formação na área e elaborando concursos

específicos, trazendo assim conhecimentos que antes estavam restritos às iniciativas privadas para dentro das instituições governamentais.

Atualmente ainda é pouco o número de servidores concursados que trabalham na área de TI nas instituições públicas. Muitas delas, para suprir as necessidades básicas dos usuários, recorrem à contratação de técnicos terceirizados para executar os serviços do dia a dia deixando assim as tarefas de gerenciamento dos sistemas e planejamento estratégico com os concursados.

Outra dificuldade que os gestores de TI encontram é que a maioria dos órgãos públicos não têm como foco, atividade fim, algo relacionado com tecnologia, sendo assim os administradores e ordenadores de despesas, por não enxergarem a TI como fundamental para a prestação dos serviços que o órgão se destina , muitas vezes não se preocupam em investir na área. Muitos projetos da área de TI são inteiramente ou parcialmente cortados por conta dos altos investimentos necessários, levando o administrador e gestor de despesas a optar em investir o montante financeiro em outros projetos que a primeira vista aparentam ter mais afinidade com a área fim do órgão.

As tarefas de gerenciamento e planejamento estratégico de TI dentro de um setor público exigem conhecimentos que vão além dos ministrados nas escolas técnicas e faculdades da área, é necessário possuir sólidos conhecimentos em legislação e especificamente na lei de licitações. É necessário também saber elaborar os editais de maneira que as especificações técnicas não sejam extremamente restritivas a um fornecedor ou fabricante para que seja garantida a concorrência entre eles, mas que também não seja muito ampla de modo que fornecedores e fabricantes incapazes de entregar o mínimo de qualidade saiam vencedores do certame por apresentar o menor preço.

Existem maneiras simples de um gestor de TI amenizar esses problemas, e a base disso está na capacitação e motivação dos envolvidos. É necessário promover ações de capacitação freqüentes não só em áreas específicas de TI, mas também nas áreas de licitação e legislação. Cabe a um bom gestor de TI conseguir demonstrar aos administradores e ordenadores de despesa que todo e qualquer processo existente dentro de uma repartição pública, em algum momento, é dependente da TI, e que a falta de investimentos e modernização na área coloca em risco toda a atividade governamental à qual o órgão se presta.

5 FERRAMENTAS E METODOLOGIAS DISPONÍVEIS

Existem várias ferramentas no mercado que se propõem a ajudar os gestores de TI a gerenciar seus ativos, onde uma tarefa difícil é escolher qual a melhor ferramenta utilizar. Com a grande diversidade de fabricantes e fornecedores de equipamentos fica impossível dispor de uma única ferramenta que gerencie tudo e da maneira que o gestor necessita.

Primeiramente é fundamental que o gestor seja uma pessoa que possua conhecimento técnico específico na área de atuação e esteja alinhado com o planejamento estratégico da organização, para saber o que monitorar e o que fazer com as informações que as ferramentas produzem. As ferramentas não são a solução dos problemas e sim uma parcela da solução, de maneira que é fundamental o conhecimento aliado às ferramentas para que o resultado seja efetivamente uma solução. O processo de gerenciamento de TI não termina nunca, é uma tarefa contínua. A tecnologia está sempre evoluindo, novos problemas vão surgir e com eles novas soluções. Por isso a análise dos dados deve ser feita por gerentes dedicados e não por profissionais compartilhados e sem experiência.

Não existe uma receita pronta que contenha as ferramentas que solucionem todos os problemas de qualquer organização. Cada uma possui sua estratégia de negócio, seu parque de equipamentos e sua estrutura de TI e o seu orçamento, e o que é essencial gerenciar em uma pode ser supérfluo para outra.

No universo de gerenciamento de TI há vários problemas que são comuns para qualquer organização. Saber a taxa de ocupação dos circuitos de dados, qual a banda consumida pelos servidores e estações de trabalho, saber quais servidores e estações necessitam de um melhor dimensionamento de recursos de hardware, informações sobre os softwares instalados, saber o conteúdo que está sendo acessado pelas estações de trabalho, quais ações devem ser implementadas para melhor atender o cliente, etc, são todas informações úteis que certamente auxiliam na tomada de decisões, correção de falhas e direcionamento dos investimentos.

Extraídas de um universo amplo de protocolos, soluções e ferramentas, as que foram utilizadas no estudo de caso são abordadas na sequência.

5.1 SNMP (*SIMPLE NETWORK MANAGEMENT PROTOCOL*)

> No Ambiente de Protocolos TCP/IP o modelo de informação de gerência é mais simples que no Modelo de Referência OSI. A construção das MIBs obedece as especificações contidas nos documentos denominados SMI que foram padronizados pelas RFCs 1155 e 1212 para a versão 1 do SNMP e, mais recentemente, pela RFC 1902 (substituída pela RFC 2578) para o SNMPv2. Estas especificações impõem um alto grau de simplicidade na descrição das MIBs para tornar o processo de gerência de fácil implementação. (RECH FILHO, 1996, p. 35).

O protocolo SNMP (Simple Network Management Protocol) foi desenvolvido pelo IETF (*Internet Engineering Task Force)*, com o objetivo de ser um protocolo simples que permitisse a gestão nos ativos de redes.

Inicialmente, o protocolo SNMP versão 1 era muito limitado para satisfazer todas as necessidades de gestão de ativos de rede, posteriormente foram surgindo novas versões com novas funcionalidades. Atualmente o SNMP tornou-se indispensável na gestão de redes, haja vista o grande aumento no número de MIBs (*Management Information Base*) existentes e a disseminação do seu uso nos equipamentos.

Este protocolo tem como objetivo a flexibilidade e a facilidade de implementação, pensando também nos produtos futuros. Sua especificação está contida na RFC 1157.

Segundo Dias e Alves (2001, p. 11) o SNMP é um protocolo de gerência que trabalha na camada de aplicação, é utilizado para obter informações de agentes espalhados em uma rede TCP/IP. Os dados são obtidos mediante requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP (*User Datagram Protocol*)para enviar e receber suas mensagens através da rede. As variáveis que podem ser requisitadas sempre fazem parte da MIB que vem de fábrica implementada nos equipamentos ou nos ambiente operacionais.

MIB (*Management Information Base*) é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede, possibilitando assim, a automatização de grande parte das tarefas de gerência.

O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil dos parâmetros da rede em tempo real, podendo ser utilizado para coletar informações e gerenciar diferentes tipos de sistemas.

Os comandos disponíveis nesse protocolo são limitados e baseados no mecanismo de leitura/escrita. Isso torna o SNMP um protocolo de fácil implementação, simples, estável e flexível. Conseqüentemente reduz o tráfego de mensagens de gerenciamento através da rede e permite a introdução de novas funcionalidades.

O funcionamento do SNMP é baseado em dois dispositivos: o agente e o gerente. Cada equipamento gerenciado é visto como um conjunto de variáveis que representam informações referentes ao seu estado atual, estas informações ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

5.2 WMI (*WINDOWS MANAGEMENT INSTRUMENTATION*)

Segundo Rocha (2011, p. 1) O *Windows Management System*, ou simplesmente WMI, é uma das tecnologias introduzidas pela Microsoft para suportar o gerenciamento de sistemas corporativos. Ela é fruto de um esforço entre companhias de computação interessadas em desenvolver uma camada de software padronizada para gerenciamento corporativo de sistemas e de dispositivos, cuja iniciativa foi denominada WBEM, sigla para *Web Based Enterprise Management* (Gerenciamento Corporativo Baseado na WEB). O objetivo era desenvolver um único conjunto de padrões para gerenciar qualquer componente de uma rede corporativa. Dessa forma, futuramente as companhias desenvolveriam hardware, software e sistemas que pudessem ser gerenciados da mesma maneira, através da adoção do padrão WBEM. A responsabilidade pela iniciativa WBEM foi assumida pela organização DTMF (*Distributed Management Task Force*), que é responsável em manter os padrões que irão ajudar a atingir os objetivos da iniciativa WBEM.

> Além de definir normas de gestão, o DMTF também desenvolve programas de conformidade para promover a interoperabilidade entre os produtos de gerenciamento que suportam padrões DMTF. Basicamente os programas do DMTF realizam testes padrões com o intuito de habilitar os produtos dos fornecedores de TI a interagir perfeitamente com produtos de fabricantes distintos. A implantação de soluções interoperáveis de gestão que atendam

> os padrões DMTF, permite aos administradores simplificar o gerenciamento de seus ambientes de TI. (DMTF, 2011).

Portanto, a camada WMI é uma implementação da iniciativa WBEM para os sistemas operacionais Windows e permite aos desenvolvedores usar um mecanismo simples e consistente para pesquisar informações ou parâmetros de configuração em computadores dentro de uma empresa ou corporação. A quantidade de informação disponível através da interface WMI é imensa – configurações de hardware, informações de desempenho, configuração de *drivers*, informações sobre a BIOS, configurações de aplicações, informações de log de eventos, e muito mais. A interface WMI recupera essas informações utilizando vários conjuntos de APIs (*Application Programming Interfaces*), mas apresenta essas informações seguindo um modelo de gerenciamento de objetos simples e padronizado. Isto torna desnecessário aos desenvolvedores de aplicação aprender os detalhes de cada API fornecida pelo Windows.

5.3 MRTG (*MULTI ROUTER TRAFFIC GRAPHER*)

5.3.1 O que é:

De acordo com Oetiker (2011), o MRTG é uma ferramenta de monitoramento do tráfego de dados nos circuitos de dados. Ele é capaz de monitorar o volume de dados de uma interface em tempo real, gerando páginas em HTML (*Hyper Text Markup Language*) contendo figuras com os gráficos do volume de dados trafegados em função do tempo.

A ferramenta MRTG não tem custos e está disponível através dos termos da Licença Geral Pública (GNU), ou seja, pode-se fazer o que quiser com ela desde que os créditos sejam do criador da ferramenta.

No ano de 1994 o criador do MRTG Tobias Oetiker estava trabalhando em site que tinha um *link* de dados de saída para o mundo de 64Kbps e surgiu a necessidade de saber como o *link* estava se comportando, foi então que Tobias escreveu um rápido programa que atualizava um gráfico na WEB que mostrava o volume de tráfego deste *link*. Rapidamente a idéia evoluiu para um programa configurável que hoje é utilizado pelo mundo inteiro.

O MRTG então surgiu com o principal intuito de monitorar o tráfego nos circuitos de dados, sejam eles nos roteadores ou switches. É muito útil para analisar a taxa de ocupação de um circuito de dados em função do tempo. Com ele é possível descobrir se congestionamentos no canal de comunicação estão ocorrendo e em quais horários ocorrem, aferir se a banda fornecida pela operadora está de acordo com o contratado e fornece dados concretos para argumentar com os usuários remotos que sempre alegam que seus sistemas estão lentos devido a congestionamentos nos circuitos de comunicação.

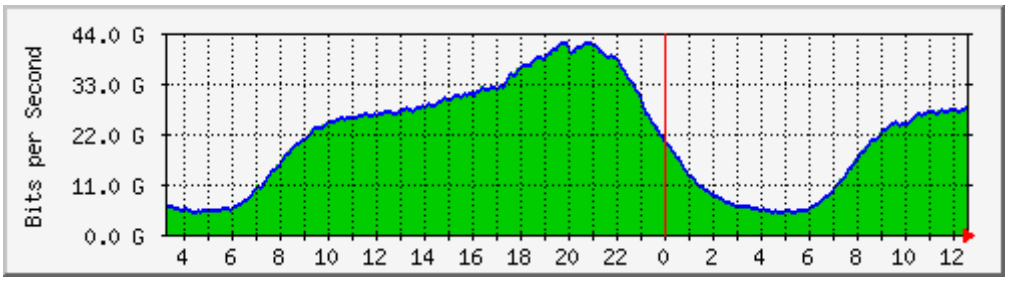
5.3.2 Funcionamento:

Atualmente os equipamentos responsáveis por encaminhar os pacotes de dados, switches, roteadores, placas de rede, etc. possuem implementados em seus *firmares* um agente que troca informações através do protocolo de gerenciamento SNMP, que está amplamente difundido e tornou-se padrão em equipamentos de redes. Um dos parâmetros contidos na MIB dos equipamentos que é lido pelo gerente MRTG é um contador de bytes. Esse contador está sempre atualizado com o número de bytes que trafegaram pela interface. O MRTG nada mais é que um programa escrito em *Perl* que lê esses contadores de bytes que já estão implementados nos equipamentos e, através da diferença numérica do contador entre duas leituras consecutivas, disponibiliza em um formato gráfico bastante amigável a taxa de bits ou bytes trafegados naquela interface naquele determinado espaço de tempo. Fazendo disso uma rotina constante e com um intervalo de tempo pequeno, é possível criar gráficos diários e com bastante resolução da taxa de dados da interface. Por padrão, ele já cria gráficos diários, semanais, mensais e anuais. Fornecendo assim informações estatísticas a respeito do volume de dados da interface bastante confiáveis e precisos.

Como o MRTG trabalha baseado em um esquema de gerente e agente onde as informações da MIB são lidas através do protocolo SNMP, qualquer equipamento que possua um agente SNMP poderá ser gerenciado pelo MRTG, com isso ele pode não só monitorar o tráfego de pacotes, mas também qualquer outro parâmetro contido na MIB como por exemplo: espaço em disco, nível de processamento, etc.

Exemplos de gráficos são mostrados nas figuras 1 a 4.

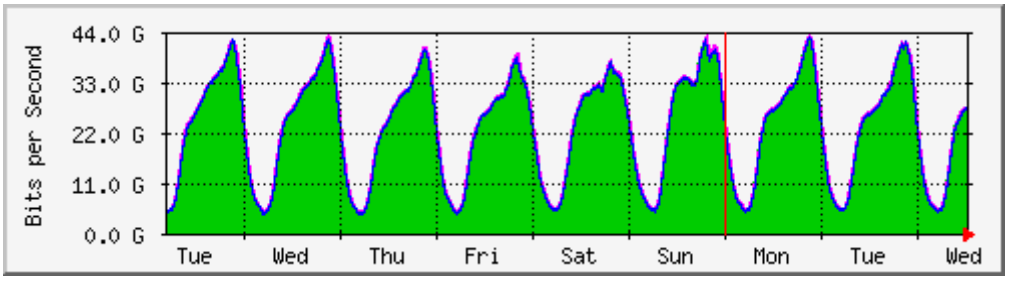
Gráfico diário



	Max	Average	Current
In	41.9 Gb/s	21.0 Gb/s	27.5 Gb/s
Out	41.8 Gb/s	21.0 Gb/s	27.4 Gb/s

Figura 1 – Exemplo de gráfico diário gerado pelo MRTG 3
Fonte: SIX (2011)

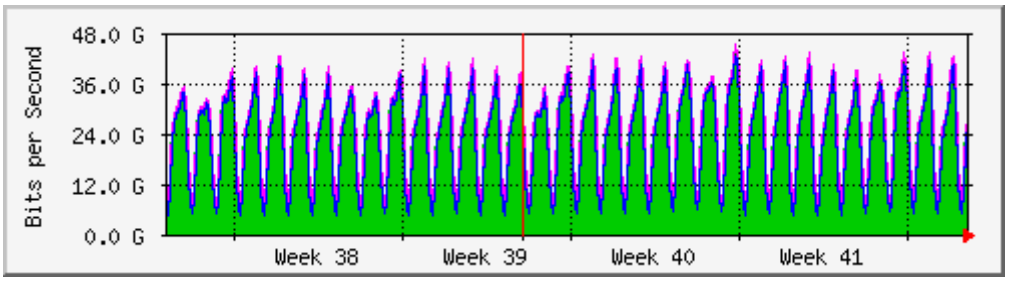
Gráfico semanal



	Max	Average	Current
In	43.2 Gb/s	22.9 Gb/s	27.1 Gb/s
Out	43.0 Gb/s	22.9 Gb/s	27.0 Gb/s

Figura 2 – Exemplo de gráfico semanal gerado pelo MRTG
Fonte: SIX (2011)

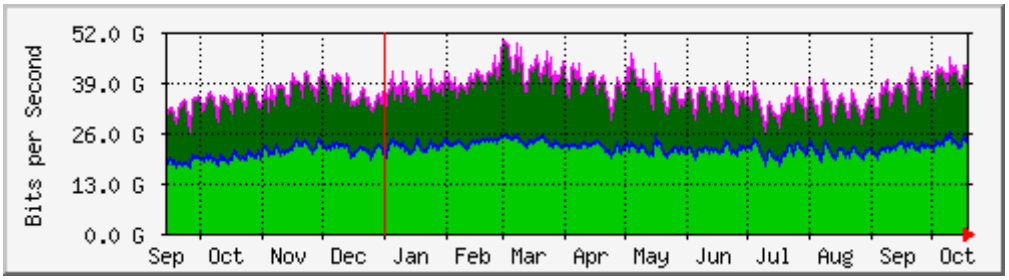
Gráfico mensal



	Max	Average	Current
In	44.9 Gb/s	22.7 Gb/s	26.3 Gb/s
Out	44.8 Gb/s	22.7 Gb/s	26.2 Gb/s

Figura 3 - Exemplo de gráfico mensal gerado pelo MRTG
Fonte: SIX (2011)

Gráfico anual



	Max	Average	Current
In	49.1 Gb/s	21.6 Gb/s	23.2 Gb/s
Out	49.3 Gb/s	21.6 Gb/s	23.1 Gb/s

Figura 4 - Exemplo de gráfico anual gerado pelo MRTG
Fonte: SIX (2011)

5.3.3 Requisitos:

A instalação da ferramenta MRTG não necessita de requisitos de hardware avançados, e o que determina o desempenho da ferramenta é o número de interfaces a ser monitorada. Quanto mais interfaces forem monitoradas mais tempo leva para enviar e receber os pacotes SNMP de cada uma, de maneira que é importante o gestor prever que o tempo de atualização dos gráficos, que é configurado por padrão em 5 minutos, deve ser maior que o tempo gasto para enviar e receber os pacotes SNMP de cada interface, ou seja, o tempo gasto para ler os dados de todas as interfaces deve ser menor que o tempo de atualização dos gráficos, senão haverá interfaces que nunca serão atualizadas.

Apesar de ser desenvolvido inicialmente para sistemas Linux o MRTG pode ser instalado também em sistemas Windows, de maneira que em ambos é necessário instalar os pacotes PERL de acordo com a versão do sistema operacional.

A configuração é igual para ambos os sistemas, há um comando disponível no próprio pacote da ferramenta, o *cfgmaker,* que monta o arquivo de configuração e os arquivos HTML automaticamente a partir do endereço IP dos equipamentos. É recomendado instalar também um servidor WEB, para que os gráficos possam ser acessados a partir de outros terminais.

A ferramenta MRTG é considerada de fácil implementação, pois além de ser uma ferramenta de uso gratuito, possui grande documentação e tutoriais disponíveis

para consulta. O MRTG pode ser obtido gratuitamente em seu site oficial: http://oss.oetiker.ch/mrtg/

5.4 BANDWIDTHD

5.4.1 O que é:

Segundo o site oficial o BANDWIDTHD é uma ferramenta utilizada para monitorar todos os pacotes que trafegam em uma rede. Programado por David Hinkle é uma ferramenta de livre distribuição através dos termos da GNU. Essa ferramenta captura todos os pacotes que trafegam em uma rede de dados, gerando gráficos no formato HTML mostrando a utilização da banda e classificando pelos tipos de pacotes: TCP, UDP, HTTP, FTP, etc. Os gráficos são construídos separando a utilização da banda de cada endereço IP. É possível armazenar os dados monitorados em um banco de dados para se ter um histórico de utilização. Pode-se variar o intervalo de tempo de monitoramento e dividir o tráfego de acordo com o tipo por cores, inclusive o tráfego P2P (BANDWIDTHD, 2011).

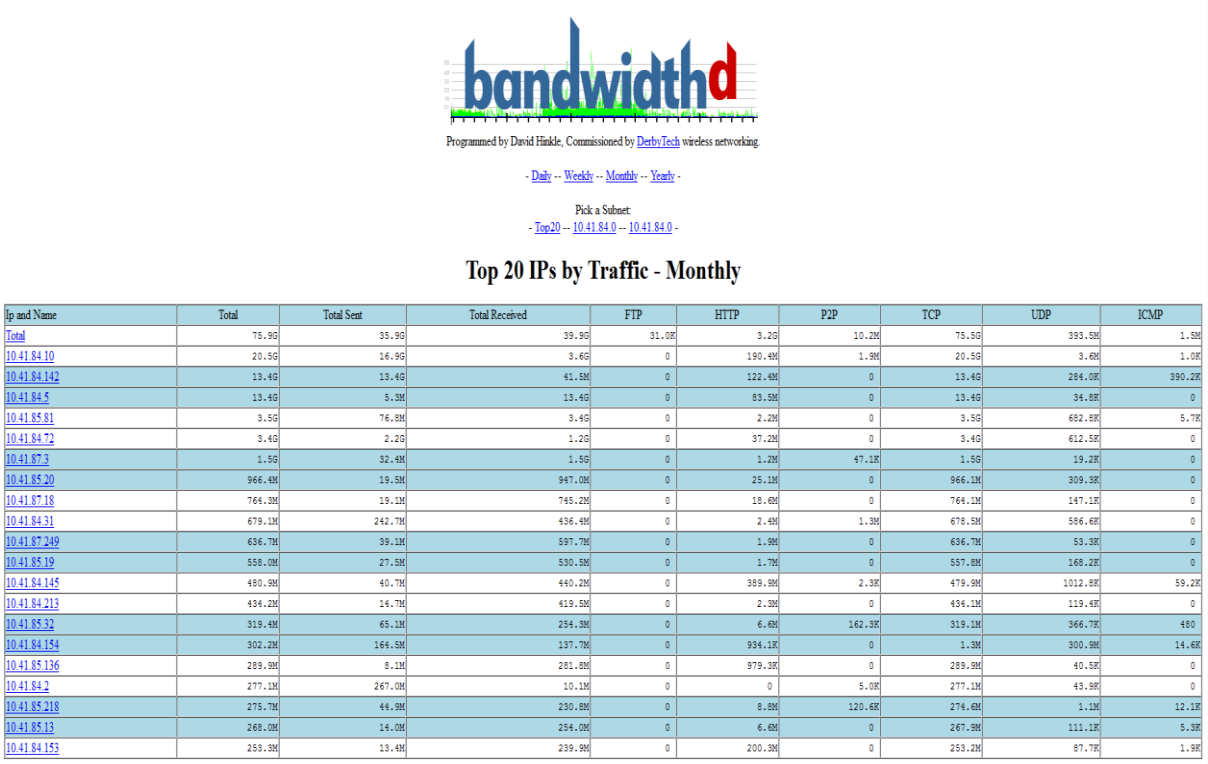
Com isso é possível detectar quais os terminais que estão consumindo a banda disponível e com qual tipo de serviço, fornecendo subsídios para o gestor de TI auditar se os equipamentos que estão consumindo a banda realmente deveriam consumir e direcionar os recursos para melhorar a disponibilidade do circuito de dados para equipamentos que são essenciais para o funcionamento da organização. Verificar a quantidade de pacotes de um determinado tipo, por exemplo o UDP, que se estiver em quantidades muito elevadas podem ser indícios de que a rede está sofrendo ataques de vírus.

5.4.2 Funcionamento:

A ferramenta *BANDWIDTHD* funciona coletando os pacotes que circulam em uma rede de dados. Para tanto é necessário que o computador onde rodar o *BANDWIDTHD* esteja fisicamente conectado em um ponto da rede para o qual seja possível desviar todos os pacotes do circuito de dados que se deseja monitorar. O

mais comum nas organizações é monitorar o consumo do circuito de dados que provê os serviços de Internet e circuitos que interligam as unidades. Esse ponto da rede deve funcionar como um *sniffer, e* o mais comum é utilizar uma porta do switch espelhada da porta onde o circuito a ser monitorado está conectado. É fundamental que a placa de rede conectada ao computador que faz o monitoramento esteja configurada em modo promíscuo.

Com a interface de rede do computador fisicamente conectada em um ponto onde todos os pacotes do circuito monitorado estejam trafegando, juntamente com a configuração da placa de rede em modo promíscuo, o *BANDWIDTHD* coleta todos os pacotes e os separa de acordo com o endereço IP de origem. Detalhando o tráfego de cada IP pelo tipo de pacote. Armazenando essas informações e em conjunto com um servidor WEB é possível realizar as consultas filtrando pelas informações de interesse do gestor. A própria ferramenta cria páginas em HTML com os resultados, criando uma interface com o gestor bastante amigável de fácil entendimento. Um exemplo de tela com informações é mostrado na figura 5.



Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	P2P	TCP	UDP	ICMP
Total	75.9G	35.9G	39.9G	31.0K	3.2G	10.2M	75.5G	393.5M	1.5M
10.41.84.10	20.5G	16.9G	3.6G	0	190.4M	1.9M	20.5G	3.6M	1.0K
10.41.84.142	13.4G	13.4G	41.5M	0	122.4M	0	13.4G	284.0K	390.2K
10.41.84.5	13.4G	5.3M	13.4G	0	83.5M	0	13.4G	34.8K	0
10.41.85.81	3.5G	76.8M	3.4G	0	2.2M	0	3.5G	682.8K	5.7K
10.41.84.72	3.4G	2.2G	1.2G	0	37.2M	0	3.4G	612.5K	0
10.41.87.3	1.5G	32.4M	1.5G	0	1.2M	47.1K	1.5G	19.2K	0
10.41.85.20	966.4M	19.5M	947.0M	0	25.1M	0	966.1M	309.3K	0
10.41.87.18	766.3M	19.1M	745.2M	0	18.6M	0	766.1M	147.1K	0
10.41.84.31	679.1M	242.7M	436.4M	0	2.4M	1.3M	678.5M	586.6K	0
10.41.87.249	636.7M	39.1M	597.7M	0	1.9M	0	636.7M	53.3K	0
10.41.85.19	558.0M	27.5M	530.5M	0	1.7M	0	557.8M	168.2K	0
10.41.84.145	480.9M	40.7M	440.2M	0	389.9M	2.3K	479.9M	1012.8K	59.2K
10.41.84.213	436.2M	14.7M	419.5M	0	2.3M	0	436.1M	119.4K	0
10.41.85.32	319.4M	65.1M	254.3M	0	6.6M	162.3K	319.1M	366.7K	480
10.41.84.154	302.2M	164.5M	137.7M	0	934.1K	0	1.3M	300.9M	14.6K
10.41.85.136	289.9M	8.1M	281.8M	0	979.3K	0	289.9M	40.5K	0
10.41.84.2	277.1M	267.0M	10.1M	0	0	5.0K	277.1M	43.9K	0
10.41.85.218	275.7M	44.9M	230.8M	0	8.8M	120.6K	274.6M	1.1M	12.1K
10.41.85.13	268.0M	14.0M	254.0M	0	6.6M	0	267.9M	111.1K	5.8K
10.41.84.153	253.3M	13.4M	239.9M	0	200.5M	0	253.2M	87.7K	1.9K

Figura 5 - Exemplo de gráfico mensal gerado pelo *BANDWIDTHD*

5.4.3 Requisitos:

Assim como a ferramenta MRTG o *BANDWIDTHD* não necessita de requisitos de hardware avançados, e o seu desempenho depende do volume de tráfego a ser monitorado. Quanto mais volume de dados e mais endereços IP houver na rede, mais demanda de processamento a ferramenta exigirá.

O *BANDWIDTHD* é escrito em linguagem C e PHP, pode ser instalado em vários sistemas operacionais inclusive Windows.

A configuração do *BANDWIDTHD* é feita alterando os parâmetros do arquivo de configuração bandwidthd.conf.

A ferramenta *BANDWIDTHD* é classificada como sendo de média dificuldade de implementação, pois apesar de ser uma ferramenta gratuita que possui muita documentação disponível para ajudar na implementação, necessita que o gestor faça uma modificação simples no ponto lógico da rede onde a interface de rede será conectada para que ela possa capturar todos os pacotes. Tal modificação requer conhecimentos na arquitetura da rede e configurações dos switches envolvidos no processo. A ferramenta *BANDWIDTHD* pode ser obtida gratuitamente através de seu site oficial: http://bandwidthd.sourceforge.net/

5.5 NTOP

5.5.1 O que é:

De acordo com o site oficial do NTop, a ferramenta NTop começou como um projeto *open source* em 1998, cujo objetivo era criar uma ferramenta simples e eficaz baseada na plataforma WEB para monitorar o tráfego de pacotes em uma rede. Desde então muita coisa evoluiu, como os sistemas operacionais e a natureza do tráfego, e junto com isso a ferramenta NTop também evoluiu para acompanhar as mudanças e inovações tecnológicas (NTop, 2011).

O NTop é um programa de código-fonte aberto, escrito em linguagem C, que tem por finalidade monitorar a utilização de uma rede de dados, permitindo identificar as atividades de rede, estabelecimento de conexões, o uso de protocolos de rede e classificação do tráfego. Ele é capaz de gerar dados estatísticos

destacando o desempenho da rede local, qual terminal está consumindo a maior parte da banda, quais terminais estão consumindo recursos dos servidores, a porcentagem de banda que cada estação consome, quais estações produzem tráfego *multicast*, etc.

Todas essas informações são disponibilizadas em um ambiente WEB amigável e de fácil entendimento, ajudando a tornar o trabalho dos gestores de TI mais rápido e eficiente.

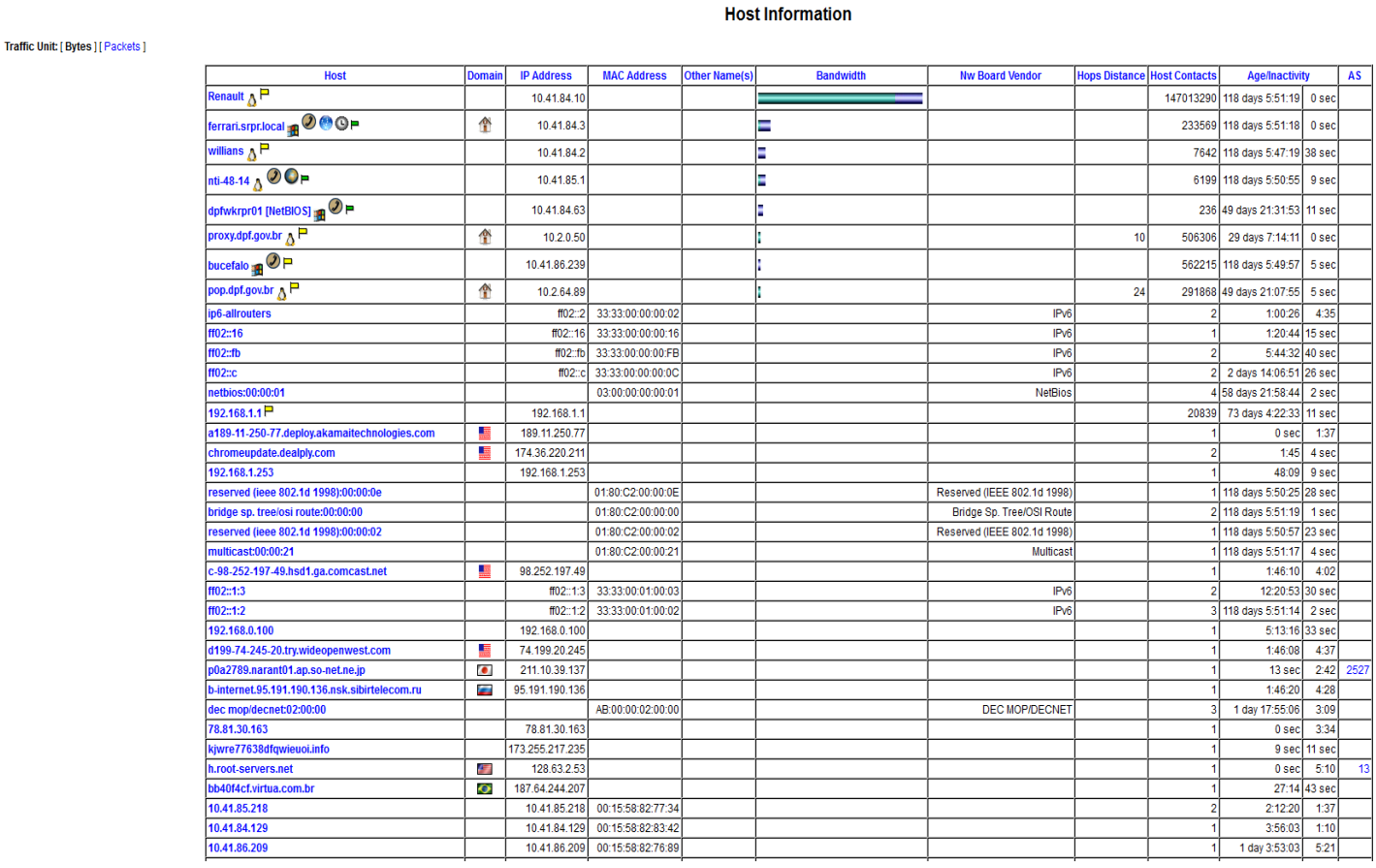
5.5.2 Funcionamento:

Tal como a ferramenta *BANDWIDTHD* o NTop funciona coletando os pacotes que circulam em uma rede de dados. Para tanto é necessário que o computador no qual rodar o *NTop* esteja fisicamente conectado em um ponto da rede para o qual seja possível desviar todos os pacotes do circuito de dados que se deseja monitorar. Esse ponto da rede deve funcionar como um *sniffer,* o mais comum é utilizar uma porta do switch espelhada da porta onde o circuito a ser monitorado está conectado. É fundamental que a placa de rede conectada ao computador que faz o monitoramento esteja configurada em modo promíscuo.

De acordo com Roncero, Albuquerque e Albuquerque (2002), após os pacotes serem coletados eles são analisados por um analisador de pacotes implementado dentro da própria ferramenta. O analisador de pacote processa cada pacote individualmente. Os cabeçalhos dos pacotes são analisados de acordo com a interface de rede que está sendo usada, pois os cabeçalhos são diferentes dependendo da interface de rede. As informações sobre as estações são armazenadas em uma tabela *hash* cuja chave é MAC (Controle de Acesso ao Meio) que garante sua singularidade e permite que diferentes protocolos de rede sejam controlados. Cada entrada possui contadores que armazenam a quantidade de dados enviados e recebidos pelo terminal, classificados de acordo com os protocolos de rede suportados. Para cada pacote, a entrada *hash* corresponde à fonte e destino do pacote, e ela é atualizada em casos onde já existe ou criada se ainda não existir. Como não é possível estimar o número de terminais distintos cujos pacotes serão controlados através do NTop, é praticamente impossível dispor de uma tabela *hash* grande o suficiente para armazenar todas os possíveis terminais. Sendo assim, quando necessário o NTop elimina a tabela de terminais para evitar

uma utilização de toda memória disponível e a criação de enormes tabelas que diminuem o desempenho da ferramenta. As entradas eliminadas correspondem a terminais que não possuem dados enviados ou recebidos por um longo período de tempo. Isto garante que a utilização da memória e o tempo de processamento do pacote não aumentem indefinidamente. Se o pacote recebido for um pacote não IP, os contadores de entrada de protocolo são atualizados e o pacote é descartado. Se o pacote recebido for um pacote IP, então o processamento é executado.

A figura 6 mostra um exemplo de gráfico do NTop.



Host Information

Traffic Unit: [Bytes] [Packets]

Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth	Nw Board Vendor	Hops Distance	Host Contacts	Age/Inactivity		AS
Renault		10.41.84.10						147013290	118 days 5:51:19	0 sec	
ferrari.srpr.local		10.41.84.3						233569	118 days 5:51:18	0 sec	
willians		10.41.84.2						7642	118 days 5:47:19	38 sec	
nti-48-14		10.41.85.1						6199	118 days 5:50:55	9 sec	
dpfwkrpr01 [NetBIOS]		10.41.84.63						236	49 days 21:31:53	11 sec	
proxy.dpf.gov.br		10.2.0.50					10	506306	29 days 7:14:11	0 sec	
bucefalo		10.41.86.239						562215	118 days 5:49:57	5 sec	
pop.dpf.gov.br		10.2.64.89					24	291868	49 days 21:07:55	5 sec	
ip6-allrouters		ff02::2	33:33:00:00:00:02			IPv6		2	1:00:26	4:35	
ff02::16		ff02::16	33:33:00:00:00:16			IPv6		1	1:20:44	15 sec	
ff02::fb		ff02::fb	33:33:00:00:00:FB			IPv6		2	5:44:32	40 sec	
ff02::c		ff02::c	33:33:00:00:00:0C			IPv6		2	2 days 14:06:51	26 sec	
netbios:00:00:01			03:00:00:00:00:01			NetBios		4	58 days 21:58:44	2 sec	
192.168.1.1		192.168.1.1						20839	73 days 4:22:33	11 sec	
a189-11-250-77.deploy.akamaitechnologies.com		189.11.250.77						1	0 sec	1:37	
chromeupdate.dealply.com		174.36.220.211						2	1:45	4 sec	
192.168.1.253		192.168.1.253						1	48:09	9 sec	
reserved (ieee 802.1d 1998):00:00:0e			01:80:C2:00:00:0E			Reserved (IEEE 802.1d 1998)		1	118 days 5:50:25	28 sec	
bridge sp. tree/osi route:00:00:00			01:80:C2:00:00:00			Bridge Sp. Tree/OSI Route		2	118 days 5:51:19	1 sec	
reserved (ieee 802.1d 1998):00:00:02			01:80:C2:00:00:02			Reserved (IEEE 802.1d 1998)		1	118 days 5:50:57	23 sec	
multicast:00:00:21			01:80:C2:00:00:21			Multicast		1	118 days 5:51:17	4 sec	
c-98-252-197-49.hsd1.ga.comcast.net		98.252.197.49						1	1:46:10	4:02	
ff02::1:3		ff02::1:3	33:33:00:01:00:03			IPv6		2	12:20:53	30 sec	
ff02::1:2		ff02::1:2	33:33:00:01:00:02			IPv6		3	118 days 5:51:14	2 sec	
192.168.0.100		192.168.0.100						1	5:13:16	33 sec	
d199-74-245-20.try.wideopenwest.com		74.199.20.245						1	1:46:08	4:37	
p0a2789.narant01.ap.so-net.ne.jp		211.10.39.137						1	13 sec	2:42	2527
b-internet.95.191.190.136.nsk.sibirtelecom.ru		95.191.190.136						1	1:46:20	4:28	
dec mop/decnet:02:00:00			AB:00:00:02:00:00			DEC MOP/DECNET		3	1 day 17:55:06	3:09	
78.81.30.163		78.81.30.163						1	0 sec	3:34	
kjwre77638dfqwieuoi.info		173.255.217.235						1	9 sec	11 sec	
h.root-servers.net		128.63.2.53						1	0 sec	5:10	13
bb40f4cf.virtua.com.br		187.64.244.207						1	27:14	43 sec	
10.41.85.218		10.41.85.218	00:15:58:82:77:34					2	2:12:20	1:37	
10.41.84.129		10.41.84.129	00:15:58:82:83:42					1	3:56:03	1:10	
10.41.86.209		10.41.86.209	00:15:58:82:76:89					1	1 day 3:53:03	5:21	

Figura 6 - Exemplo de gráfico gerado pelo NTop

5.5.3 Requisitos:

A instalação da ferramenta NTop também não necessita de requisitos de hardware avançados, podendo ser o mesmo equipamento usado pela ferramenta *BANDWIDTHD*, o que facilita por o NTop também ter a necessidade da placa de

rede do equipamento ter que operar em modo promíscuo, funciona em qualquer sistema operacional, mas recomenda-se o Linux por apresentar melhor desempenho e confiabilidade.

Em geral, o desempenho do NTop é influenciado pelos outros processos paralelos, pois algumas aplicações “gananciosas” de CPU podem utilizar todos os ciclos disponíveis durante alguns segundos, causando a perda de pacotes.

O desempenho do NTop também é influenciado se forem definidos mais segmentos de rede, pois mais tempo de processamento será necessário, podendo causar a perda de pacotes.

O NTop possui um servidor WEB nativo, o que dispensa a necessidade de se instalar e configurar um serviço externo para disponibilização dos relatórios, ele armazena as informações em um banco de dados SQL (*Structured Query Language* ou Linguagem de Consulta Estruturada) e possui integração com várias ferramentas de gerência de rede, o que torna o NTop uma ferramenta bastante adequada para quem deseja analisar o tráfego de rede sem ter que pagar por ferramentas caras e que não possuem todas as funcionalidades oferecidas pelo NTop.

A configuração do NTop é feita através das linhas de comando do arquivo de configuração, assim como no MRTG. Alterando os parâmetros das linhas de comando é possível personalizar o aplicativo para monitorar os pacotes de acordo com as necessidades do gestor da rede. Há disponível na internet vários documentos com exemplos de configurações e explicação dos parâmetros, de maneira que o NTop é uma ferramenta de ótimo custo benefício, valendo a pena o esforço e tempo gasto para configurar e aprender a utilizar a ferramenta.

A ferramenta NTop é considerada de media complexidade de implementação, tal como o *BANDWIDTHD* ela é gratuita, possui ampla documentação disponível mas também requer a mesma necessidade de adaptação do ponto lógico a ser conectada a interface de rede, para que possa capturar todos os pacotes. O NTop pode ser obtido gratuitamente em seu site oficial: http://www.ntop.org/

5.6 OPEN-AUDIT

5.6.1 O que é:

De acordo com o site oficial, o *Open-Audit* é uma ferramenta *open source* que tem por finalidade efetuar um inventário de hardware e software em todos os terminais pertencentes a uma rede. Ele gera um banco de dados com as informações das estações de trabalho, servidores e periféricos que podem ser consultados e classificados de acordo com o hardware, software, configurações, sistema operacional, configurações de segurança, Configurações do IIS, Apache, tipos de serviços, usuários e grupos e muito mais. É escrito em PHP, *bash* e VBScript com acesso a um banco de dados MySQL (OPEN-AUDIT, 2011).

Dentre as várias atribuições de um gestor de redes, uma das mais fundamentais é a função de monitorar e controlar todos os ativos e respectivos softwares em seu parque de TI. A princípio pode-se considerar uma tarefa simples apenas para ambientes pequenos, porém torna-se bastante complexo realizar a gestão em parques maiores de que algumas dezenas de equipamentos. O *Open-Audit* é a solução ideal para auditar sistemas Linux e Windows conectados em uma rede local, sem a necessidade da instalação de qualquer programa cliente/agente nas estações.

Com essa ferramenta é possível gerar relatórios de quantos equipamentos há na rede que possuem determinados processadores, quantidade de memória, softwares instalados, licenças, versões dos softwares de anti-vírus, entre outras inúmeras possibilidades. Permitindo ao gestor controlar desde a parte do *hardware* dos equipamentos quanto a parte do *software* e suas licenças de uso.

5.6.2 Funcionamento:

O projeto do *Open-Audit* consiste em uma interface WEB, desenvolvida em PHP e com suporte ao banco de dados MySQL. Sua estrutura também é baseada em *scripts* bash (para sistemas Linux) e em VBS (para sistemas Windows), utilizados para a varredura dos equipamentos. Toda a especificação do que deve ser

inventariado é definido nesse *script* que, após executado, armazena toda a informação – hardware e software – no banco de dados.

De acordo com Mendes (2010, p.64) com um conhecimento básico de *queries* SQL, é possível extrair e disponibilizar via Internet as informações que o gestor desejar. Adiante é mostrado como é fácil utilizar e customizar o Open-Audit, definindo como e o que inventariar.

Para obter as informações do parque de equipamentos da rede o Open-Audit utiliza-se de *scripts* que rodam nos terminais. Nos terminais Windows o arquivo de script VBS é o responsável por coletar as informações, contendo rotinas e funções que utilizam o recurso WMI, o que dispensa a necessidade de instalação de agentes nos terminais clientes. O *script* possui um arquivo de configuração onde é possível definir quantas máquinas serão auditadas ao mesmo tempo, além da forma como o *script* irá atuar. Depois do *script* devidamente configurado para atender as necessidades do gestor, basta configurar o servidor para que execute o *script* nos terminais ao fazer o *logon*, dessa maneira os terminais serão auditados à medida que forem efetuando o *logon* na rede.

A figura 7 mostra um exemplo de gráfico gerado pelo *Open-Audit.*

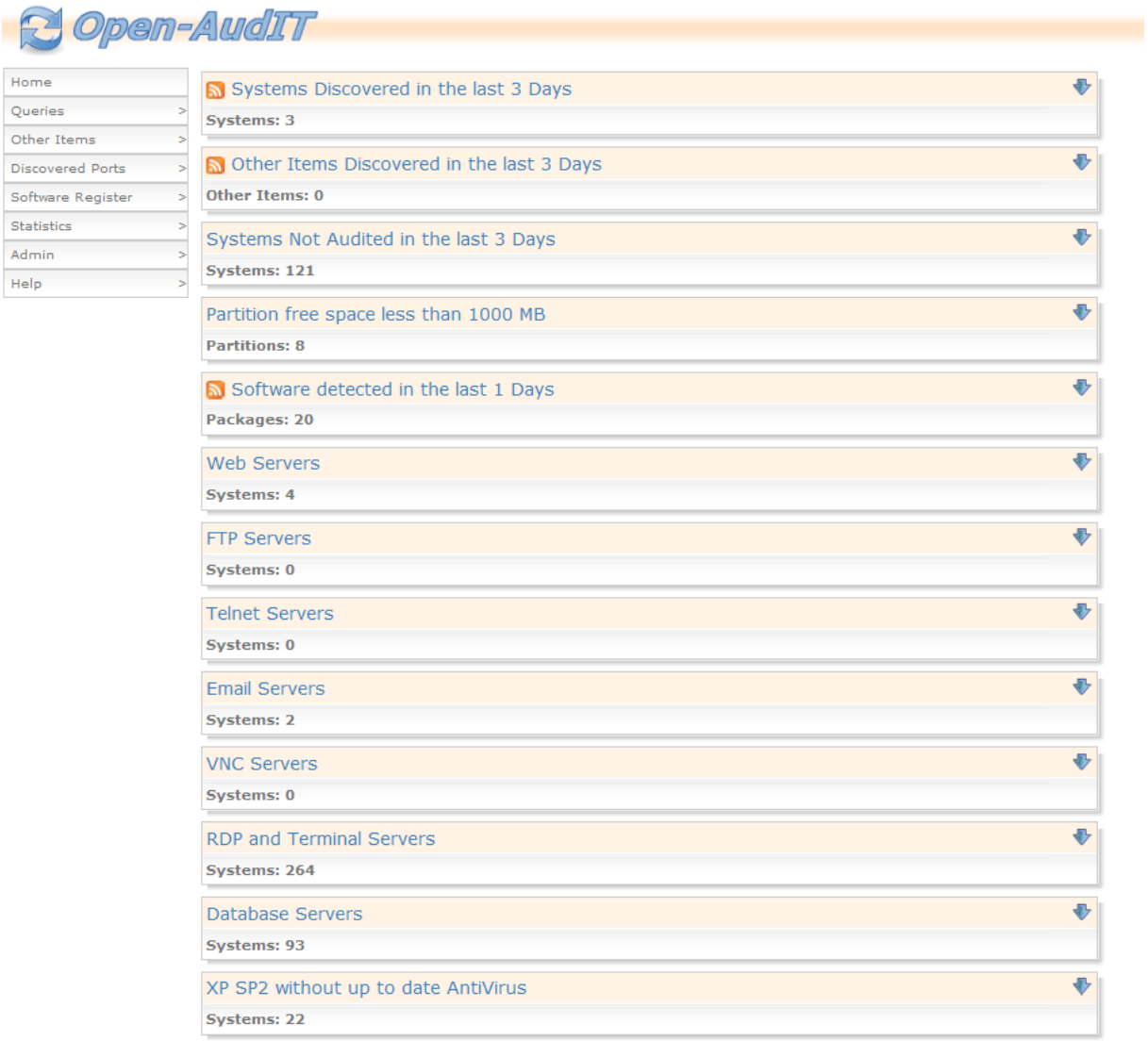


Figura 7 - Exemplo de relatório gerado pelo Open-AudiT

5.6.3 Requisitos:

A ferramenta *Open-Audit* pode ser implementada nos sistemas operacionais Linux (*Kernel* 2.4.x.x ou 2.6.x.x) ou Windows, e ela requer um servidor WEB instalado com suporte a PHP e banco de dados MySQL. Os requisitos de hardware não são específicos, de maneira que cabe ao gestor de TI avaliar quais os serviços que estarão rodando em paralelo com o *Open-Audit* e verificar se o equipamento atende satisfatoriamente sem prejuízo a nenhuma outra aplicação.

A configuração do *Open-Audit* é feita no *script* que os equipamentos executarão. Nesse *script* é possível configurar quais os comandos que serão executados e assim definir o que será auditado, bastando o gestor definir quais são

as informações relevantes e adaptar o *script* para atender às necessidades do seu ambiente.

A ferramenta *Open-Audit* é considerada de média complexidade de implementação, pois necessita que os clientes executem um *script* para a coleta dos dados. Recomenda-se que ele trabalhe em conjunto com um AD (*Active Directory*) para que os *scripts* possam ser executados automaticamente a cada autenticação no servidor de domínio. O *Open-Audit* pode ser obtido gratuitamente em seu site oficial: http://www.open-audit.org/

5.7 SQUID

5.7.1 O que é:

De acordo com o site oficial, a ferramenta SQUID é um *proxy cache* de alta capacidade e desempenho voltada para clientes WEB. O servidor *SQUID WEB Proxy Cache* é gratuito e funciona em código aberto para Unix e Linux. O SQUID originou-se de um programa desenvolvido pelo projeto Harvest chamado *cached (Cache Daemon)*. A *National Science Foundation* (NSF) financia o desenvolvimento do SQUID através do *National Laboratory of Network Research (NLANR)* SQUID, 2011).

O objetivo principal de um servidor *proxy* é permitir que estações de trabalho de uma rede local possam acessar outra rede como outras intranets ou a Internet, sem que para isso seja necessário um circuito de dados direto com essas redes. O servidor *proxy* costuma ser implementado em um terminal que tenha acesso à Internet, sendo que os demais terminais efetuam solicitações de acesso à Internet através do servidor *proxy*.

Laureano (2002) destaca que funcionários de uma organização tendem a passar cada vez mais tempo navegando por *sites* não relativos ao seu trabalho primário, acessam *sites* que não condizem com a política da empresa, utilizam a banda de Internet destinada a serviços como WEB ou VPN e podem, em muitos casos, acabar infectando toda a rede da empresa com vírus e *worms* que são adquiridos em *sites* impróprios. Isso sem contar na ameaça sempre presente de

propagação de *downloads* de softwares piratas e músicas, fatores que podem complicar a vida de uma empresa durante fiscalizações.

De acordo com a Rede Nacional de Ensino e Pesquisa (RNP, 2011), 65% da largura de banda das empresas é utilizada em navegação WEB. E esse número tende a crescer. O SQUID é um servidor *proxy cache* implementado na camada de aplicativo, ele é capaz de processar protocolos Internet específicos, tais como HTTP e FTP. É possível definir regras no servidor *proxy* para determinar como uma solicitação de uma estação de trabalho deve ser processada. Por ser um *proxy cache*, o SQUID pode armazenar temporariamente as paginas da WEB e arquivos FTP para os clientes, e com isso o desempenho da rede pode aumentar significativamente, haja vista que se um segundo cliente solicitar a mesma informação já processada e armazenada pelo servidor *proxy* por um primeiro cliente, essa solicitação será atendida sem um novo acesso às redes externas, pois o próprio servidor *proxy* atende diretamente a solicitação com base nas informações armazenadas, economizando acessos e a banda com as redes externas.

O SQUID mantém meta dados e especialmente objetos armazenados na memória RAM, armazena buscas de DNS e implementa *cache* negativo de *requests* falhos. Ele suporta SSL, listas de acesso complexas e *logging* completo. Por utilizar o Internet Cache Protocol, o SQUID pode ser configurado para trabalhar de forma hierárquica ou mista para melhor aproveitamento da banda. Pode-se dizer que o SQUID consiste em um programa principal - SQUID -, um sistema de busca e resolução de nomes - dnsserver - e alguns programas adicionais para re-escrever *requests*, fazer autenticação e gerenciar ferramentas de clientes.

5.7.2 Funcionamento:

De acordo com Laureano (2002) o SQUID é um WEB *proxy cache* que atende à especificação HTTP 1.1. É utilizado somente por clientes *proxy*, tais como navegadores WEB que acessem à Internet utilizando HTTP, Gopher e FTP. Além disso, ele não trabalha com a maioria dos protocolos Internet. Isto significa que ele não pode ser utilizado com protocolos que suportem aplicativos como vídeo-conferência, *newsgroups*, RealAudio, ou videogames como o Quake ou Counter Strike. O principal motivo destas limitações é que o SQUID não é compatível com

programas que utilizem UDP. O SQUID usa o UDP somente para comunicação *inter-cache*.

Os protocolos funcionarão se forem solicitados pelo navegador WEB e se ele estiver configurado como um cliente *proxy* para o servidor WEB *proxy cache*.

O SQUID também suporta protocolos internos e de administração. Tais protocolos são usados entre os *caches* que puderem existir no mesmo ou em outros servidores de *proxy-caching*, ou para a administração de um *proxy cache*.

O SQUID utiliza mais recursos de sistema do que outros aplicativos. Os dois principais subsistemas de hardware que o SQUID utiliza, e para os quais deve ter um bom desempenho, é o tempo de busca aleatória e a quantidade de memória no sistema.

Tempo de busca aleatória em disco para um *proxy cache* deve ser o mais baixo possível. O problema é que os sistemas operacionais procuram aumentar a velocidade de acesso em disco utilizando vários métodos que geralmente reduzem o desempenho do sistema.

A memória RAM é extremamente importante para a utilização de um *proxy cache*. O SQUID mantém uma tabela na memória RAM sobre os seus objetos. Se uma parte dessa tabela tiver que sofrer *swapping*, o desempenho do SQUID será bastante degradado. O SQUID é um processo, então qualquer *swapping* tornará o programa mais lento. Por exemplo, se existirem 16 GB armazenados no *cache*, precisará de 96 MB (aproximadamente) de RAM para o índice de objetos.

Outros requisitos do sistema, como velocidade de CPU, não são tão importantes assim. A velocidade do processador somente será notada durante o início do sistema (durante a criação do índice de objetos). Um sistema multiprocessado não costuma fazer diferença no desempenho do *proxy cache*, pois o SQUID contém uma pequena porção de código encadeado.

O arquivo squid.conf é definido com as configurações padrão do SQUID e pode ser utilizado após várias modificações. É necessário realizar as alterações, pois por padrão, o squid.conf nega o acesso a todos os navegadores. O SQUID será completamente inútil até que se façam as alterações no arquivo.

Um cliente *proxy* é um sistema que utiliza os serviços de um servidor WEB de *proxy-caching*. Dependendo da configuração da rede, um cliente pode ou não ter que ser configurado como cliente *proxy* para poder usar um servidor *proxy cache* na

WEB. Por exemplo, alguns *firewalls* são configurados para encaminhar todo o tráfego da porta 80 que estiver saindo da rede para o servidor de *proxy cache* na WEB. Neste caso, os clientes *proxy* não precisam de configuração manual. Em outros casos, o cliente detecta automaticamente a informação do servidor *proxy* na rede e a utiliza para todo o acesso à Internet. Configurar um cliente *proxy* é muito mais fácil do que configurar o SQUID. Toda a configuração do cliente *proxy* é concluída dentro do aplicativo do navegador.

5.7.3 Requisitos:

Os requisitos de hardware para implementação da ferramenta SQUID dependem muito do número de clientes que efetuarão as solicitações, sendo que é prioridade uma alta capacidade de memória RAM, e um rápido acesso aleatório em disco. Parâmetros como alta capacidade de processamento e armazenamento em disco não são tão relevantes para o bom funcionamento da ferramenta.

A ferramenta SQUID é considerada de alta complexidade de implementação, pois exige tempo de estudo para compreender cada parâmetro de seu arquivo de configuração, porém é uma ferramenta indispensável para o controle eficiente do acesso à Internet de uma estrutura corporativa. O SQUID pode ser obtida gratuitamente no site oficial: http://www.squid-cache.org/

5.8 SARG

5.8.1 O que é:

De acordo com o site oficial, a ferramenta SARG (*SQUID Analysis Report Generator*) é um utilitário gerador de relatórios sobre os arquivos de log do SQUID. O SARG gera os relatórios no formato HTML e qualquer terminal conectado na rede ou mesmo via WEB tem acesso aos relatórios em um servidor WEB, que são relatórios e gráficos ricos em detalhes que fornecem de uma maneira bastante amigável as informações geradas pela ferramenta anterior SQUID (SARG, 2011).

De nada adianta a existência de uma poderosa ferramenta de controle como o SQUID se os arquivos de log e informações importantes não forem facilmente

interpretados pelo gerente da rede. A ferramenta SARG foi criada por um brasileiro, Pedro Orso, que tem por finalidade traduzir as informações geradas pelo SQUID e gerar relatórios gráficos com estatísticas detalhadas dos *sites* e locais onde os terminais da rede estão andando pela Internet. As características mais relevantes dessa ferramenta são o fato da riqueza de detalhes dos relatórios e gráficos gerados permanecerem à disposição de uma forma fácil via WEB e a configuração permitir uma série de escolhas e personalizações. Sua interface é bastante amigável na parte dos relatórios, permitindo uma navegação fácil e eficiente.

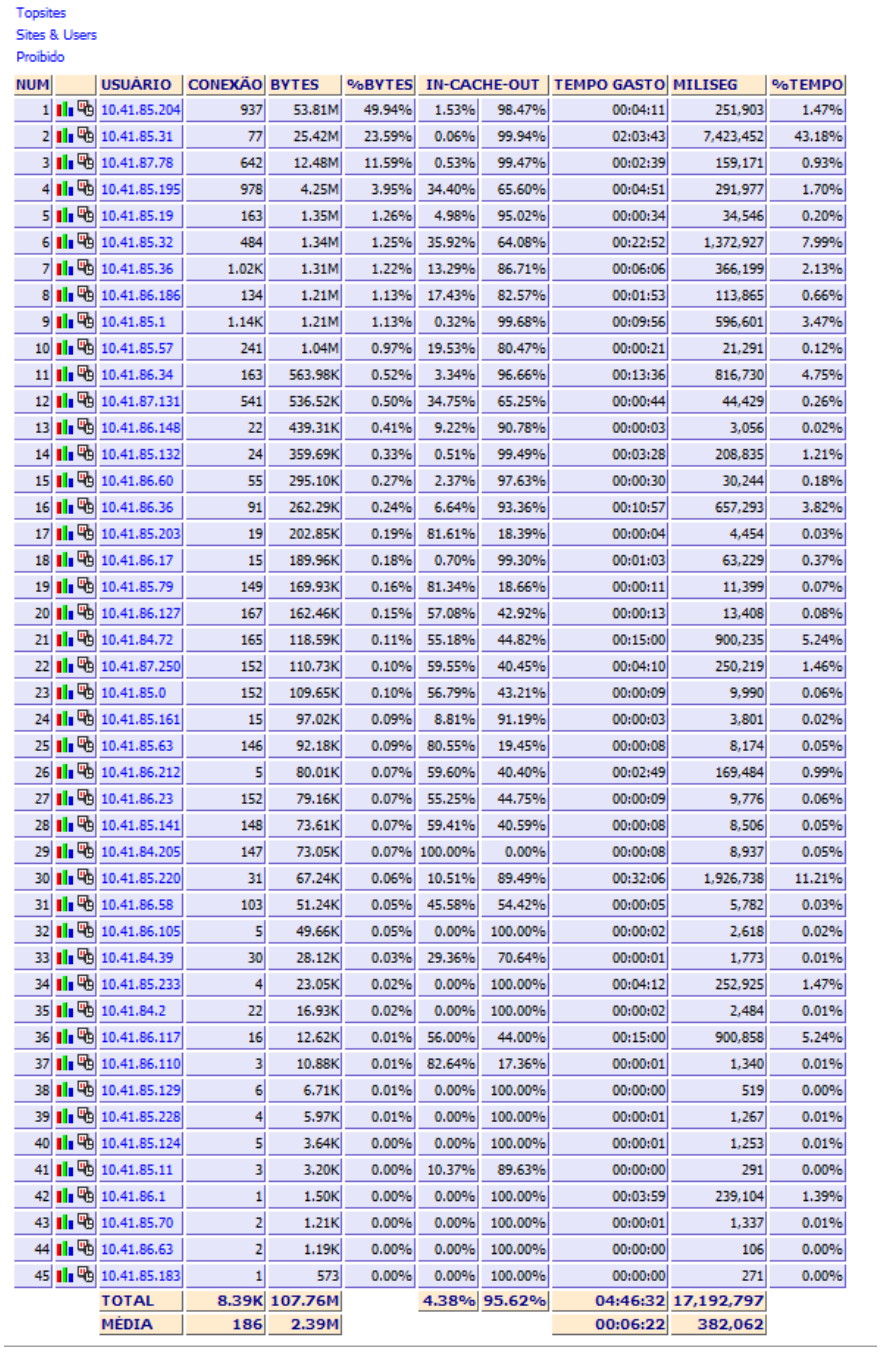
O SARG é adequado especialmente para gestores que desejam ter um controle bastante detalhado, preciso e fácil dos acessos à Internet dos clientes proxy de uma rede corporativa.

5.8.2 Funcionamento:

A configuração da ferramenta SARG é feita editando um arquivo texto de configuração, e a geração dos relatórios é feita através de linha de comando pelo executável sarg.exe, permitindo alterações na configuração que define o período de abrangência do relatório, entre outras opções. Além disso, é possível configurá-lo através do webmin.

O site oficial pode ser acessado em Português, e há pacotes binários para diversas distribuições Linux e também para BSDs no próprio site. A ferramenta tem traduções para diversos idiomas, incluindo Português. O arquivo de configuração é simples e intuitivo, e não exige conhecimentos muito avançados. Quem for capaz de configurar o básico do SQUID, conseguirá configurar bem o SARG. Para usá-lo basta instalá-lo (o SQUID precisa estar instalado, obviamente) e executar o aplicativo. Uma página de relatório será gerada e colocada, por padrão, em /var/www/htdocs/squid-reports. Para maiores funcionalidades é recomendável acessá-lo em um servidor WEB com PHP, mas mesmo que não se possua esta estrutura, é possível usá-lo localmente no navegador.

Na figura 8 é mostrado um exemplo de um relatório gerado pelo SARG.



Topsites
Sites & Users
Proibido

NUM		USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO
1		10.41.85.204	937	53.81M	49.94%	1.53%	98.47%	00:04:11	251,903	1.47%
2		10.41.85.31	77	25.42M	23.59%	0.06%	99.94%	02:03:43	7,423,452	43.18%
3		10.41.87.78	642	12.48M	11.59%	0.53%	99.47%	00:02:39	159,171	0.93%
4		10.41.85.195	978	4.25M	3.95%	34.40%	65.60%	00:04:51	291,977	1.70%
5		10.41.85.19	163	1.35M	1.26%	4.98%	95.02%	00:00:34	34,546	0.20%
6		10.41.85.32	484	1.34M	1.25%	35.92%	64.08%	00:22:52	1,372,927	7.99%
7		10.41.85.36	1.02K	1.31M	1.22%	13.29%	86.71%	00:06:06	366,199	2.13%
8		10.41.86.186	134	1.21M	1.13%	17.43%	82.57%	00:01:53	113,865	0.66%
9		10.41.85.1	1.14K	1.21M	1.13%	0.32%	99.68%	00:09:56	596,601	3.47%
10		10.41.85.57	241	1.04M	0.97%	19.53%	80.47%	00:00:21	21,291	0.12%
11		10.41.86.34	163	563.98K	0.52%	3.34%	96.66%	00:13:36	816,730	4.75%
12		10.41.87.131	541	536.52K	0.50%	34.75%	65.25%	00:00:44	44,429	0.26%
13		10.41.86.148	22	439.31K	0.41%	9.22%	90.78%	00:00:03	3,056	0.02%
14		10.41.85.132	24	359.69K	0.33%	0.51%	99.49%	00:03:28	208,835	1.21%
15		10.41.86.60	55	295.10K	0.27%	2.37%	97.63%	00:00:30	30,244	0.18%
16		10.41.86.36	91	262.29K	0.24%	6.64%	93.36%	00:10:57	657,293	3.82%
17		10.41.85.203	19	202.85K	0.19%	81.61%	18.39%	00:00:04	4,454	0.03%
18		10.41.86.17	15	189.96K	0.18%	0.70%	99.30%	00:01:03	63,229	0.37%
19		10.41.85.79	149	169.93K	0.16%	81.34%	18.66%	00:00:11	11,399	0.07%
20		10.41.86.127	167	162.46K	0.15%	57.08%	42.92%	00:00:13	13,408	0.08%
21		10.41.84.72	165	118.59K	0.11%	55.18%	44.82%	00:15:00	900,235	5.24%
22		10.41.87.250	152	110.73K	0.10%	59.55%	40.45%	00:04:10	250,219	1.46%
23		10.41.85.0	152	109.65K	0.10%	56.79%	43.21%	00:00:09	9,990	0.06%
24		10.41.85.161	15	97.02K	0.09%	8.81%	91.19%	00:00:03	3,801	0.02%
25		10.41.85.63	146	92.18K	0.09%	80.55%	19.45%	00:00:08	8,174	0.05%
26		10.41.86.212	5	80.01K	0.07%	59.60%	40.40%	00:02:49	169,484	0.99%
27		10.41.86.23	152	79.16K	0.07%	55.25%	44.75%	00:00:09	9,776	0.06%
28		10.41.85.141	148	73.61K	0.07%	59.41%	40.59%	00:00:08	8,506	0.05%
29		10.41.84.205	147	73.05K	0.07%	100.00%	0.00%	00:00:08	8,937	0.05%
30		10.41.85.220	31	67.24K	0.06%	10.51%	89.49%	00:32:06	1,926,738	11.21%
31		10.41.86.58	103	51.24K	0.05%	45.58%	54.42%	00:00:05	5,782	0.03%
32		10.41.86.105	5	49.66K	0.05%	0.00%	100.00%	00:00:02	2,618	0.02%
33		10.41.84.39	30	28.12K	0.03%	29.36%	70.64%	00:00:01	1,773	0.01%
34		10.41.85.233	4	23.05K	0.02%	0.00%	100.00%	00:04:12	252,925	1.47%
35		10.41.84.2	22	16.93K	0.02%	0.00%	100.00%	00:00:02	2,484	0.01%
36		10.41.86.117	16	12.62K	0.01%	56.00%	44.00%	00:15:00	900,858	5.24%
37		10.41.86.110	3	10.88K	0.01%	82.64%	17.36%	00:00:01	1,340	0.01%
38		10.41.85.129	6	6.71K	0.01%	0.00%	100.00%	00:00:00	519	0.00%
39		10.41.85.228	4	5.97K	0.01%	0.00%	100.00%	00:00:01	1,267	0.01%
40		10.41.85.124	5	3.64K	0.00%	0.00%	100.00%	00:00:01	1,253	0.01%
41		10.41.85.11	3	3.20K	0.00%	10.37%	89.63%	00:00:00	291	0.00%
42		10.41.86.1	1	1.50K	0.00%	0.00%	100.00%	00:03:59	239,104	1.39%
43		10.41.85.70	2	1.21K	0.00%	0.00%	100.00%	00:00:01	1,337	0.01%
44		10.41.86.63	2	1.19K	0.00%	0.00%	100.00%	00:00:00	106	0.00%
45		10.41.85.183	1	573	0.00%	0.00%	100.00%	00:00:00	271	0.00%
		TOTAL	8.39K	107.76M		4.38%	95.62%	04:46:32	17,192,797	
		MÉDIA	186	2.39M				00:06:22	382,062	

Figura 8 - Exemplo de relatório gerado pelo SARG

5.8.3 Requisitos:

Por se tratar de um complemento da ferramenta SQUID, os requisitos para o bom funcionamento do SARG são os mesmos do SQUID, podendo ser implementado no mesmo equipamento. Evidentemente o principal requisito é que a ferramenta SQUID esteja funcionando.

A ferramenta SARG isoladamente é considerada de fácil implementação, e pode ser obtida gratuitamente em seu site oficial: http://sarg.sourceforge.net/pt-sarg.php

5.9 ITIL

O ITIL (*Information Technology Infrastructure Library)* não é uma ferramenta propriamente dita, mas trata-se de um conjunto de melhores práticas padronizadas que o gestor de TI deve conhecer, para melhor implementar o gerenciamento de um ambiente de TI.

Com o crescimento físico da estrutura de TI de uma organização, e com a dependência que a estratégia de negócio possui com um ambiente de Ti eficiente, criaram-se padrões que servem de referência mundial para melhor gerenciar os ambientes tecnológicos.

Um desses padrões é o ITIL, e ele por si só geraria uma monografia exclusiva, pois ele trata desde os processos para gerência direta dos ativos até os necessários para o gerenciamento de crises. Hoje em dia é um assunto visto como complexo pelos gestores de TI já consolidados no mercado, pois demanda mudança nas práticas e costumes, “vícios” adquiridos. Os resultados do emprego das metodologias do ITIL em uma organização são de longo prazo.

> A metodologia foi criada pela secretaria de comércio OGC (Office of Government Commerce), do governo Inglês, a partir de pesquisas realizadas por Consultores, Especialistas e Doutores, para desenvolver as melhores práticas para a gestão da área de TI nas empresas privadas e públicas. Atualmente se tornou a norma BS-15000, sendo esta um anexo da ISO 9000/2000. O foco deste modelo é descrever os processos necessários para gerenciar a infra-estrutura de TI eficientemente e eficazmente de modo a garantir os níveis de serviço acordados com os clientes internos e externos Apresenta uma abordagem prática dos processos de produção e entrega dos serviços, baseada em experiência. Seu foco, portanto, é no serviço prestado pela TI das Organizações, visando aumentar a qualidade desses serviços.
>
> Na Gestão de segurança, o ITIL possui um processo específico para a Segurança da Informação, enfatizando a importância do adequado

> gerenciamento da SI e considerando os SLA's entre os processos do Negócio e os da TI. Além disso, recomenda que o gerenciamento de Segurança é parte integrante do trabalho de cada Gerente, em todos os níveis. (SCHREIBER; CALASSO, 2010, P.25).

A figura mostra um modelo de atuação.

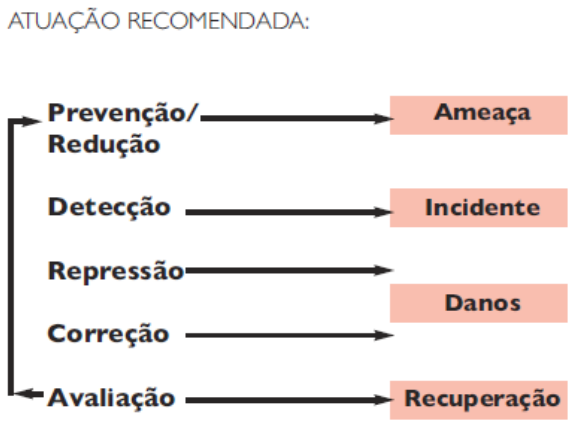


Figura 9 – Atuação recomendada no ITIL
Fonte: Schreiber, Calasso e Astor (2010, P.25).

Ainda conforme os mesmos autores, o ITIL é dividido em 10 Processos Principais e 4 Processos de Apoio (satélites). Os Processos Principais são agrupados em dois Grupos:

- Grupo de Suporte aos Serviços (*Service Support Set*):
  - Gestão de Configuração e de Ativos;
  - Controle de Incidentes / *Help Desk*;
  - Gestão de Problemas;
  - Gestão de Mudanças;
  - Gestão de Liberação.

- Grupo de Serviços Prestados (Service Delivery set):
  - Gestão de Níveis de Serviço (SLA);
  - Gestão de Disponibilidade;
  - Gestão de Desempenho e Capacidade;
  - Plano de Continuidade de Negócios;
  - Custeio e Gestão Financeira.

Os Processos de Apoio são:

- SLA (*Service Level Agreement*);
- Segurança;
- Informação;
- Rede e Operações.

6 ESTUDO DE CASO

O objetivo desse capítulo é demonstrar os resultados obtidos na utilização das ferramentas descritas no capitulo 5, mostrar quais foram as dificuldades e melhorias obtidas com cada uma delas. O ambiente deste estudo de caso é um ambiente real de uma instituição pública federal, a SR/PR Superintendência Regional de Polícia Federal no Paraná.

Nos últimos cinco anos, a SR/PR passou por um processo intenso de modernização, onde vários novos equipamentos foram adquiridos melhorando significativamente a qualidade dos recursos em TI da instituição. Com isso, vários processos internos ficaram cada vez mais dependentes de uma estrutura de TI eficiente e operacional. Houve investimentos em mão de obra terceirizada para a manutenção dos equipamentos e infraestrutura de rede. Porém, não havia nada planejado em termos de gerenciamento de todo esse novo parque de equipamentos.

Foi por necessidade de melhor gerenciar os recursos humanos e financeiros, que nos últimos 2 anos o foco da gestão da TI dessa instituição foi investir no gerenciamento de todo o sistema. Sem recursos financeiros disponíveis para aquisição de softwares, que em uma instituição pública depende de processos licitatórios complexos e morosos, foram adotadas exclusivamente ferramentas de distribuição livre.

Primeiramente foram analisados quais os principais parâmetros e quesitos que são relevantes de serem gerenciados dentro do escopo da estratégia de negócio da instituição. Não adianta investir tempo para estudar, implementar e configurar uma ferramenta que gerencie parâmetros que não são relevantes para o negócio da organização, e por isso essa etapa de planejamento e priorização dos parâmetros a serem gerenciados é essencial para evitar desperdícios.

6.1 MRTG

A primeira ferramenta implementada foi o MRTG, pois havia uma grande necessidade de se conhecer quais eram as taxas de ocupação dos circuitos de dados, comprovar se a velocidade contratada com a operadora estava de fato sendo

disponibilizada e verificar quais eram os circuitos mais utilizados e em quais horários.

Com a utilização dessa ferramenta foi possível detectar problemas em terminais contaminados que estavam gerando tráfego excessivo nos circuitos de dados. Forneceu dados concretos para responder solicitações de aumento de banda por conta de lentidão nos sistemas, onde várias solicitações para aumento de banda foram negadas por conta de que o MRTG mostrou que havia sobra no dimensionamento da capacidade dos circuitos, e que a lentidão dos sistemas tinha causas alheias à capacidade dos circuitos.

Atualmente não só os circuitos de dados estão monitorados pelo MRTG mas todas as portas dos switches do prédio da SR/PR são monitoradas, gerando um histórico do volume de dados de cada terminal, proporcionando dados concretos da ocupação dos recursos.

Na figura 10 é mostrado o gráfico do MRTG em ambiente real.

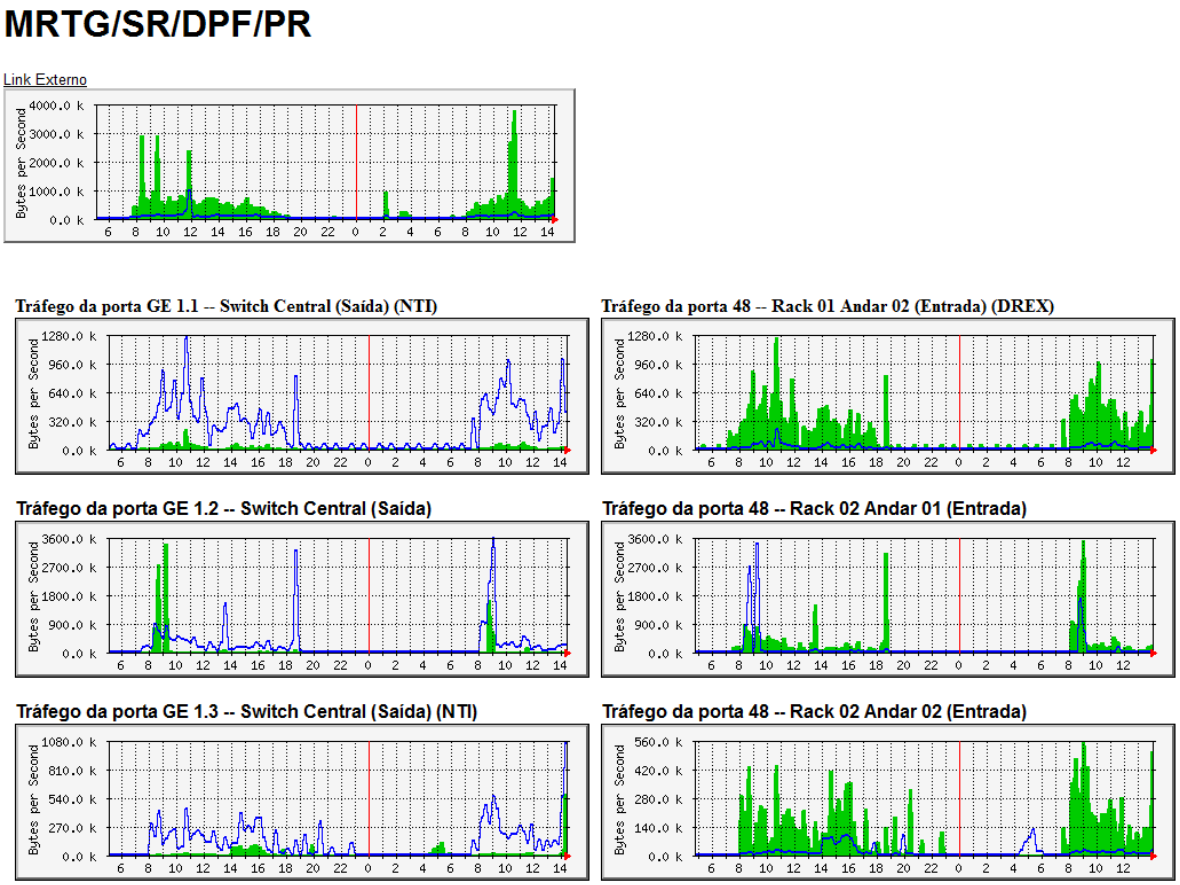


Figura 10 – Gráficos do MRTG em ambiente real.

O MRTG mostrou ser uma ferramenta bastante simples de ser implementada, e a maior dificuldade encontrada foi adequar o tempo de atualização

de leitura dos dispositivos. Como são muitas portas monitoradas, o tempo padrão de 5 min. não era suficiente para que todas elas fossem lidas, e com alguns gráficos não eram gerados. Bastou aumentar o tempo de atualização para que o problema fosse solucionado.

Foi montada uma simples página WEB com os gráficos principais, e clicando nos gráficos principais as informações detalhadas de cada porta do switch são mostradas. O gráfico principal (Figura 10) foi montado de maneira que a coluna da esquerda corresponde à porta do switch central "*core"* da rede, e a coluna da direita os swtiches de borda. Cada porta do switch central está ligada à porta num. 48 do switch de borda. Com os gráficos correspondentes na mesma linha é possível observar que o gráfico de entrada (azul) da coluna da esquerda é o mesmo que o gráfico de saída (verde) da coluna da direita, e não poderia ser diferente, uma vez que se trata do mesmo cabo físico que ao entrar dados de um lado sai do outro.

6.2 BANDWIDTHD

Essa ferramenta foi implementada a partir da necessidade de maiores detalhes de utilização da banda, pois o MRTG fornece informações de quanto da banda está sendo utilizada, mas não fornece claramente quem está utilizando e para qual tipo de serviço.

Foi então que o BANDWIDTHD resolveu o problema. Com ele foi possível descobrir qual terminal está consumindo a maior parte da banda, e se esse consumo é justificado ou não, pois essa ferramenta é capaz de detalhar os serviços que estão sendo utilizados pelos terminais: FTP, HTTP, P2P, TCP, UDP e ICMP.

Essa ferramenta ainda gera estatísticas diárias, semanais e mensais dos terminais que mais utilizam a rede, proporcionando ao gestor de TI informações quantitativas e qualitativas concretas da utilização dos recursos.

6.3 NTOP

A ferramenta NTop é um complemento do BANDWIDTHD, e ela faz basicamente a mesma coisa, mas é mais completa. Porém não substitui a

ferramenta anterior, que é mais prática e amigável ao usuário quando se quer informações objetivas sobre o consumo de banda por terminal.

Com ele é possível visualizar de maneira mais detalhada a divisão da banda utilizada separando por serviços (FTP, HTTP, P2P, TCP, UDP e ICMP) e não somente por endereços IP´s como o BANDWIDTHD.

O NTop também fornece dados brutos de consumo de banda, tal como o MRTG. Com ele também é possível verificar o tráfego interno entre os terminais da rede, podendo ser útil na verificação de tráfegos de rede intensos entre servidores ou entre uma estação de trabalho e os servidores, fornecendo ao gestor informações úteis para melhor dimensionamento e configurações dos terminais e servidores da rede.

6.4 OPEN AUDIT

A ferramenta Open Audit foi implementada para solucionar várias demandas por gerenciamento que um ambiente complexo de TI exige; instalada primeiramente para testes essa ferramenta se mostrou bastante útil e eficiente, fornecendo dados concretos sobre a real situação dos terminais da rede, desde sua configuração de hardware e software como versões dos aplicativos instalados e controle das licenças de softwares pagos e sistemas operacionais.

Outros equipamentos que compartilham a rede de dados como impressoras e scanners também são identificados pela ferramenta, proporcionando um gerenciamento bastante eficiente dos dispositivos IP.

Ela é capaz de gerar dados estatísticos indexados em parâmetros muito variáveis, como versão do sistema operacional, fabricante, quantidade de memória RAM, tamanho do disco rígido, etc.

Na figura 11 é mostrada uma estatística gerada pelo *Open-Audit* de terminais indexada pelo modelo do processador

Processor	Count	Percentage
Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz	96	29.81 %
AMD Athlon(tm) 64 X2 Dual Core Processor 4200	75	23.29 %
Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz	41	12.73 %
Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz	28	8.70 %
Processador Intel Pentium III Xeon	8	2.48 %
Intel(R) Core(TM)2 Quad CPU Q9505 @ 2.83GHz	7	2.17 %
AMD Phenom(tm) II X4 B97 Processor	5	1.55 %
Intel(R) Pentium(R) 4 CPU 1.50GHz	5	1.55 %
Intel(R) Pentium(R) 4 CPU 3.06GHz	4	1.24 %
Dual-Core AMD Opteron(tm) Processor 2220	4	1.24 %
AMD Athlon(tm) 64 X2 Dual-Core Processor TK-57	4	1.24 %
Intel(R) Celeron(R) CPU 2.80GHz	3	0.93 %
Genuine Intel(R) CPU 2140 @ 1.60GHz	2	0.62 %
Intel(R) Core(TM)2 Duo CPU T8300 @ 2.40GHz	2	0.62 %
AMD Duron(tm) processor	2	0.62 %
AMD Turion(tm) 64 X2 Mobile Technology TL-52	2	0.62 %
Intel(R) Pentium(R) Dual CPU T2390 @ 1.86GHz	2	0.62 %
Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz	2	0.62 %
Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz	2	0.62 %
Intel(R) Pentium(R) D CPU 3.40GHz	2	0.62 %
Intel(R) Pentium(R) D CPU 2.80GHz	2	0.62 %
AMD Sempron(tm) 2200	1	0.31 %
Intel(R) Core(TM)2 Duo CPU T5750 @ 2.00GHz	1	0.31 %
Intel(R) Core(TM)2 Duo CPU T5550 @ 1.83GHz	1	0.31 %
Mobile Intel(R) Pentium(R) 4 - M CPU 1.80GHz	1	0.31 %
AMD Sempron(tm) Processor 3000	1	0.31 %
Intel(R) Celeron(R) CPU 2.66GHz	1	0.31 %
AMD Sempron(tm) 2300	1	0.31 %
Intel(R) Celeron(R) CPU 2.40GHz	1	0.31 %
Intel(R) Core(TM)2 Duo CPU T5800 @ 2.00GHz	1	0.31 %
AMD Athlon(tm) X2 Dual-Core QL-64	1	0.31 %
AMD Athlon(tm) 64 X2 Dual Core Processor 4000	1	0.31 %
AMD Sempron(tm) 2800	1	0.31 %
Processador Intel Pentium III	1	0.31 %
AMD Turion(tm) X2 Dual-Core Mobile RM-72	1	0.31 %
Mobile Intel(R) Pentium(R) 4 CPU 3.20GHz	1	0.31 %
Intel(R) Core(TM)2 CPU 6300 @ 1.86GHz	1	0.31 %
Intel(R) Pentium(R) 4 CPU 2.40GHz	1	0.31 %
Intel(R) Celeron(R) CPU 540 @ 1.86GHz	1	0.31 %
Genuine Intel(R) CPU 3.06GHz	1	0.31 %
Intel(R) Pentium(R) Dual CPU T2370 @ 1.73GHz	1	0.31 %
AMD Sempron(tm) Processor 2800	1	0.31 %
Processador Intel Pentium II	1	0.31 %
Intel(R) Pentium(R) 4 CPU 3.00GHz	1	0.31 %
Intel(R) Celeron(R) M processor 1300MHz	1	0.31 %

Figura 11 – Estatística de terminais por modelo de processador.

Com essa ferramenta foi possível detectar terminais que estavam com o software antivírus desatualizados ou mesmo sem o software, programas com a licença expirada ou inexistente, terminais com hardware demasiadamente obsoletos, sistemas operacionais desatualizados, etc... Para um ambiente de rede seguro, atualizado e controlado, essa ferramenta se mostrou indispensável.

Para que os terminais da rede sejam monitorados pelo Open Audit, é necessário que eles executem um comando. Para isso, foi criado um *script* que junto com os serviços do AD (*Active Directory*) é executado toda vez que um usuário se autentica no servidor de domínio. Com isso a ferramenta torna-se extremamente fácil de ser implementada.

6.5 SQUID

Toda organização possui a necessidade de otimizar seus recursos de TI, que geralmente são onerosos. Em uma organização pública esse trabalho torna-se mais complexo, pois é impossível vigiar o conteúdo que os funcionários estão acessando na Internet, e políticas educativas nem sempre surtem efeito.

O SQUID hoje é uma necessidade, por não ser apenas uma ferramenta de gerenciamento passiva e sim uma ferramenta capaz de controlar e melhorar o desempenho dos acessos à Internet.

Essa ferramenta possibilitou efetuar uma gerência muito complexa devido à natureza da organização. Em alguns casos é necessário que o servidor acesse, como parte do seu trabalho, páginas com conteúdo pornográfico, sites de relacionamento, sistemas de compartilhamento de arquivos entre outros, que normalmente fazem parte da regra de bloqueio nas políticas das organizações. Com o SQUID é possível tratar esses casos isoladamente, dando o acesso a esses conteúdos somente para as pessoas envolvidas com esse tipo de investigação.

Ele também proporciona a possibilidade de auditar o conteúdo acessado por um terminal da rede, o que pode ser útil em investigações internas.

Por ter a capacidade de armazenar o conteúdo dos sites acessados em um *cache*, o SQUID além de todas as funcionalidades descritas anteriormente, é capaz de otimizar a capacidade do circuito de acesso à Internet. Se um terminal efetuar uma solicitação de um conteúdo que já esteja disponível no *cache* do SQUID, ele fornece esse conteúdo diretamente ao solicitante, sem fazer um acesso externo à Internet, economizando banda.

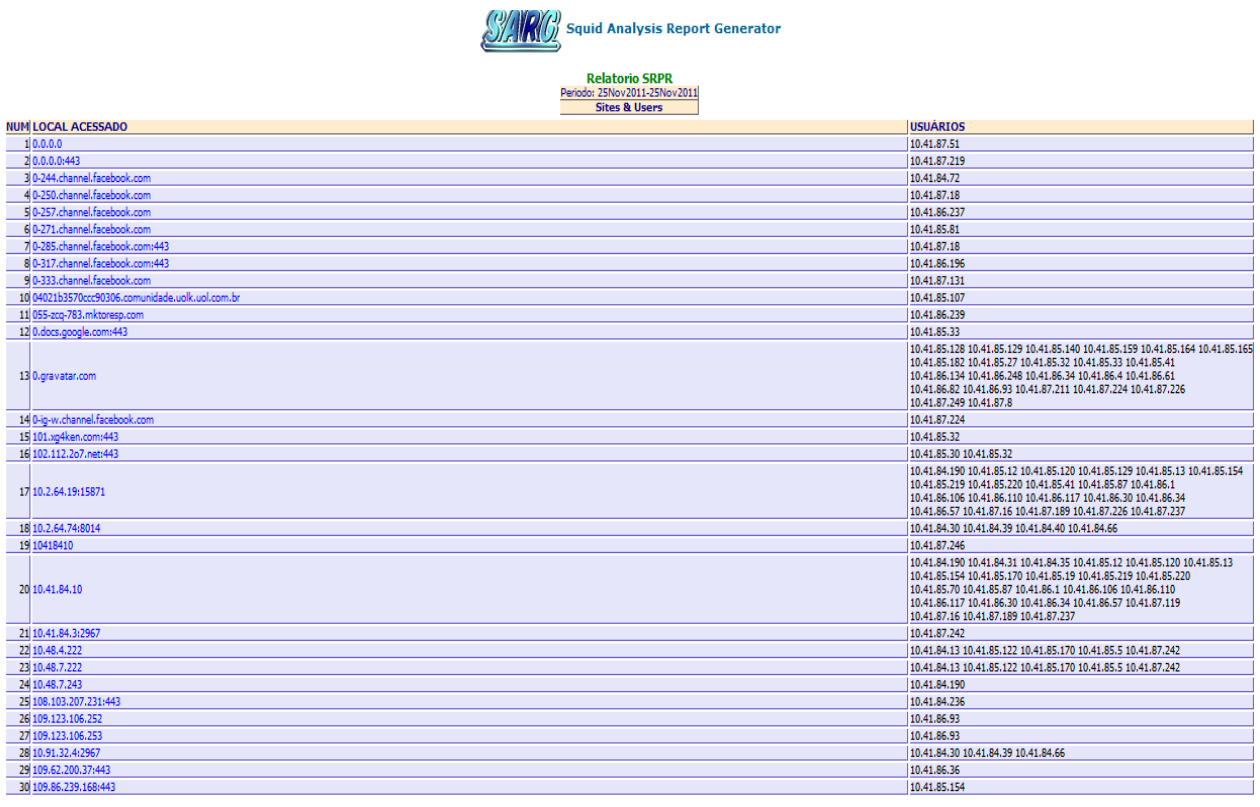
6.6 SARG

A ferramenta SQUID, como foi dito, é uma necessidade. Porém os relatórios gerados por ele não são nada amigáveis. São arquivos de texto puro que demandam tempo e paciência para serem interpretados, e muitas das informações úteis passam despercebidas por ser humanamente impossível de enxergá-las com clareza em um arquivo log de texto puro.

O SARG é um complemento indispensável para o SQUID, pois ele é capaz de transformar o arquivo texto gerado pelo SQUID em um relatório bastante amigável, em formato WEB e com todas as estatísticas necessárias para um bom gerenciamento. Com essa ferramenta o gestor tem a capacidade de enxergar de maneira bastante clara os efeitos e resultados das regras implementadas, observar fatos estranhos e explorar ao máximo o potencial do SQUID. Tão importante quanto o SQUID, o SARG cumpre muito bem o propósito para que foi desenvolvido.

Em suma, o SARG não faz nada, apenas traduz os importantíssimos dados gerados pelo SQUID para uma linguagem mais humana. Por isso ele é tão importante, e valoriza ainda mais uma ferramenta nativamente poderosa.

Na figura 12 é mostrado um relatório de um ambiente real gerado pelo SARG.



Squid Analysis Report Generator

Relatorio SRPR
Periodo: 25Nov2011-25Nov2011
Sites & Users

NUM	LOCAL ACESSADO	USUÁRIOS
1	0.0.0.0	10.41.87.51
2	0.0.0.0:443	10.41.87.219
3	0-244.channel.facebook.com	10.41.84.72
4	0-250.channel.facebook.com	10.41.87.18
5	0-257.channel.facebook.com	10.41.86.237
6	0-271.channel.facebook.com	10.41.85.81
7	0-285.channel.facebook.com:443	10.41.87.18
8	0-317.channel.facebook.com:443	10.41.86.196
9	0-333.channel.facebook.com	10.41.87.131
10	04021b3570ccc90306.comunidade.uolk.uol.com.br	10.41.85.107
11	055-zcq-783.mktoresp.com	10.41.86.239
12	0.docs.google.com:443	10.41.85.33
13	0.gravatar.com	10.41.85.128 10.41.85.129 10.41.85.140 10.41.85.159 10.41.85.164 10.41.85.165 10.41.85.182 10.41.85.27 10.41.85.32 10.41.85.33 10.41.85.41 10.41.86.134 10.41.86.248 10.41.86.34 10.41.86.4 10.41.86.61 10.41.86.82 10.41.86.93 10.41.87.211 10.41.87.224 10.41.87.226 10.41.87.249 10.41.87.8
14	0-ig-w.channel.facebook.com	10.41.87.224
15	101.xg4ken.com:443	10.41.85.32
16	102.112.2o7.net:443	10.41.85.30 10.41.85.32
17	10.2.64.19:15871	10.41.84.190 10.41.85.12 10.41.85.120 10.41.85.129 10.41.85.13 10.41.85.154 10.41.85.219 10.41.85.220 10.41.85.41 10.41.85.87 10.41.86.1 10.41.86.106 10.41.86.110 10.41.86.117 10.41.86.30 10.41.86.34 10.41.86.57 10.41.87.16 10.41.87.189 10.41.87.226 10.41.87.237
18	10.2.64.74:8014	10.41.84.30 10.41.84.39 10.41.84.40 10.41.84.66
19	10418410	10.41.87.246
20	10.41.84.10	10.41.84.190 10.41.84.31 10.41.84.35 10.41.85.12 10.41.85.120 10.41.85.13 10.41.85.154 10.41.85.170 10.41.85.19 10.41.85.219 10.41.85.220 10.41.85.70 10.41.85.87 10.41.86.1 10.41.86.106 10.41.86.110 10.41.86.117 10.41.86.30 10.41.86.34 10.41.86.57 10.41.87.119 10.41.87.16 10.41.87.189 10.41.87.237
21	10.41.84.3:2967	10.41.87.242
22	10.48.4.222	10.41.84.13 10.41.85.122 10.41.85.170 10.41.85.5 10.41.87.242
23	10.48.7.222	10.41.84.13 10.41.85.122 10.41.85.170 10.41.85.5 10.41.87.242
24	10.48.7.243	10.41.84.190
25	108.103.207.231:443	10.41.84.236
26	109.123.106.252	10.41.86.93
27	109.123.106.253	10.41.86.93
28	10.91.32.4:2967	10.41.84.30 10.41.84.39 10.41.84.66
29	109.62.200.37:443	10.41.86.36
30	109.86.239.168:443	10.41.85.154

Figura 12 – Relatório gerado pelo SARG

7 CONCLUSÃO

Todas as ferramentas analisadas nesse trabalho são de livre distribuição, não necessitando que o gestor de TI de uma organização pública tenha a difícil tarefa de angariar recursos financeiros para colocar em prática um projeto de implementação de ambiente gerenciável. Não é necessário efetuar licitações, projetos básicos e outros pré-requisitos previstos na legislação brasileira para obter nenhuma das ferramentas vistas. Basta ter disponibilidade de hardware e conhecimentos profundos da arquitetura da rede que se deseja gerenciar.

A configuração de cada ferramenta analisada é específica para cada ambiente de rede, mas a essência é a mesma. Diferenciando apenas variáveis específicas como endereçamento IP e particularidades de cada organização. Há disponível na Internet muitos tutoriais que auxiliam na instalação e configuração dessas ferramentas. Vários exemplos práticos com fotos das telas são encontrados facilmente. Fóruns e listas de discussão sempre são boas fontes de informação para problemas comuns.

Portanto, a premissa que gerenciar TI é caro e complexo deve ser analisada com mais propriedade. Um nível de gerência básico a médio, que é suficiente para a grande maioria das organizações, pode ser alcançado sem custos com softwares, utilizando ferramentas de fácil implementação e configuração e com material didático de simples acesso. Cabe ao gestor de TI entender do negócio da organização para assim poder priorizar os sistemas e recursos fundamentais, planejar ações para evitar que esses recursos fiquem indisponíveis ou que os investimentos sejam canalizados neles para um melhor resultado.

Como temas para estudos futuros podem ser propostos a demonstração das melhorias e resultados obtidos com o emprego de metodologias e conjuntos de boas práticas de gestão em TI, tais como ITIL, COBIT, etc. nas organizações públicas.

REFERÊNCIAS

BAHIENSE, G. C; NOGUEIRA, R. Uso estratégico de tecnologia da informação em Secretarias de Fazenda no Brasil. In: XXVI Encontro Nacional da Associação Nacional dos Programas de Pós-Graduação em Administração, 2002. **Resumos**. Salvador, 2002.

BANDWIDTHD. **Site Oficial**. Disponível em <http://bandwidthd.sourceforge.net/> Acessado em Novembro de 2011.

BRASIL. **Portal de Governo Eletrônico**. Disponível em: www.governoeletronico.gov.br. Acessado em Novembro de 2011.

CUNHA, M. A. V. C.;MARQUES V. E.; MEIRELLES S. F. Tecnologia de informação no setor público: estudo da percepção dos gestores do executivo estadual. In: XXVI Encontro Nacional da Associação Nacional dos Programas de Pós-Graduação em Administração. **Resumos**. Salvador, 2002.

DIAS, B. Z. ; JUNIOR. N. A. **Protocolo de gerenciamento SNMP**. 2001.Disponível em <www.rederio.br/downloads/pdf/nt00601.pdf> Acessado em Outubro de 2011.

DMTF. **Distributed Management Task Force, site oficial.** Disponível em <http://www.dmtf.org/>. Acessado em Novembro de 2011.

FAGUNDES, E. M. **COBIT - Um kit de ferramentas para a excelência na gestão de TI**, 2004. Disponível em: <http://www.efagundes.com/artigos/Arquivos_pdf/cobit.pdf>. Acesso em Agosto de 2011.

LAUREANO, M. A. P. **Instalando e configurando o SQUID**. 2012. Disponível em <http://www.mlaureano.org/guias_tutoriais/GuiaInstSquid.htm> Acessado em Novembro de 2011.

LEITE et al. **Gerenciamento de serviços de TI: um estudo de caso em uma empresa de suporte remoto em Tecnologia da Informação**. Revista Eletrônica Sistemas & Gestão. 2005. Disponível em < http://www.uff.br/sg/index.php/sg/article/viewFile/V5N2A2/5N2A2> Acessado em Outubro de 2011.

MENDES, S. **Auditoria com qualidade.** 2010 Disponível em <http://lnm.com.br/images/uploads/pdf_aberto/LM_71_64_67_04_tut_openaudit.pdf> Acessado em Novembro de 2011.

NATAL, Rui. **Gerenciamento de ativos de ti. O elo perdido do ITIL.** Csc Brasil, 2010. Disponível em: <http://www.cscbrasil.com.br/assinaturas/Artigo_Gerenciamento_de_Ativos_de_TI.pdf> Acessado em Novembro de 2011.

NTop. **Site oficial**. Disponível em <http://www.ntop.org/>. Acessado em Novembro de 2011.

OETIKER, T. **Tobi Oetiker's MRTG - The Multi Router Traffic Grapher**. Disponível em <http://oss.oetiker.ch/mrtg/> Acessado em Outubro de 2011.

OPEN-AUDIT. **Site Oficial**. Disponível em <http://www.open-audit.org/index.php> Acessado em Novembro de 2011.

ORTOLANI, L. F. B. **A Tecnologia da Informação na administração pública**, 2008. Disponível em <www.sad.ms.gov.br/controle/ShowFile.php?id=803> Acessado em Outubro de 2011.

PINTO, P. R. S. **Uma TI bem organizada muda qualquer órgão público.** 2009. Disponível em: <http://www.planoeditorial.com.br/ti_governo/pdfs/PAG_04_08_governanca.pdf> Acessado em Novembro de 2011.

RECH FILHO, A. **Estudos para implantação de uma gerência de rede corporativa utilizando arquitetura de protocolos abertos. 1996. 147f.** Dissertação (Mestrado em Engenharia Elétrica e Informática Industrial) – Centro Federal de Educação Tecnológica do Paraná, Curitiba, 1996.

RNP. **Rede Nacional de Ensino e Pesquisa, Site Oficial.** Disponível em <http://www.rnp.br/newsgen/0103/wccp.html>.

ROCHA, R. N. **Entendendo a camada WMI**. Disponível em <http://www.devmedia.com.br/post-651-Entendendo-a-camada-WMI.html>. Acessado em Novembro de 2011.

RONCERO, V. G. ; ALBUQUERQUE, M. P. ; ALBUQUERQUE, M. P. **Monitoramento do protocolo RTSP (Real Time Streaming Protocol) utilizando o NTop**. Disponível em <http://www.rederio.br/downloads/pdf/nt00402.pdf> Acessado em Novembro de 2011.

SARG. **Site Oficial**. Disponível em <http://sarg.sourceforge.net/pt-sarg.php> Acessado em Novembro de 2011.

SCHREIBER, V.; CALASSO, A;. **ITIL – Infastructure Library**. 2010. Disponível em < http://computerworld.uol.com.br/estaticas/downloads/catalogo_parte2.pdf> Acessado em Novembro de 2011.

SIX. **Slovack Internet eXchange**. Disponível em < www.six.sk/mrtg/aggregated.html> Acessado em Novembro de 2011.

SQUID, site oficial. Disponível em <http://www.squid-cache.org/> Acessado em Novembro de 2011.

VIEIRA, D. M. **Governança de TI no Setor Público – Caso DATAPREV**. 2005. Dissertação (Mestrado em Sistemas de Gestão) – Universidade Federal Fluminense, Niterói-RJ.