

Ferramentas para Gerenciamento de Rede HFC

Elaborador:	Fernando Pereira Da Cunha
Orientador:	Marcus Vinícius Lahr Giraldi

C978f CUNHA, Fernando Pereira da

Ferramentas para Gerenciamento de Rede HFC. / Fernando Pereira da Cunha. – Americana, 2018.

35f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinícius Lahr Giraldi

1 Redes de computadores 2. Telecomunicações I. GIRALDI, Marcus Vinícius Lahr II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU:681.519

621.39

Faculdade de Tecnologia de Americana

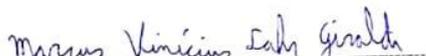
Fernando Pereira da Cunha

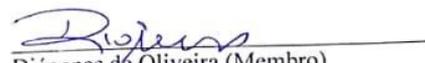
FERRAMENTAS PARA GERENCIAMENTO DE REDE HFC

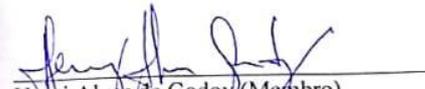
Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.
Área de concentração: Gerenciamento de Rede

Americana, 04 de dezembro de 2018.

Banca Examinadora:


Marcus Vinicius Lahr Giraldo (Presidente)
Especialista
Fatec Americana


Diógenes de Oliveira (Membro)
Mestre
Fatec Americana


Henri Alves de Godoy (Membro)
Mestre
Fatec Americana

SUMÁRIO

1	Objetivo deste documento.....	6
2	Fundamentação teórica.....	6
2.1	Gerenciamento de rede.....	6
2.2	Rede HFC (Híbrida Fibra-Coaxial).....	7
2.3	Protocolo SNMP (<i>Simple Network Management Protocol</i>).....	9
2.4	Nagios.....	11
2.5	Visium Live.....	11
3	Comparando funcionalidades em comum.....	12
3.1	Consulta node.....	12
3.2	Consulta e monitoramento de fontes.....	16
3.3	Painel de alarmes.....	20
4	Funcionalidades presentes apenas no Visium Live.....	25
4.1	Consulta massiva de MACS.....	25
4.2	Níveis de referência.....	26
4.3	Maps.....	28
5	Exemplo utilizando incidente real.....	30
6	Resultados.....	32
6.1	Queda no Tempo Médio de Recuperação (TMR).....	32
6.2	Aumento no Número de Incidentes Proativos.....	33
7	Considerações finais.....	34

Lista de figuras

Figura 1	Rede de acesso híbrida fibra-coaxial.....	8
Figura 2	Estrutura do cabo coaxial.....	8
Figura 3	Estrutura do cabo de fibra óptica.....	9
Figura 4	Modelo de gerenciamento do SNMP.....	10
Figura 5	Estrutura do Nagios.....	11
Figura 6	Estrutura do Visium Live.....	12
Figura 7	Sistema de consulta de interface.....	13
Figura 8	Tela de login do Nagios.....	13
Figura 9	Seleção do CMTS e placa cable.....	14
Figura 10	Gráfico Nagios.....	15
Figura 11	Interface do Visium Live.....	15
Figura 12	Seleção do node no Visium Live.....	16
Figura 13	Interface Nagios Fonte.....	17
Figura 14	Detalhes de um alarme de fonte.....	18

Figura 15 Seleção da fonte	18
Figura 16 Gráfico de voltagem de entrada da fonte	19
Figura 17 Gráfico da autonomia da bateria da fonte	19
Figura 18 Painel de alarmes do Nagios	20
Figura 19 Painel de alarmes do Visium Live	21
Figura 20 Filtros do painel de alarmes	21
Figura 21 Filtro para a seleção de equipamento	22
Figura 22 Aba de alarmes restabelecidos	22
Figura 23 Aba de alarmes novos	23
Figura 24 Detalhes de um alarme novo	23
Figura 25 Aba de alarmes em análise	24
Figura 26 Detalhes de um alarme em tratamento	24
Figura 27 Aba de alarmes encaminhados para campo	25
Figura 28 Consulta massiva de MACS	26
Figura 29 Interface da funcionalidade níveis de referência	27
Figura 30 Consulta de MACS antes e depois	28
Figura 31 Interface Maps	29
Figura 32 Consulta dos níveis de todos os clientes do node	29
Figura 33 Projeto de rede no CAD	30
Figura 34 Projeto de rede no Visium Live	31
Figura 35 Fechamento do Incidente	31
Figura 36 Gráfico de tempo médio de recuperação	33
Figura 37 Gráfico de incidentes proativos	33

Lista de tabelas

Tabela 1 Tempo médio de recuperação	32
Tabela 2 Incidentes proativos	33

1 Objetivo deste documento

É indiscutível que o monitoramento dos ativos de rede é de fundamental importância para o bom funcionamento da infraestrutura de TI. Com o crescimento da Internet no final dos anos 90, passamos a ter sistemas e redes cada vez maiores e mais complexas, com um grande número de equipamentos, diferentes tecnologias e fabricantes.

Em consequência disso, viu-se uma grande evolução nas ferramentas de monitoramento, pois as organizações buscavam cada vez mais a disponibilidade de seus serviços, identificando falhas e perdas de conexão de maneira proativa, o que outrora era identificado apenas de forma reativa.

Esse relatório técnico visa demonstrar as vantagens obtidas pelo NOC (**Network Operations Center**) de uma grande empresa do setor de telecomunicações, ao realizar a migração para uma nova ferramenta de monitoramento no mês de outubro de 2017, o Visium Live, onde anteriormente era utilizado apenas o Nagios, para monitorar toda a sua infraestrutura de rede HFC em 84 cidades do estado de São Paulo.

Mas como a migração do monitoramento da rede HFC do Nagios para o Visium Live reduziu o tempo de análise dos incidentes emergenciais de infraestrutura e consequentemente o tempo de recuperação da falha por parte da equipe de campo?

O objetivo geral ao longo do relatório será comparar as funcionalidades presentes em ambas às ferramentas e demonstrar as novas funções que o Visium Live trouxe ao departamento, que contribuiram de maneira positiva para que houvesse a otimização no tempo de análise dos incidentes, a redução no tempo de recuperação das falhas de infraestrutura e o aumento dos incidentes identificados de maneira proativa, através de alarmes.

2 Fundamentação teórica

Durante esse capítulo serão abordados conceitos, ferramentas e protocolos referentes ao monitoramento de rede, de forma a facilitar o entendimento dos pontos que serão discutidos no decorrer deste relatório técnico.

2.1 Gerenciamento de rede

Quando falamos em gerenciamento de rede, Saydam (1996, p. 581) declara que:

Gerenciamento de rede inclui a implementação, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer as exigências operacionais, de desempenho e de qualidade de serviço a um custo razoável.

Uma parte fundamental no gerenciamento de redes é o NOC (**Network Operations Center** ou Centro de Operações de Rede), que segundo Kurose (2013) é um departamento responsável por monitorar todos os aspectos de sua rede e o desempenho dos serviços todos os dias do ano, 24 horas por dia, utilizando processos e ferramentas.

A *International Organization for Standardization* (ISO) segmenta o gerenciamento de rede em cinco áreas:

- Gerenciamento de Desempenho;
- Gerenciamento de Falhas;
- Gerenciamento de Configuração;
- Gerenciamento de Contabilização;
- Gerenciamento de Segurança.

No cenário desse relatório, o NOC tem como foco o gerenciamento de desempenho e falhas de uma rede HFC, ou seja, manter a rede operando dentro das condições predefinidas, detectando e sanando os problemas que estejam impactando ou possam vir a impactar os clientes desta rede.

2.2 Rede HFC (Híbrida Fibra-Coaxial)

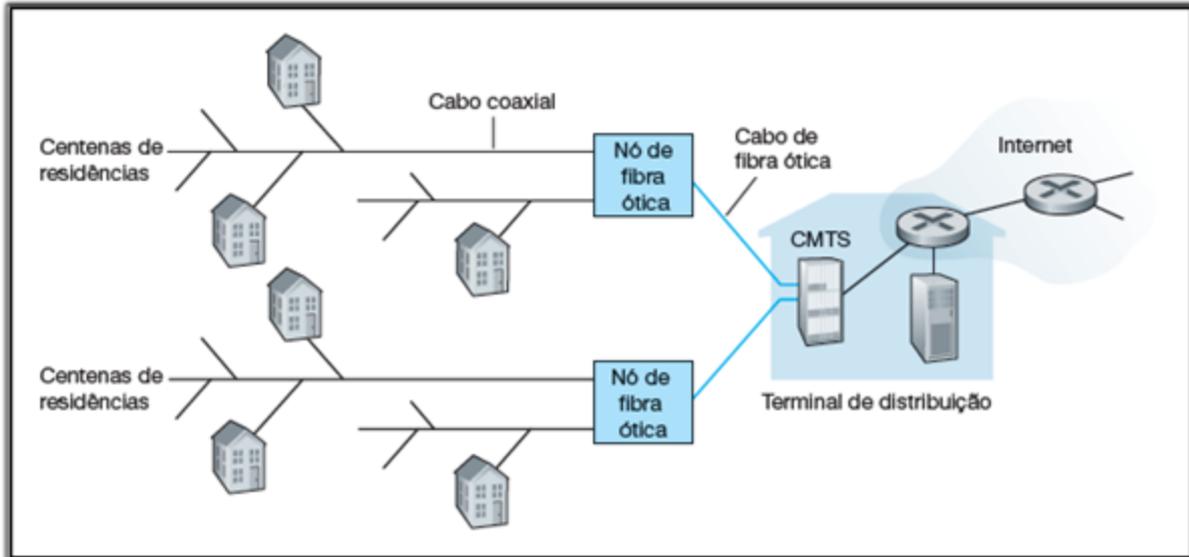
Segundo Kurose (2013), uma rede pode ser denominada híbrida fibra-coaxial quando o sinal chega através de um cabo de fibra ótica ao terminal de distribuição da região (*node* ou nó óptico) e a partir dela é utilizado o cabo coaxial para chegar às casas e apartamento dos clientes, conforme apresentado na figura 1. Cada *node*, equipamento que transforma o sinal de luz para RF (radiofrequência), tem capacidade para atender de 500 à 5000 residências.

Para que o assinante acesse a internet a cabo é necessário utilizar um *cable modem* (modem a cabo), conectando-o ao computador através da porta *Ethernet*.

Ainda a respeito da rede coaxial, Kurose (2013, p. 34), declara:

Uma característica importante do acesso a cabo é o fato de ser um meio de transmissão compartilhado. Em especial, cada pacote enviado pelo terminal viaja pelos enlaces downstream até cada residência e cada pacote enviado por uma residência percorre o canal upstream até o terminal de transmissão. Por essa razão, se diversos usuários estiverem fazendo o download de um arquivo em vídeo ao mesmo tempo no canal downstream, cada um receberá o arquivo a uma taxa bem menor do que a taxa de transmissão a cabo agregada. Por outro lado, se há somente alguns usuários ativos navegando, então cada um poderá receber páginas da Web a uma taxa de downstream máxima, pois esses usuários raramente solicitarão uma página ao mesmo tempo. Como o canal upstream também é compartilhado, é necessário um protocolo de acesso múltiplo distribuído para coordenar as transmissões e evitar colisões.

Figura 1- Rede de acesso híbrida fibra-coaxial

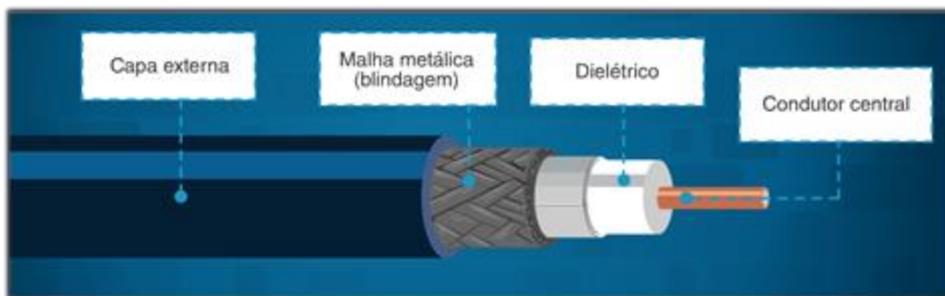


Fonte: KUROSE, Jim; ROSS, Keith (2013)

O cabo coaxial, de acordo com Kurose (2013), é constituído de dois condutores de cobre concêntricos, podendo alcançar taxas altas de transmissão de dados devido a essa configuração. Dessa forma, os cabos coaxiais tornaram-se muito comuns em sistemas de televisão e internet a cabo.

Na figura 2 pode-se identificar os principais componentes da estrutura de um cabo coaxial.

Figura 2- Estrutura do cabo coaxial

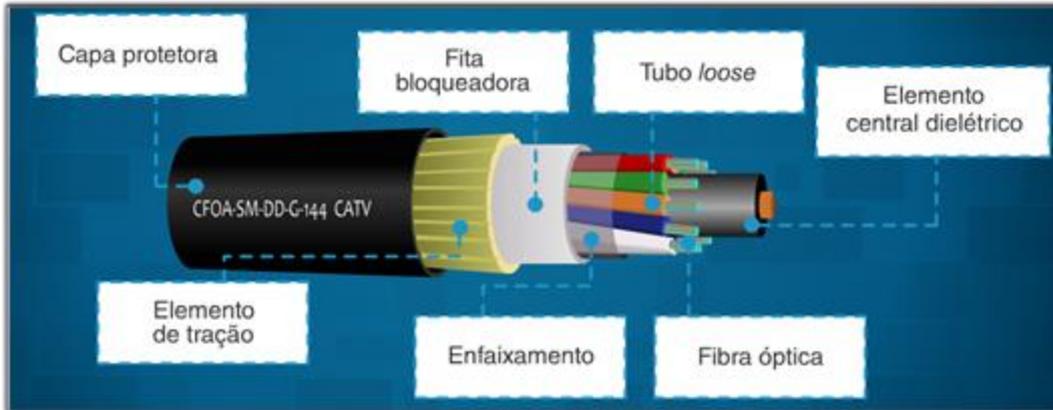


Fonte: Site de treinamento interno

A fibra ótica é um meio delgado e flexível que conduz pulsos de luz, cada um deles representando um bit. Fibras óticas são imunes à interferência eletromagnética, têm baixíssima atenuação de sinal até cem quilômetros (KUROSE, 2013).

Na figura 3 pode-se observar todos os itens que compõem a estrutura de um cabo de fibra ótica.

Figura 3- Estrutura do cabo de fibra óptica



Fonte: Site de treinamento interno

2.3 Protocolo SNMP (*Simple Network Management Protocol*)

Segundo Kocjan (2014), o protocolo SNMP foi desenvolvido, no final dos anos 80, para monitorar e gerenciar sistemas e dispositivos conectados a uma rede, atuando na camada de aplicação do TCP/IP e utilizando o protocolo de transporte UDP na porta 161

Como demonstrado na figura 4, o SNMP é usado para transmitir informações e comandos entre uma entidade gerenciadora e um agente que os executa em nome da entidade dentro de um dispositivo de rede gerenciado. (KUROSE, 2013).

Ele tem como seu principal objetivo estabelecer um padrão para a comunicação, independente do fabricante do equipamento, e facilitar a troca de informações entre os dispositivos, enviando notificações caso haja falha em algum serviço ou dispositivo.

Referente às principais utilizações do protocolo SNMP, Kurose (2013), afirma:

A utilização mais comum do SNMP é em um modo comando-resposta, no qual a entidade gerenciadora envia uma requisição a um agente, que a recebe, realiza alguma ação e envia uma resposta a requisição. Em geral, uma requisição é usada para consultar (recuperar) ou modificar (definir) valores de objetos MIB associados a um dispositivo gerenciado. Um segundo uso comum do SNMP é para um agente enviar uma mensagem não solicitada, conhecida como mensagem trap, à entidade gerenciadora. As mensagens trap são usadas para notificar uma entidade gerenciadora de uma situação excepcional que resultou em mudança nos valores dos objetos MIB. (p. 591).

Ainda segundo Kurose (2013), para o monitoramento da rede HFC, o SNMP fornece uma funcionalidade importante, o SNMP *trap*, que permite um agente enviar uma notificação ao gerente de que seu status foi alterado, o que pode indicar que há uma falha naquele dispositivo.

Em uma rede gerenciada utilizando o protocolo SNMP temos três componentes importantes:

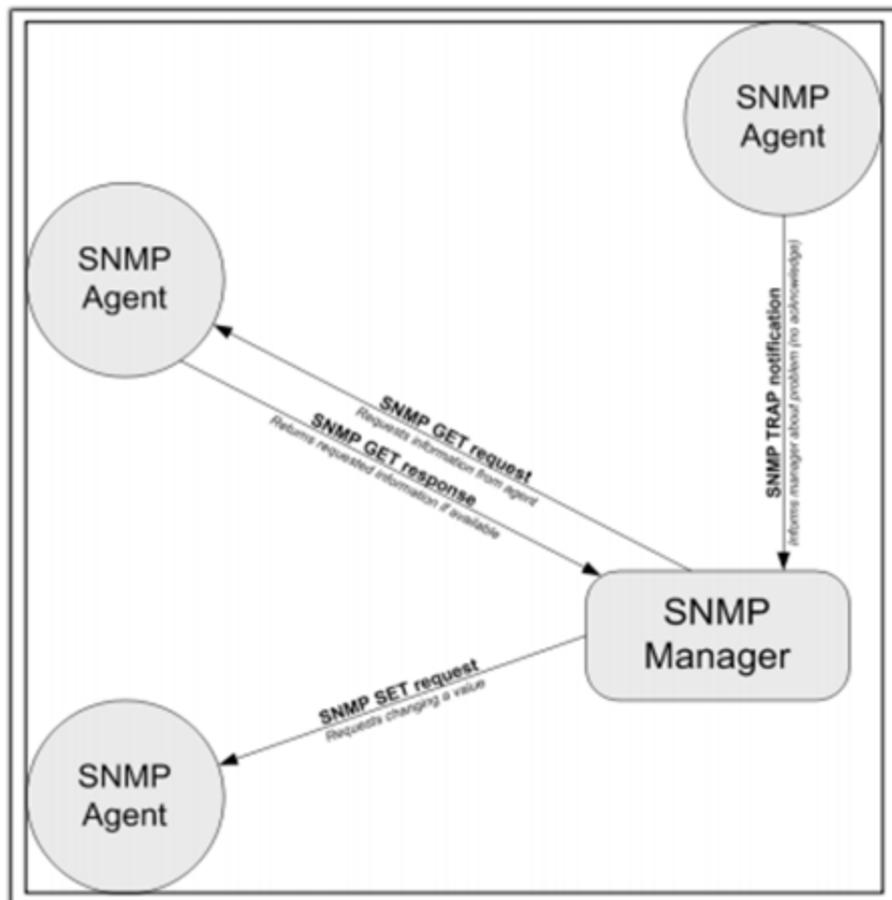
- **Gerente:** Interface de gerenciamento que envia e recebe requisições SNMP aos agentes.

- **Agente:** Está associado ao dispositivo ou sistema que está na presente na rede, seu papel é responder as requisições realizadas pelo gerente e encaminhar notificações caso haja mudança de status ou atinja algum parâmetro previamente configurado, através do SNMP trap.
- **MIB (Base de Informações de Gerenciamento):** Base de dados com objetos que podem representam o status dos dispositivos da rede.

Ao utilizar o SNMP para o gerenciamento da rede, podemos obter diversas vantagens e benefícios, como por exemplo:

- Pode ser utilizado para gerenciar dispositivos de diversos fabricantes;
- Consome poucos recursos da rede;
- Aumento da disponibilidade dos sistemas, serviços e dispositivos presentes na rede;
- Agilidade na identificação de falhas na rede.

Figura 4- Modelo de gerenciamento do SNMP



Fonte: KOCJAN, Wojciech (2014)

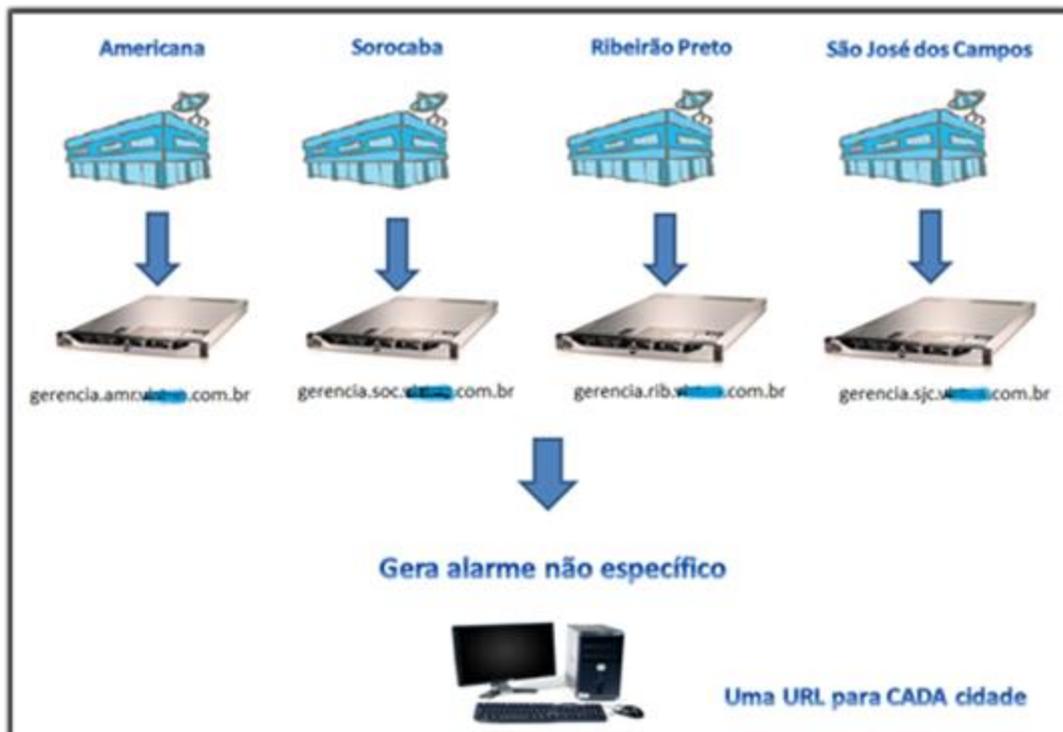
2.4 Nagios

De acordo com Kocjan (2014), o Nagios é uma ferramenta de código aberto para monitoramento de sistemas, redes e infraestrutura, desenvolvida por Ethan Galstad. A aplicação oferece recursos de monitoramento e alarmes para os serviços e ativos monitorados.

Os servidores do Nagios são responsáveis pela coleta de informações diretamente dos pontos de concentração (*Headend*), realizando requisições ao CMTS (**Cable Modem Termination System**) através do protocolo SNMP. O CMTS é um equipamento instalado no *headend* para liberação do sinal de retorno, realizando a comunicação com a rede HFC através das placas cable, que faz a interface entre o CMTS e o sinal RF da rede HFC.

A figura 5 mostra a antiga infraestrutura utilizada pela empresa, em que cada operação possuía um servidor Nagios, dessa forma havia uma página web do Nagios para cada cidade, totalizando 64 páginas de monitoramento para as cidades do interior de São Paulo e 20 para as cidades da região metropolitana de São Paulo.

Figura 5- Estrutura do Nagios



Fonte: Autor

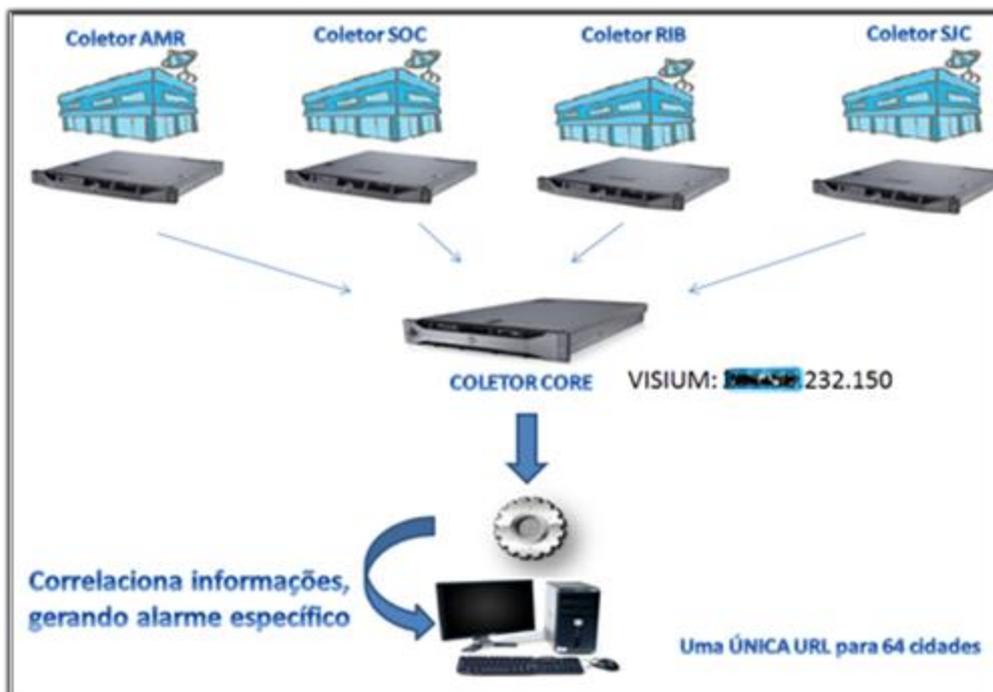
2.5 Visium Live

Segundo Humberto Pinheiro, CEO da Visium Soluções em TI, o Visium Live é uma solução de monitoramento e gerência de incidentes de infraestrutura para rede HFC, modular, escalável e baseada no protocolo SNMP.

Conforme figura 6, a estrutura do Visium também utiliza um servidor (Coletor Visium) para cada operação, que é responsável por efetuar as requisições SNMP aos equipamentos, realizar coletas e tratamento de dados de monitoração e encaminha-los ao núcleo de inteligência, o servidor Coletor Core, que consolida os dados de todos os servidores de coleta, disponibilizando em apenas uma página Web, o monitoramento de todas as operações.

O Visium Live entrou em operação em todas as cidades a partir do mês de outubro de 2017.

Figura 6- Estrutura do Visium Live



Fonte: Autor

3 Comparando funcionalidades em comum

As funcionalidades das ferramentas são utilizadas para monitorar a rede HFC, gerando gráficos de fácil visualização para o usuário final, auxiliando na identificação e acompanhamento de eventos massivos.

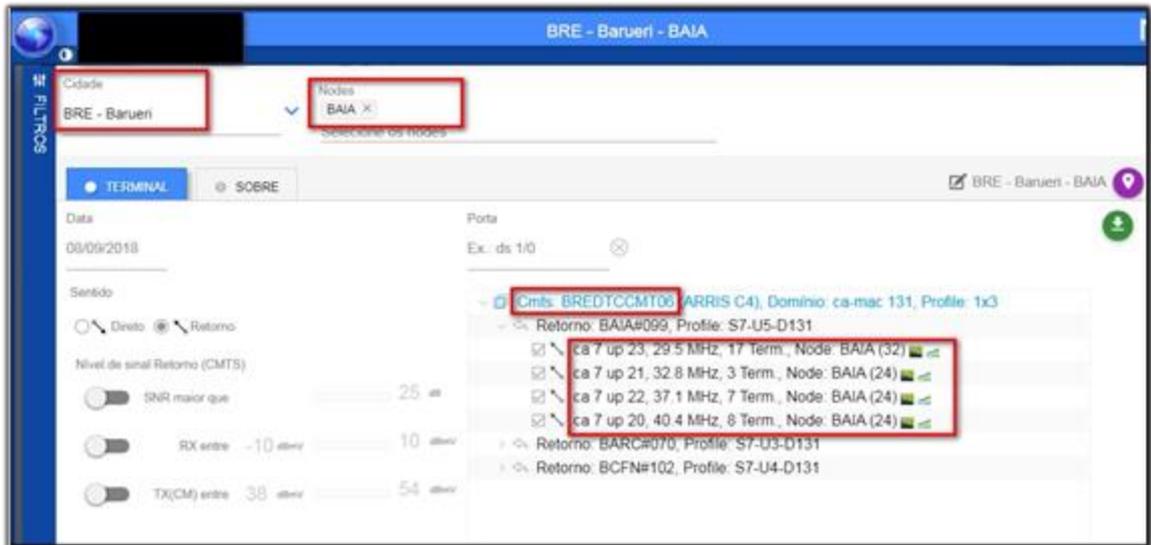
Nesse capítulo serão comparadas as funcionalidades em comum nas duas ferramentas.

3.1 Consulta node

Para realizar uma consulta a um *node* no Nagios, primeiramente é necessário saber em qual CMTS e placa *cab* esse *node* está alocado. Para obter essa informação é

preciso acessar outro sistema interno, que contém esses dados sobre os *nodes*, como pode ser visto na figura 7.

Figura 7- Sistema de consulta interface



Fonte: Autor

Com essas informações, o próximo passo é acessar o Nagios da cidade desejada e inserir o usuário e senha, conforme figura 8.

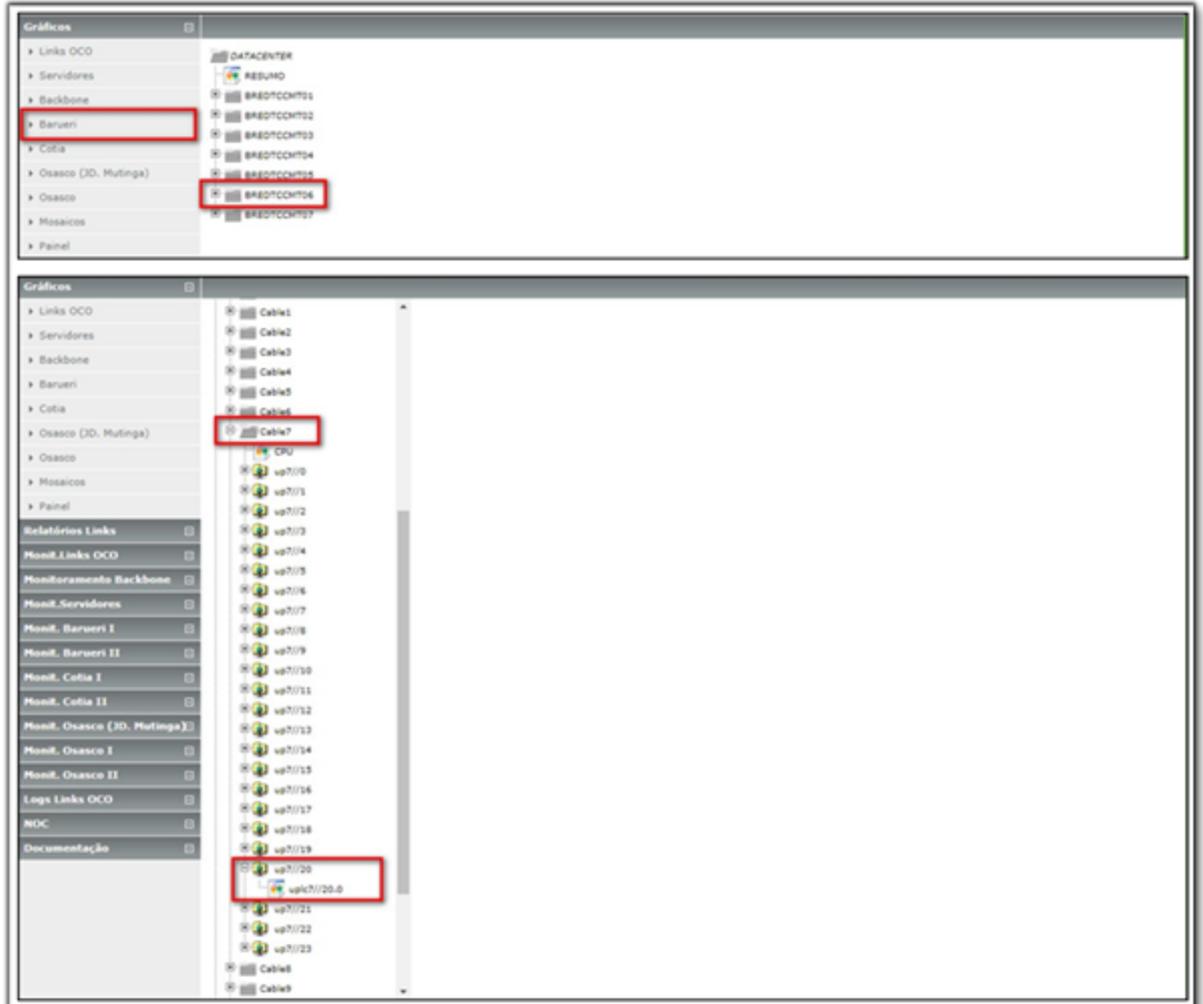
Figura 8- Tela de login do Nagios



Fonte: Autor

Após o *login* ter sido realizado com sucesso, na barra lateral, seleciona-se a opção de gráficos, conforme figura 9. Em gráficos, seleciona-se a cidade, o CMTS e as placas *cabre* que foram obtidos anteriormente.

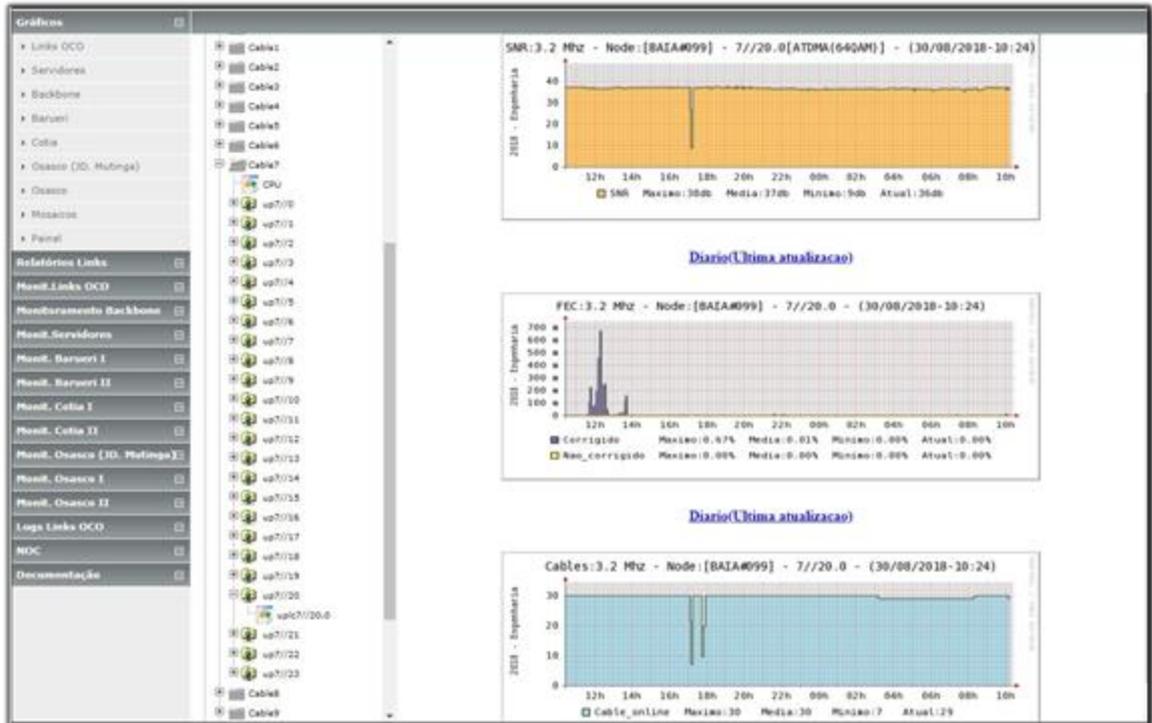
Figura 9- Seleção do CMTS e placa *cab*le



Fonte: Autor

Seguindo todos esses passos, o gráfico do node desejado será exibido, conforme figura 10, e o analista poderá começar a sua análise, podendo verificar os níveis de ruído e quantidade de clientes online em determinada placa.

Figura 10- Gráfico Nagios



Fonte: Autor

Diferente da consulta no Nagios, no Visium Live não é necessário realizar consultas em outros sistemas e seguir diversos passos para a visualização dos gráficos dos *nodes*.

Após o login no sistema, acessasse no menu superior a opção de gráficos e em seguida, no menu lateral, a opção *node*, conforme figura 11.

Figura 11- Interface do Visium Live

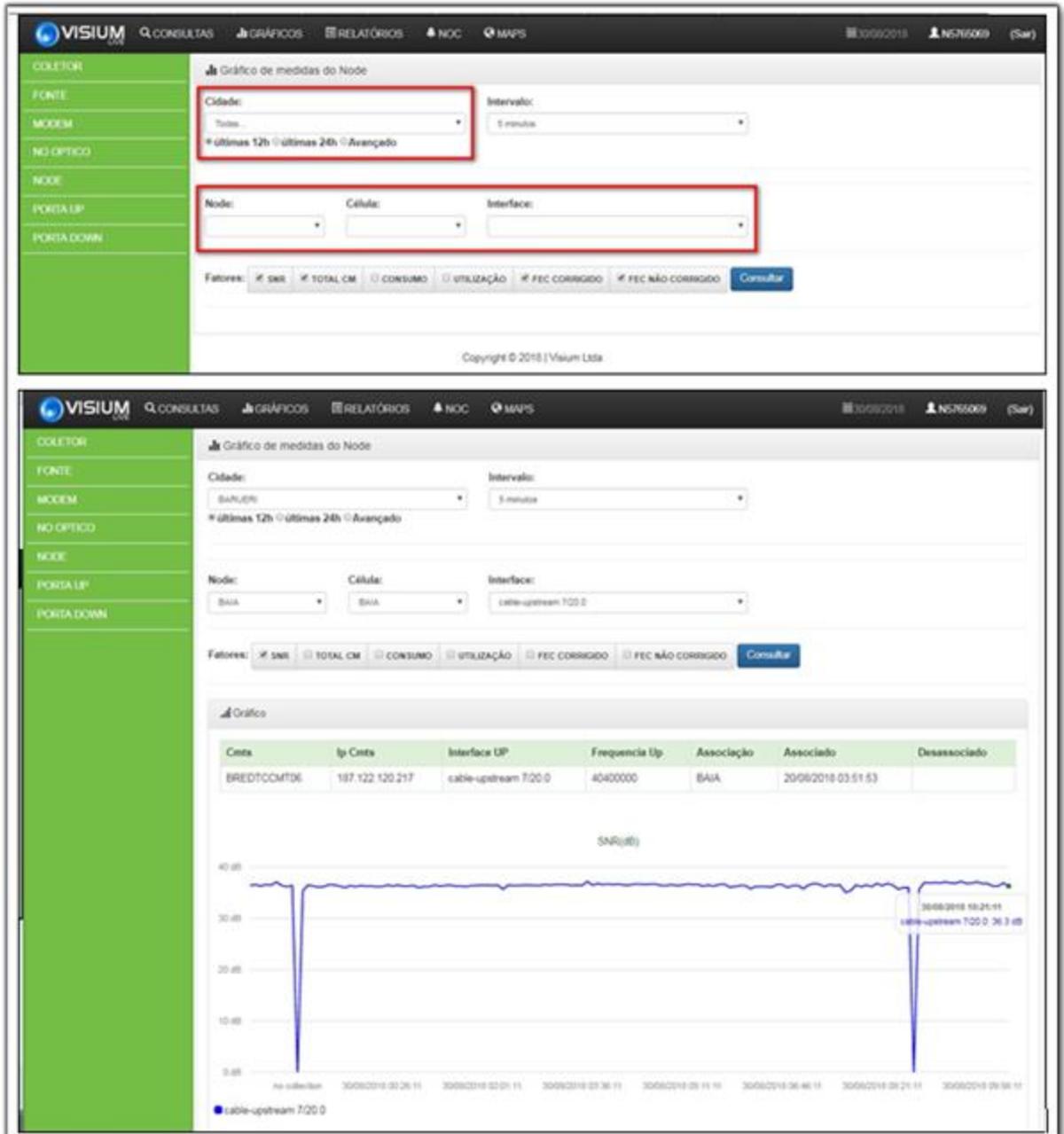


Fonte: Autor

E então, como pode ser visto na figura 12, é necessário apenas selecionar a cidade, o *node* e os itens que deseja visualizar e o gráfico será exibido.

Dessa forma o analista consegue iniciar a sua análise de maneira mais rápida, se comparado ao Nagios.

Figura 12- Seleção do node no Visium Live



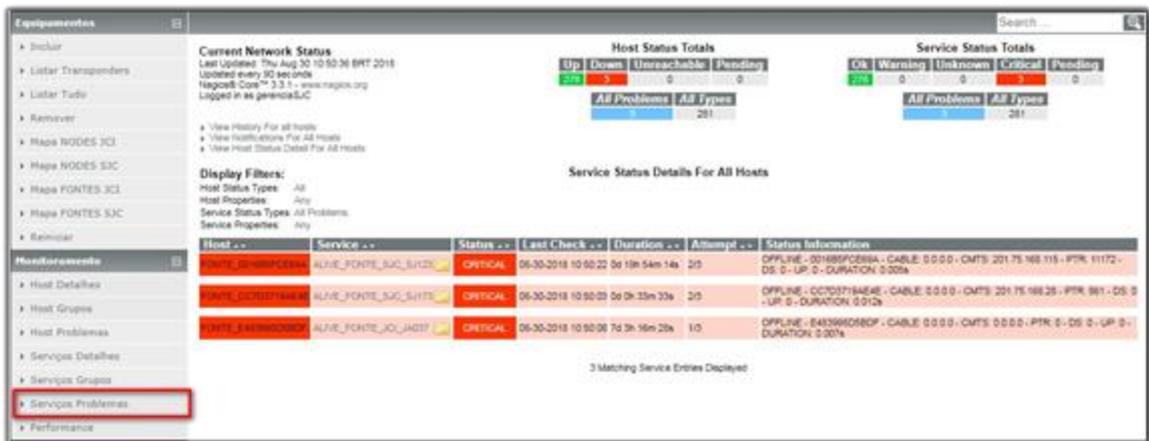
Fonte: Autor

3.2 Consulta e monitoramento de fontes

No Nagios Fontes tudo o que podemos obter de informação é se o *cable modem* da fonte está alarmado e o endereço em que ela está localizada. Não temos informações adicionais referentes ao banco de baterias, por exemplo.

Após o login no Nagios Fonte da cidade, selecionamos a opção Serviços Problemas no menu lateral, conforme figura 13. Nessa tela são exibidas todas as fontes que estão com o status *down*, ou seja, as fontes que estão com o MAC do *cable modem* off-line.

Figura 13- Interface do Nagios Fonte



Fonte: Autor

Ao selecionar a fonte desejada, podem-se visualizar alguns detalhes técnicos, endereço e o tempo que o serviço está apresentando falha, conforme figura 14.

Figura 14- Detalhes de um alarme de fonte

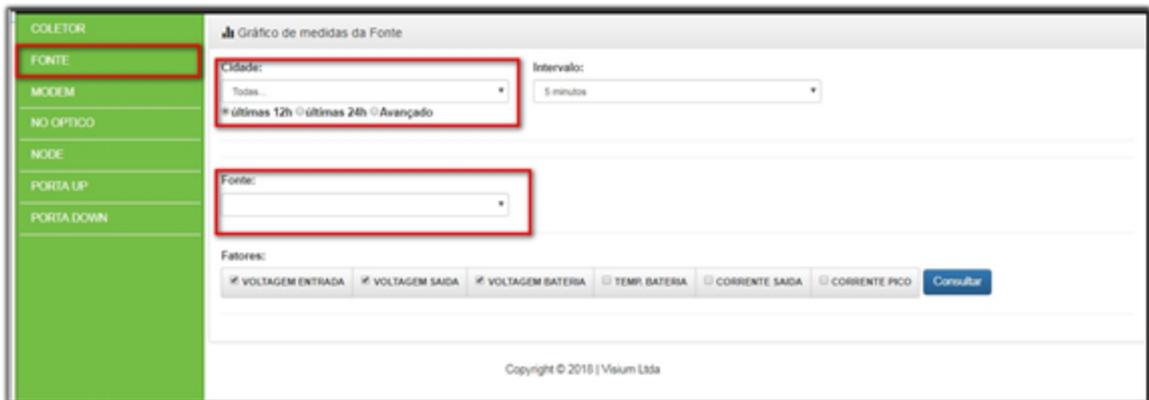


Fonte: Autor

O grande diferencial do monitoramento de fontes do Visium é a capacidade de verificar informações sobre o banco de baterias, além de todas as outras informações já obtidas pelo Nagios, como detalhes técnicos, tempo de indisponibilidade e endereço em que está localizado o equipamento.

Como mostra a figura 15, pode-se acessar esses dados através da opção fonte do menu lateral e em seguida selecionando a cidade e o *node*.

Figura 15- Seleção da fonte

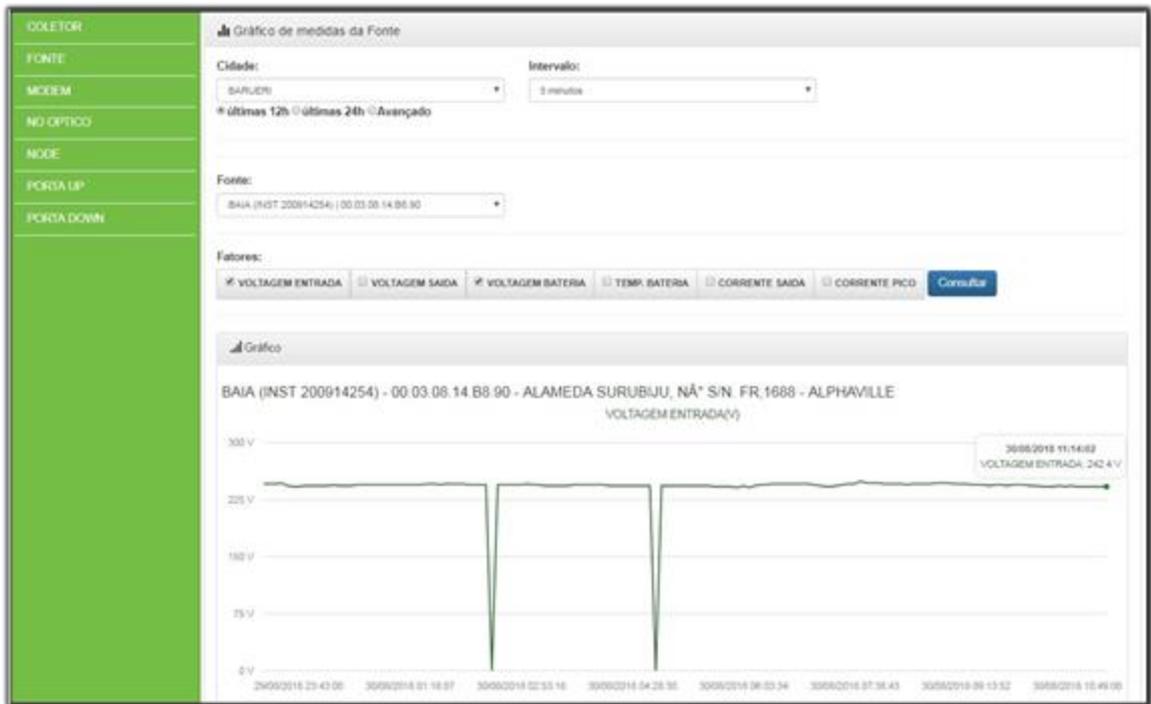


Fonte: Autor

Nos gráficos referentes ao banco de baterias é possível identificar o momento em que houve uma falha de energia externa, o momento em que as baterias assumiram e o principal, o tempo de autonomia das baterias, sendo possível deslocar o técnico para acionar o gerador com maior assertividade.

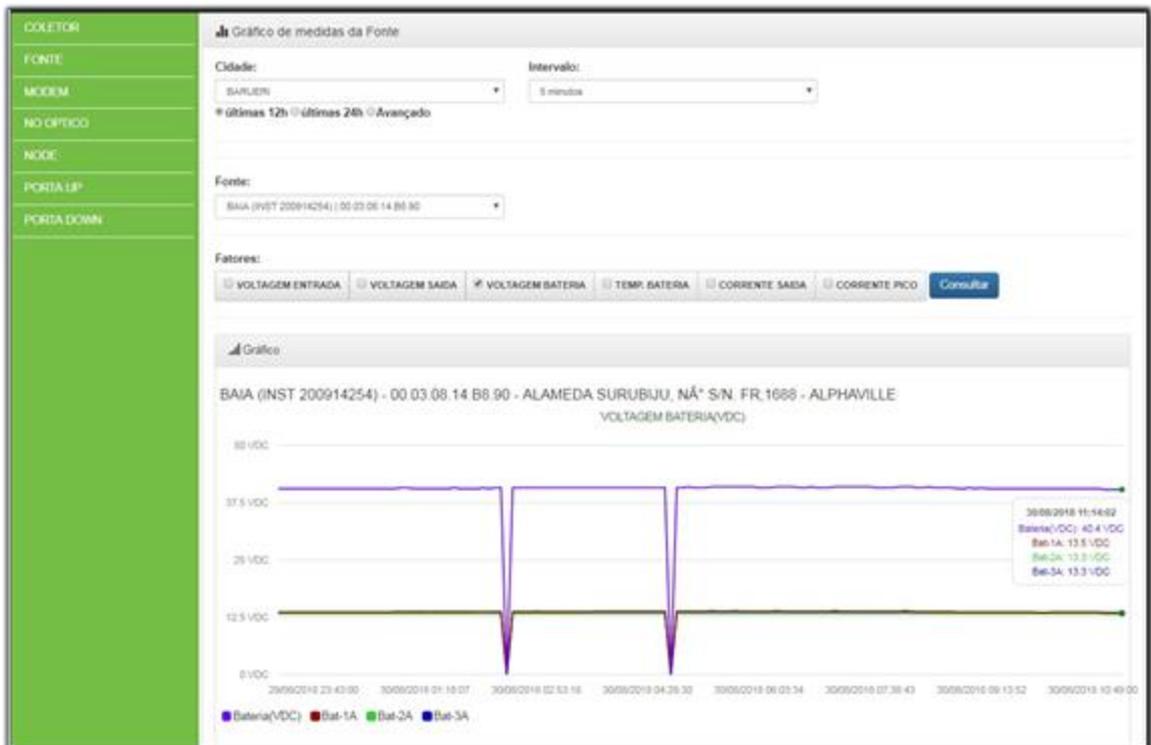
Nas figuras 16 e 17, respectivamente, é possível verificar se há voltagem de entrada na fonte e autonomia da bateria, caso haja falha na alimentação de energia por parte da concessionária.

Figura 16- Gráfico voltagem de entrada da fonte



Fonte: Autor

Figura 17- Gráfico representando a autonomia da bateria da fonte



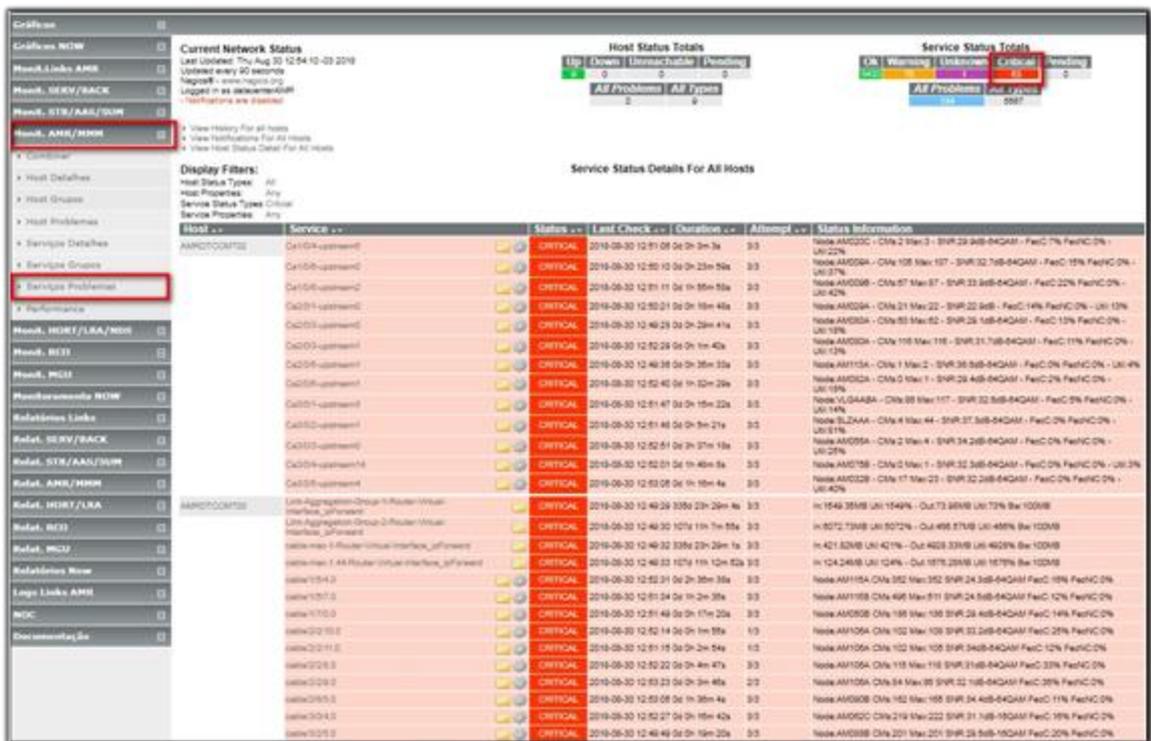
Fonte: Autor

3.3 Painel de alarmes

O Nagios oferece um painel de alarmes simples e sem opções de filtros, tornando o monitoramento dos serviços complicado, resultando na demora na identificação de possíveis problemas massivos. Conforme figura 18, ele pode ser acessado selecionando a aba monitoramento, a opção Serviços Problemas e o *Status Critical* no canto direito superior.

Para complicar ainda mais a situação, é necessário abrir uma página web para cada cidade que se deseja monitorar.

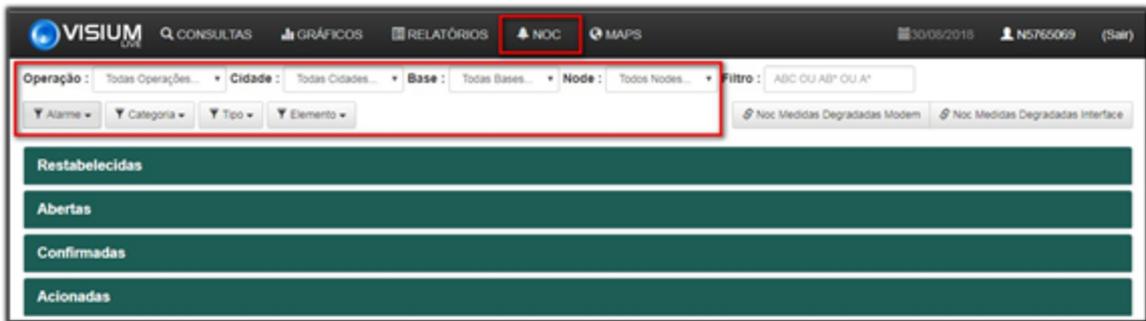
Figura 18- Painel de alarmes do Nagios



Fonte: Autor

De acordo com a figura 19, ao acessar a aba NOC no menu superior, temos acesso ao painel de alarmes do Visium, que conta com diversos filtros e abas para segmentar o tratamento dos alarmes, dessa forma temos um painel organizado, o que torna a identificação dos incidentes mais fácil e rápida.

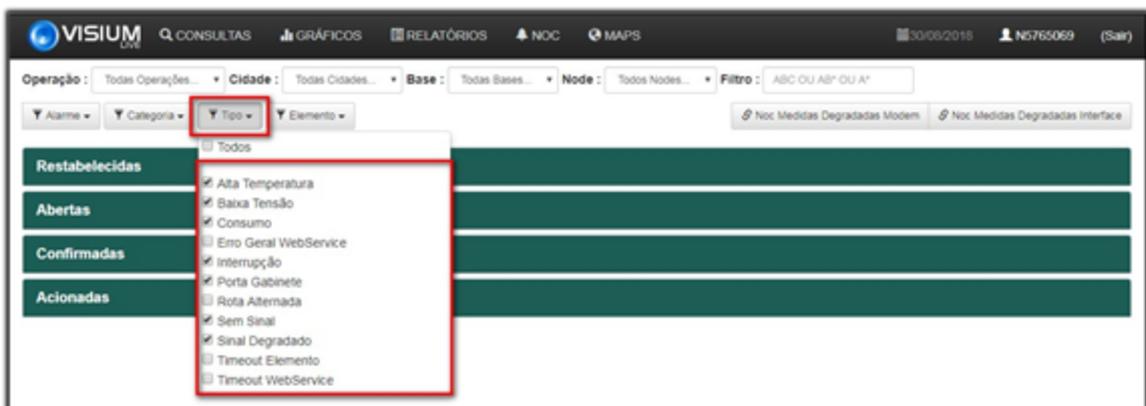
Figura 19- Interface painel de alarmes Visium Live



Fonte: Autor

No filtro 'Tipo' selecionam-se os tipos de alarmes, conforme figura 20. Os alarmes mais comuns são os de interrupção e degradação de sinal.

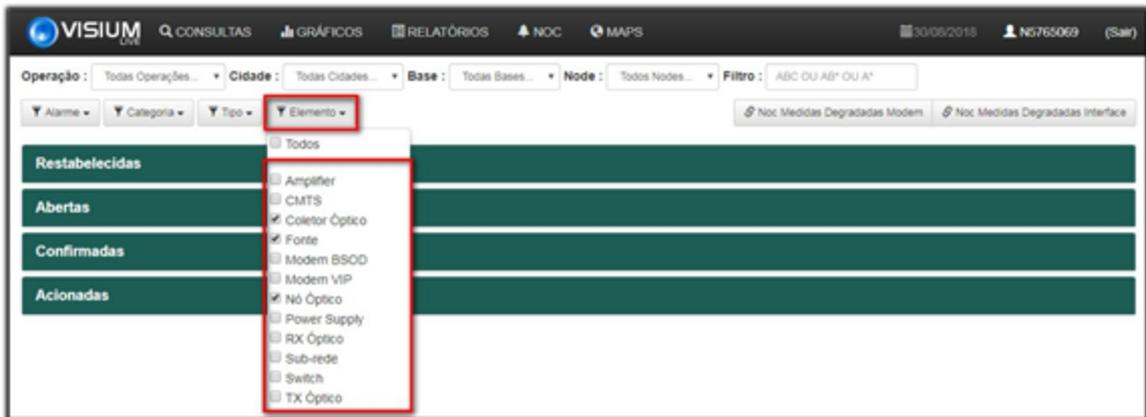
Figura 20- Filtros do painel de alarme



Fonte: Autor

A figura 21 mostra a opção 'Elemento' onde são selecionados quais ativos de rede serão exibidos os alarmes, tendo como os principais elementos a serem monitorados os coletores e os nós ópticos (*nodes*).

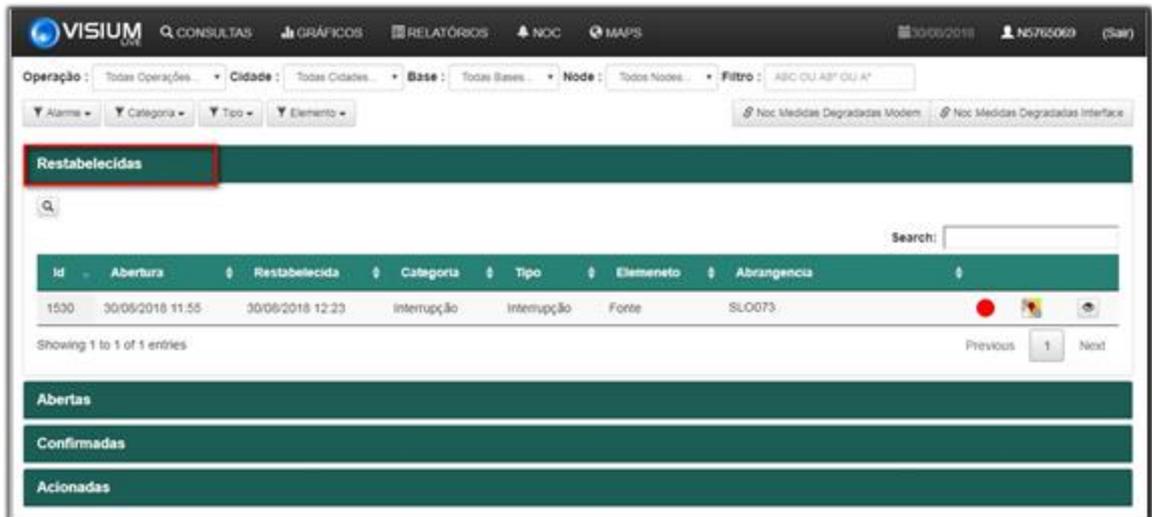
Figura 21- Filtro para a seleção de equipamento



Fonte: Autor

Na aba dos alarmes restabelecidos são exibidos os alarmes em que os problemas já foram sanados, como mostra a figura 22. Esses alarmes ficam em monitoramento durante 15 minutos e caso não haja nova falha são finalizados automaticamente.

Figura 22- Aba de alarmes restabelecidos



Fonte: Autor

Na aba abertos são os alarmes que ainda não foram tratados e seguem os filtros que foram definidos no menu superior, conforme figura 23.

Figura 23- Aba de alarmes novos

ID	Abertura	Categoria	Tipo	Elemento	Abrangência	Log
1534	30/05/2018 12:23	Degradação	Sinal Degradado	Nó Óptico	GTAD45	0
1533	30/05/2018 12:16	Interrupção	Interrupção	Fonte	PRF004	0
1532	30/05/2018 12:09	Degradação	Sinal Degradado	Nó Óptico	LNA023	0
1531	30/05/2018 12:06	Interrupção	Interrupção	Fonte	BL0021	0
1526	30/05/2018 11:36	Interrupção	Interrupção	Fonte	PRF012	0
1521	30/05/2018 11:14	Degradação	Sinal Degradado	Nó Óptico	GTAD03	0
1506	30/05/2018 09:56	Interrupção	Interrupção	Fonte	PRF009	0
1504	30/05/2018 09:53	Interrupção	Interrupção	Fonte	MOR011	0
1503	30/05/2018 09:51	Interrupção	Interrupção	Fonte	PRF026	0
1501	30/05/2018 09:31	Interrupção	Interrupção	Fonte	PRF025	0

Fonte: Autor

De acordo com a figura 24, ao clicar sobre o alarme pode-se visualizar os detalhes técnicos sobre o possível problema,

Figura 24- Detalhes de um alarme novo

Hipótese: 1535

Descrição: Monitorando o transponder da fonte ADA029 (MAC 00 90 EA 00 39 96), detectou que está offline.

Node Abrangência: ADA029

Confirmada:

Restabelecida:

Usuário:

Área Aclonado:

Previsão Retorno:

Ticket Externo: Ticket Externo - Max 40 caracteres

Log

Histórico Log:

Incluir	Usuário	Descrição

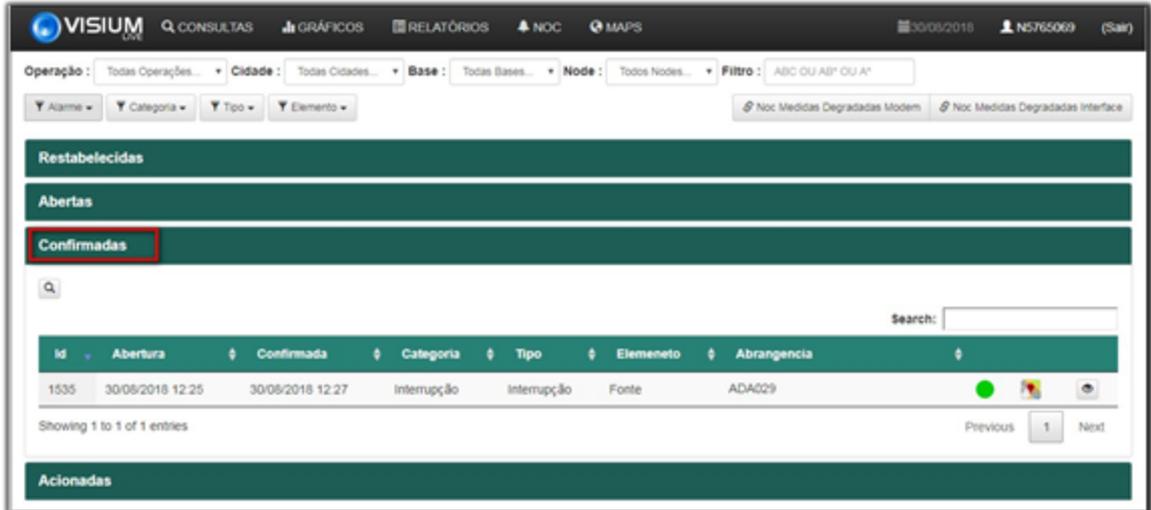
Eventos da Hipótese

Data e Hora	Tipo	Descrição
30/05/2018 12:25:36	Interrupção	Transponder de FONTE: ADA029, MAC: ADDRESS: 00 90 EA 00 39 96, IP: 10.57.8.16, OFFLINE. Consultado às 30/05/2018 12:25:36

Fonte: Autor

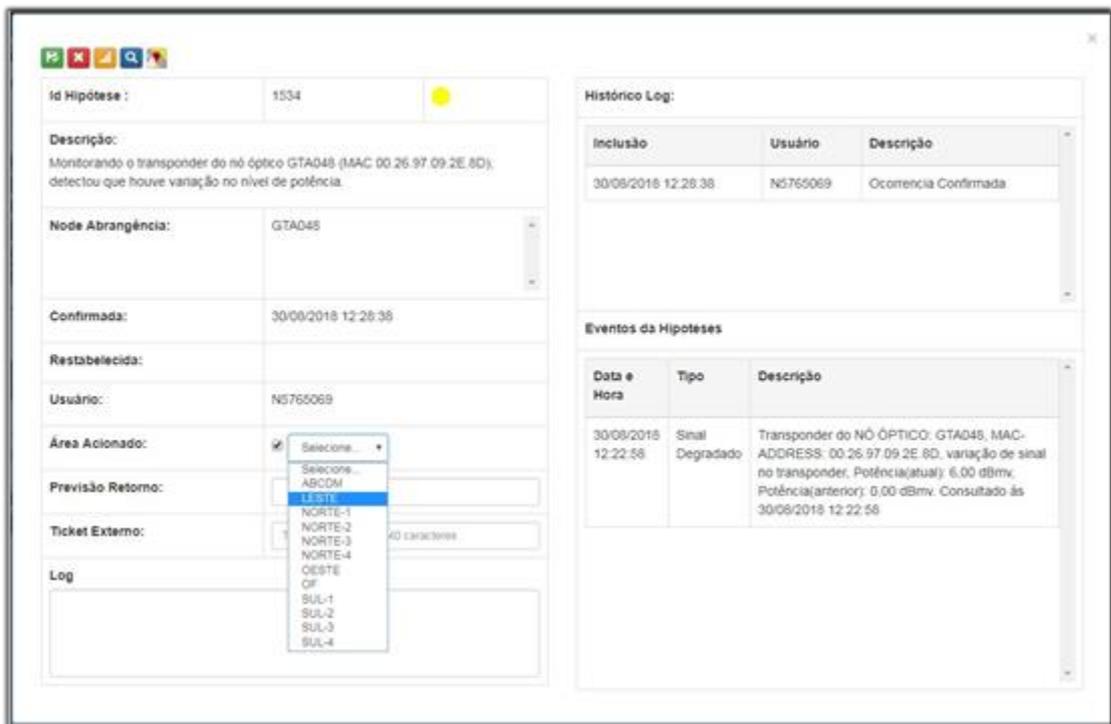
Na figura 25, pode-se visualizar a aba dos alarmes que foram confirmados e estão em tratamento, ao entrar nos detalhes o analista, caso o alarme seja procedente, realizara o acionamento, encaminhando o alarme para a aba de acionados, conforme figura 26.

Figura 25- Aba de alarmes em análise



Fonte: Autor

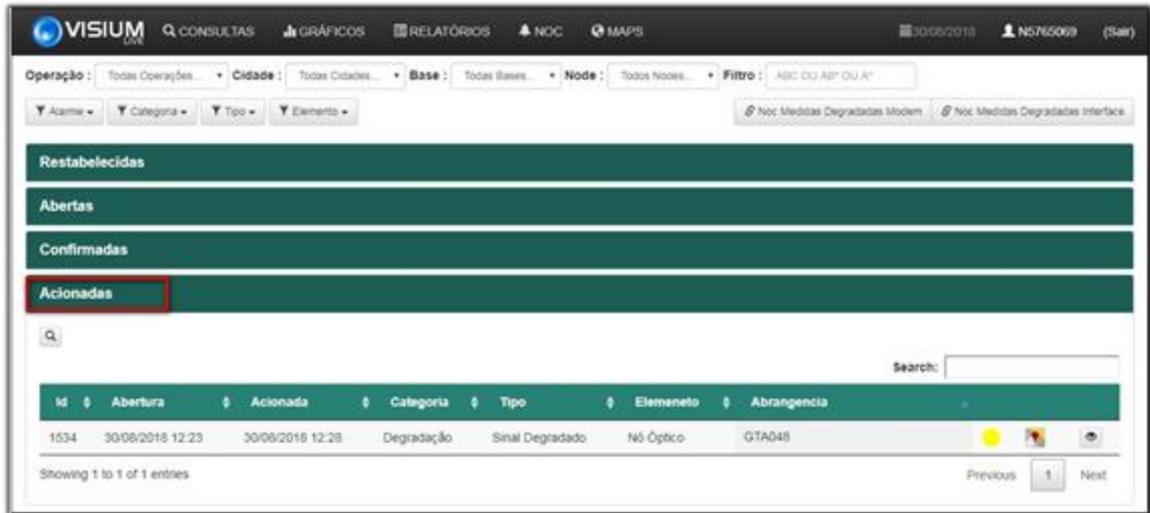
Figura 26- Detalhes de um alarme em tratamento



Fonte: Autor

Na aba 'Acionadas' estão todos os alarmes em que foi identificado problema de infraestrutura e a equipe de campo está acionada para a verificação e correção da falha, conforme figura 27.

Figura 27- Aba de alarmes encaminhados para campo



Fonte: Autor

4 Funcionalidades presentes apenas no Visium Live

4.1 Consulta massiva de MACS

Através da funcionalidade de consulta modem lista, o analista pode fazer a verificação de um grande bloco de MACS de uma só vez, como pode ser visto na figura 28, dessa forma têm-se um aumento no tempo de consulta dos níveis de sinal durante o fechamento de incidentes ou ao realizar testes com o técnico de campo.

Anteriormente essa consulta podia ser realizada através de outro sistema, porém apenas um MAC por vez, o que tornava essa consulta demorada e massante, podendo levar de 10 a 15 minutos e através do Visium Live pode ser feita em no máximo 1 minuto.

Figura 28- Consulta massiva de MACS

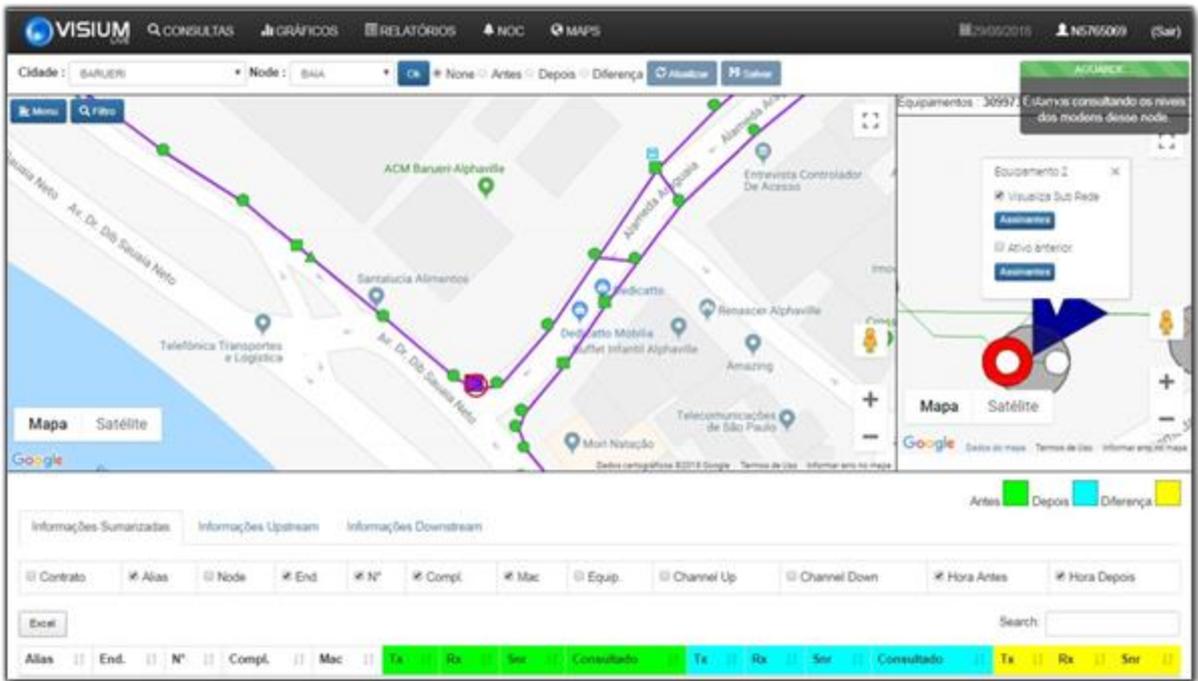
MAC	IP	MODEM STATUS	NODE	SNR UP	SNR DOWN	RX UP	RX DOWN	TX UP	DOC SIS
00D037F56BEF	10.66.227.222	Online	BAIR	36.6 dB	38.4 dB	0 dBmV	-2.7 dBmV	46.7 dBmV	2
00D037F6F95D	10.66.225.164	Online	BAIR	33.6 dB	38.1 dB	0 dBmV	-0.7 dBmV	43.2 dBmV	2
08952AA6627C	10.18.128.171	Online	BAIR	34.7 dB	42.5 dB	-1 dBmV	1.3 dBmV	45 dBmV	3
08952AB01F9A	10.66.232.146	Online	BAIR	33.9 dB	42.7 dB	-0.5 dBmV	1.4 dBmV	44.2 dBmV	2
105F49180926	10.28.128.194	Online	BAIR	36.1 dB	43.2 dB	-0.5 dBmV	10.1 dBmV	32.2 dBmV	3
105F49C5457C	10.18.128.196	Online	BAIR	34.7 dB	42 dB	-0.5 dBmV	-0.5 dBmV	51 dBmV	3
105F49D1CEE6	10.28.128.218	Online	BAIR	35.1 dB	43.6 dB	0 dBmV	7.4 dBmV	40.7 dBmV	3
105F49D22DF0	10.28.131.107	Online	BAIR	36.1 dB	42.5 dB	0 dBmV	0.5 dBmV	43.7 dBmV	3
105F49D41732	10.28.129.18	Online	BAIR	33.9 dB	41.5 dB	0.5 dBmV	-6.2 dBmV	43 dBmV	3
105F49D6D77E	10.28.128.226	Online	BAIR	36.6 dB	40.3 dB	0.5 dBmV	-4.4 dBmV	41.7 dBmV	3
105F49E14A4C	10.28.128.250	Online	BAIR	33.6 dB	43.9 dB	-0.5 dBmV	2.6 dBmV	49.2 dBmV	3

Fonte: Autor

4.2 Níveis de referência

Na funcionalidade chamada níveis de referência, que pode ser vista na figura 29, o analista pode selecionar um equipamento de rede, consultar os níveis de sinal de todos os assinantes conectados naquele equipamento, salvar esses dados e depois realizar uma consulta futura e comparar as duas consultas, a fim de identificar a mudança dos níveis de sinal.

Figura 29- Interface da funcionalidade níveis de referência



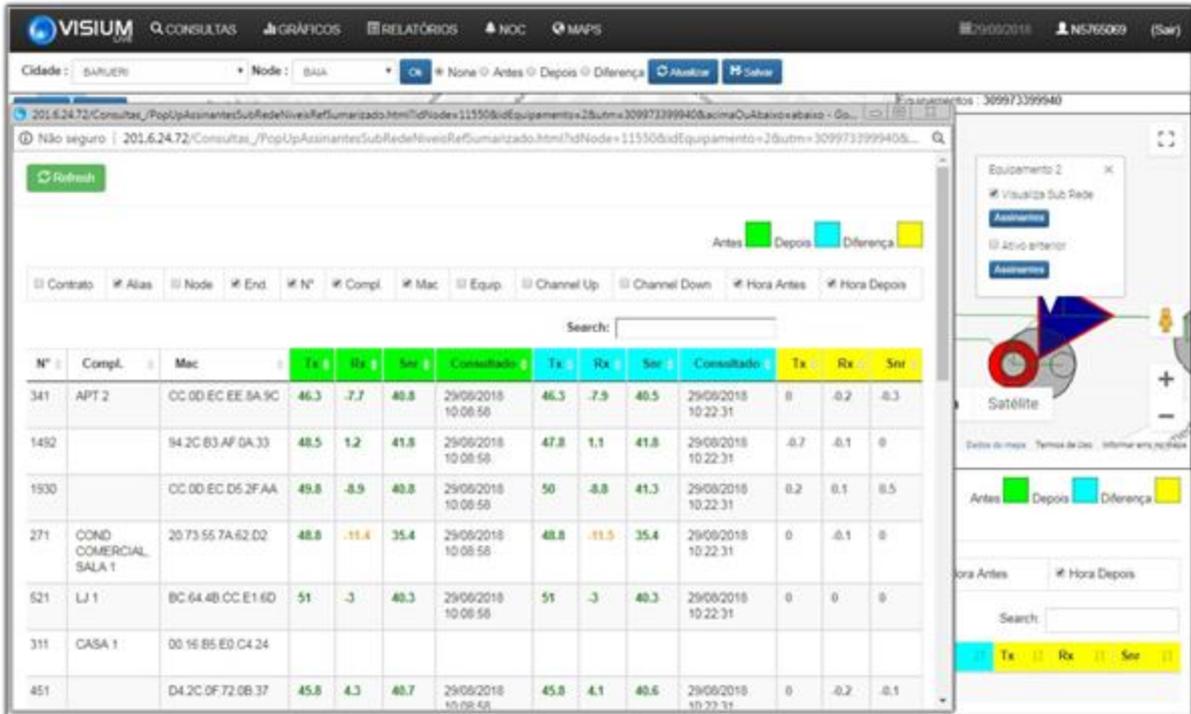
Fonte: Autor

O pré e pós manobra é um processo utilizado para comparar os níveis de sinal antes e depois da manutenção, coletando evidências de que houve melhoria após a intervenção técnica.

A principal função dos níveis de referência no departamento é auxiliar no pré e pós-manobra, pois como se pode verificar na figura 30, a ferramenta tornou a visualização dos níveis antes e depois da manutenção muito fácil e rápida, através dessa funcionalidade pode-se fazer todo esse processo em 2 minutos, anteriormente levava-se mais de 1 hora, e muitas vezes não era realizado por falta de tempo.

Esse processo, antes da implementação do Visium Live era realizado, em média, por seis analistas, devido à demora na obtenção das evidências de que os níveis pós-manutenção estavam dentro do padrão, agora é realizada por dois analistas.

Figura 30- Consulta de MACS antes e depois



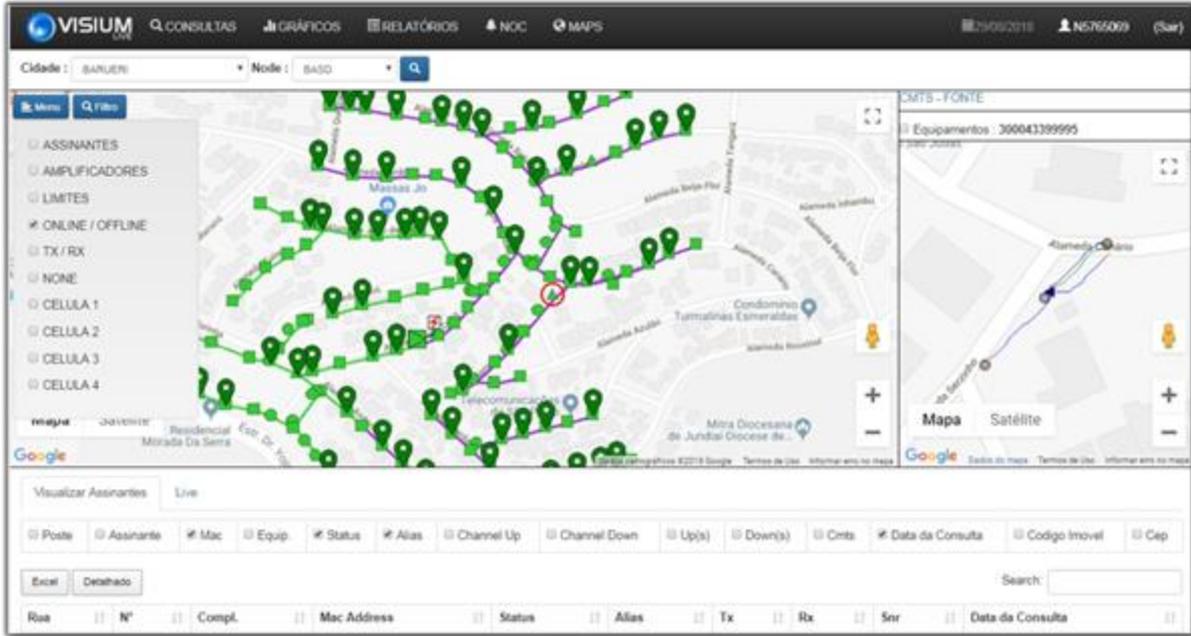
Fonte: Autor

4.3 Maps

O *Maps* oferece visualização detalhada da topologia da rede, conforme figura 31, e se podem consultar os *cable modems* de todos os assinantes conectados ao equipamento selecionado, como por exemplo, o *node*, amplificador, divisor ou *tap* (equipamento passivo que conecta o cliente à rede), como pode ser visto na figura 32. Porém, sua principal função é determinar o possível ponto da falha nos casos de interrupção de sinal, como veremos de forma detalhada durante o capítulo 5, onde será demonstrado um caso real.

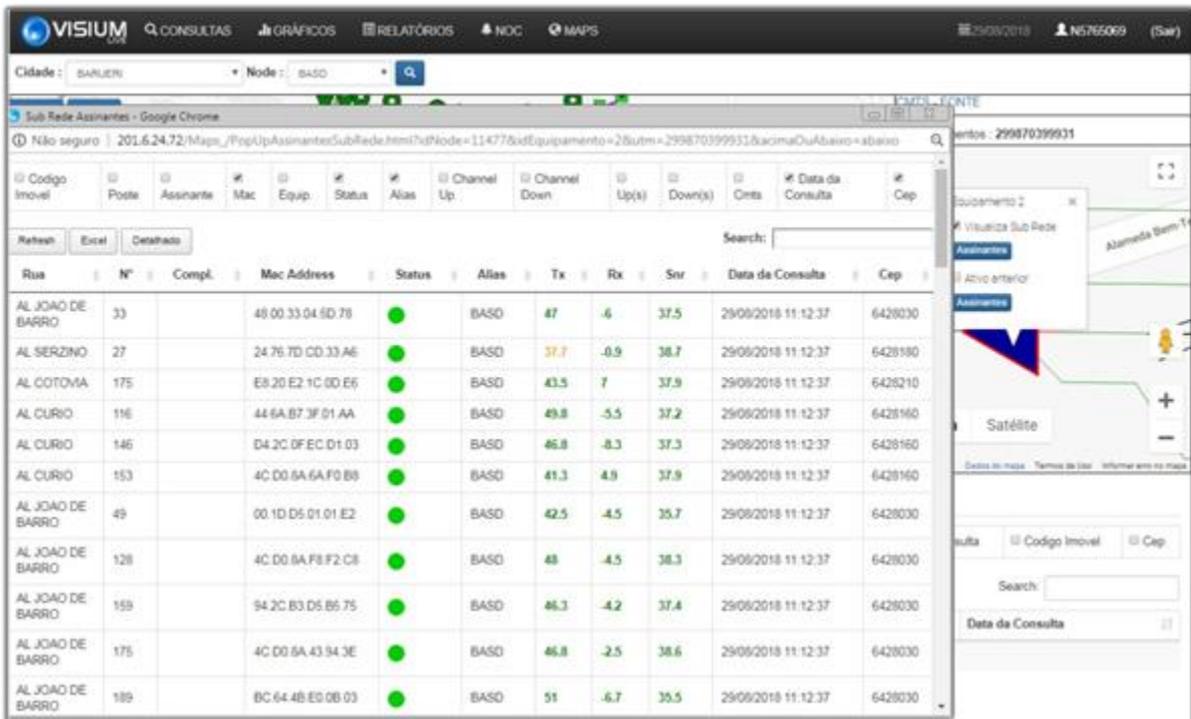
O tempo ganho com essa funcionalidade impacta diretamente nos indicadores de negócio da empresa, reduzindo drasticamente o tempo médio de recuperação, auxiliando diversas operações a atingir o SLA (**Service Level Agreement**) de 90 minutos.

Figura 31- Interface *Maps*



Fonte: Autor

Figura 32- Consulta dos níveis de todos os clientes do *node*



Fonte: Autor

5 Exemplo utilizando incidente real

Nesse capítulo veremos como era realizada a tratativa de um incidente sem sinal antes da implementação do Visium Live e compará-lo ao método utilizado agora.

Sem o auxílio do Visium Live, normalmente o técnico era encaminhado para o endereço do reclamante, no ponto 1 da figura 33, onde realiza a medição dos sinais e verifica se o *tap* está queimado, oxidado ou com água, caso o equipamento esteja dentro do padrão, mas com ausência ou degradação do sinal, é necessário voltar a rede e ir para o ponto 2, o amplificador, onde são verificados os níveis de sinal e conexões, caso o sinal já esteja chegando fora do padrão na entrada do amplificador, é necessário voltar a rede novamente, dessa vez ao divisor, identificado pelo ponto 3, onde serão realizados os mesmos procedimentos realizados no *tap*.

Nesse exemplo da figura 33, o técnico teria que voltar a rede até o ponto 5, onde foi trocado o amplificador que estava queimado, como pode ser visto no fechamento do incidente na figura 35.

Figura 33- Projeto de rede no CAD



Fonte: Autor

Ao realizar a tratativa pelo Visium Live, através da funcionalidade *Maps*, ao visualizar a topologia já é possível identificar que o amplificador, ponto 2 na figura 34, é o ponto da falha, pois a partir dele todos os assinantes estão *offline*, indicado pelos pontos em vermelho.

Utilizando esse método, o técnico vai direto no ponto da falha e, conseqüentemente, consegue resolver o problema dentro do SLA (90 minutos), o que será comprovado no capítulo 6, através dos relatórios de tempo médio de recuperação.

Figura 34- Projeto de rede no Visium Live



Fonte: Autor

Na figura 35 temos a resolução do incidente, onde foi constatado que o amplificador identificado pelo Visium Live como o ponto de falha, estava queimado, foi realizada a substituição do equipamento e o incidente foi finalizado com 59 minutos, ficando dentro do SLA de 90 minutos, quando essa funcionalidade não era utilizada, a média de recuperação fica era de 120 minutos, de acordo com a tabela 1.

Figura 35- Fechamento do incidente

[!]. Fechamento [!]	
Data:	06/10/2018 11:12
Fechamento:	REDE COAXIAL
Solução:	ATIVO QUEIMADO
Análise:	[REDACTED]
	TÉCNICO DOUGLAS INFORMA QUE FOI TROCADO ATIVO QUEIMADO 203, RUA ZENETE FURAKAWA N. 1088
	NÍVEIS DO ATIVO
Mensagem:	CA 46 CB 36 TX 38 RX39 MER 38 BER -9
Tipo:	Rede Coaxial/Optica
Parte rede:	COAXIAL
Parte falha:	ATIVO
Natureza:	CORRETIVA
Total ativos:	1
Total canais:	230
[!]. Dados do Outage [!]	
Aberto por:	[REDACTED]
Data Inicio:	06/10/2018 10:01
Data Final:	06/10/2018 11:00

Fonte: Autor

6 Resultados

Logo após os primeiros meses de uso da nova ferramenta, que foi implementada em outubro de 2017, foi possível identificar uma melhora significativa em diversos indicadores, como por exemplo uma queda de 25% no tempo médio de recuperação dos incidentes e o um aumento em 30% no número de incidentes proativos.

6.1 Queda no Tempo Médio de Recuperação (TMR)

Com o uso do Visium Live, o tempo de análise foi otimizado e o analista é capaz de encaminhar o técnico no ponto exato da falha, por consequência houve queda significativa no tempo de recuperação dos incidentes de interrupção. Em algumas cidade já foi possível alcançar o SLA de 90 minutos, como pode-se ver na tabela 1 e no gráfico demonstrado na figura 35.

O Visium Live começou a ser utilizado a partir do mês de outubro de 2017.

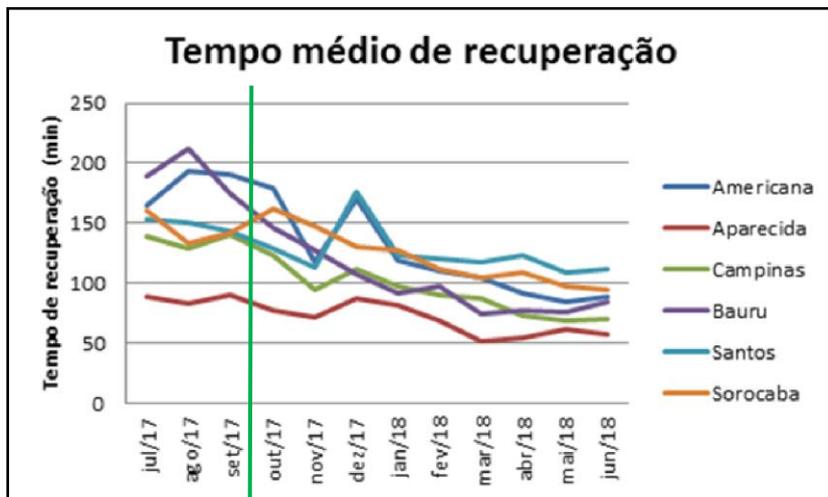
Tabela 1- Tempo médio de recuperação

TMR	jul/17	ago/17	set/17	out/17	nov/17	dez/17	jan/18	fev/18	mar/18	abr/18	mai/18	jun/18
Americana	164	194	191	179	117	170	119	110	104	92	85	89
Aparecida	89	83	91	77	72	88	82	69	51	55	61	57
Campinas	139	129	140	124	94	112	97	90	88	74	69	70
Bauru	189	212	175	146	127	108	92	97	74	78	76	84
Santos	154	151	143	129	113	176	124	121	118	123	109	112
Sorocaba	161	134	142	162	147	131	128	112	104	109	98	94

Fonte: Autor

Início da utilização do visium

Figura 36- Gráfico de tempo médio de recuperação



Fonte: Autor

6.2 Aumento no Número de Incidentes Proativos

Utilizando o painel de alarmes do Visium Live, uma grande parte dos incidentes de interrupção de sinal é identificada antes da reclamação do cliente, gerando uma grande economia para a empresa, pois quando o cliente liga e o incidente já está aberto, essa ligação fica retida na URA (unidade de resposta audível), que informa ao assinante que a área está em manutenção, caso o incidente ainda não esteja aberto, essa ligação é direcionada ao atendente na central de relacionamento. O custo de uma ligação retida na URA é de R\$ 0,80 centavos e a que passa para o atendente é de, em média, R\$ 8,80 reais.

Através da tabela 2 e do gráfico da figura 36 pode-se identificar o aumento nos incidentes abertos de maneira proativa, ou seja, sem que houvesse reclamação dos assinantes.

O Visium Live começou a ser utilizado a partir do mês de outubro de 2017.

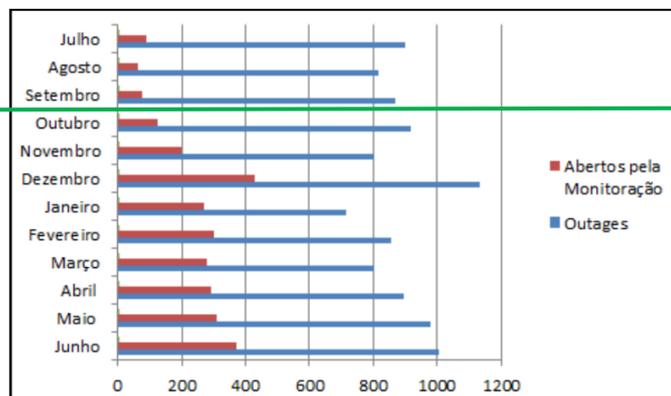
Tabela 2- Incidentes proativos

	Incidentes	Abertos pela Monitoração	% Abertos pela Monitoração
Jul/17	901	89	10%
Ago/17	817	64	8%
Set/17	869	78	9%
Out/17	917	127	14%
Nov/17	804	198	25%
Dez/17	1134	427	38%
Jan/18	715	271	38%
Fev/18	858	301	35%
Mar/18	805	278	35%
Abr/18	896	292	33%
Mai/18	980	312	32%
Jun/18	1008	372	37%

Início da utilização do visium

Fonte: Autor

Figura 37- Gráfico de incidentes proativos



Início da utilização do visium

Fonte: Autor

7 Considerações finais

Com o objetivo de analisar os impactos operacionais que recaem sobre o NOC e a empresa como um todo, verificou-se que um aspecto muito relevante são as ferramentas utilizadas para o gerenciamento da rede HFC. Observou-se, após a mudança do Nagios para o Visium Live, um aumento significativo na produtividade dos analistas, sobretudo aqueles que são responsáveis pelo monitoramento de alarmes e abertura proativa de incidentes de interrupção de sinal, pois antes era necessário 6 analistas para essa função e hoje são necessários apenas 2.

Não se trata apenas de uma mudança nas atividades cotidianas do NOC, mas um quadro geral de melhorias para a empresa, causando impacto positivo tanto tecnicamente quanto financeiramente. Dessa forma, pode-se dizer que a mudança entre ferramentas foi altamente benéfica para a companhia, como pôde ser visto no capítulo 6, através da redução do tempo médio de recuperação, auxiliando as operações a atingir o SLA no restabelecimento dos serviços em incidentes de interrupção de sinal, e com potencial de ganhos financeiros, pois ao abrir incidentes proativos, a grande maioria das ligações dos clientes são retidas na URA, e não passam ao atendente, gerando uma economia de aproximadamente R\$ 8,00 por ligação.

REFERÊNCIAS BIBLIOGRÁFICAS:

Canal de Retorno. Disponível em: <<http://www.net.atenalms.com.br>>. Acesso em: 19 Out. 2018.

KOCJAN, Wojciech. **Learning Nagios 4.** 2ª Edição. Birmingham: Packt Publishing, 2014.

KUROSE, Jim; ROSS, Keith. **Redes de computadores e a Internet:** uma abordagem top-down. 6ª Edição. São Paulo: Pearson, 2013.

Nagios, The industry standard in IT infrastructure monitoring. Disponível em: <<https://www.nagios.com/products/nagios-xi>>. Acesso em: 02 Out. 2018.

SAYDAM, T; MAGEDANZ, T. From Networks and Network Management into Service and Service Management, **Journal of Networks and System Management**, volume 4, 1996.

VISIUM Soluções em TI e telecom. Disponível em: <http://www.visium.com.br/visium_suite_5.html>. Acesso em: 25 Nov. 2018.