intellectus
REVISTA ACADÊMICA DIGITAL DO GRUPO POLIS EDUCACIONAL



David – 1501/1504 - Michelangelo di Lodovico Buonarroti Simoni

ISSN 1679-8902 **Ano VIII | Nº. 19 | Jan-Mar 2012**
Ciências Exatas e Tecnológicas

ISSN 1679-8902

INTELLECTUS. Revista científica das seguintes instituições: Faculdade de Jaguariúna, Faculdade Politécnica de Campinas, Faculdade Max Planck, Faculdade de Tecnologia César Lattes, Faculdade Politécnica de Sumaré e Faculdade Unopec.

Jaguariúna – SP

Eletrônica

Trimestral

Inclui bibliografia

EDITORIAL

A Faculdade de Jaguariúna, a Faculdade Max Planck, a Faculdade Politécnica de Campinas, a Faculdade de Tecnologia César Lattes, a Faculdade Politécnica de Sumaré e a Faculdade Unopec disponibilizam para a comunidade acadêmica o número 19 da Revista Intellectus, uma publicação científica do grupo de faculdades.

Este exemplar compreende oito artigos do campo das **Ciências Exatas e Tecnológicas**. Os resultados desses estudos ora divulgados são contribuições de professores e pesquisadores dessa grande área do conhecimento, constituindo-se em importante material de pesquisa para os nossos professores e estudantes, além de outros estudiosos desses temas.

Os artigos publicados e assinados são de responsabilidade dos autores e só poderão ser reproduzidos mediante autorização expressa dos mesmos.

Boas leituras.

Editor: Prof. Dr. Rubens Pantano Filho

Faculdade de Tecnologia César Lattes

Editores Associados: Profª. Drª. Ana Maria Sperandio

Faculdade de Jaguariúna

Profª. Drª. Telma Dagmar Oberg

Faculdade de Jaguariúna

Conselho Editorial

Educação, Cultura e Sociedade

Prof. Dr. Adauto Fernandes Marconsin – Faculdade Max Planck

Profª. Dnda. Maria Ângela Lourençoni – Faculdade Max Planck

Prof. Dr. Samuel Mendonça – Pontifícia Universidade Católica de Campinas

Profª. Drª. Solange Muglia Wechsler – Pontifícia Universidade Católica de Campinas

Ciências Exatas e Tecnológicas

Prof. Dr. André Luís Helleno – Faculdade de Jaguariúna

Prof. Dr. André Mendeleck – Faculdade de Jaguariúna

Prof. Dr. Claudemir Adriano Borgo – Faculdade de Tecnologia César Lattes

Prof. Dr. Derval dos Santos Rosa – Universidade Federal do ABC

Prof. Dr. Pedro Luis Christiano – Universidade Federal da Paraíba

Profª. Drª. Vanice Aparecida Perin – US Nuclear Regulatory Commission

Ciências Sociais Aplicadas

Prof. Dr. Cássio Modenessi Barbosa – Faculdade de Jaguariúna

Prof. Dr. Olavo Pudenci Furtado – Faculdade Max Planck

Prof. Dr. Oscar Mellin Filho – Faculdade de Jaguariúna

Profª. Drª. Tércia Zavaglia Torres – Empresa Brasileira de Pesquisa Agropecuária

Saúde

Profª. Drª. Celene Ferrari Audi – Faculdade de Jaguariúna

Profª. Drª. Helena Cruz Oliveira – Faculdade Max Planck

Prof. Dr. José Meciano Filho – Pontifícia Universidade Católica de Campinas

Prof. Dr. Roberto Foz Filho – Faculdade Max Planck

Prof. Dr. Sérgio Fernando Zavarize – Faculdade de Jaguariúna

Correspondência

Núcleo de Publicação

Campus II – Rodovia Adhemar de Barros – km 127 – Pista Sul

Tanquinho Velho – Jaguariúna – SP – 13820-000

(19) 3837-8500 - http://www.seufuturonapratica.com.br/intellectus

ÍNDICE

* UMA PROPOSTA PARA A SIMULAÇÃO DA DISTRIBUIÇÃO EFICIENTE DE CARGAS ATRAVÉS DE SISTEMAS IMUNOLÓGICOS ARTIFICIAIS 07

* PROPOSTA TEÓRICA PARA SELEÇÃO ALGORÍTMICA DE ENTONAÇÃO VOCAL BASEADA EM CORRELAÇÃO E SIMILARIDADE 29

* ESTUDO DE UM ROBÔ DE BUSCA BASEADO EM WEB SEMÂNTICA 43

* MEDIÇÃO DA RESISTIVIDADE ELÉTRICA EM CONDUTORES METÁLICOS 55

* GESTÃO DE REQUISITOS LEGAIS E CONFORMIDADE AMBIENTAL UTILIZANDO O MÉTODO ZOPP 70

* SUSTENTABILIDADE - UMA NECESSIDADE, ÉTICA ECOLÓGICA - UM CAMINHO 80

* PROPOSTA DE UM CONJUNTO DE BOAS PRÁTICAS PARA A UTILIZAÇÃO E CONSTRUÇÃO DE SERVIÇOS WEB BASEADOS EM REST 96

* SOLUÇÃO PROPOSTA DE AUDITORIA DE SEGURANÇA EM *FIREWALLS* CISCO PARA EMPRESAS COM GRANDE QUANTIDADE DE EQUIPAMENTOS DE SEGURANÇA EM REDE 112

UMA PROPOSTA PARA A SIMULAÇÃO DA DISTRIBUIÇÃO EFICIENTE DE CARGAS ATRAVÉS DE SISTEMAS IMUNOLÓGICOS ARTIFICIAIS

A proposal for simulation of efficient distribution of loads through artificial immune systems

ALVARENGA, Maria Cristina Campos Mendonça
Faculdade de Jaguariúna

PETROLI NETO, Silvio
Faculdade de Jaguariúna

Resumo: O objetivo deste trabalho é o desenvolvimento de um algoritmo, utilizando os princípios dos Sistemas Imunológicos Artificiais, para a simulação de uma distribuição eficiente de cargas. O conceito de carga usado aqui se refere aquilo que é ou pode ser transportado ou suportado por estrutura, pessoa, veículo, aparelho, etc. e que, consequentemente, gera um custo econômico, energético ou mesmo de tempo. Através de estudos sobre o Sistema Imunológico Humano, Sistemas Imunológicos Artificiais, Complexidade Computacional, P-Medianas e algoritmos como o ClonalG, pretende-se propor uma modelagem computacional aplicável a sistemas complexos simuláveis que demonstre que o sistema imunológico artificial pode ser usado como ferramenta na busca de “boas soluções”.

Palavras-chave: Sistemas Imunológicos Artificiais, ClonalG, NP-Completo, P-medianas.

Abstract: The main goal of this work is the development of an algorithm using the principles of Artificial Immune Systems for the simulation of an efficient distribution of loads. The concept of loads used here refers to what is or can be transported or supported by structure, person, vehicle, apparatus, etc. consequently generates an economic cost, energy or time. Through studies about Human Immune System, Artificial Immune Systems, Computational Complexity, P-Median and algorithms as ClonalG, we intend to propose a computational model applicable to complex systems that can be simulated to

show that the artificial immune system can be used as tool in pursuit of "good solutions"

Keywords: Artificial Immune Systems, ClonalG, NP-Complete, P-median.

INTRODUÇÃO

A ciência da computação como a conhecemos é uma ciência nova que não tem ainda nem um século de vida, contudo é uma das áreas do conhecimento que mais tem crescido nos últimos anos. Um dos temas mais novos desta ciência é a computação natural. Apesar da ampla abordagem da computação natural, ela pode ser sintetizada na aplicação de modelos de fenômenos e sistemas complexos observados na natureza à ciência da computação.

Em 2006, a Sociedade Brasileira de Computação (SBC) promoveu um seminário onde cientistas e pesquisadores debateram sobre os Grandes Desafios da Pesquisa em Computação no Brasil para os próximos dez anos. Dentre os cinco grandes temas eleitos naquela ocasião está o tema "*Modelagem Computacional de Sistemas Complexos Artificiais, Naturais e Sócio-culturais e da Interação Homem-natureza"*. Dentro deste contexto, identifica-se um quadro promissor para a pesquisa científica neste campo, o qual está atrelado a fatores como o aumento da complexidade dos problemas computacionais, a necessidade de se combinar várias áreas de conhecimento, o aumento sistemático do volume de dados e a constante evolução de hardware e softwares.

O objetivo deste trabalho é o desenvolvimento de uma modelagem computacional, utilizando os princípios dos Sistemas Imunológicos Artificiais, para o fornecimento de "possíveis soluções" a problemas que possam ser simulados. É o caso do problema de alocação de clientes a servidores, objetivando-se o menor custo e respeitando-se as capacidades de processamento e de armazenamento destes últimos. O objetivo não é desenvolver um programa para a solução desta questão específica, mas a

partir deste exemplo, modelar um algoritmo baseado em SIA que possibilite a simulação de outros problemas similares a este.

COMPLEXIDADE COMPUTACIONAL E OS PROBLEMAS NP-COMPLETOS

Problemas no contexto da ciência da computação são avaliados de acordo com o seu grau de complexidade. Esta complexidade está relacionada ao consumo de tempo que um sistema computacional leva para solucionar determinados tipos de problemas.

Para a análise desta complexidade, Russel e Norvig (2004, p.943) efetuam uma "primeira divisão bruta" classificando-os em *"problemas que podem ser resolvidos em tempo polinomial"* e aqueles que não podem, independente do algoritmo usado. Estes problemas são considerados tratáveis, enquanto que, uma outra classe denominada NP (polinomiais não determinísticos), que possuem um tempo de solução exponencial, são considerados "intratáveis".

Os problemas NP-Completos são tidos como os problemas de nível de complexidade mais elevados e somente são provados a partir de outros problemas também NP-Completos já conhecidos. De acordo com Pfützenreuter (2005, p.2), eles possuem três características peculiares que, de certa forma, viabilizam a identificação de um problema como NP-Completo, ou não: se a análise do problema resulta em uma solução ideal não polinomial; ou se soluções não tidas como as ideais são aceitáveis e úteis; ou se estas podem ser obtidas por algoritmos polinomiais, por tentativas aleatórias ou pelo uso de ambas as técnicas; então podemos dizer que o problema é um NP-Completo.

P-MEDIANAS

O problema selecionado descreve um grafo, cabendo portanto, relembrar alguns conceitos da Teoria de Grafos. Um grafo é dado pela

representação G(V,E) onde G é composto por um conjunto finito de vértices V e um conjunto de arestas E. Os vértices são os nodos (nós) que representam pontos fixos, enquanto as arestas são as linhas que ligam estes pontos. Um vértice é chamado de adjacente a outro quando existe uma aresta que os conecta, enquanto uma aresta é dita adjacente a outra quando se conectam ao mesmo vértice.

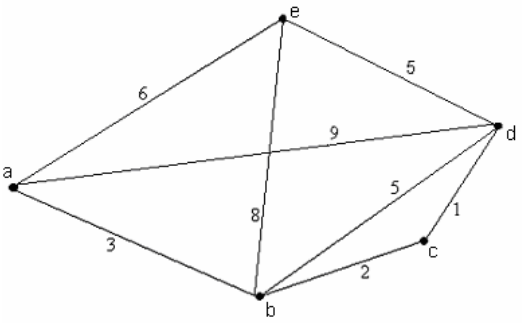


Figura 1: Grafo não orientado. **Fonte:** CAMICIA & VICENTE, 2008, p. 6

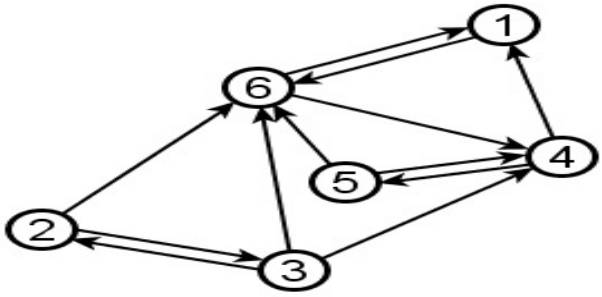


Figura 2: Grafo orientado. **Fonte:** FEOFILOFF, 2010

Um grafo pode ser orientado (figura 1) ou não orientado (figura 2). Chamamos de grafo não orientado àquele onde uma mesma aresta possui um sentido duplo. O grafo orientado ou dirigido, por sua vez, é àquele onde existem arestas que possuem um sentido único definido de um nó para outro, ou seja, possuem orientação e direção.

> Um grafo é dito valorado quando se atribuem valores as suas arestas. A ordem de um grafo é dada pela cardinalidade do conjunto de vértices. [...] Em um grafo não orientado, o grau de um vértice é o numero de arcos que incidem sobre ele. No caso do grafo ser dirigido, fala-se em grau de entrada e grau de saída. O grau de entrada é o numero de arestas que chegam a

> ele, e o grau de saída é o numero de arestas que saem dele (CAMICIA & VICENTE, 2010, p. 3).

Uma das formas mais utilizadas de representação de grafos é a matriz de adjacência. Atribui-se a identificação do vértice a uma linha (*i*) e coluna (*j*). Se existir aresta que conecte *i* a *j*, o "custo" da aresta E(*i*, *j*) será 1 e será 0, se os vértices não forem adjacentes.

O grau de um vértice pode ser obtido a partir da soma dos elementos da linha ou coluna da matriz de adjacência, em se tratando de um grafo não orientado. Já no dígrafo ou grafo orientado ou dirigido, *"a soma dos elementos na coluna i representa o grau de saída do vértice v_i enquanto a soma dos elementos na coluna i representa o grau de entrada de v_i"* (NONATO, 2000).

Duas outras formas de representação são a matriz de incidência e a matriz de custos. Na de incidência cada linha (*i*) representa cada um dos nós do grafo, e as colunas (*j*), os seus possíveis arcos (ou arestas). Nos grafos não orientados, ao elemento M(*i,j*) será atribuído 1 se *i* for o vértice inicial de *j* e 0 caso contrário; enquanto nos dígrafos, atribui-se 1 se *i* for o vértice inicial, -1 se final e 0 se for laço.

A matriz de custos é utilizada na representação de grafos valorados, podendo estes valores representar distância, tempo de viagem, etc. e *"são chamados custo, independentemente do que estejam representando"*. Em síntese, o elemento M(i,j) será o custo da aresta (i, j) se esta existir, 0 se i=j e ∞ se não existir a aresta (CAMICIA; VICENTE, 2010, p. 4).

A mediana de um grafo corresponde ao nó a partir do qual é possível "visitar" os outros nós com a menor soma de "custos". Um problema pode possuir como resultado apenas 1 vértice como mediana, 2 ou até um número "p" de medianas. Os problemas que possuem um número indefinido de medianas como possíveis resultados são ditos como Problemas de P-medianas.

Em um grafo não orientado onde V é o conjunto dos vértices do grafo *"deve-se encontrar um conjunto de vértices $V_p \subset V$ (V_p é o conjunto das medianas do problema) com cardinalidade p, tal que a soma das distâncias de*

cada vértice pertencente a V até seu vértice mais próximo em V_p seja a mínima possível". (ROSÁRIO; CARNIERI; STEINER, 2010)

SISTEMA IMUNOLÓGICO HUMANO (SIH)

A computação natural está fundamentada na observação dos fenômenos naturais e de sua aplicação de forma análoga em sistemas computacionais. O Sistema Imunológico Artificial como o próprio nome revela, se baseia nos princípios e conceitos observados no Sistema Imunológico Humano (SIH) sendo, portanto, importante elucidar estes conceitos e princípios no seu contexto original.

Três conceitos fundamentais para a compreensão do mecanismo de defesa do SIH são os patógenos, antígenos e anticorpos. Os patógenos são agentes infecciosos que carregam a substância nociva que chamamos de antígeno, podendo ser extra ou intracelular de acordo com a forma que se alojam no organismo atacado. São exemplos de intracelulares, os vírus, as bactérias e os protozoários, sendo que estes últimos se replicam no interior das células do hospedeiro. Algumas bactérias e parasitas maiores se alojam em tecidos e fluídos corpóreos e por isto são chamadas de extracelulares.

Segundo Trevisan et al (2010), o antígeno é uma *"substância orgânica nociva, de natureza geralmente protéica, que, inoculada no organismo, provoca, como reação, a produção de anticorpos específicos".* Enquanto o anticorpo é uma *"substância específica de origem celular, que torna inócuas substâncias orgânicas capazes de produzir moléstias, quando introduzidas no organismo".*

O organismo humano possui um mecanismo de defesa que ocorre em multicamadas e cobre toda a extensão do corpo. Além das barreiras físicas como a pele e barreiras bioquímicas como o nível de pH da saliva, o sistema imunológico pode ser divido em inato e adaptativo (CASTRO, 2006, p.268).

No processo inato temos a primeira defesa onde o SIH reconhece o antígeno, envia sinais para as células e responde de forma inalterada ao ataque. No adaptativo, o SIH memoriza antígenos já anteriormente

 ISSN 1679-8902

reconhecidos, produzindo anticorpos específicos e se tornando mais eficaz a cada encontro com patógenos do mesmo tipo.

Neste contexto de defesa adaptativa o SIH conta com os linfócitos que, segundo Machado (2005, p.14), são células de glóbulos brancos responsáveis pelas atividades de reconhecimento de patogenias, respostas e memorização imunológicas. Estas células dão origem a duas importantes células: B e T.

As células B são oriundas da medula óssea e codificam o receptor de superfície específico para o reconhecimento do antígeno. Se este for reconhecido, a célula B se divide e diferencia em plasmócitos e linfócitos de memória. Os plasmócitos são responsáveis pela produção de anticorpos em grande escala e pela distribuição nas células infectadas. Os linfócitos de memória, por sua vez, não produzem anticorpos, vivem por longos períodos e, se forem re-expostos ao antígeno, o reconhecem e novamente se dividem e diferenciam. As células T amadurecem no Timo e daí a origem do seu nome. Elas atuam diretamente nas células atacadas por antígenos, destruindo os patógenos intracelulares. São também responsáveis pela produção e distribuição de anticorpos.

A teoria da seleção clonal está relacionada ao SIH adaptativo e, de acordo com Machado (2005, p.18):

> Quando há exposição a um antígeno, uma subpopulação de linfócitos (células B) responde por meio da produção de anticorpos. Cada célula secreta um único tipo de anticorpo, que é relativamente específico para o antígeno. Por meio da ligação do antígeno com o receptor da célula B e, dado um sinal co-estimulatório de células acessórias como a T-Helper, um antígeno estimula a célula B a se proliferar (clones produzidos por meio de divisão celular). Esse processo é denominado expansão clonal e as células B resultantes possuem receptores modificados devido à hipermutação somática ocorrida durante a clonagem.

Estes novos linfócitos são também expostos ao antígeno competindo com os anteriores e ocorre uma seleção das células que são capazes de reconhecer o antígeno, determinando assim o princípio da Seleção Clonal.

SISTEMA IMUNOLÓGICO ARTIFICIAL (SIA)

Hoje já existem várias técnicas para o desenvolvimento de algoritmos baseados no Sistema Imunológico Artificial. Entre eles podemos destacar: Medula óssea, Seleção negativa, Seleção clonal, Modelos Contínuos de Rede Imunológica e Modelos Discretos de rede imunológica.

No SIA, os algoritmos de Seleção Clonal possuem três características próprias que os identificam: o encontro com antígenos é sequencial, a taxa de proliferação é proporcional à afinidade e a taxa de mutação é inversamente proporcional à afinidade.

A AFINIDADE ENTRE ANTÍGENOS E ANTICORPOS

Para a representação dos antígenos e anticorpos no SIA, Perelson e Oster desenvolveram o conceito de “espaço de formas” onde a molécula é representada por uma String sendo os mais conhecidos: O espaço de forma Real, Inteiro, Hamming e o simbólico. Os dois primeiros reconhecem valores reais e inteiros respectivamente. Já o de Hamming é baseado em um determinado alfabeto finito e o simbólico aceita quaisquer tipos de atributos, desde que entre eles exista ao menos um símbolo.

A partir do espaço de formas de Hamming, que considera um determinado alfabeto K, é possível estabelecer uma medida de afinidade. Castro (2006, p. 282-283) exemplifica a verificação do grau de afinidade de forma simples utilizando um alfabeto binário, conforme segue:

> A Equação (...) descreve a distância Hamming usada para avaliar a afinidade entre duas strings de atributos de tamanho L no espaço de formas de Hamming:
>
> $$D = \sum_{i=1}^{L} \delta \text{, onde } \delta = \begin{cases} 1 \text{ se } Ab_i \neq Ag_i \\ 0 \quad \text{senão} \end{cases}$$

 ISSN 1679-8902

(...) Para poder ilustrar melhor, considere as strings
Ag = [1000111010] e **Ab** = [1010101010].
Ag = [1000111010]
Ab = [1010101010]
Ligação (**Ab**, **Ag**): 0010010000

Complementaridade: $D(Ab, Ag) = \sum Ligação\ (Afinidade = 2)$

Similaridade: $L - D(Ab, Ag)$ $(Afinidade = 8)$

ALGORITMO CLONALG

O algoritmo de seleção clonal conhecido por ClonalG foi proposto em 2002 por Castro e Von Zuben e apresenta os passos básicos descritos a seguir de acordo com Castro e Timmis (2002, apud Castro, 2006, p. 298-299):

1. **Inicialização**: cria-se uma população de indivíduos
2. **Apresentação do antígeno**: cada elemento da população é apresentado ao antígeno (padrão)
3. **Avaliação da afinidade**: calcula-se a afinidade de cada anticorpo com o antígeno.
4. **Seleção Clonal e Expansão**: são selecionados os n1 com maiores afinidades e são clonados proporcionalmente, quanto maior a afinidade, maior o número de cópias.
5. **Maturação da Afinidade**: as cópias são alteradas na proporção inversa de sua afinidade, e adicionadas à população de anticorpos.
6. **Metadinamica**: um número n2 de indivíduos de baixa afinidade são substituídos por novos indivíduos gerados randomicamente

Ciclo: o Passo 2 é repetido até que um certo critério de parada seja alcançado.

RESULTADOS

A modelagem constante na figura 3 foi implementada em Java, tendo em vista a sua modularidade e a gama de recursos disponíveis (bibliotecas)

favorecendo o desenvolvimento de um código que viabiliza o seu aperfeiçoamento futuro.

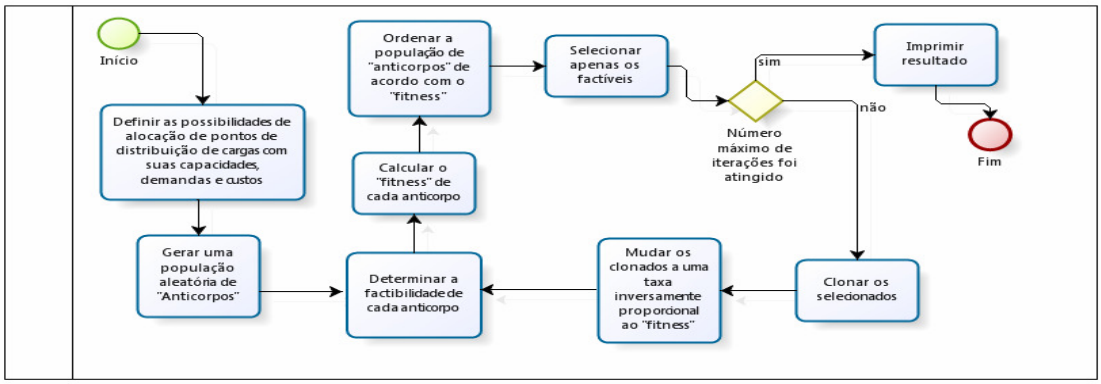


Figura 3: Algoritmo para a alocação de pontos para a distribuição de cargas baseado em princípios da seleção clonal. **Fonte:** construído com a ferramenta freeware *BizAgi Process Modeler* (BIZAGI - BUSINESS AGILITY, 2010)

O primeiro passo foi a definição de um problema com dados determinados e com um volume que permitisse a visualização dos resultados de maneira mais clara. Para tanto, optou-se pela representação de um grafo (figura 4) com dois servidores e cinco estações o que gera no “pior caso” a “ativação” de 10 arestas, conectando cada uma das estações aos dois servidores.

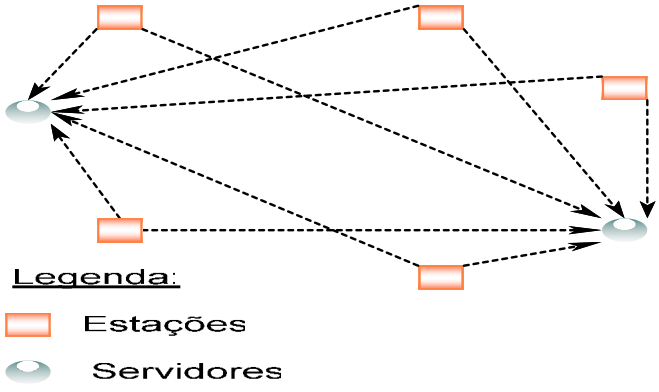


Figura 4: Representação básica do problema.

Inicialmente modelou-se as classes estruturais: “Servidor”, “Estacao” e “aresta” conforme diagrama de classe apresentado na figura 5. Os objetos

destas classes foram instanciados na classe “sia” com a atribuição dos valores correspondentes os quais são demonstrados na representação gráfica da figura 6.

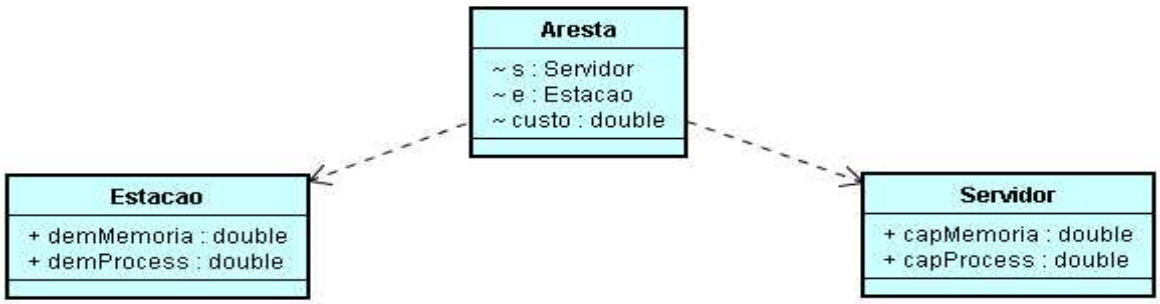


Figura 5: Diagrama de classes estrutural

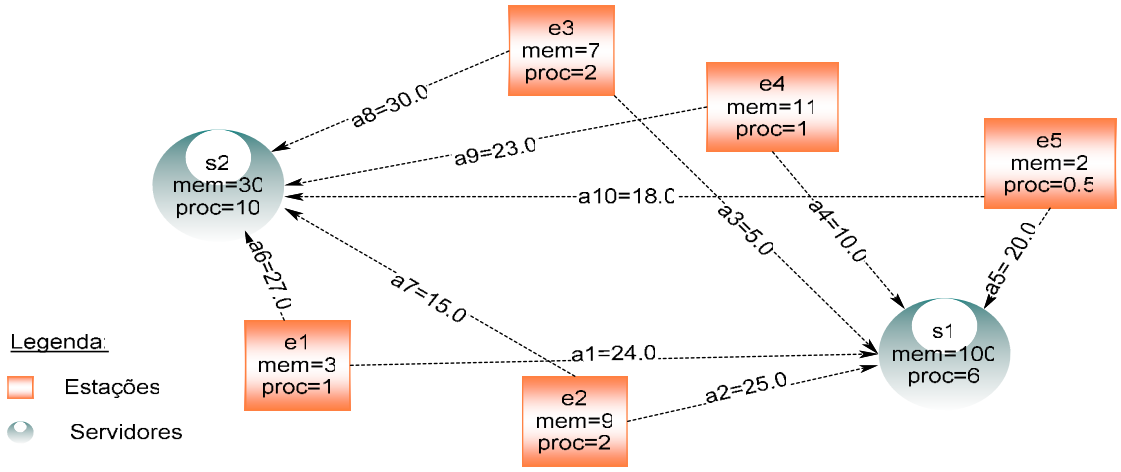


Figura 6: Representação do problema com os valores atribuídos

O anticorpo é representado como um vetor de arestas, onde se considerou todas as arestas possíveis do problema que, neste caso são 10. A cada aresta, é atribuído um dos valores 0 ou 1, sendo que 0 indica que a aresta não compõe aquela solução (ou anticorpo) e 1 indica que compõe. Assim, é

possível a geração aleatória de anticorpos os quais são armazenados em uma matriz conforme demonstrado na figura 7.

```
run:
0  0  1  1  0  0  1  1  1  1  => Anticorpo 1
0  0  1  1  0  0  0  1  0  1  => Anticorpo 2
1  0  0  1  1  1  0  1  1  1  => Anticorpo 3
0  0  1  1  0  1  0  0  0  1  => Anticorpo 4
0  0  1  1  1  0  0  0  1  1  => Anticorpo 5
```

Figura 7: Exemplo da matriz de anticorpos (arestas ativas)

Estes anticorpos são verificados quanto à sua factibilidade, ou seja, se os servidores são capazes de absorver a demanda de carga (armazenamento e processamento) das estações a eles associadas. Se alguma das arestas ultrapassar a capacidade do servidor, o anticorpo é considerado infactível e terá somado ao seu custo específico o custo total das arestas.

O próximo passo consiste no estabelecimento de um “fitness” que neste problema coincide com o custo. Contudo, como esta modelagem pretende servir como base para a simulação de outros problemas, é importante que este parâmetro seja definido. Assim, apurou-se o fitness de cada anticorpo, atribuindo-se a este, a diferença entre o custo total da população e o seu custo específico. Com isto tem-se que, o anticorpo com menor custo, ou seja a melhor solução, terá o maior *fitness*.

Para a ordenação da população de anticorpos de acordo com o *fitness*, foi necessário agregar à matriz novas colunas contendo os dados de *fitness*, custo e identificação de cada anticorpo. Após sua ordenação uma nova matriz foi gerada, contendo apenas os anticorpos factíveis e que serão submetidos à clonagem e mutação. Estes procedimentos foram definidos dentro da classe “Populacao”.

Neste momento efetua-se a seleção apenas dos anticorpos factíveis, os quais serão clonados e posteriormente mudados. A taxa de mutação é inversamente proporcional ao *fitness*, ou seja, os anticorpos de maior *fitness*

serão os menos alterados, enquanto os de menor *fitness* terão mais elementos (arestas) alteradas.

O resultado da mutação é fornecido novamente para o teste de factibilidade, o cálculo do fitness, nova ordenação e seleção, por N vezes e finalmente, é impresso o resultado.

DISCUSSÃO

Os testes foram efetuados considerando-se três parâmetros variáveis: o número inicial de anticorpos gerados aleatoriamente, o número de iterações do ciclo e o número de resultados capturados.

Os resultados gerados pelo algoritmo implementado foram impressos no formato abaixo, onde estão demonstrados: o número do resultado, a sua classificação dentro de cada conjunto de iterações, a identificação das arestas ativas que compõe a solução e o custo do resultado, conforme exemplo ilustrado na figura 8. Estes resultados foram transportados para uma planilha do Excel para serem ordenados por custo, de forma a facilitar o cálculo dos subtotais.

9891, 1, , 1, , 3, 4, , , 7, , , 10, , , 72,
9892, 1, , 1, , 3, 4, , , 7, , 9, 10, , , 95,
9893, 1, , 1, , 3, , , , 7, , 9, 10, , , 85,

Figura 8: Exemplo da impressão oferecida pelo programa.

Primeiramente optou-se por fixar o número de anticorpos em 500, e de iterações em 100, alterando apenas o número de resultados recuperados gerando os dados conforme demonstrado na tabela 1, onde é possível observar que as 7(sete) melhores soluções aparecem em todas as simulações, independente do número de resultados recuperados.

Tabela 1. Resultados obtidos **variando o número de resultados** e fixando o número de anticorpos iniciais em 500 e de iterações em 100

50		100		500		1000		2000		5000		10000	
Qua	**Cus**	**Qua**	**Cus**	**Qua**	**Cus**	**Qua**	**Cus**	**Qua**	**Cus**	**Qua**	**Cus**	**Qua**	**Cus**
19	72	33	72	157	72	356	72	660	72	1656	72	3365	72
13	74	21	74	98	74	231	74	458	74	1094	74	2144	74
3	75	8	75	80	75	148	75	322	75	743	75	1516	75
5	77	11	77	60	77	93	77	181	77	489	77	990	77
3	82	9	82	45	82	63	82	111	82	334	82	673	82
3	85	11	85	35	85	63	85	150	85	383	85	725	85
3	87	5	87	10	87	26	87	66	87	169	87	321	87
1	95	1	97	3	88	7	88	20	88	40	88	82	88
-	-	1	98	5	90	4	90	9	90	31	90	53	90
-	-	-	-	2	92	3	92	7	92	20	92	36	92
-	-	-	-	4	95	3	95	11	95	27	95	71	95
-	-	-	-	1	97	1	97	3	97	12	97	21	97
-	-	-	-	-	-	1	98	1	98	2	98	1	98
-	-	-	-	-	-	1	99	1	99	-	-	2	99

Os gráficos apresentados na figura 9 demonstram que à medida que o número de resultados recuperados aumenta, a representação de uma curva exponencial decrescente se torna mais evidente.

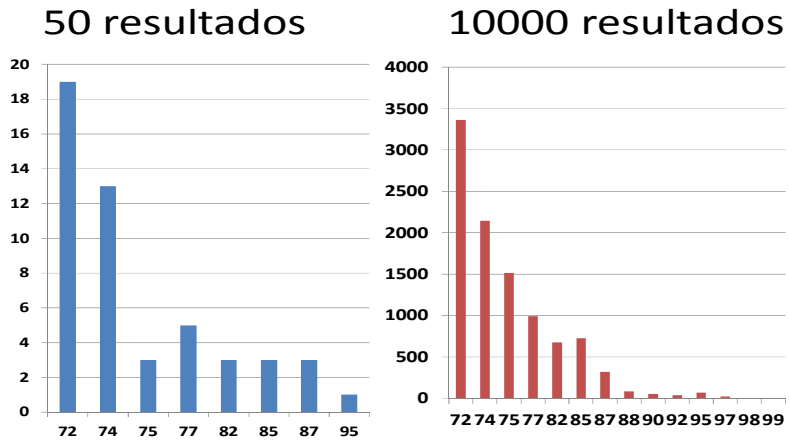


Figura 9: Distribuição de Quantidade de Resultados Obtidos (eixo y) por custo (eixo x)

Estes dados também foram analisados através de um gráfico de ajuste de curva, de forma a demonstrar se o algoritmo seguia um padrão de

 ISSN 1679-8902

comportamento. Para tanto foi utilizada a versão demo da ferramenta computacional DataFit (OAKDALE ENGINEERING, 2010).

No caso da variação do número de resultados gerados foram obtidos os gráficos de ajustes de curva conforme a figura 10 para o menor (50) número de resultados verificados e a figura 11 para o maior (10000).

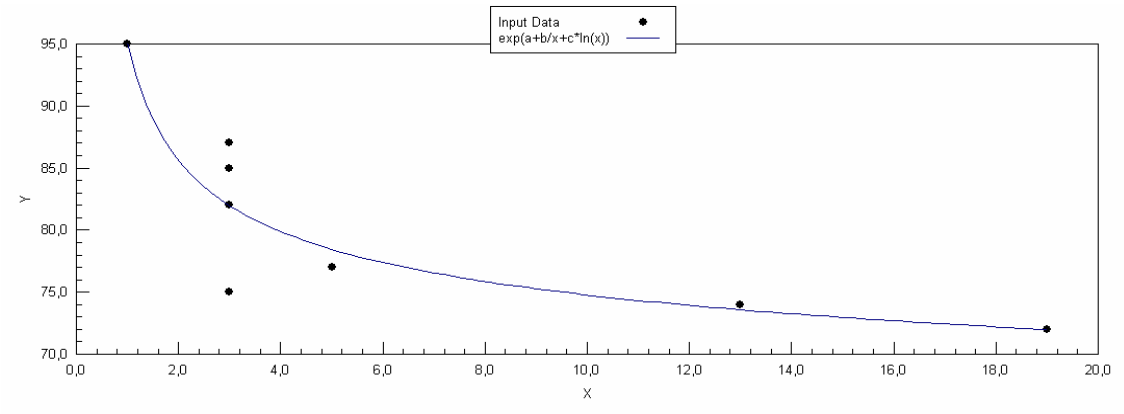


Figura 10: Ajuste de curva para a distribuição de custos (y) por quantidade de resultados recuperados (x), considerando 500 anticorpos iniciais, 100 iterações e 50 resultados recuperados.

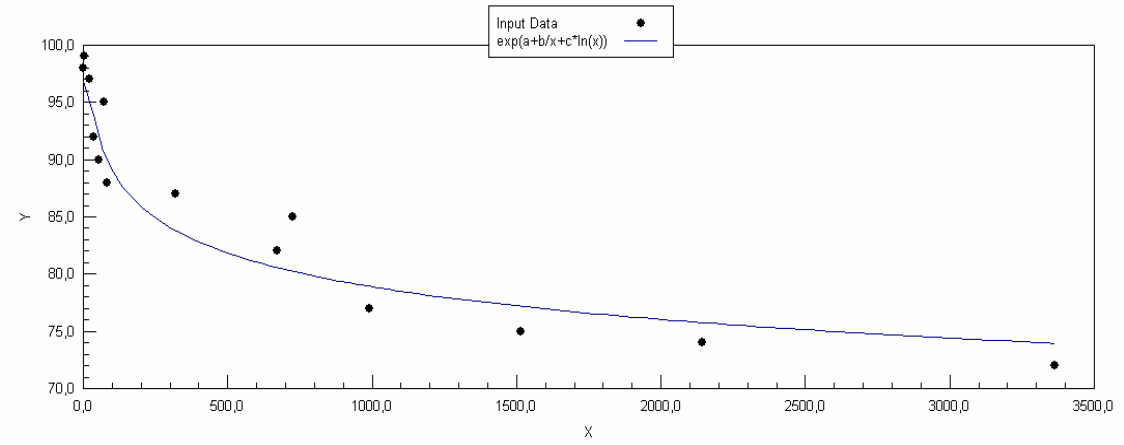


Figura 11: Ajuste de curva para a distribuição de custos por quantidade de resultados recuperados, considerando 500 anticorpos iniciais, 100 iterações e 10000 resultados recuperados.

Deve-se perceber que a assíntota foi obtida em ambos os resultados, tendo sido observado também nos testes com valores intermediários denotando um padrão de comportamento exponencial do algoritmo no tratamento do problema piloto. Na sequência, fixou-se o número de resultados

em 5000 e de anticorpos em 500, alterando apenas o número de iterações gerando os dados conforme demonstrado na tabela 2:

Tabela 2. Resultados obtidos variando o número de iterações e fixando o número de anticorpos iniciais e de resultados capturados em 100

5		10		100		1000	
Qtde	**Custo**	**Qtde**	**Custo**	**Qtde**	**Custo**	**Qtde**	**Custo**
1577	72	1667	72	1743	72	1702	72
1108	74	1078	74	1066	74	1103	74
800	75	739	75	776	75	741	75
496	77	492	77	447	77	473	77
333	82	376	82	324	82	326	82
391	85	346	85	356	85	351	85
164	87	165	87	152	87	164	87
45	88	40	88	45	88	41	88
29	90	38	90	32	90	39	90
26	92	17	92	17	92	17	92
25	95	37	95	29	95	29	95
4	97	4	97	13	97	11	97
2	99	1	100	-	-	2	98
-	-	-	-	-	-	1	100

Estes testes também geraram gráficos de colunas com a mesma tendência exponencial tanto nos gráficos de coluna como no gráfico de ajuste de curva. São apresentados exemplos destes gráficos para 5 e 1000 iterações respectivamente nas figuras 12, 13, 14 e 15.

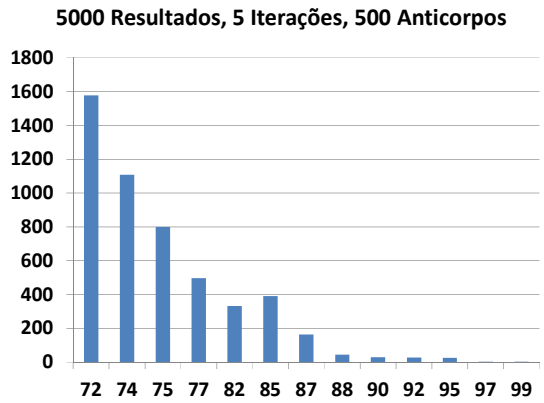


Figura 12 Distribuição de quantidade de resultados obtidos (eixo y) por custo (eixo x).

 ISSN 1679-8902

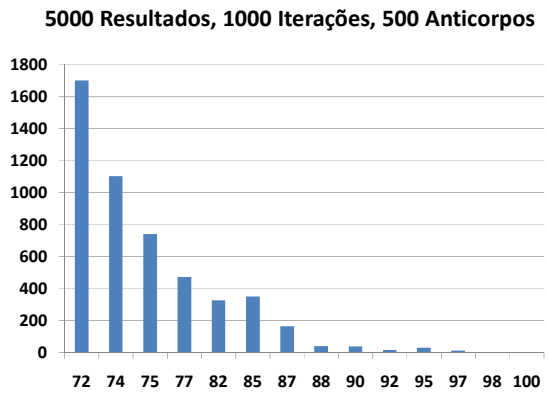


Figura 13: Distribuição de quantidade de resultados obtidos (eixo y) por custo (eixo x)

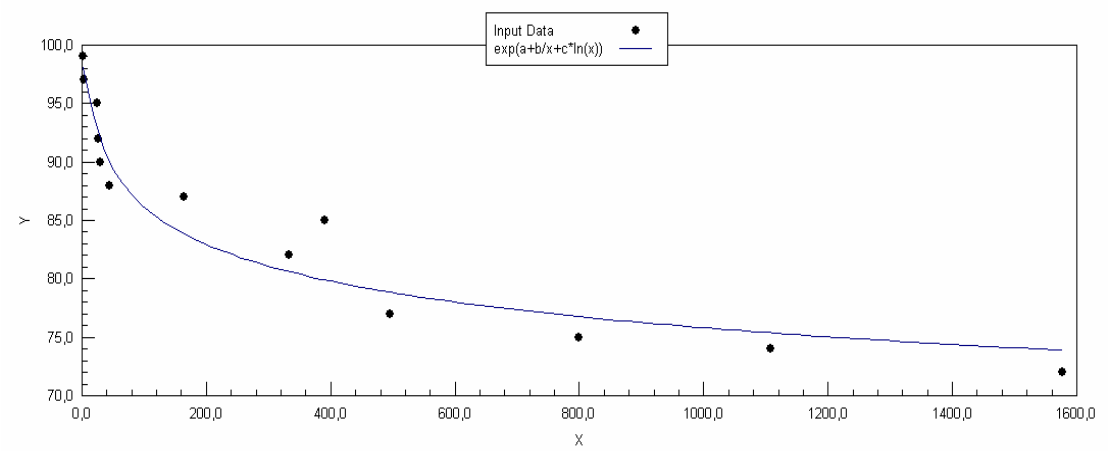


Figura 14: Ajuste de curva para a distribuição de custos (y) por quantidade de resultados recuperados (x), considerando 500 anticorpos iniciais, **5 iterações** e 5000 resultados recuperados.

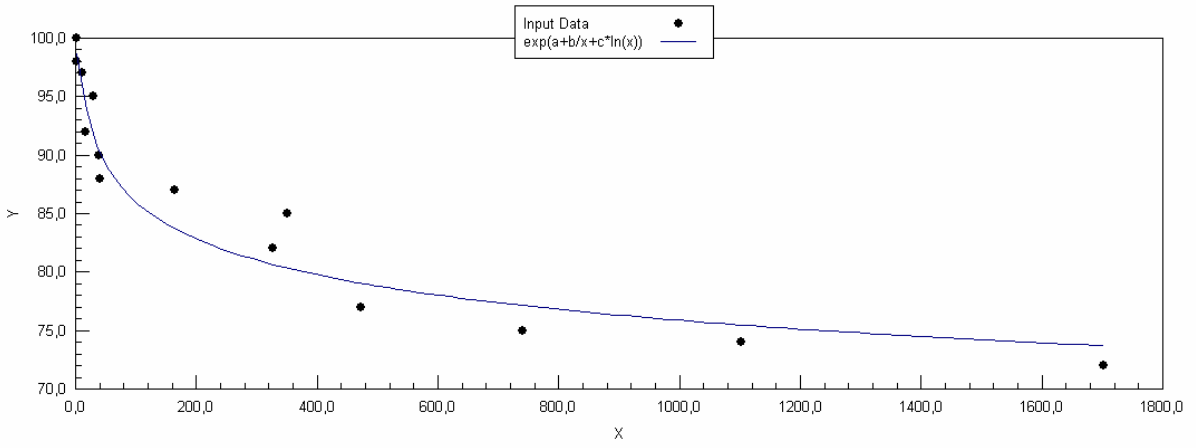


Figura 15: Ajuste de curva para a distribuição de custos (y) por quantidade de resultados recuperados (x), considerando 500 anticorpos iniciais, **1000 iterações** e 5000 resultados recuperados.

Foram realizados ainda testes fixando-se o número de resultados e de iterações em 100, alterando apenas o número de anticorpos iniciais gerando os dados conforme a tabela 3. Observa-se que com um número baixo de

anticorpos iniciais a diversidade de anticorpos encontrados é grande e que quanto maior o “número de anticorpos iniciais”, maior a concentração de resultados na “melhor solução”, o que também é mostrado nas figuras, 16 e 17.

Tabela 3. Resultados obtidos variando o número de anticorpos e fixando o número de iterações e de resultados capturados em 100.

50		250		500		1000		2500		5000	
Qtde	**Custo**	**Qtde**	**Custo**	**Qtde**	**Custo**	**Qtde**	**Custo**	**Qtde**	**Custo**	**Qtde**	**Custo**
2	72	20	72	31	72	56	72	85	72	99	72
6	74	18	74	26	74	26	74	15	74	1	74
6	75	9	75	12	75	11	75	-	-	-	-
2	77	4	77	7	77	3	77	-	-	-	-
6	82	7	82	9	82	2	82	-	-	-	-
5	85	14	85	10	85	2	85	-	-	-	-
5	87	12	87	2	87	-	-	-	-	-	-
4	88	3	88	2	90	-	-	-	-	-	-
5	90	2	90	1	95	-	-	-	-	-	-
5	92	2	92	-	-	-	-	-	-	-	-
6	95	5	95	-	-	-	-	-	-	-	-
4	97	3	97	-	-	-	-	-	-	-	-
3	98	1	100	-	-	-	-	-	-	-	-
6	99	-	-	-	-	-	-	-	-	-	-
3	100	-	-	-	-	-	-	-	-	-	-
4	102	-	-	-	-	-	-	-	-	-	-
2	104	-	-	-	-	-	-	-	-	-	-
4	105	-	-	-	-	-	-	-	-	-	-
1	107	-	-	-	-	-	-	-	-	-	-
3	109	-	-	-	-	-	-	-	-	-	-
4	110	-	-	-	-	-	-	-	-	-	-
2	112	-	-	-	-	-	-	-	-	-	-
2	113	-	-	-	-	-	-	-	-	-	-
1	115	-	-	-	-	-	-	-	-	-	-
1	117	-	-	-	-	-	-	-	-	-	-
1	124	-	-	-	-	-	-	-	-	-	-
1	125	-	-	-	-	-	-	-	-	-	-
1	126	-	-	-	-	-	-	-	-	-	-
2	127	-	-	-	-	-	-	-	-	-	-
1	128	-	-	-	-	-	-	-	-	-	-
1	132	-	-	-	-	-	-	-	-	-	-
1	144	-	-	-	-	-	-	-	-	-	-

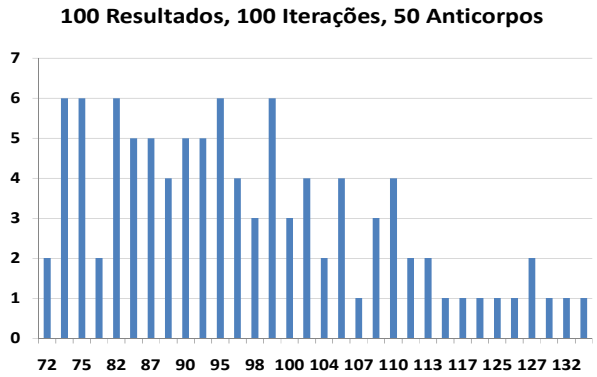


Figura 16: Distribuição das quantidades de resultados obtidos (y) por custo (x).

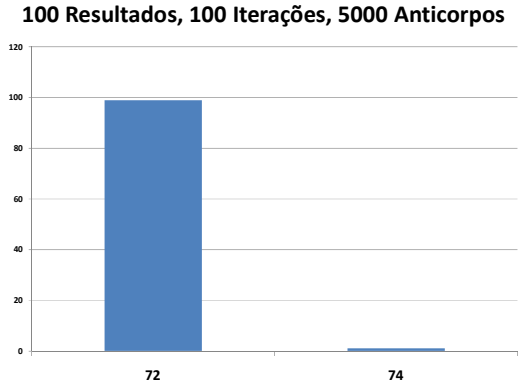


Figura 17: Distribuição das quantidades de resultados obtidos (y) por custo (x).

Estes testes geraram ajustes de curva, cujos gráficos também demonstraram a mesma tendência de curva exponencial assintótica como exemplificado nas figuras 18 e 19.

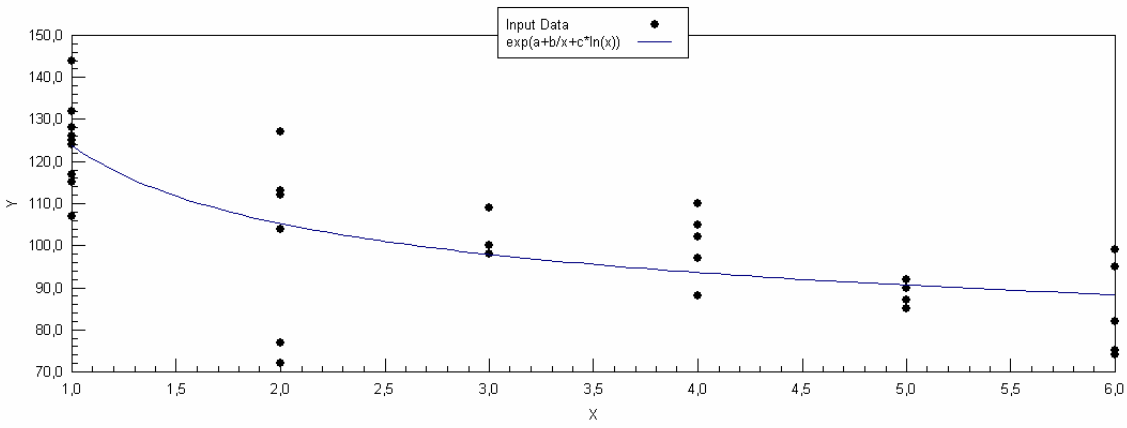


Figura 18: Ajuste de curva para os resultados obtidos com 100 iterações, 100 resultados e 50 anticorpos iniciais.

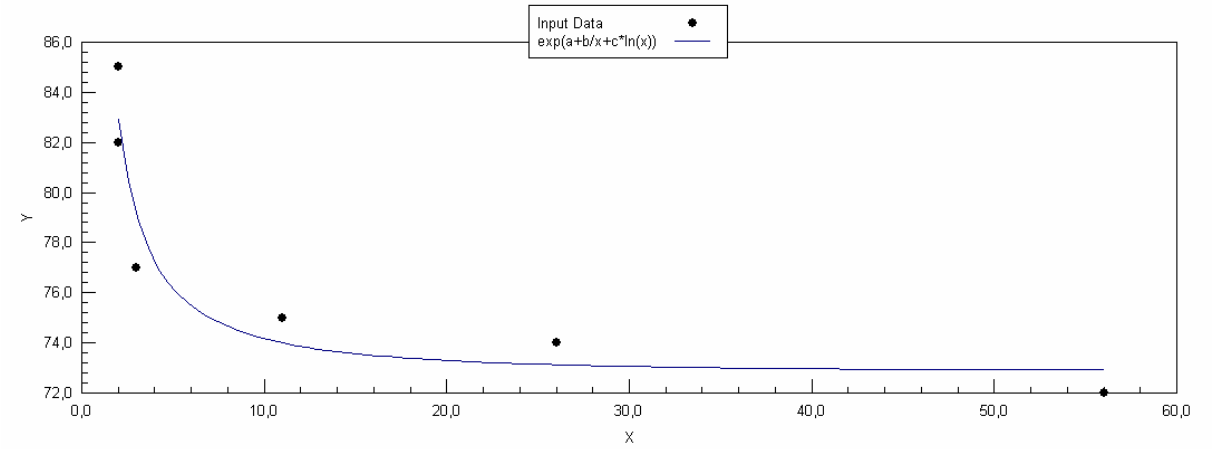


Figura 19: Ajuste de curva para os resultados obtidos com 100 iterações, 100 resultados e 1000 anticorpos iniciais.

Por fim, observa-se na tabela 4 que o tempo varia de acordo com a quantidade de ciclos solicitados, porém as mesmas melhores soluções foram obtidas em todos os testes realizados.

Tabela 4: Tempo de processamento

Anticorpos (A)	Iterações (I)	Resultados Recuperados (RR)	A x I x RR	Tempo de processamento (em segundos)
50	100	100	500000	1
250	100	100	2500000	6
500	100	50	2500000	7
500	100	100	5000000	13
500	100	100	5000000	13
1000	100	100	10000000	27
500	5	5000	12500000	44
500	100	500	25000000	70
500	10	5000	25000000	82
2500	100	100	25000000	93
500	100	1000	50000000	139
5000	100	100	50000000	301
500	100	2000	100000000	295
500	100	5000	250000000	780
500	100	5000	250000000	668
500	100	10000	500000000	1358
500	1000	5000	2500000000	6011

 ISSN 1679-8902

CONSIDERAÇÕES FINAIS

Considerando que a alocação de clientes a servidores a custo mínimo, a exemplo do problema do caixeiro viajante, é tido como um problema NP-completo, a implementação de um algoritmo que trate qualquer volume maior de dados, poderia inviabilizar o trabalho. A representação de um problema fictício de pequeno porte permitiu a observação da tendência dos resultados e do comportamento do algoritmo proposto. Foi possível a obtenção de soluções ótimas para um volume de dados determinados e "tratáveis", o que vislumbra uma necessidade de se explorar a aplicação deste modelo computacional na simulação de novos problemas com níveis de complexidade variados e com volumes de dados maiores em futuras pesquisas. É importante observar ainda que os resultados apresentados demonstram a característica de multimodalidade dos "Sistemas Imunológicos Artificiais", ou seja, não apenas a solução ótima global do problema é obtida, mas também soluções locais de otimalidade. Essa característica permite explorar soluções que, apesar de não serem a melhor, continuam sendo viáveis e factíveis.

REFERÊNCIAS

ALMEIDA, T. A.; YAMAKAMI, A. and TAKAHASHI, M. T. **Sistema imunológico artificial para resolver o problema da árvore geradora mínima com parâmetros *fuzzy***. *Pesqui. Oper.* [online]. 2007, v. 27, n.1, pp. 131-154. ISSN 0101-7438.

BIZAGI - BUSINESS AGILITY. **BizAgi Process Modeler.** Disponível em: <http://www.bizagi.com/>. Acesso em: 24 mar. 2010.

CAMICIA, R. G. M.; VICENTE, A. **Grafos e Mediana.** Disponível em: <http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/15.pdf>. Acesso em: 01 maio 2010.

CASTRO, L. N. **Fundamentals of Natural Computing:basic concepts, algorithms, and applications.** Boca Raton, FL, USA: Chapman & Hall/crc, 2006. 662 p.

CEZAR, C. C. **Estudo da Otimização de Funções através de Sistemas Imunológicos Artificiais.** 2009. 22 f. Trabalho de Conclusão de Curso (Graduação) - Curso de Ciência da Computação, Faculdade de Jaguariúna, Jaguariúna, 2009.

FEOFILOFF, P. ***Análise de Algoritmos***. Disponível em: <http://www.ime.usp.br/~pf/analise_de_algoritmos/> Acesso em: 3 abr. 2010.

NONATO, L. G. **Matriz de Adjacência.** 2000. Disponível em: <http://www.lcad.icmc.usp.br/~nonato/ED/Grafos/node73.html>. Acesso em: 01 maio 2010.

OAKDALE ENGINEERING (USA). **DataFit:** version 9.0.59. Evaluation Copy. Disponível em: <http://www.curvefitting.com/datafit.htm>. Acesso em: 13 nov. 2010.

PFÜTZENREUTER. **O que são problemas Np-Completos.** 2005. Disponível em: <http://epx.com.br/artigos/npcompleto.php>. Acesso em: 17 abr. 2010.

ROSÁRIO, R. R. L.; CARNIERI, C.; STEINER, M. T. A. **Proposta de Solução para o Problema das P-Medianas na Localização de Unidades de Saúde 24 Horas.** Disponível em: <http://www.abepro.org.br/biblioteca/ENEGEP2002_TR61_0949.pdf>. Acesso em: 29 ago. 2010.

RUSSEL, S.; NORVIG, P. **Inteligência Artificial.** 2. ed. Rio de Janeiro: Campus, 2004. 1021 p.

TREVISAN, R. et al. **Michaelis – Moderno Dicionário da Língua Portuguesa.** Editora Melhoramentos Ltda. Disponível em: <http://michaelis.uol.com.br/moderno/portugues/index.php> Acesso em: 18 jun. 2010.

PROPOSTA TEÓRICA PARA SELEÇÃO ALGORÍTMICA DE ENTONAÇÃO VOCAL BASEADA EM CORRELAÇÃO E SIMILARIDADE

Theoretical proposal for algorithm selection of vocal intonation based on correlation and similarity

RIBEIRO, Anderson da Silva
Faculdade Politécnica de Campinas

MOREIRA, Juliana da Costa
Faculdade Politécnica de Campinas

OLIVEIRA, Vanessa Hipólito de
Faculdade Politécnica de Campinas

MENDELECK, André
Faculdade de Jaguariúna

Resumo: Neste artigo é apresentado um modelo teórico para seleção de entonação de voz a partir de uma base de dados previamente conhecida, cujas informações são fornecidas pelo sistema de conversão texto-fala [5]. O objetivo é criar um modelo teórico funcional para selecionar um padrão de entonação interrogativo de uma frase, a ser aplicado em frases afirmativas. A metodologia utilizada baseia-se na avaliação da correlação entre a estrutura gramatical do texto de entrada e a estrutura gramatical das sentenças presentes na base de dados, aplicando-se um modelo estruturado semelhante ao implementado em compiladores.

Palavras-chave: entonação, compilador, padrão interrogativo, regras de ponderação.

ABSTRACT: This paper shows a theoretical model to select a voice intonation from one previously established database, this database contains information from the text-to-speech conversion systems. The purpose is to create the theoretical and functional model to find the intonation pattern for interrogative sentences. The applied methodology is based on the evaluation of the correlation between the grammatical structure of the input text and the

grammatical structure of sentences in the database, applying a structured model for compilers implementation

Key-words: intonation, compiler, question pattern, weighting rules

1. Introdução

Este artigo refere-se à criação de um modelo teórico funcional que tem como objetivo selecionar um padrão de entonação interrogativo de uma frase gravada na base de dados, para ser aplicado a uma frase afirmativa utilizando o produto CPqD Texto Fala, desenvolvido por pesquisadores da Fundação CPqD [1] – Centro de Pesquisa e Desenvolvimento em Telecomunicações, situado na cidade de Campinas, SP. O Texto Fala é um software especializado em converter uma frase textual em sinais de áudio. Este software utiliza uma base de dados com arquivos de áudio e os seus correspondentes elementos textuais. Os arquivos de áudio contêm frases gravadas por locutores com os perfis de entonação que se deseja aplicar. E assim, para cada perfil de entonação que se deseja aplicar à frase textual de entrada, é necessário que hajam frases gravadas na base de dados com o perfil desejado. A proposta deste trabalho é que, dada uma frase no formato textual afirmativo, o software faça a escolha do perfil de entonação interrogativo independente do cadastro ou não na base de áudio, não havendo a necessidade de realizar uma nova gravação.

Baseado nos conceitos de compiladores, propõe-se, neste artigo, um modelo de implementação, que a partir da classificação gramatical de uma frase textual em português, o software efetue a busca na base de dados com frases interrogativas e escolha um perfil interrogativo que será aplicado à frase original. O CPqD Texto Fala é utilizado por uma grande variedade de segmentos comerciais, desde pequenas a grandes empresas, tais como, em sistemas de caixas eletrônicos para ajuda a deficientes visuais, em call Center de companhias de telecomunicações, podendo ser usado para leitura de correios eletrônicos através de um aparelho de telefone. Selecionado o padrão

de entonação, devem-se efetuar estudos específicos focando a pronúncia final da fala a ser apresentada ao usuário final. Este estudo será realizado pela equipe técnica do CPqD.

2. Objetivo

O objetivo é propor um Modelo Teórico para Seleção Algorítmica de Entonação Vocal Baseado em Correlação e Similaridade. Utilizando como recurso o produto "CPqD Texto Fala" [5], é apresentado um modelo computacional que selecione um perfil de entonação em uma base de dados contendo frases interrogativas, e escolha a frase com maior similaridade de entonação, e então a mesma é selecionada para aplicação sobre a frase de entrada, inicialmente não cadastrada na base.

3. Justificativa

O produto CPqD Texto Fala contém uma base de frases gravadas por locutores com perfis de entonação afirmativos. Para se obter um novo perfil de entonação interrogativa, é necessário realizar novas gravações. Isso representa um problema, pois se para cada frase for necessário gravar amostras no padrão afirmativo, interrogativo e exclamativo isso tornaria a base muito grande e diminuiria o desempenho do sistema. Espera-se que o modelo proposto ajude a melhorar o desempenho do software, e, como conseqüência, possa servir como incentivo para mais investimentos em estudos futuros na área da comunicação.

4. Metodologia

O modelo que este trabalho apresenta, utiliza técnicas tradicionais aplicadas no desenvolvimento de compiladores e técnicas de correlação para a

seleção probabilística de modelos de entonação. O modelo está estruturado em cinco etapas:

1) Identificação do código fonte
2) Análise Léxica
3) Análise Sintática
4) Máquina de Validação/Ponderação Sintática - Sintática de Estado
5) Máquina de Seleção

O código fonte, ou seja, uma frase textual é submetida a um analisador léxico para validação das palavras (tokens). A sequência de tokens é submetida ao analisador sintático para validação e obtenção de uma seqüência sintática. A seqüência sintática é então ponderada com padrões sintáticos das frases/entonação previamente armazenadas no banco de dados. O resultado desta etapa é um valor de correlação entre a sintaxe de origem e as sintaxes armazenadas. A sintaxe que apresentar maior correlação é selecionada. Como resultado, a frase originalmente com entonação afirmativa é pronunciada na forma interrogativa.

5. Conceito de um compilador

Segundo Aho [2], um compilador é um software que tem o propósito de fazer a conversão de um programa escrito numa linguagem - a linguagem fonte – em um programa equivalente numa outra linguagem - a linguagem alvo (ver figura 1.1). Como importante parte desse processo de tradução, o compilador relata ao seu usuário a presença de erros no programa fonte.

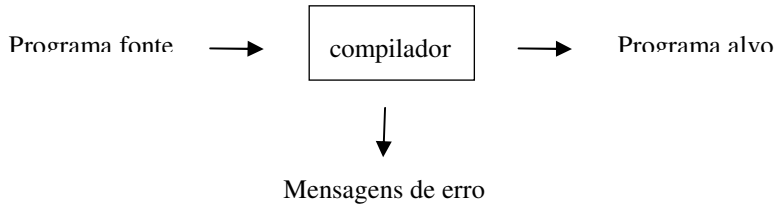


Figura 1 - Um compilador [2]

Rotinas de Análise e fases do processo de compilação

Segundo Aho [2], a análise do processo de compilação é feita em seis etapas:

- Análise linear ou análise léxica: Lê os caracteres do programa fonte da esquerda para a direita e os agrupa em uma sequência de tokens com um significado coletivo.
- Análise hierárquica ou análise sintática: Os tokens, identificados na análise léxica, são agrupados nesta fase seguindo uma hierarquia que faz com que esse agrupamento possua um significado coletivo.
- Análise semântica: efetuar verificações a fim de assegurar a combinação significativa dos componentes do programa.
- Após as análises (léxica-sintática-semântica), é gerada uma representação intermediária do código fonte, processo ao qual dá-se o nome de “Geração de Código Intermediário”.
- Após a “Geração de Código Intermediário”, acontece o processo chamado de “Otimização de Código”. Esse processo tem a finalidade de otimizar o código intermediário de forma a torná-lo um código de máquina mais rápido em tempo de execução.
- Por fim, é gerado o código alvo. Geralmente, trata-se de um código realocável ou código de montagem. A esse processo dá-se o nome de “Geração de Código”. Para a aplicação em questão, o código gerado é uma frase interrogativa, com similaridade sintática ao código fonte.

Na figura 2 é representado um processo de compilação como descrito na proposta por Aho [2], e que norteou o modelo proposto neste trabalho.



Figura 2 - Fases de um processo de compilação [4]

6. CPqD Texto Fala

O CPqD Texto Fala [5] é um software capaz de transformar qualquer informação textual em fala, transformação esta feita em tempo real. É uma tecnologia que converte qualquer texto escrito em português do Brasil em sinal auditivo.

Existe uma diferença entre síntese de voz e síntese de fala. Voz pode ser qualquer som ou ruído emitido pelo aparelho fonador humano, enquanto a fala é um som emitido com significado lingüístico. Portanto, o CPqD Texto Fala sintetiza fala e não voz. A expressão inglesa correspondente a “síntese de fala” é speech synthesis.

Uma característica do CPqD Texto Fala, é a facilidade de integração com outras aplicações, além da variedade de mensagens que podem ser geradas. A seguir são apresentados alguns exemplos de aplicações:

“ATM e postos de auto-atendimento: pode ser utilizado em caixas de banco e terminais de atendimento, entre outros, facilitando a interação com usuários em geral que possuem dificuldade de leitura" [5].

"*Auxílio a pessoas portadoras de deficiência*: Aplicações que são capazes de reproduzir sons podem utilizar o CPqD Texto Fala para interagir facilmente com pessoas portadoras de deficiência visual existindo uma comunicação mais natural e uma transferência de informação mais precisa" [5].

"*Auxílio à navegação no computador pessoal*: Pode ser usado para navegação de janelas, leituras de conteúdo de páginas da Internet, bem como para leitura de mensagens de correio eletrônico em forma de áudio" [5].

"*Leitura de informações de ajuda em softwares*: Pode ser aplicado para leitura de textos de ajuda de softwares, permitindo assim um acompanhamento das instruções passo-a-passo em forma de áudio" [5].

"*Serviços de tele-atendimento*: Pode ser usado para leitura de e-mails por telefone, conta bancária, conta de telefone, água, energia elétrica, previsão do

 ISSN 1679-8902

tempo, horóscopo, consulta de hotéis, variados serviços de call center, notícias, etc.” [5]

"*Substituição de interface visual por interface de áudio*: Útil em ambientes de monitoramento, como salas de controle, convertendo alarmes visuais de texto em fala, bem como em dispositivos inteligentes que recebam mensagens em formato textual, seja em casa, no escritório ou em um automóvel" [5].

7. Estrutura básica do modelo proposto

Na figura 3 é apresentado o modelo teórico proposto por este trabalho.

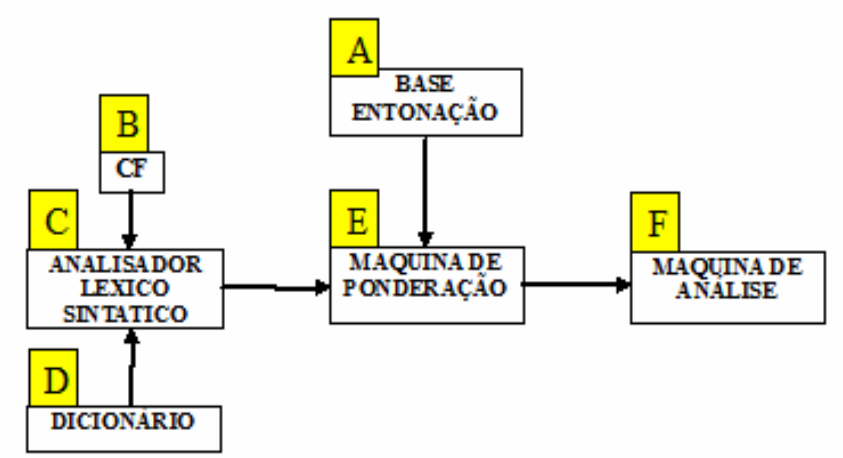


Figura 3 - Estrutura do modelo

A seguir serão explicadas cada uma das partes apresentadas na figura 3:

A. Base Entonação - Base de Frases Gravadas com Entonação Interrogativa

Incorporado ao sistema Texto Fala [5], foi definida uma base de dados auxiliar contendo frases (amostras) gravadas com entonação interrogativa, que auxiliará no processo de seleção. Essa base será a fonte de busca para ser selecionado o padrão de entonação a ser aplicado à frase de entrada. Para

cada amostra, existem informações em modo textual e modo de áudio. O modo textual dessas amostras servirá de insumo para o processo de seleção incorporado no modelo proposto.

B. CF – Texto de Entrada

O texto de entrada é a frase em modo textual, a qual será aplicada o processo de correlação e similaridade que visa selecionar o padrão de entonação interrogativo. Esse texto de entrada será referenciado aqui como Código Fonte (CF). Este CF é no primeiro momento só uma frase em formato textual e passará pelos analisadores léxico e sintático, tendo como base os dados de um dicionário (palavra e classe sintática dessa palavra) e um conjunto de regras sintáticas.

C. Analisador Léxico Sintático

Para cada uma das amostras da base de entonação, será gerada uma frase sintática contendo classes gramaticais (artigo, substantivo, verbo...) para cada um dos elementos. Por exemplo: a frase “O gato pulou?” possui um artigo (o), um substantivo (gato) e um verbo (pulou). Então é montada uma frase sintática dessa frase e formam-se os tokens sintáticos “artigo substantivo verbo”. Esse processo é repetido para cada uma das amostras da base de entonação.

Da mesma forma, a saída do Analisador Léxico Sintático terá uma seqüência sintática e uma seqüência de tokens. Exemplo: a frase “A casa é azul” possui um artigo (a), um substantivo (casa), um verbo (é) e um adjetivo (azul). Esses elementos de saída serão usados como entrada para a máquina de ponderação.

O Analisador Léxico Sintático faz a separação do CF em tokens (palavras) e os classifica gramaticalmente, atribuindo para cada frase de

 ISSN 1679-8902

entrada uma frase sintática de acordo com o dicionário. Ou seja, após o CF passar pelo analisador Léxico Sintático, haverá duas saídas: 1 seqüência textual (separada em tokens) e uma seqüência Sintática (classificação gramatical de cada token). Conforme exemplo abaixo, temos três vetores (V1, V2 e V3), onde o primeiro vetor conterá o CF, no segundo vetor será gravada a seqüência sintática do CF e no terceiro vetor será gravada separadamente a seqüência sintática (tokens sintáticos) de cada token textual.

D. Dicionário

É um arquivo contendo as palavras mais comuns da língua portuguesa e sua classificação gramatical. Será utilizado pelo analisador léxico sintático para devolver a seqüência sintática do CF. Caso a palavra não conste no arquivo, é selecionada uma classificação gramatical padrão.

E. Máquina de Ponderação

É um conjunto de regras que será aplicado a cada uma das amostras da base usando como referência a frase inserida como CF, que no exemplo seria “A casa é azul”. Na máquina de ponderação terão que ser aplicadas regras para, por exemplo, pré-selecionar um conjunto de amostras da base que têm um perfil parecido com o perfil alvo.

1) Tamanho da Amostra

A primeira regra a ser aplicada tem por objetivo selecionar amostras por tamanho (Fator de Escala), buscando frases com tamanho sintático aproximado ao do CF: Para cada amostra da base serão selecionadas aquelas que têm o tamanho próximo ao tamanho da frase alvo. A frase “A casa é azul” tem tamanho igual a 3 palavras, e nas amostras da base serão encontradas

frases com vários tamanhos, desde apenas uma palavra até dezenas de palavras.

Seleção de frases da base pelo tamanho

Define-se um fator de escala e aplica-se esse fator.

Na frase “A casa é azul”, o alvo tem tamanho igual a 3. Se for aplicado um fator de escala de 20% sobre 3, será obtida uma faixa de 2,4 a 3,6. Se arredondarmos os valores para os inteiros maior e menor, mais próximos, teremos 2 e 4. Então, nesse caso, serão selecionadas na base todas as amostras que têm tamanho de 2 a 4 palavras. Essa regra servirá para selecionar frases da Base de Entonação que tenham o mesmo tamanho ou tamanho similar à frase entrada (CF), usando um fator de escala de, por exemplo, 20% para mais e para menos.

2) Regras de Ponderação por Energia

Na próxima etapa, as frases selecionadas da base de entonação serão submetidas à máquina de ponderação.

Para cada elemento sintático das frases selecionadas, serão aplicados fatores de ponderação indicando a correlação sintática com o CF. Este fator de ponderação é chamado de **energia**, indicando o nível de proximidade sintática entre o token do CF e o token no banco de dados.

Status: Ao procurar na base de entonação as frases com os tamanhos desejados, usa-se um *status* para indicar se uma determinada amostra foi selecionada ou não. Ex.: Se a amostra tem o tamanho definido pelo fator de escala, atribui-se a esta um *status* = 1, e, em caso negativo, atribui-se a esta um *status* = -1.

 ISSN 1679-8902

Isso servirá para indicar a quais amostras devem ser aplicadas as regras de ponderação. Pode-se também criar um *status* = 0, que significa estar pendente a seleção daquela amostra – isso pode acontecer se houver algum critério de empate durante o cálculo de energia. Essas amostras podem ser usadas após passarem por outras regras ou análise.

Nota: este modelo não apresenta regras para tratar critérios de desempate. Estas regras deverão ser definidas futuramente.

3) Zerar todos os pontos de energia

O objetivo é encontrar a regra que tem a maior energia possível. Aquela que tiver maior energia tem a maior correlação e a maior similaridade com o alvo. Para cada token do CF, que é o alvo, verificar se existe na regra da base. Se existir, ponderar com 1. Se o token está na mesma posição da regra da base, somar 1. Equivalência funcional - todo artigo é igual (+0,1) e todo substantivo é igual (+0,5). Cálculo da distância funcional – ponderar negativamente a distância entre a posição ao token da regra da base e o token ao código fonte com -0,1. Se um token sintático não existir, ponderar fortemente com -0,8.

Descrevendo a máquina de ponderação

Foi selecionada uma amostra qualquer da base e esta será comparada com o CF. Temos como exemplo o CF: “O gato preto pulou rapidamente”, e como amostra interrogativa, temos na base de dados a seguinte frase: “O carro saiu?”

O primeiro token da amostra é um artigo. Verifica se o primeiro token do alvo (CF) é um artigo. Se for, pondera com 1. No exemplo que este trabalho propõe, isso é verdade, então é ponderado positivamente.

O segundo token da amostra é um substantivo. Verifica se o segundo token do alvo (CF) é um substantivo. Se for pondera com 1. No exemplo que este trabalho propõe, isso é verdade, então é ponderado positivamente.

O terceiro elemento da amostra é um verbo. Verifica se o terceiro token do alvo (CF) é um verbo, se for pondera com 1. No exemplo que este trabalho propõe, isso não é verdade, então não é ponderado positivamente.

Verifica se o terceiro elemento com o quarto elemento é um verbo e se for pondera, porém negativamente. No exemplo que este trabalho propõe isso é verdade, portanto é ponderado.

CF		Amostra
O = artigo	⟶	**O** = artigo
gato = substantivo	⟶	**carro** = substantivo
preto = adjetivo	⟶	**saiu** = verbo
pulou = verbo	⟶	“ ”
rapidamente = advérbio	⟶	“ ”

Pode-se notar que na amostra não existe adjetivo e nem advérbio, e que o verbo do CF não está na mesma posição do verbo da amostra.

Tabela ponderação

Token Sintático (Amostra da Base de Entonação)	
0	Artigo
1	substantivo
2	Verbo
3	
.	
.	
N	

Token Sintático (CF alvo)	
0	artigo
1	substantivo
2	adjetivo
3	verbo
4	advérbio
.	
N	

Energia (CF alvo)	
0	1
1	1
2	-1
3	-0,1
4	-0,8
.	
N	

 ISSN 1679-8902

F. Máquina de Análise

Aplicada a ponderação de energia para todas as amostras selecionadas na base de entonação, tem-se o *status* energético de cada uma das amostras. A próxima etapa consiste em selecionar a amostra que tenha a maior energia. A amostra que tiver a maior energia é a que tem a maior similaridade com a frase de entrada. Por exemplo, suponha que a base de entonação possua 100 amostras, e que foram selecionadas, por tamanho (conforme item E.1), 10 amostras e que, por exemplo, das 10 amostras selecionadas, a que tem a maior energia é a de nº 52 (que é a soma de todas as energias - positiva e negativa - atribuídas à frase). A amostra da base de entonação que possuir a maior energia será indicada como sendo a amostra que tem um possível perfil de entonação que deverá ser aplicado na frase alvo (CF). Neste exemplo, na base de entonação a amostra de número 52 foi selecionada como a que possui a maior energia, e o perfil desta amostra é aplicado ao alvo (CF).

8. Conclusão

Neste trabalho foi apresentada uma proposta de modelagem algorítmica para seleção de entonação de voz. Por se tratar de um modelo, neste momento, não há resultados, pois não foi realizada nenhuma implementação para testes finais. Diante de pesquisas teóricas, esta proposta de modelagem algorítmica para seleção de entonação de voz parece ser um método adequado para se obter uma pronuncia ideal, mais próxima da real (fala humana).

O modelo proposto foi submetido para a equipe responsável pelo sistema “CPqD Texto Fala”, que aprovou a sugestão. Serão realizados testes e, em um próximo trabalho, será feita implementado e testado.

Referências

[1] FUNDAÇÃO CPqD. **CPqD.** Disponível em: http://www.cpqd.com.br. Acessado em: 27 de novembro de 2009.

[2] Compiladores: princípios, técnicas e ferramentas/ Alfred V. Aho et al.; tradução Daniel Vieira – 2. Ed.- São Paulo: Pearson Addison- Wesley, 2008.

[3] FUNDAÇÃO CPqD. **CPqD Texto Fala.** Disponível em: https://www.cpqd.com.br/textofala/telefonia/index.htm. Acessado em: 27 de novembro de 2009.

[4] Compiladores: princípios, técnicas e ferramentas/ Alfred V. Aho et al.; tradução Daniel Vieira – 2. Ed.- São Paulo: Pearson Addison- Wesley, 2008.

[5] FUNDAÇÃO CPqD. CPqD Texto Fala. Disponível em: http://www.cpqd.com.br/component/docman/doc_download/16-cpqd-texto-fala.html. Acessado em: 27 de novembro de 2009.

ESTUDO DE UM ROBÔ DE BUSCA BASEADO EM WEB SEMÂNTICA

Study of a search robot based on semantic Web

AREIAS NETO, Alexandre
Faculdade de Jaguariúna

PETROLI NETO, Silvio
Faculdade de Jaguariúna

Resumo: Esse artigo apresenta a estrutura que a Web Semântica vem propondo como um novo padrão para o desenvolvimento de páginas de Internet. Apresenta também, os conceitos básicos dessa nova estrutura, como o RDF (*Resource Description Framework*), que é recomendado para realizar a estruturação das informações; as Ontologias, que são utilizadas para demonstrar os relacionamentos entre os recursos; os benefícios que os sistemas de busca ganharão com a nova estrutura proposta e para finalizar apresenta uma aplicação que demonstra o funcionamento de um motor de busca semântica desenvolvido utilizando o Asp .Net e a linguagem C#, da Microsoft.

Palavras-chave: Web; Semântica; Busca.

Abstract: This article presents the structure of the Semantic Web proposed as a new standard for developing web pages. It also presents the basic concepts of this new structure, such a RDF (Resource Description Framework), which is recommended for making the allocation of information, Ontologies, which are used to demonstrate the relationships between resources, the benefits to use search engines and presents an application that demonstrates the operation of a semantic search engine that was developed using Microsoft ASP. Net and C# language.

Keywords: Web; Semantic; Search.

INTRODUÇÃO

Devido ao grande volume de informação que circula entre os computadores do mundo todo via Internet e da dificuldade de localizar uma informação na grande rede de computadores, pelo grande quantidade de resultados retornados pelos motores de busca, nos dias atuais surge a necessidade de desenvolvimento de novas técnicas e conceitos sobre esse assunto, visando tornar mais precisos os resultados apresentados pelos robôs de busca. Esse artigo vem apresentar o conceito da Web Semântica que está propondo uma nova estrutura para a criação de páginas da Internet com o intuito de realizar a estruturação das informações. Dessa forma, dividiu-se o artigo em duas partes:

Na primeira parte, são apresentadas as tecnologias que estão sendo recomendadas para o desenvolvimento dessa nova estrutura da Internet e os benefícios que a Web Semântica irá proporcionar aos sistemas de busca de informação. A segunda parte desse artigo apresenta uma aplicação, que baseada nas tecnologias que foram apresentadas na primeira parte do artigo, demonstra de forma prática, o funcionamento de um motor de busca diante da estruturação que está sendo proposta, tornando possível enxergar, de forma clara, a grande evolução que os sistemas de busca atuais irão sofrer, trazendo para o dia-a-dia do usuário mais agilidade e um melhor desempenho.

A Web Semântica

Com a evolução da Internet e das tecnologias de programação que atualmente permitem que os usuários que não tenham o conhecimento no setor de desenvolvimento consigam disponibilizar informações *online* com uma grande facilidade e rapidez, milhões de páginas estão disponíveis na grande rede de computadores contendo informações das mais diversas áreas [1]. Junto com essa evolução surgiram os sistemas de busca que utilizam-se de palavras chaves para localizar as informações desejadas pelos usuários da Internet com o intuito de ajudar e facilitar o acesso aos dados que sejam relevantes [2]. Porém, toda essa tecnologia está disposta de maneira que os computadores não conseguem interpretar o sentido dessas informações e, por

 ISSN 1679-8902

esse motivo, as buscas na Internet precisam ser bastante específicas para que não retornem resultados muito distantes do que, inicialmente, era a intenção do usuário. Diante desses fatos, surge o conceito da Web Semântica conforme é descrito por (Berners-Lee *apud* [1] pp. 133).

> A Web Semântica não é uma Web separada, mas uma extensão da atual. Nela, a informação é dada com um significado bem definido, permitindo melhor interação entre os computadores e as pessoas.

O principal objetivo da Web Semântica é estruturar as informações que estão disponíveis na Internet e tornar possível que os computadores consigam realizar a interpretação dos dados de maneira eficaz e não ambígua. Para isso ser possível, é necessário que as páginas possuam informações sobre seus recursos utilizando do conceito de metadados, ou seja, dados sobre os dados, para que seja feita a descrição das características e a forma de relacionamento desses recursos com os demais recursos existentes [1]. Portanto, a Web Semântica propõe uma nova estrutura que foi dividida em três camadas organizadas conforme é apresentado na Figura 1.

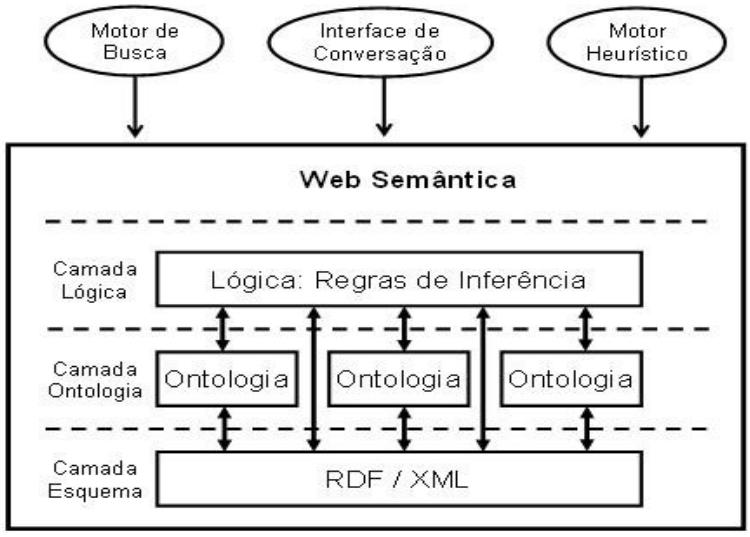


Figura 1: Arquitetura da Web Semântica [2]

Na camada esquema é feita a estruturação e a disposição dos dados de uma maneira que os sistemas web possam interpretá-los. Para realizar esse processo a W3C (Word Wide Web Consortium), recomenda o uso do padrão

RDF (Resource Description Framework). Já a segunda camada, que ganhou o nome de Ontologia, é responsável por definir o relacionamento entre os recursos e pode utilizar o padrão OIL (Ontology Inference Layer) para ser representada. A terceira e última camada, que recebeu o nome de camada lógica, é responsável por realizar a inferência dos dados. [2]

O RDF

Utilizado na camada de esquema, o RDF, é um padrão para descrição de metadados recomendado pela W3C, que utiliza do padrão XML (eXtensible Markup Language) para realizar a estruturação dos dados das páginas web. O padrão RDF permite representar o significado das informações no formato de triplas onde existe: um recurso, um atributo e um valor, conforme é ilustrado na Figura 2.

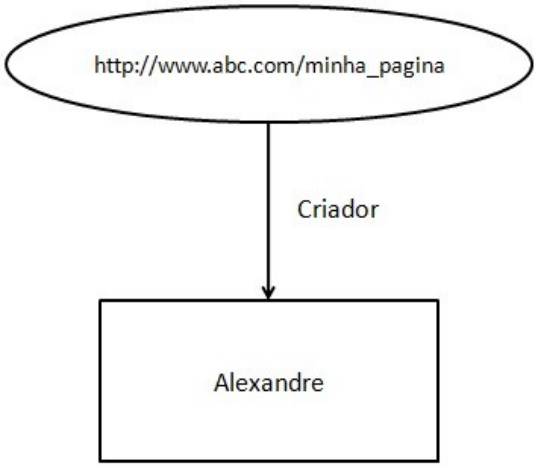


Figura 2: Grafo representando a tripla do RDF [2]

A demonstração feita na Figura 2 pode ser lida como sendo o recurso “http://www.abc.com/minha_pagina” que possui um atributo “criador” e que tem o valor Alexandre, ou seja, podemos afirmar dessa forma, que a página “http://www.abc.com/minha_pagina” foi criada pelo Alexandre [2]. Esse grafo pode ser escrito no padrão RDF conforme é mostrado no Bloco de Código 1.

ISSN 1679-8902

```
<?xml version=”1.0”?>
<rdf:RDF
  xmlns:rdf=”http://www.w3.org/1999/02/22-rdf-syntax-ns#”
  xmlns:x=”http://description.org/schema/”>

       <rdf:Description=”http://WWW.abc.com/minha_pagina”>
             <s:Creator> Alexandre </s:Creator>
       </rdf:Description>
</rdf:RDF>
```

Bloco de Código **1: Descrição da Figura 2 em RDF**

Ontologias

As ontologias são utilizadas na segunda camada da estrutura da Web Semântica e seu principal objetivo é definir como os dados se relacionam. Pode ser comparada com o modelo de entidades e relacionamentos utilizado com grande frequência no setor de planejamento de software. Segundo (SemanticWeb.org *apud* [1]), segue a definição de Ontologia:

> Uma ontologia é uma especificação de uma conceituação. É designada com o propósito de habilitar o compartilhamento e reuso de conhecimentos, de forma a criar ‘compromissos ontológicos’, ou definições necessárias à criação de um vocabulário comum.

Para demonstrar de forma conceitual a representação de uma ontologia, vamos imaginar um cenário de um *site* de comércio eletrônico onde são apresentados diversos tipos de produtos organizados por categorias. A Figura 3 exemplifica de como ficaria a estrutura dessa loja em forma de ontologia.

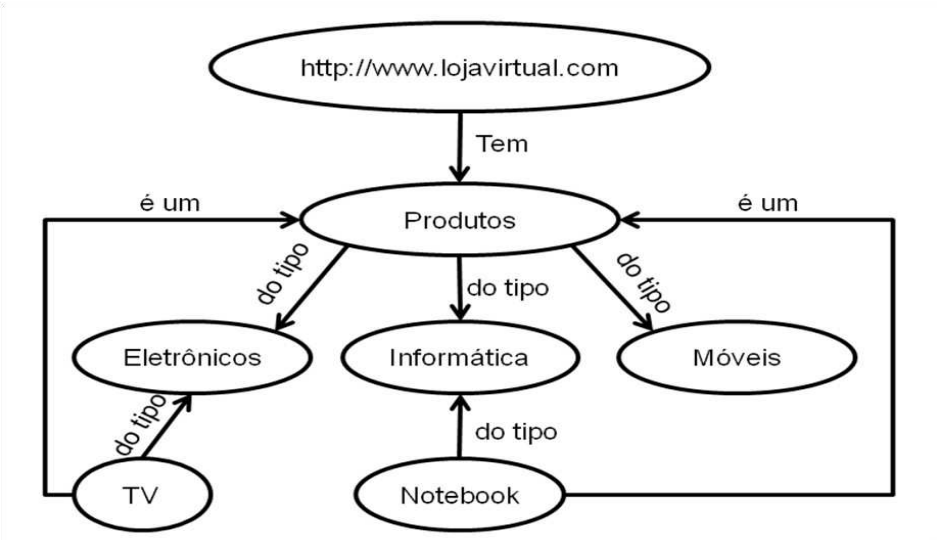


Figura 3: Exemplo de Ontologia

Diversas linguagens estão sendo estudadas para que possam representar o conceito de uma Ontologia e ser aplicada na segunda camada da Web Semântica, contudo, a W3C reuniu um grupo de estudos com o objetivo de desenvolver uma linguagem compatível com as necessidades da Web Semântica e o resultado desse estudo foi à criação da linguagem OWL (Ontology Web Language), cujo principal objetivo é realizar a representação de conceitos e relacionamentos. [4]

Aplicações

Com esse novo padrão de estruturação da Internet, existirá a possibilidade dos motores de busca se tornarem muito poderosos, eficazes e precisos. Eles serão capazes, por exemplo, de realizem a comparação de preços entre sites de comércio eletrônico, realizando o cálculo de frete e impostos do produto escolhido de forma automática e retornar a melhor opção de acordo com as necessidades especificadas pelo usuário, que poderá, nesse instante, realizar a compra do produto. Serão capazes também de realizar o agendamento de consultas médicas de maneira automática, fazendo a

ISSN 1679-8902

comparação entre a agenda do paciente com a agenda dos médicos, conseguindo, através dessa comparação, identificar a melhor opção para o usuário, ou seja, com a Web Semântica a informação irá circular de forma inteligente, o que vai gerar um ganho de desempenho nas rotinas do dia-a-dia dos usuários da Internet.

ESTUDO DE CASO

Com base nas informações obtidas durante o desenvolvimento desse trabalho, foi desenvolvida uma pequena aplicação, que simula o ambiente de uma loja virtual.

O objetivo é demonstrar o funcionamento de um robô de busca simples que utiliza somente a primeira camada da Web Semântica, sendo possível visualizar como a informação é estruturada e a forma com que o robô de busca encontra essa informação. A aplicação foi desenvolvida utilizando a linguagem C#, através do ASP.Net da Microsoft, por ser uma linguagem bastante utilizada para o desenvolvimento Web, com padrões bem definidos de controles de acesso e segurança.

Paralelo ao código fonte dessa aplicação foi construído um arquivo RDF, que é parcialmente apresentado no Bloco de Código 2, onde, todos os produtos e suas características ficam armazenados de forma estruturada. Tal arquivo será utilizado para carregar as informações dos produtos na página da aplicação e será utilizado pelo robô de busca da aplicação. É importante salientar que o arquivo RDF e o arquivo HTML (HyperText Markup Language) compõem uma mesma página. Enquanto o HTML descreve os dados, o RDF fornece o significado semântico aos mesmos.

```
<?xml version="1.0"?>
<rdf:RDF
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:produto="http://localhost/produtos#">
<rdf:Description rdf:about="dvd">
  <produto:id>1</produto:id>
```

```
  <produto:produto>dvd</produto:produto>
  <produto:titulo>Velozes e Furiosos 4</produto:titulo>
  <produto:audio1>Português</produto:audio1>
  <produto:audio2>Espanhol</produto:audio2>
  <produto:audio3>Inglês</produto:audio3>
  <produto:legenda1>Português</produto:legenda1>
  <produto:legenda2>Espanhol</produto:legenda2>
  <produto:legenda3>Inglês</produto:legenda3>
  <produto:fornecedor>Universal</produto:fornecedor>
  <produto:preco>29.90</produto:preco>
  <produto:img>img/dvd/vf4.gif</produto:img>
    ... </rdf:Description>
</rdf:RDF>
```

Bloco de Código 2: Parte do arquivo RDF desenvolvido na aplicação

Na Figura 4 é exibida a página principal da aplicação, onde são apresentados os produtos com seus respectivos títulos e preços, divididos por categorias e também o sistema de busca da aplicação.

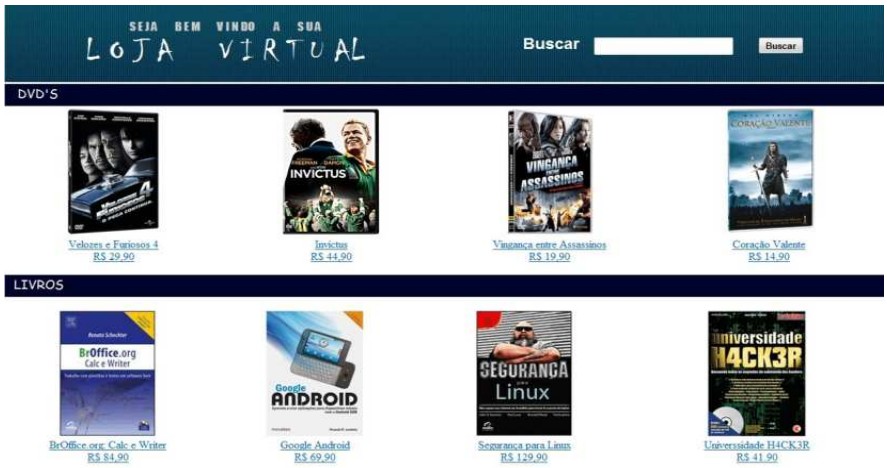


Figura 4: Página principal da aplicação

O sistema de busca da aplicação é onde podemos visualizar, de forma prática, a vantagem de se ter as informações estruturadas de forma que os computadores consigam realizar a interpretação dos dados e os conceitos que foram apresentados nesse artigo. Quando o sistema de busca é acionado, o arquivo RDF é percorrido para verificar se a informação procurada está relacionada com alguma propriedade de algum produto que esteja disponível. Caso essa condição seja verdadeira a aplicação retorna um link para que o

ISSN 1679-8902

usuário possa ter acesso ao produto encontrado. A forma como esse motor de busca percorre o arquivo RDF pode ser vista no Bloco de Código 3.

```
protected void btn_buscar_Click(object sender, EventArgs e)
{

  bool acho = false;
  menu.InnerHtml = "Resultado da Busca";
  produtos.InnerHtml = "";
  String buscando = texto.Text;
  produtos.InnerHtml = produtos.InnerHtml +
  "Elementos encontrados com a propriedade: " + buscando + " <br />";

  XmlDocument doc = new XmlDocument();
  doc.Load("e:\\produtos.xml");

  XmlElement Elem = doc.DocumentElement;

  for (int i = 0; i < Elem.ChildNodes.Count; i++)
  {

   for (int a = 0; a < Elem.ChildNodes.Item(i).ChildNodes.Count; a++)
   {
                    if(Elem.ChildNodes.Item(i).ChildNodes.Item(a).InnerText.ToString
        ().Contains(buscando))
      {
         acho = true;
                String id =
                Elem.ChildNodes.Item(i).ChildNodes.Item(0).InnerText +"";
                String tipo =  Elem.ChildNodes.Item(i).ChildNodes.Item(1).InnerText +
                "";
                String nome =
                Elem.ChildNodes.Item(i).ChildNodes.Item(2).InnerText+"";

         produtos.InnerHtml = produtos.InnerHtml + "<br />" +
                "<a href=detalhes.aspx?id=" + id + "&tpo=" + tipo +
                "> Categoria: " + tipo+ " - Título: " + nome + "</a>";
      }}}
  if (acho == false)
  {produtos.InnerHtml = "Nenhum produto encontrado"; }
    produtos.InnerHtml = produtos.InnerHtml + "<br /><br />
        <a href=home.aspx>Home Page</a>";
}
```

Bloco de Código 3: Função que realiza a busca no arquivo RDF

Basicamente a função de busca carrega o conteúdo do arquivo RDF para a variável chamada de “doc”**,** armazenando essas informações em forma

de uma estrutura de árvore, sendo que a cada tag que descreve um produto como um todo vira um nó e cada nó possui como seus filhos as propriedades que descrevem aquele produto. Após o carregamento do arquivo ser realizado, através do comando “for” o motor de busca vai percorrer todas as propriedades de cada um dos produtos e quando a informação que está sendo procurada for igual a uma propriedade de um produto, o sistema de busca retorna o nó pai daquela propriedade. É, criado então, um link na página da aplicação, tornando possível que o usuário possa visualizar todas as informações referente aquele produto. A apresentação dos resultados do sistema de busca é apresentada na Figura 5, tomando como informação a ser buscada a palavra “Velozes”.

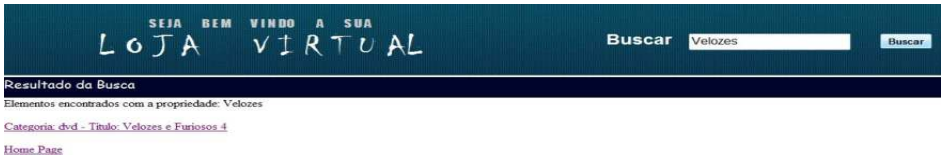


Figura 5: Exemplo de busca

Clicando sobre o link gerado, o usuário irá visualizar a tela que é exibida na Figura 6, com todos os detalhes do produto selecionado, onde ele terá a opção de retornar para a página anterior.



Figura 6: Exibição dos detalhes do produto

ISSN 1679-8902

DISCUSSÕES

A grande dificuldade no desenvolvimento de todo esse trabalho foi encontrar informações precisas sobre a Web Semântica, pois ainda é um projeto que se encontra em fase de estudos e testes.

No desenvolvimento da aplicação, o mais complicado foi realizar a busca no arquivo RDF, pois não foi encontrado nenhum exemplo de como realizar essa busca. Sendo que o RDF é uma extensão do padrão XML, foram testados diversos métodos de busca em arquivo XML até que a busca no arquivo RDF fosse favorável.

É preciso deixar claro que, na Web Semântica, a página que é apresentada pelo navegador está totalmente estruturada dentro do arquivo RDF, ou seja, toda informação - seja um título, uma imagem ou qualquer outro objeto - está descrito no RDF.

CONSIDERAÇÕES FINAIS

A Web Semântica poderá se tornar um marco histórico na evolução da Internet, onde, as informações passarão a circular de forma inteligente e os computadores serão capazes de interpretar as informações das páginas web. Com isso, os motores que realizam a busca da informação se tornarão muito mais poderosos, trazendo para o dia-a-dia dos usuários da Internet uma melhor agilidade e precisão na busca da informação.

Entretanto, esse processo deverá ocorrer de forma lenta, pois seria preciso a criação de novas IDE’s (Interface Development Environment) para o desenvolvimento de páginas semânticas. Também é necessário realizar transformações nas redes sociais, onde um grande volume de informação é disponibilizada por usuários que não possuem nenhum tipo de conhecimento em desenvolvimento. Seria necessário que essas informações fossem estruturadas de forma automática e transparente a esses usuários e, por fim,

havia necessidade ainda de uma grande transformação dos motores de busca para se adaptarem ao novo padrão de Internet.

REFERÊNCIAS

[1] SOUZA, R. R.; ALVARENGA, L. **A Web Semântica e suas contribuições para a ciência da informação**. Ci. Inf., 2004. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652004000100016&lng=pt&nrm=iso>. Acessado em 15 mai. 2010.

[2] MORAIS, E. F.; SOARES, M. B. **Web Semântica para Máquinas de Busca.** Universidade Federal de Minas Gerais, 2003. Disponível em <http://homepages.dcc.ufmg.br/~nivio/cursos/pa03/seminarios/seminario7/seminario7.pdf>. Acessado em 28 mai. 2010.

[3] MENDES, G.; XAVES, A. C.; TEIXEIRA, J.; GOMES, F. **Web Semântica**. Associação Educacional Dom Bosco, 2006. Disponível em http://www.aedb.br/seacIV/SI/Poster/websemantica.pdf. Acessado em 06 jun. 2010.

[4] BREITMAN, K. **Web Semântica: A Internet do Futuro.** LTC, 2006.

 ISSN 1679-8902

MEDIÇÃO DA RESISTIVIDADE ELÉTRICA EM CONDUTORES METÁLICOS

Measurement of electrical resistivity in metallic conductors

BERNARDI, Luis Otavio
Colégio Porto Seguro

PANTANO FILHO, Rubens
Faculdade de Tecnologia César Lattes

Resumo: A resistividade elétrica é uma importante característica dos materiais, uma vez que diferentes materiais também apresentam diferentes valores de resistividade. Esses valores podem indicar se o material é condutor, semicondutor ou isolante elétrico. Os condutores metálicos são os que apresentam menores valores de resistividade. A resistência elétrica de um fio condutor depende diretamente da resistividade do material que o constitui. Algumas substâncias, como metais e água salgada, conduzem bem a eletricidade. Outras, como a borracha, o plástico e o vidro, resistem ao fluxo de eletricidade. Esse fato está diretamente relacionado com a resistividade desses materiais. Medições de resistividade são importantes em vários ramos da Engenharia, tal como as análises de solos. As propriedades elétricas do solo podem ser medidas de várias maneiras diferentes, existindo vários métodos de medição. As características das rochas, por exemplo, podem ser avaliadas pela medição da resistividade das mesmas, segundo técnicas especializadas. O inverso da resistividade é denominado condutividade. As medições de condutividade são feitas principalmente em processos industriais para obter informações sobre concentrações iônicas totais (por exemplo, compostos dissolvidos) em soluções aquosas. Algumas das aplicações mais extensamente usadas são a purificação da água e a medição dos níveis de concentração em soluções. Assim, o principal objetivo desse trabalho consiste em determinar a resistividade de um condutor metálico pela avaliação da tensão e da intensidade de corrente nele estabelecidos, bem como de suas características geométricas.

Palavras-chave: resistividade elétrica, condutividade, tensão elétrica, corrente elétrica.

ABSTRACT: The electrical resistivity is an important characteristic of the materials, since different materials also have different values of resistivity. These figures may indicate whether the material is conductive, semiconductive and insulating electric. The metallic conductors are those with lower values of resistivity. The electrical resistance of a thread depends directly on the resistivity of material that is. Some substances, like metals and salt water, well lead to electricity. Others, such as rubber, plastic and glass, resist the flow of electricity. This fact is directly related to the resistivity of these materials. Measurements of resistivity are important in various branches of Engineering, as the analysis of soils. The electrical properties of the soil can be measured in many different ways, there are several methods of measurement. The characteristics of the rocks, for example, can be assessed by measuring the resistivity of the same, the second technical expertise. The inverse of resistivity is called conductivity. Measurements of conductivity are made mainly in industrial processes to obtain information on total ionic concentrations (eg dissolved compounds) in aqueous solutions. Some of the most widely used applications are water purification and measurement of concentration levels in solutions. Thus the main purpose of this study is to determine the resistivity of a metal driver for assessing the intensity of voltage and current it down, as well as its geometrical characteristics.

Keywords: electrical resistivity, conductivity, electrical voltage, electrical current.

1. Introdução

Na Grécia antiga, por volta de 600 a.C., Tales de Mileto realizou algumas experiências com âmbar (resina sólida fossilizada proveniente das árvores). Assim, ele descobriu que a barra de âmbar, quando atritada com a pele de animal, adquiria a propriedade de atrair pequenos pedaços de palha. De certa forma, pode-se dizer que esses foram os primeiros fenômenos elétricos estudados. A palavra eletricidade se origina do vocábulo *elektron*, palavra grega para designar o âmbar. A partir da segunda metade do século XVIII, a eletricidade teve seus conhecimentos sistematizados.

Charles Augustin Coulomb, Karl Friedrich Gauss, George Simon Ohm, Michael Faraday e James Clerk Maxwell, importantes pensadores dos séculos XVIII e XIX, notabilizaram-se pelas suas contribuições ao estudo da eletricidade e do magnetismo, imortalizando seus nomes na história da ciência. Dentre outras, há uma importante relação entre grandezas elétricas, denominada Lei de Ohm, muito útil na análise de circuitos elétricos.

Hoje, sabe-se que a eletricidade está presente a todo tempo ao nosso redor e em nós mesmos. Na natureza, a eletricidade pode ser observada, por exemplo, numa grande descarga elétrica. No corpo humano, também se pode observar a eletricidade, tal como nos impulsos elétricos do olho para o cérebro: nas células da retina existem substâncias químicas que são sensíveis à luz; quando uma imagem se forma na retina estas substâncias produzem impulsos elétricos que são transmitidos ao cérebro. Muitos outros efeitos que cotidianamente presenciamos ao nosso redor são, no fundo, resultados de forças eletromagnéticas. Por exemplo, plantas verdes absorvem a luz solar - que é uma onda eletromagnética - e convertem a energia em energia potencial eletromagnética sob a forma de moléculas de carboidrato, a base de quase toda a vida na Terra. Daí a importância do estudo dos fenômenos elétricos.

Em seus trabalhos cotidianos, pesquisadores, engenheiros e outros profissionais das mais variadas áreas do conhecimento humano têm necessidade de conhecer as características dos materiais que serão empregados em seus projetos de pesquisa ou de aplicação. Nesse contexto, também estudar e analisar as propriedades elétricas dos materiais é, na maioria das vezes, fundamentalmente necessário.

Resistividade e condutividade são duas das principais propriedades elétricas de materiais, permitindo-nos caracterizar se os mesmos são bons ou maus condutores de eletricidade. Essas duas grandezas também têm uma dependência com a temperatura dos materiais. O estudo de suas características permite uma melhor compreensão dos fenômenos elétricos, bem como a escolha adequada de materiais elétricos para determinados fins.

Assim, este trabalho tem como objetivo principal a determinação da resistividade elétrica de um condutor metálico, por intermédio da Lei de Ohm, utilizando as medições de tensões e intensidades de correntes elétricas nele estabelecidas, bem como analisar as influências de suas características geométricas nas propriedades resistivas do mesmo.

2. Revisão bibliográfica

2.1. Resistividade

A velocidade de migração dos elétrons em um fio metálico com corrente está relacionada com o campo elétrico no fio. Se a intensidade do campo for aumentada, aumenta-se a intensidade da força elétrica sobre os elétrons e a velocidade de migração também aumenta (SERWAY; JEWETT JR., 2002). Assim, pode-se verificar experimentalmente que em um metal, à temperatura constante, a densidade de corrente **J** é diretamente proporcional ao campo elétrico **E** aplicado, ou seja:

$$\vec{J} = \sigma\vec{E} \qquad (1)$$

Na equação (1) acima, σ é uma constante denominada condutividade. Dessa forma, quanto maior for a condutividade de um material menor deve ser a intensidade do campo elétrico **E** para criar uma mesma densidade de corrente **J**. Algumas vezes, σ pode depender do campo elétrico aplicado. No Sistema Internacional de Unidades, a unidade de σ é $(A/m^2)/(V/m)$, ou então, (A/V)/m, o que equivale à siemens por metro (S/m).

Em geral, os “bons” metais apresentam condutividades altas. Por “bons” metais se entendem os metais que apresentam senão todas, pelo menos a maior parte das propriedades metálicas, tais como a ductilidade e brilho, além de propriedades químicas claramente metálicas, como a valência exclusivamente positiva (EISBERG; LERNER, 1983). O recíproco da condutividade é denominado de resistividade ρ. Assim, pode-se escrever:

$$\rho = \frac{1}{\sigma} \qquad (2)$$

A unidade de resistividade é o inverso da unidade de condutividade, ou seja, metro por siemens (m/S). Agora, utilizando a equação (2), pode-se reescrever a equação (1) da seguinte forma:

$$\vec{E} = \rho \vec{J} \qquad (3)$$

De acordo com a definição de resistividade elétrica**, ρ** é uma característica específica de cada substância e não de uma amostra particular da mesma (HALLIDAY; RESNICK, 1984). Quanto melhor condutor for o material, tanto menor será sua resistividade. De um modo geral, os metais são as substâncias que apresentam menores resistividades. A resistividade de um material depende, entre outras coisas, da temperatura. Em geral, a resistência dos metais aumenta com a temperatura. Isto está em acordo com o fato de que o aumento da temperatura faz com que os átomos vibrem mais rapidamente no material, promovendo com isto o aumento do número de "colisões" entre os mesmos e os elétrons livres. Na Tabela 1, a seguir, são apresentados alguns valores característicos de resistividades de alguns materiais.

Tabela 1 – Resistividade de alguns materiais.

Material	Resistividade ρ (m/S)
Condutores	
Prata	$1{,}58.10^{-8}$
Cobre	$1{,}67.10^{-8}$
Alumínio	$2{,}65.10^{-8}$
Tungstênio	$5{,}60.10^{-8}$
Ferro	$9{,}71.10^{-8}$
Semicondutores	
Carbono (grafite)	$(3 - 60).10^{-5}$
Germânio	$(1 - 500).10^{-3}$
Silício	0,1 – 60
Isolantes	
Vidro	$10^{9} - 10^{12}$
Borracha	$10^{13} - 10^{15}$

Fonte: http://www.unb.br/iq/kleber/EaD/Eletromagnetismo/Resistividade/Resistividade.html.

2.2. Leis de Ohm

Retomando a equação (1) e integrando ambos os lados da mesma em um percurso ao longo do condutor, tem-se:

$$\int_a^b \vec{E} \cdot d\vec{\ell} = i \int_a^b \frac{\rho}{A} d\ell \qquad (4)$$

onde o vetor $\vec{dl}$ é paralelo a $\vec{J}$. Dessa forma, a integral do lado esquerdo pode ser reescrita da seguinte forma:

$$\int_a^b \vec{\nabla} V \cdot d\vec{\ell} = -\int_a^b \vec{E} \cdot d\vec{\ell} = V_b - V_a = V_{ab} \qquad (5)$$

A integral do lado direito da equação (4) é denominada resistência elétrica do condutor, ou seja:

$$R = \frac{\rho L}{A} \qquad (6)$$

Na equação (6), também denominada 2ª Lei de Ohm, **L** representa o comprimento do condutor e **A** sua área de secção transversal, conforme ilustração da Figura 1.

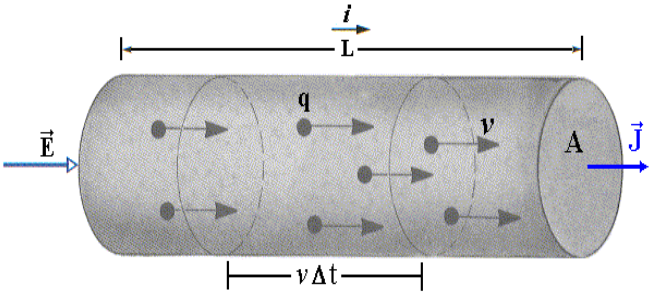


Figura 1 – Ilustração de um condutor metálico.

 ISSN 1679-8902

A equação (6) mostra que a resistência elétrica depende das características geométricas do condutor, bem como de sua resistividade. Esta equação está de acordo com o que se observa experimentalmente, ou seja, condutores feitos do mesmo material, mas que diferem pelos comprimentos e pelas áreas das seções transversais apresentam diferentes resistências ao movimento dos elétrons. Também é possível verificar que apresentam maior resistência elétrica aqueles de maior comprimento L, com a mesma seção transversal, ou seja:

$$L_2 > L_1 \quad \Rightarrow \quad R_2 > R_1 \qquad (7)$$

Por outro lado, para condutores de mesmo comprimento, apresenta maior resistência o condutor de menor área de seção transversal.

$$A_3 > A_2 \quad \Rightarrow \quad R_3 > R_2 \qquad (8)$$

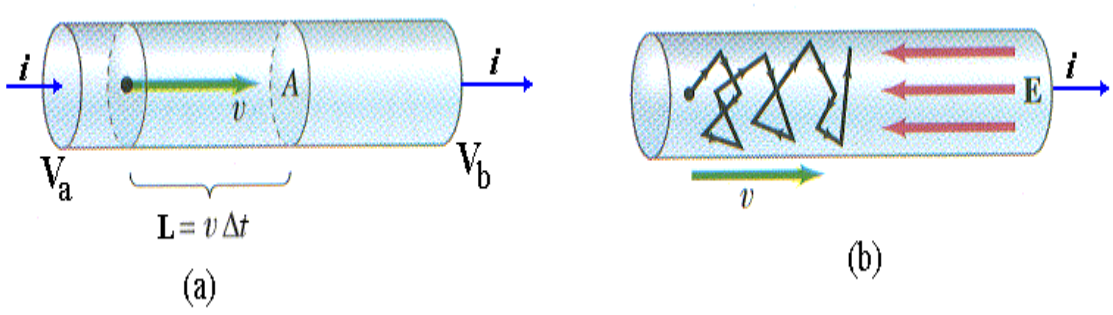


Figura 2 – Ilustração da resistência à passagem de elétrons no interior do condutor.

Utilizando-se a definição estabelecida pela equação (6), pode-se voltar à equação (4) e escrevê-la na forma:

$$V_{ab} = iR \qquad (9)$$

No Sistema Internacional de Unidades, a resistência **R** do condutor é medida em (volt/ampère) ou ohm (Ω). Para muitos materiais, incluindo os metais, experimentos mostram que a resistência é constante para grande parte das voltagens aplicadas. Esse comportamento é conhecido como 1ª Lei de

Ohm. Os materiais ou dispositivos que obedecem à Lei de Ohm são denominados ôhmicos. Assim, para esses materiais há uma relação linear entre a voltagem aplicada e a intensidade de corrente estabelecida (SERWAY, JEWETT JR., 2002).

As duas Leis de Ohm não valem apenas para os metais. De modo aproximado, elas valem também para a maioria dos materiais sólidos, inclusive os maus condutores de eletricidade (AMALDI, 1995). Convém também ressaltar que o âmbito da validade da equação (9) pode ser muito limitado para justificar o termo “lei”. Não é um enunciado fundamental sobre a natureza, como o é, por exemplo, a Lei de Coulomb. Na verdade, é uma expressão empírica que descreve com precisão o comportamento de muitos materiais numa faixa de valores de tensão tipicamente encontrados nos circuitos elétricos (KELLER, GETTYS e SKOVE, 1999).

3. Materiais e Métodos

Para determinação da resistividade, utilizou-se um fio de material metálico, com 11 m de comprimento, disposto em torno de um suporte de madeira de forma cúbica, com arestas de comprimentos 25 cm, de modo que a extensão de cada volta em torno da armação correspondia a 1 metro do comprimento fio, conforme ilustração da Figura 3.



Figura 3 – Ilustração do suporte com o condutor.

Para alimentar o circuito montado, utilizou-se uma fonte de tensão, marca MINIPA, modelo MPC 3003D, conforme ilustração na Figura 4.



Figura 4 – Ilustração fonte de tensão utilizada.

A primeira extremidade do fio metálico foi conectada em uma fonte de tensão, utilizando-se um resistor R = 330 Ω como limitador de corrente, conforme esquema ilustrado na Figura 5.

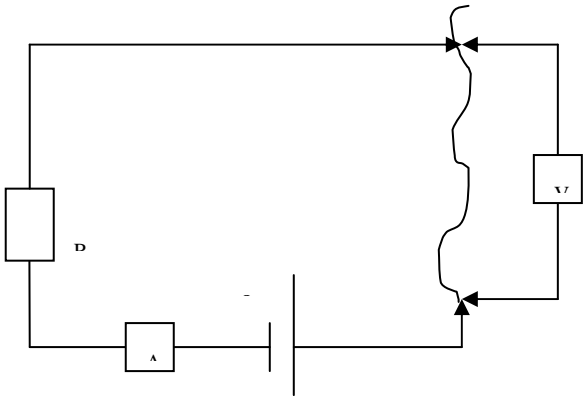


Figura 5 – Ilustração do circuito utilizado.

Inicialmente, ajustou-se a fonte de tensão de modo a manter uma corrente de intensidade constante da ordem de 9 mA. Em seguida, a outra conexão entre a fonte e o fio ocorreu em um ponto de sua extensão correspondente a 1 m do mesmo, medindo-se então a tensão estabelecida. Depois disso, variando-se o comprimento de 1 em 1 m a partir da primeira extremidade, as medições de tensão e de intensidade de corrente foram feitas por meio de multímetros, marca DAWER, modelo DM 3340. Numa segunda etapa, retirou-se o resistor R limitador de corrente, ajustando-se a fonte para manter uma corrente de intensidade da ordem 100 mA.

Além desses dois procedimentos, mediu-se também diretamente a resistência elétrica do condutor, para os diferentes comprimentos, utilizando-se o multímetro. Com um micrômetro, marca MITUTOYO, mediu-se também o diâmetro do fio metálico.

4. Resultados e discussão

4.1. Resultados

Os resultados obtidos para as tensões e intensidades de corrente elétrica estão mostrados na Tabelas 2; nesse caso, utilizando-se o resistor R limitador de corrente.

Tabela 2 – Tensão e intensidade de corrente no condutor (com resistor de limitação).

L (m)	U (volt)	I (mA)
1	3,045	8,78
2	3,158	8,72
3	3,208	8,60
4	3,334	8,60
5	3,450	8,60
6	3,557	8,49
7	3,780	8,39
8	3,840	8,22
9	3,912	8,14
10	4,030	8,06
11	4,150	8,02

 ISSN 1679-8902

Os valores da Tabela 2 também estão mostrados no gráfico da Figura 6.

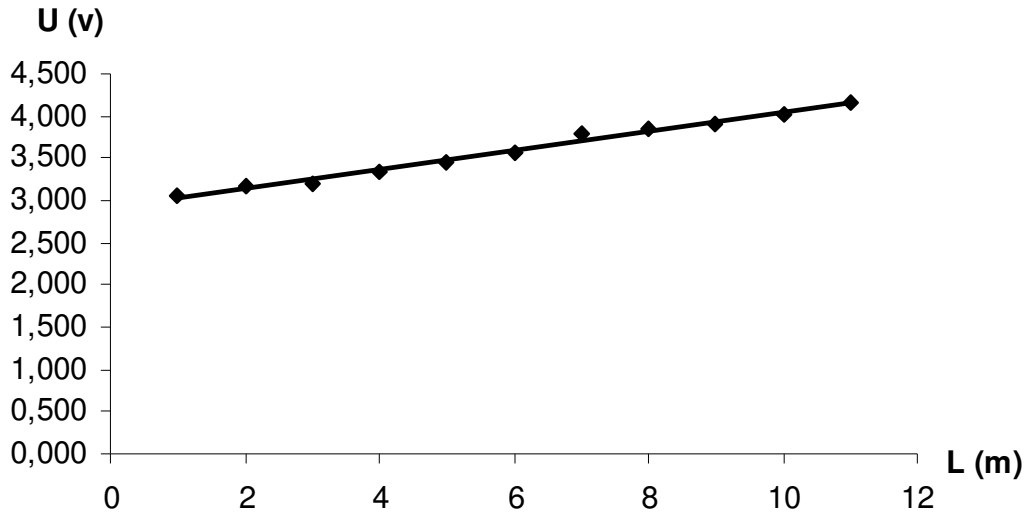


Figura 6 – Gráfico da tensão em função do comprimento do condutor (com limitador).

Da mesma forma, a Tabela 3 mostra os resultados obtidos para a mesma situação sem o resistor R limitador de corrente.

Tabela 3 – Tensão e intensidade de corrente no condutor (sem resistor de limitação).

L (m)	U (volt)	I (mA)
1	1,817	113,4
2	3,578	113,1
3	5,290	112,6
4	7,020	112,5
5	8,750	112,3
6	10,470	112,0
7	13,870	111,2
8	15,540	110,9
9	17,230	110,6
10	18,900	110,3
11	20,600	110,0

Os valores da Tabela 3 estão mostrados no gráfico da Figura 7.

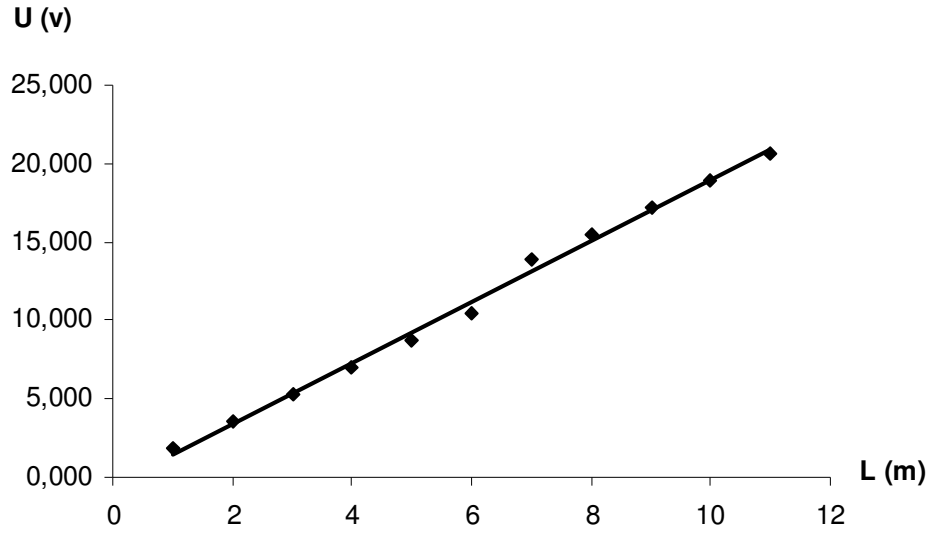


Figura 7 – Gráfico da tensão em função do comprimento do condutor (sem limitador).

Na Tabela 4, a seguir, estão mostrados os valores da resistência elétrica do condutor, em função do comprimento L do mesmo, medindo diretamente com o ohmímetro.

Tabela 4 – Resistência elétrica e comprimento do fio condutor.

L (m)	R (ohm)
1	17
2	37
3	49
4	63
5	78
6	94
7	122
8	138
9	155
10	173
11	192

Os valores da Tabela 4 estão mostrados no gráfico da Figura 8.

 ISSN 1679-8902

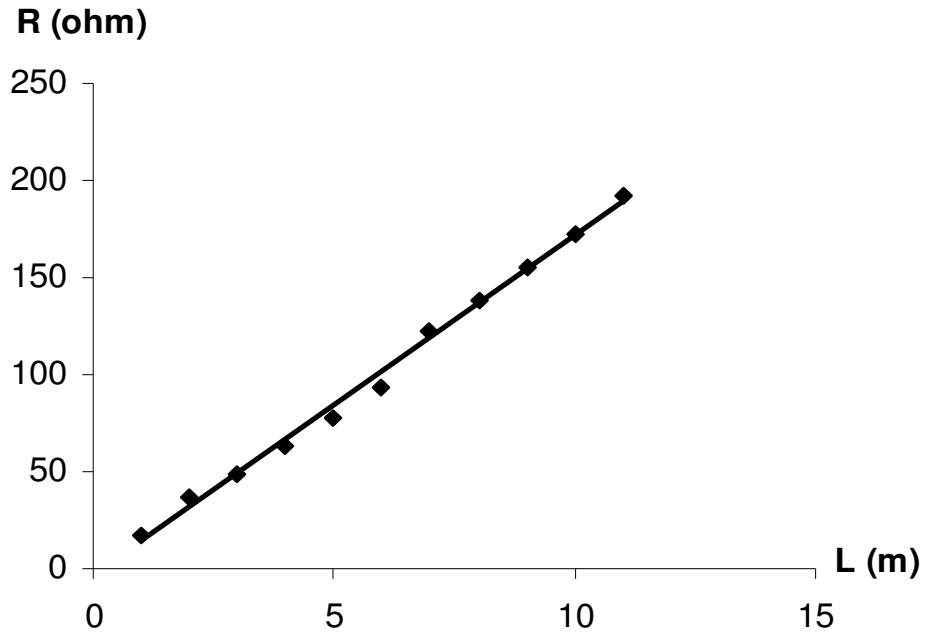


Figura 8 – Gráfico da resistência elétrica em função do comprimento do condutor.

O valor obtido para o diâmetro do fio metálico, medido diretamente com o micrômetro, foi (0,32 ± 0,01) mm.

4.2. Determinação da resistividade

A resistividade do material foi obtida pelos gráficos da tensão em função comprimento do condutor. Deve-se observar que, pelas equações (6) e (9), pode-se escrever $\rho = (U/L).A/i$, onde o quociente (U/L) representa o coeficiente angular da reta obtida nos gráficos das Figuras 6 e 7. Assim, obteve-se o valor médio $\rho = (5,14 \pm 0,40).10^{-6}$ Ω.m para o caso do circuito com o resistor de limitação.

Da mesma forma, obteve-se o valor médio $\rho = (5,30 \pm 0,29).10^{-6}$ Ω.m para o caso do circuito sem o resistor de limitação de corrente.

Também se calculou a resistividade por meio dos valores da resistência elétrica, medidos diretamente com o ohmímetro, utilizando-se da equação (6). Nesse caso, o valor médio obtido foi $\rho = (5,43 \pm 0,30).10^{-6}\ \Omega.m$.

4.3. Discussão

Analisando-se os valores médios obtidos para a resistividade, observa-se que a utilização ou não do resistor limitador de corrente influencia nos resultados.

Utilizando-se o resistor limitador de corrente, a fonte ficou mais instável, aumentando-se os erros nas leituras dos valores da tensão e da corrente. Para comprimentos do fio acima de 5 m, com o limitador de corrente, os valores da tensão e da intensidade da corrente ficaram mais estáveis. Assim, considerando somente esses valores, obtém-se o valor médio de $\rho = (5,36 \pm 0,29).10^{-6}\ \Omega.m$, ou seja, mais próximo daquele obtido por medição direta com o ohmímetro. Isso ocorre, provavelmente, porque para esses valores de comprimento, as resistências dos segmentos do fio já estão mais próximas do valor da resistência do limitador de corrente. Assim, pequenas mudanças no posicionamento do cursor sobre o fio não alteram significativamente a resistência total e, também, a distribuição da tensão entre o fio e o resistor. Ao contrário, sem o limitador de corrente, as pequenas mudanças no posicionamento do cursor provocam alterações significativas na resistência do segmento de fio, tornando mais estável a leitura dos valores nos aparelhos.

5. Conclusões

O método utilizado permite a determinação da resistividade do material, possibilitando assim avaliar se o material é bom condutor ou isolante elétrico. Os valores calculados para a resistividade indicam que o material que compõe o fio metálico pode ser o Zn (zinco), uma vez que, para este metal, o valor encontrado na literatura foi $6,2.\ 10^{-6}\ \Omega.m$ (CALLISTER JR., 2002).

 ISSN 1679-8902

Pode-se verificar que a resistência elétrica do condutor metálico é aproximadamente constante quando a temperatura do mesmo não varia significativamente. Em outras palavras, significa que, nessas condições, a intensidade de corrente elétrica no condutor metálico é diretamente proporcional à tensão aplicada em seus terminais. Também é possível concluir que a resistência elétrica do condutor metálico (na forma de fio) aumenta proporcionalmente com o aumento do comprimento do mesmo. Dessa forma, houve necessidade de aumento da tensão para manter a intensidade da corrente elétrica quando se aumentou o comprimento do condutor.

Verificou-se também que a resistividade do material é praticamente invariável com as alterações de comprimento, tensão aplicada e corrente estabelecida. As pequenas diferenças observadas se devem aos erros inerentes ao processo.

Referências

AMALDI, H. **Imagens da Física.** 1ª ed. *São Paulo*: Scipione. 1995. p. 539.

CALLISTER JR., W. D. **Ciência e engenharia de materiais:** uma introdução. 5ª ed. Trad. SOARES, S. M. S. *Rio de Janeiro*: Livros Técnicos e Científicos. 2002. p. 589.

EISBERG, R. M.; LERNER, L. S. **Física:** fundamentos e aplicações. 1ª ed. v. 3. *São Paulo*: McGraw-Hill do Brasil Ltda. 1983. p. 422.

HALLIDAY, D.; RESNICK, R. **Física**. 4ª ed. v. 3. *Rio de Janeiro*: Livros Técnicos e Científicos. 1984. p. 322.

http://www.unb.br/iq/kleber/EaD/Eletromagnetismo/Resistividade/Resistividade.html.Acessado em 02/12/08.

KELLER, F. J.; GETTYS, W. E.; SKOVE, M. J. **Física**. 1ª ed. v. 2. *São Paulo*: Makron Books. 1999. p. 615.

SERWAY, R. A.; JEWETT JR., J. W. **Princípios de Física:** eletromagnetismo. 1ª ed. v. 3. *São Paulo*: Pioneira Thomson Learning. 2004. p. 200.

GESTÃO DE REQUISITOS LEGAIS E CONFORMIDADE AMBIENTAL UTILIZANDO O MÉTODO ZOPP

Legal requirements and environmental compliance management through Zopp method

RIGOLETTO, Ivan de Paula
Centro Universitário das Faculdades Associadas de Ensino
Universidade Estadual de Campinas

GONÇALVES, Monica Maria
Centro Universitário das Faculdades Associadas de Ensino

Resumo: Este trabalho apresenta o método Zopp de planejamento orientado a objetivos, devidamente adaptado, descrevendo um processo de implementação dos aspectos legais abordados na norma ISO 14001 (sistemas de gestão ambiental - especificação e diretrizes para uso), discutindo-se também as vantagens e desvantagens da adaptação desta metodologia, que se mostrou aplicável a este estudo.

Palavras-chave: Meio Ambiente; Gestão Ambiental; ISO 14001

Abstract: This paper presents the Zopp methodology for planning oriented to objectives, properly adapted, describing an implementation process for the legal aspects outlined on ISO 14001 standard (environmental management systems - specification with guidance for use), also analyzing benefits and disadvantages of this methodology, applicable to this study.

Key-words: Environment; Environment Management; ISO 14001

INTRODUÇÃO

A série ISO 14000, desenvolvida pela ISO (*International Organization for Standarization*, responsável pela edição de normas para aplicação em caráter

mundial) é o conjunto de normas que definem o estado da arte em gestão ambiental de produtos e processos. Nesta série, a norma ISO 14001 define os requisitos de um sistema de gestão ambiental, sendo também a única certificável, ou seja, é a única passível de ter seu cumprimento verificado e registrado por empresas externas de auditoria. Define, em seu conteúdo um Sistema de Gestão Ambiental (SGA) baseado em processos e procedimentos abrangendo planejamento, desenvolvimento, controle e ação, tendo sido desenvolvida para propiciar às organizações uma metodologia estruturada de forma a garantir desempenho ambiental satisfatório (ABNT, 2004).

A implementação de sistemas de gestão ambiental em empresas, e sua certificação, é monitorada pela ISO, que publica desde o final da década de 90 pesquisas sobre certificação ambiental. Os resultados descritos na Figura 1 mostram o crescente interesse pela implementação - e conseqüente certificação - de sistemas de gestão ambiental (Rigoletto, 1999; ISO, 2009; ISO, 2011).

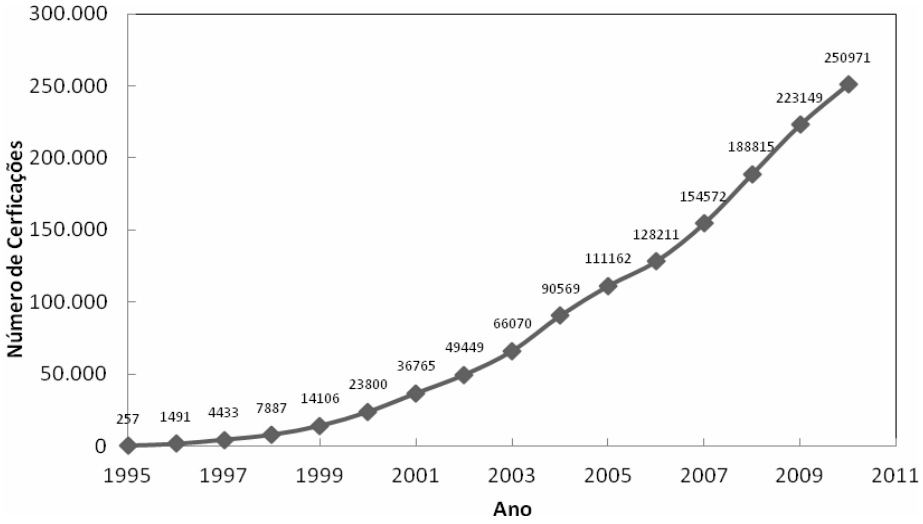


Figura 1 - Certificações ambientais no mundo até 31/12/2010. (Rigoletto, 1999; ISO 2009, ISSO, 2011)

Quanto ao número de empresas certificadas, destacam-se a China (69.784), Japão (35.016), Espanha (18.347), Itália (17.064) e Reino Unido (14.346), tendo o Brasil pelo menos 3100 empresas certificadas,

aproximadamente 1% do total mundial, onde quase 160 países possuem empresas certificadas (ISO, 2011).

PLANEJAMENTO ORIENTADO A OBJETIVOS

Para a implementação dos requisitos da ISO 14001, com destaque para aqueles relacionados à Conformidade Legal ambiental, é necessária a escolha ou adoção de um modelo que permita a análise das condições existentes ou planejadas e que forneça subsídios, ferramentas ou metodologia para transportar requisitos de uma norma para a realidade de quem a implementa. Nesse sentido, objetivou-se discutir a aplicação do **método Zopp** (GTZ, 1991) de Planejamento Orientado a Objetivos, que é uma ferramenta que permite elaborar os fundamentos de uma proposta, estabelecendo definições claras e objetivando se chegar a uma compreensão comum dos problemas envolvidos. Esta metodologia permite, também, visualizar um caminho a se seguir para se atingir um objetivo, através de pontos de referência para monitoramento e avaliação das propostas (ou ambientes). Ainda, este método auxilia na comunicação e cooperação entre as partes envolvidas. As etapas que compõem o método Zopp são cinco, descritas a seguir.

Etapa de análise da participação

Nesta etapa, a empresa deve identificar todos os envolvidos com a questão ambiental, para permitir uma visão de conjunto das organizações diretamente afetadas com o assunto, e também conhecer os interesses e expectativas de outras áreas. O envolvimento de partes interessadas, aqui podendo ser representadas por comunidades, acionistas ou órgãos ambientais pode ser incluído nesta etapa, visando obter informações que possam ser relevantes nas etapas posteriores, quando se definem os objetivos e metas.

 ISSN 1679-8902

Etapa de análise dos problemas

O problema aqui é interpretado pela maneira como as questões legais ambientais serão analisadas dentro do Sistema de Gestão Ambiental. Nesta etapa, é fundamental considerar itens como divisão de responsabilidades e participação mais ativa das funções envolvidas diretamente. Em resumo, o problema se traduz em como identificar os aspectos ambientais das atividades da empresa, os requisitos legais a ela aplicáveis e como comprovar conformidade em relação a eles. E, caso existam não-conformidades, em como corrigi-las.

Etapa de análise de objetivos

O objetivo desta análise é garantir, através de ferramentas gerenciais, o conhecimento e a conformidade em relação aos requisitos legais, abrangendo deste a identificação de novos requisitos legais até a obtenção sistemática de registros que comprovem esta conformidade. A análise deste objetivo se encontra planificada na Figura 2 - árvore de objetivos.

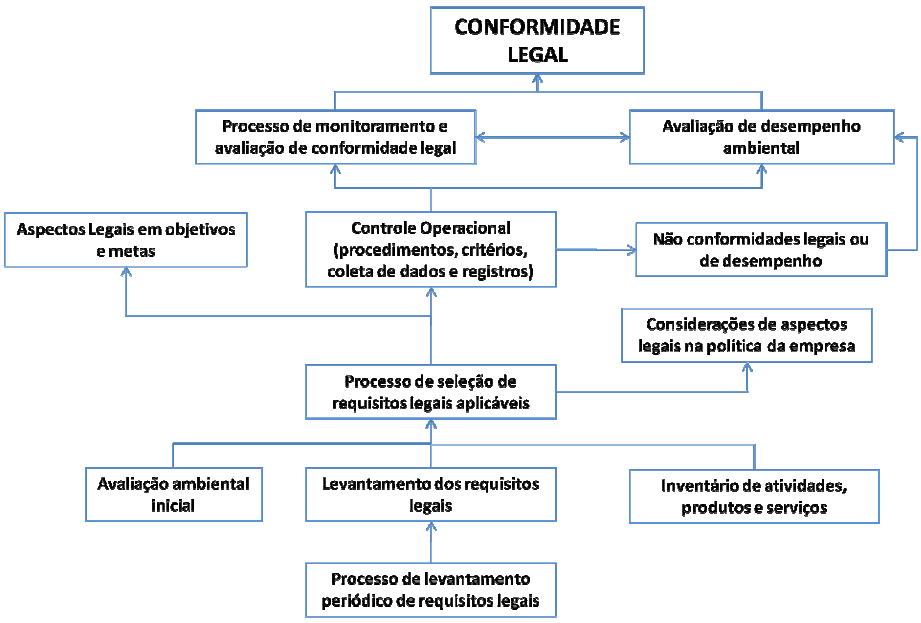


Figura 2 - Conformidade legal através da árvore de objetivos, segundo o método Zopp.

Etapa de análise de alternativas

As alternativas, neste caso, devem ser analisadas considerando-se a necessidade de se atender os requisitos referentes à conformidade legal inserida na ISO 14001. A alternativa a ser proposta, aqui, envolve a adoção dos seguintes procedimentos, que se farão necessários durante a implementação da ISO 14001.

Procedimento de atualização de requisitos legais existentes (Stat-a-Matrix, 1997)

> **4.3.2 Requisitos legais e outros**
> A organização deve estabelecer, implementar e manter procedimentos(s) para:
> a) identificar e ter acesso a requisitos legais aplicáveis e a outros requisitos subscritos pela organização, relacionados aos seus aspectos ambientais, e
> b) determinar como esses requisitos se aplicam aos aspectos ambientais.
> A organização deve assegurar que esses requisitos legais aplicáveis e outros requisitos subscritos pela organização sejam levados em consideração no estabelecimento, implementação manutenção de seu sistema de gestão ambiental. (ABNT, 2004)

Para atender a este requisito normativo, a empresa que implementa o SGA deve orientar seu Departamento Jurídico para estar atento e acompanhar a evolução dos requisitos legais ambientais. Como esta atividade na prática se torna inviável, pois estes departamentos trabalham com outras prioridades por eles consideradas mais relevantes para o negócio das empresas - como direito fiscal e tributário, trabalhista, direito civil contratual, por exemplo – este processo corre um sério risco de desatualização quanto aos requisitos legais existentes.

Uma alternativa que resolve este problema é a associação a um serviço de banco de dados de regulamentação ambiental, de atualização periódica (em alguns casos, até mesmo mensal) que mantenha a empresa ciente dos

 ISSN 1679-8902

requisitos legais existentes e vigentes no país. Esta opção tem sido adotada pela muitas empresas que realmente desejam ter um processo de atualização dos requisitos legais que seja ao mesmo tempo prático e eficiente. E, ao se utilizar esta ferramenta, é necessário avançar para a definição de um processo de identificação dos requisitos legais relacionados às atividades, produtos e serviços da empresa. Itens como licenciamento ambiental, cadastramento ambiental, parâmetros de emissões e de qualidade de poluentes atmosféricos e efluentes certamente serão aplicáveis. Também, regulamentação específica para setores industriais específicos também podem existir, como é o caso da limitação de chumbo para tintas imobiliárias e de uso em bens de consumo destinados a crianças (Brasil, 2008). Para tanto, o que se faz necessário nesta etapa é um processo de reuniões periódicas entre o "departamento ambiental" e as funções relevantes na empresa para análise conjunta dos requisitos ambientais aplicáveis, sem deixar de incluir áreas como Desenvolvimento de Produtos, Jurídico e Manufatura, entre outras.

Procedimento para avaliação de conformidade legal

> **4.5.2 Avaliação do atendimento a requisitos legais e outros**
> 4.5.2.1 De maneira coerente com o seu comprometimento de atendimento a requisitos, a organização deve estabelecer, implementar e manter procedimento(s) para avaliar periodicamente o atendimento aos requisitos legais aplicáveis.
> 4.5.2.2 A organização deve avaliar o atendimento a outros requisitos por ela subscritos. A organização pode combinar esta avaliação com a avaliação referida em 4.5.2.1 ou estabelecer um procedimento em separado.
> A organização deve manter registros dos resultados das avaliações periódicas. (ABNT, 2004*)*

Como se observa, a norma ISO 14001 também requer das empresas um processo para avaliação periódica de sua conformidade legal através da

verificação de registros gerados. Estes registros podem ser divididos em licenças ambientais, cadastros ambientais, correspondências trocadas com o órgão ambiental, entre outros, no campo de documentos legais que viabilizem as operações da empresa.

No campo de monitoramento, é necessário adotar indicadores ambientais definidos nos documentos legais, e os conseqüentes resultados e análises destes indicadores vai demonstrar ou não esta conformidade legal. A seleção destes indicadores é um processo que deve ser feito considerando-se as atividades da empresa, seus aspectos e impactos ambientais e requisitos legais aplicáveis. A facilidade operacional, representatividade e reprodutibilidade destes indicadores também deve ser considerada. Procedimentos operacionais que definam condições aceitáveis de desempenho ou faixas de tolerância são as ferramentas mais usuais para o acompanhamento destes indicadores.

Matrizes de planejamento de projetos

A matriz de planejamento de projetos para análise da questão legal deve sintetizar o planejamento, respondendo aos seguintes questionamentos:

- Por que se leva a cabo uma proposta (ou conceito de gestão) - Objetivo superior
- Que efeitos são esperados - Objetivo da proposta
- O que se deseja obter com a proposta - Resultados
- Como alcançar os resultados esperados - Atividades
- Que fatores externos devem ser considerados - Suposições
- Como verificar o sucesso do projeto - Indicadores objetivos
- Onde encontrar dados para avaliação do projeto - Fontes de verificação
- Quanto custa o projeto - Especificação de custos

 ISSN 1679-8902

A Tabela 1, resume um modelo de matriz de planejamento aplicada ao caso estudado.

Tabela 1 - Matriz de planejamento para conformidade legal em meio ambiente

Por que se busca a conformidade	• Parte do processo de certificação ambiental • Imagem da empresa • Retorno financeiro • Vantagem competitiva • Não ser considerada criminosa
Quais os efeitos esperados	Estar 100% em conformidade com a legislação ambiental aplicável e vigente
O que se deseja obter	Facilidade no trato das questões ambientais tanto internamente quando externamente junto a partes interessadas e órgãos ambientais
Como alcançar os resultados esperados	• Ferramentas de atualização e identificação da legislação • Uso de indicadores ambientais para monitoramento e avaliação periódica da conformidade através dos registros definidos
Que fatores externos devem ser considerados	• Fiscalização por parte do órgão ambiental responsável • Opiniões da comunidade quanto à responsabilidade ambiental da empresa • Surgimento de novos requisitos legais
Como verificar o sucesso neste processo	Uso de indicadores ambientais baseados nos requisitos legais aplicáveis e registros de ordem legal. Fiscalização ambiental serve também para esta verificação.
Onde encontrar dados para avaliação	Resultados de monitoramento comparado contra critérios definidos, como critérios operacionais ou critérios legais.
Quanto custa o processo	Os custos referentes ao processo de gestão são custos baixos, referentes a rotinas internas. No caso de não-conformidade legal que necessite investimento, os custos vão depender da complexidade da solução a ser adotada

CONSIDERAÇÕES FINAIS

A hipótese de que a metodologia Zopp de planejamento orientado a objetivos possa ser totalmente utilizada na gestão de requisitos legais aplicáveis em um ambiente de gestão ambiental baseado na ISO 14001 se comprova, considerando-se os seguintes fatores:

- O conceito de planeje-desenvolva-controle-atue (PDCA), que é o conceito de gestão da norma ISO 14001 também se encontra descrito na metodologia Zopp, ainda que com outras palavras. Há uma clara similaridade entre a estrutura da norma e tal metodologia.
- A metodologia Zopp, por ser notadamente uma metodologia de planejamento, pode ser adotada a partir da etapa de planejamento, onde se definem as premissas e processos administrativos de um SGA (Sistema de Gestão Ambiental). A partir de uma etapa de planejamento bem executada, a implementação do sistema de gestão se torna menos complexa. Portanto, observa-se uma vez mais a comunhão de objetivos.
- Entretanto, ao se analisar o contexto do Sistema de Gestão Ambiental como um todo, é possível concluir que a metodologia Zopp não deve ser aplicada ao processo Certificação Ambiental ou Implementação de SGA como apenas um macro-processo único, sob o risco de se transformar num mero processo administrativo e não em uma ferramenta metodológica efetiva. Deve, sim, ser aplicada para planejar a implementação dos conceitos e processos definidos na ISO 14001, como Conformidade Legal, abordado neste estudo, ou outros requisitos do sistema de gestão ambiental, tais como Atendimento a Emergências, Comunicação Ambiental, Controle Operacional, Auditorias Internas, Avaliação de Aspectos Ambientais, Estabelecimento de Objetivos e Metas, e outros processos. É importante observar que a norma ISO 14001 especifica os requisitos de um sistema de gestão, ou seja, fornece as diretrizes sobre “o que” deve ser feito, e versa muito pouco sobre “como” deve ser feito. A metodologia Zopp atua no sentido de preencher tal lacuna.

Um aspecto que parece óbvio mas que é extremamente relevante - principalmente para pequenas e médias empresas - é que a metodologia Zopp é pública e pode ser usada sem restrições. Existem diversas metodologias desenvolvidas para implementação de SGAs com vistas à certificação ambiental, todas elas desenvolvidas por empresas privadas de engenharia, consultoria, ou até mesmo por grandes conglomerados multinacionais. Neste caso, para se adotar alguma dessas metodologias deve-se comprá-la e, consequentemente, pagar por isso, com custos que podem inviabilizar a

implementação e certificação de um SGA, independente de outros investimentos que se façam necessários na empresa.

Portanto, este trabalho tem sua utilidade futura na medida em que fornece algumas diretrizes sobre como implementar os elementos do SGA - através da exemplificação pelo processo de Conformidade Legal, um dos mais importantes e essenciais - através de uma metodologia acessível, praticamente, a qualquer pessoa.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 14001:** Sistemas da gestão ambiental - Requisitos com orientações para uso. Rio de Janeiro, 2004.

BRASIL. **Lei Ordinária 11.762**, de 01 de agosto de 2008. Fixa o limite máximo de Chumbo permitido na fabricação de tintas imobiliárias e de uso infantil e escolar, vernizes e materiais similares e dá outras providencias.

DEUTSCHE GESELLSCHAFT FÜR TECHNISCHE ZUSAMMENARBEIT (GTZ). **Planificación de proyectos orientado a objetivos.** Eschborn, 1998. 35 p.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). **The ISO survey of certifications - 2008**. Genebra: ISO, 2009. 67 p.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO). **The ISO Survey of certifications 2010 – principal findings**. Genebra: ISO, 2011. 12 p.

RIGOLETTO, I. P. **Analogias entre a série ISO 14000, os instrumentos legais brasileiros de controle ambiental e o método Zopp.** Campinas: Faculdade de Engenharia Civil, Universidade Estadual de Campinas, 1999. 105 p. Dissertação (Mestrado).

STAT-A-MATRIX. **Interpreting and documenting an ISO 14001 environmental management system**. New York, 1997. 156 p.

SUSTENTABILIDADE - UMA NECESSIDADE, ÉTICA ECOLÓGICA - UM CAMINHO

Sustainability – an ecological ethics need - one way

RODRIGUES, Murilo Rogério
Faculdade de Tecnologia César Lattes

RESUMO: Os estudos ambientais vêm ganhando muita importância nos dias atuais, sobretudo devido os desastres e catástrofes naturais que parecem ter colocado a discussão deste tema no centro das atenções em todo o mundo. Sabe-se que o modelo antropocêntrico contribuiu muito para o atual estado de crise ecológica, a visão de que o homem é "o ser supremo do planeta" desencadeou comportamentos contrários à ideia de convivência harmônica entre a humanidade e natureza. Nesta linha, os seres da natureza não têm valor intrínseco e são propriedade e domínio do homem. As populações sempre se utilizaram da natureza como uma fonte de recursos, apossando-se deles de forma avassaladora e com a ideia errônea de que são infinitos. Um exemplo clássico são os chamados "países desenvolvidos": a maioria deles começou a explorar seus recursos naturais sem nenhum planejamento fazendo com que boa parte destes se esgotassem rapidamente. Com o passar do tempo, os resultados desta agressão apareceram, provocando consequências graves e mudando os rumos dos estudos sobre meio ambiente no mundo. Fica cada vez mais evidente a importância de se abordar assuntos com esta temática. É necessário criar políticas corretas de manejo ambiental visando proteger ao máximo a natureza. Isso deve ser discutido constantemente e não somente na hora em que os problemas causam as mutações do clima, dos ecossistemas e de todos os aspectos físicos do planeta. O modelo da ética ecológica vem ganhando muito espaço atualmente, uma vez que é debatida nas mais diversas esferas de pensamento. A ideia de ética ecológica aparece quando se supera a relação de domínio dos recursos naturais e o homem passa a agir como zelador da comunidade da vida, da qual faz parte como membro.

 ISSN 1679-8902

Palavras-chave: Ética ecológica, Preservação ambiental, Sustentabilidade, Desenvolvimento.

ABSTRACT: Environmental studies are gaining increased importance nowadays, especially because of the disasters, both natural and manmade, which have put discussions on this issue in the worldwide spotlight. We know that the anthropocentric model has contributed greatly to the current state of ecological crises; the view of man being 'the supreme being of the planet' has always triggered contrary behavior to the idea of harmonious co-existence between mankind and nature. According to this original viewpoint, the beings of nature have intrinsic value and are the property and domain of man. People have always misused nature as a source, taking for granted that these sources are endless. A classic example of this is the so-called 'developed countries'; most of them began to exploit their natural resources without any planning, resulting in a rapid decline of these natural resources. As time goes by, the results of this aggression have impacted directly upon us, causing serious consequences and changing the course of studies on the world environment. The importance of approaching issues relating to this topic is clear. Clear policies must be created in order to protect nature. These should be discussed constantly, and not only when we have drastic changes in the weather, ecosystem problems and the physical aspects of the planet. The model of ecological ethics has gained much publicity as it is currently being debated in many different spheres of thought. The word "ethics" originates from the Greek word 'ethos', which means "way of acting and being". Ecological ethics is the wisdom of putting the law in the service of life; it is creating a membership of co-existence and self-care, both with each other and with nature, land, water and all living things, from an awareness of sustainable use and interdependence. The idea of ecological ethics appears when we get over the relationship of controlling the natural resources and start acting as caretakers of the community of life to which we belong as members.

Keywords: Ecological ethics, preservation environmentalist, sustainability, development.

Introdução

O estudo e a preocupação com o meio ambiente e a natureza vem tomando enorme proporção nas últimas décadas no Brasil e no mundo. Os desastres e as catástrofes ambientais parecem ter colocado o tema no centro das atenções da mídia nacional e internacional.

Poluição, aquecimento global, ilhas de calor e chuvas ácidas estão em alta quando se fala de Geografia em jornais, revistas e nas escolas. A humanidade costuma associar estes fenômenos ao “fim dos tempos”, extinção da vida na Terra etc., fazendo infelizmente com que muitas informações sejam colocadas de maneira incorreta pela mídia e muitos acontecimentos sejam desvirtuados de sua verdadeira realidade. É muito comum deparar-se com informações erradas sobre estes temas também nos meios de comunicação em massa. Essas informações têm como consequência a assimilação e a disseminação de ideias abstratas sobre a natureza e o planeta provocando transtornos e causando pânico na humanidade.

Sabe-se que o modelo antropocêntrico contribuiu muito para o atual estado de crise ecológica, a visão de que o homem é “o ser supremo do planeta” sempre desencadeou comportamentos contrários a idéia de convivência harmônica entre homem e natureza. Na visão antropocêntrica, os seres da natureza não têm valor intrínseco e são propriedade e domínio do homem.

Algumas religiões derivadas do monoteísmo também contribuíram para disseminar esta ideia de centralidade do ser humano. Elas têm como ideia principal a separação entre o plano da natureza e o da sociedade, o que evidencia claramente a perspectiva antagônica entre ambos. Porém, vale ressaltar que algumas religiões politeístas possuem uma orientação mística que aponta para a unidade entre natureza e sociedade como, por exemplo, o hinduismo.

 ISSN 1679-8902

O sistema capitalista

Atualmente, o sistema capitalista domina as sociedades, o lucro e o acúmulo de capital assumem uma importância inigualável, valores morais e éticos são invertidos, lógicas são questionadas e a racionalidade humana passa a dar lugar a práticas insanas. Os sentimentos de reciprocidade e convivência já não estão mais presentes com tanta frequência, as relações sociais obedecem a um padrão hegemônico e homogêneo, de modo que uma pequena parcela da população domina o restante impondo seus valores e suas vontades. A vida tem seu valor diminuído como nunca e os agentes hegemônicos decidem o destino dos cidadãos assim como o do planeta Terra.

A busca de alguns pela riqueza e por um melhor status provoca um desequilíbrio social. O lucro, o prestígio e o poder substituem valores mais importantes como o sentimento de enraizamento, o equilíbrio e a solidariedade. Tudo passa a ter um valor de acordo com sua importância dentro desse sistema. O próprio ser humano é visto como recurso e acaba ficando refém das "novidades" que lhes são impostas por uma voracidade técnica inerente a esta racionalidade cruel e perversa.

Não bastasse isso, os cidadãos que concentram o capital e, consequentemente o poder, querem possuir além dos valores materiais individuais, os valores coletivos e de bem comum dentre os quais a natureza. Esses valores vêm na forma de recursos naturais e tem como finalidade suprir a base material da espécie humana.

A humanidade sempre se utilizou da natureza no seu cotidiano, sempre a observou como uma fonte de recursos, apossando-se deles de forma avassaladora e com a ideia errônea de que são infinitos. Um exemplo clássico são os chamados "países desenvolvidos": a maioria deles começou a explorar seus recursos naturais sem nenhum planejamento, fazendo com que boa parte destes se esgotassem rapidamente. A solução então foi apossar-se também dos recursos naturais de outros países, no caso suas colônias, levando a destruição ambiental muito além dos limites de onde ela começou.

Com o passar do tempo, os resultados dessa agressão foram surgindo e atingindo diretamente a humanidade, provocando consequências graves e mudando os rumos dos estudos sobre meio ambiente no mundo. Fica cada vez mais evidente a importância de se abordar assuntos com esta temática; é de extrema importância criar políticas corretas de manejo ambiental, visando proteger ao máximo a natureza. Isso deve ser discutido constantemente e não somente na hora dos problemas que nos causam as mutações do clima, dos ecossistemas e de todos os aspectos físicos do planeta.

Colapso ecológico

A preocupação com um colapso ecológico é recente. Somente há algumas décadas surgiram estudos, encontros e conferências nos quais a principal preocupação era abordar a preservação ambiental, assim como discutir formas de explorar os recursos naturais de maneira sustentável.

Em 1987, a comissão de meio ambiente da ONU divulga no relatório intitulado “Nosso futuro comum” o termo “desenvolvimento sustentável”, que significa evoluir sem colocar em risco as gerações futuras. A junção das duas palavras – “desenvolvimento” e “sustentável” – tornou-se senso comum, consenso para a formulação de políticas para utilizar as riquezas naturais (os recursos) de modo a não destruí-las e, ao mesmo tempo, continuar com o desenvolvimento, promover a diminuição da pobreza. Tornou-se unânime a preocupação com a biosfera, o “bem comum”. Criou um ideário de que todos são igualmente responsáveis pela depredação das riquezas e pela preservação para as gerações futuras. Transformou a questão ambiental em agenda política (Rodrigues, 2005).

É necessário respeitar a capacidade de suporte dos geossistemas e promover atividades que, ao mesmo tempo, gerem renda e não degradem a natureza e o meio ambiente. Para tanto, é imprescindível ter em mente um futuro comum, ter consciência da importância da preservação do ambiente

natural para as próximas gerações. A sustentabilidade não é só uma alternativa, mas também uma necessidade.

O maior problema está em contrariar a lógica capitalista e seus agentes principais, uma vez que estes têm como ideologia o individualismo e a obtenção de lucros a qualquer custo. Exemplos de como este sistema é impositivo e desigual não faltam, sobretudo nos países subdesenvolvidos, onde o poder dele é praticamente inatingível. O estado pouco faz, pois o capital é mais forte, e, aliado á mídia e a debilidade cultural de parte da população, acaba por reger sozinho e soberano toda uma sociedade, impondo seus interesses e ofuscando minorias e modos alternativos. O capitalismo é homogêneo ao máximo, ele destrói as particularidades e impõe a vontade dos dominantes. Culturas milenares são ameaçadas, uma vez que muitos povos estão modificando seus costumes, enfim, a diversidade cultural está deixando de existir. Vale ressaltar que, apesar dessa situação, existem povos tentando resistir a este modelo em diversas partes do mundo, mesmo tendo pouco apoio por parte do governo ou da sociedade em geral.

Os seringueiros e os quilombolas

No Brasil. um exemplo típico é o caso dos seringueiros do Estado do Acre. Durante os anos 70, o governo militar iniciou um processo de ocupação da Amazônia baseado em empresas agropecuárias e projetos de colonização. Esse processo levou a uma prática de depredação dos recursos naturais da Amazônia e à expulsão de índios e seringueiros de seus territórios. No caso do Acre, a onda de especulação fundiária levou à venda dos antigos seringais a grupos empresariais e fazendeiros do centro-sul do país, interessados principalmente na derrubada da floresta para a implantação de grandes obras e o cultivo da pastagem para prática da pecuária extensiva.

Praticantes do extrativismo, os seringueiros sempre dependeram da floresta para sobreviver e manter suas famílias. Eles ocupavam aquelas terras muito antes da chegada dos grandes empresários e fazendeiros à região e, por

isso, lutavam pela criação de reservas extrativistas que lhes garantissem o direito de retirar da floresta o seu sustento de uma forma alternativa.

A reserva extrativista é a reforma agrária dos seringueiros. É o reconhecimento de áreas de floresta, ocupadas tradicionalmente por eles, como áreas de domínio da União, com usufruto exclusivo dos povos da floresta, organizados em cooperativas ou associações. Nas reservas não há títulos individuais de propriedade de terra, são respeitadas a cultura e as formas tradicionais de organização e de trabalho dos seringueiros, que continuarão a realizar a extração de produtos de valor comercial como a borracha, a castanha e muitos outros, juntamente com pequenos roçados de subsistência, em harmonia com a regeneração da mata. As reservas extrativistas não são áreas inviáveis economicamente: garantida a floresta, os seringueiros organizados aumentarão a produtividade, introduzindo inovações tecnológicas adequadas. Além disso, são também uma forma de preservação da natureza pelos que dela dependem, e uma alternativa econômica para a Amazônia (*Revista Chico Mendes, CNS 2005)*. O extrativismo é uma forma de sustentabilidade que ajuda a preservar a natureza e a levar renda a muitas famílias em diversos lugares, promovendo assim uma estreita relação de interdependência entre eles.

Contudo, apesar de todo o esforço da população local para manter seu modo de vida e a preservação ambiental, mais uma vez os agentes principais do sistema capitalista mostraram seu poder. Para eles, o extrativismo era uma ameaça aos seus interesses de obtenção e acumulação de capital, já que precisariam desmatar a floresta para iniciar a construção das grandes obras e as atividades agropecuárias. Era um conflito entre uma maioria com pouco poder econômico e político contra uma minoria abastada e poderosa politicamente, uma disputa entre subsistência X lucro.

A partir disso, esses agentes capitalistas começaram a agir de maneira agressiva, perseguindo, torturando e eliminando seringueiros e líderes sindicais tais como: Wilson de Souza Pinheiro, presidente do Sindicato dos Trabalhadores Rurais de Brasiléia, em 1980; o dirigente do Sindicato de Xapuri,

Ivair Higino de Almeida e, o mais célebre deles, Chico Mendes, morto em 1988, em Xapuri-AC, a mando dos grandes fazendeiros da região.

Mesmo sendo clara a participação dessa elite hegemônica nas perseguições e assassinatos contra extrativistas, sindicalistas e ambientalistas, pouca coisa foi feita para puni-los. Somente depois da morte de Chico Mendes e sobre fortes pressões internacionais, inclusive da ONU, os órgãos públicos municipais, estaduais e federais resolveram agir, prendendo alguns fazendeiros da região. Tudo isso mostra a fraqueza do poder público diante destes agentes globalizadores - muitas vezes havendo inclusive cumplicidade entre ambos. Infelizmente, as populações locais, com poucos recursos, acabam ficando a mercê da própria sorte assim como a natureza, por conseqüência, o sistema se impõe cada vez mais sobre os menos favorecidos, destruindo tudo e todos os que se opõem a ele.

Outro caso que pode ser mencionado é o caso dos remanescentes de quilombos, situados no vale do Ribeira –SP. Na cidade de Eldorado-SP situam-se diversas vilas habitadas por pessoas descendentes de escravos, que no século passado fugiam e constituíam comunidades, onde o lema principal era a ajuda mútua e o respeito. Estas comunidades apresentam, ainda hoje, uma organização exemplar, dando ênfase, sobretudo, à preservação da cultura herdada dos seus ancestrais. Com estrutura de trabalho familiar e comunitária, eles produzem quase 100% dos alimentos que consomem, de forma sustentável; a natureza é preservada ao máximo, pois os habitantes locais têm um sentimento de respeito e interdependência com ela. Apesar de não possuírem um bom nível escolar, são extremamente apegados a regras e tradições seculares, fazendo questão de cultivá-las e preservá-las a qualquer custo.

É visível o apego desse povo com a terra que ocupam e cultivam há tanto tempo; é mais do que clara a vontade de permanecerem ali para sempre. Todavia, toda esta diversidade e riqueza cultural estão sendo ameaçadas. O bom exemplo dado por eles, evidenciados pela preservação de suas tradições e pela relação de respeito com a natureza e o meio ambiente, não é seguido por muitos, principalmente por grandes proprietários de terras e empresários

locais. A construção de barragens ao longo do rio Ribeira do Iguape para fins de geração de energia para empresas instaladas na região esta ameaçando todo este patrimônio histórico-cultural brasileiro. A obra, além de gerar impactos ambientais gravíssimos, ainda provocaria a inundação das terras ocupadas pelos quilombolas, o que obrigaria a transferência destes para outras regiões.

Mudança de paradigma

Não se pode pensar o meio somente por uma visão econômica; o mesmo deve ser pensado também no seu aspecto cultural. A ideia de que tudo tem um valor monetário é falha, pois existem coisas que não podem ser quantificadas. Pensando assim, a comunidade dos quilombolas criou um movimento denominado MOAB (Movimento dos Atingidos por Barragem). Este movimento é atuante não só na região do Vale do Ribeira, como também na capital São Paulo, onde promovem protestos contra a aprovação do projeto de construção de barragens pelo poder público estadual.

A organização está encontrando muitas dificuldades, afinal são seus interesses contra o interesse dos agentes principais do sistema capitalista. Por mais que seja evidente a importância cultural deste povo e a quantidade de pessoas que batalham por este ideal, a luta é desigual e, na maioria dos casos, o principal beneficiado é sempre a elite hegemônica capitalista.

Dentro deste quadro, o desafio maior é alcançar um novo estágio de consciência repensando os efeitos do atual sistema econômico, tecnológico e cultural sobre as populações locais, os excluídos e a natureza. Este sistema tende a privilegiar o modo exploratório, a produção em larga escala e o consumismo exagerado em detrimento aos modos de produção e culturas alternativas.

É evidente que a atual crise ambiental é também resultado da crise desse sistema baseado sempre na política do descartável e do desperdício. Deve-se discutir os princípios éticos e orientações para a gestão econômica,

social e para a sustentabilidade, fazendo com que a humanidade visualize a importância da preservação ambiental para as gerações futuras.

Surge então um modelo importante, a ética ecológica, que vem ganhando espaço no mundo todo, sendo debatida nas mais diversas esferas de pensamento. É necessário discutir formas de contornar os problemas gerados pelo sistema capitalista sobre a natureza. Isso se dá através da elaboração de conceitos, discussão dos problemas que atingem a humanidade nesta questão e elaboração de medidas mitigadoras que possam ser aplicadas na prática, não ficando apenas na discussão.

Ética ecológica

Ética vem do termo grego *ethos* e significa modo de agir e de ser. É importante porque nossas ações não ocorrem por acaso, arbitrariamente, de acordo com algum impulso de momento. Elas obedecem a princípios e critérios que servem como uma direção a ser seguida ou uma indicação segura de quando se precisa de orientação para atingir algum objetivo. A ética é exatamente a sabedoria de colocar a lei a serviço da vida. É como criar uma relação de convivência e cuidado consigo mesmo, uns com os outros e com a natureza, a terra, a água e todo ser vivo, a partir de uma consciência de interdependência.

Existe uma ética ecológica quando se supera a relação de dono e proprietário da terra, dos animais e das plantas, para a relação de que o homem é gerente e zelador da comunidade da vida a qual pertence como membro. É um padrão de comportamento que flui através da percepção de que todos pertencem à comunidade global da biosfera.

A ética ecológica critica o antropocentrismo, não se pode colocar o homem acima e fora da natureza, de modo a nada possuir sentido sem a presença humana. É necessário fixar a idéia de interdependência entre a humanidade, os demais seres vivos e a natureza.

Na XIII reunião do foro de ministros do meio ambiente da América Latina e Caribe, em Bogotá 2002, foi aprovado um documento, dentro do simpósio sobre ética ambiental e desenvolvimento sustentável, que trata exatamente da ideia de uma ética para a sustentabilidade. O documento é dividido em tópicos que tratam de vários assuntos relacionados à ética. São eles:

Ética de uma produção para a vida – Aponta que a justiça social é a principal condição para a Sustentabilidade. A degradação ecológica está estritamente relacionada com a injustiça social. É necessário também respeitar a capacidade de suporte da natureza, diminuindo a intervenção tecnológica na ordem natural ecológica.

Ética do conhecimento e diálogo dos saberes – É preciso orientar os esforços científicos para a solução dos problemas ambientais, a ciência é instrumento de conhecimento e não pode ser submetida somente a ideais econômicos hegemônicos, devendo ser usada na busca de interesses coletivos.

Ética da cidadania global, o espaço público e os movimentos sociais - O princípio da democracia tem que ser resgatado, pois o processo de globalização tem como característica a desigualdade entre os homens, subordinando-os a processos políticos e econômicos autoritários e impositivos.

Ética da governabilidade global e a democracia participativa – A ética sustentável é fundamentada em princípios de respeito, pluralismo político e diversidade cultural. Ela questiona toda e qualquer forma de dominação, sendo necessário então repensar as relações sociais, os modos de produção e consumo vigentes.

Ética dos direito, justiça e democracia - Os direitos devem ser garantidos a todos os cidadãos, independente de classe social, cor ou religião. A igualdade deve ser colocada como meta principal a ser alcançada.

Ética dos bens de consumo e do bem de consumo – Os bens comuns são bens coletivos, devem ser usufruídos de forma sustentável por todos e não somente pelos mais poderosos. A mercantilização da natureza, a apropriação da biodiversidade e as privatizações não devem ser praticadas.

 ISSN 1679-8902

Ética da diversidade cultural e de uma política da diferença – O conceito de bem estar deve ser referir sempre a um grupo nunca somente a um indivíduo. Deve-se incluir corretamente as visões dos diferentes grupos sociais e populações e não somente a do grupo dominante.

Ética da paz e do diálogo para a resolução de conflitos – Quando grupos com interesses antagônicos se depararem, é preciso superar sempre as dicotomias para se chegar a uma decisão de bem comum; um acordo com princípios de igualdade é o mais interessante neste caso.

Ética do ser e o tempo da sustentabilidade – Saber conhecer o tempo é muito importante para se entender o ciclo permanente da vida; a perpetuação desta tem que ser vista sempre como valor fundamental do ser vivo.

A ideia da elaboração do manifesto foi produzi-lo em comum, para se tornar um bem comum, baseado principalmente nos sentimentos de igualdade, solidariedade e na construção de sociedades sustentáveis.

Maria Teresa La Valle tece considerações sobre os temas desenvolvimento sustentável e ética ecológica no seu artigo intitulado “Quem representará as gerações futuras?” e que está publicado na obra “Etica ecologica. Propuestas para una reorientación.” (Riechmann, 2004). Para ela, ao contrário do que se esperava, a situação ambiental piorou muito desde a Rio 92, a poluição aumentou muito, espécies entraram em extinção e muito pouco foi feito pelos órgãos públicos nacionais para minimizar estes problemas. A autora destaca que na hora de enfocar o tema gerações futuras e preservação do meio ambiente pode-se indicar duas linhas de análise:

A primeira sustenta a ideia de que existe somente uma obrigação ética quando há uma relação recíproca de indivíduos que se encontram em situações parecidas de poder, e que só se tem obrigações morais com aqueles com os quais se tem laços especiais. Deste modo, as obrigações se limitam hoje com pessoas as quais se tem laços de afeto, sangue ou comunitários.

A segunda considera que, em vista do risco implícito que a humanidade atual tem para afetar a natureza, é necessário elaborar pautas sobre a ética que contribuam para garantir a sobrevivência da humanidade.

Ambas as linhas coincidem na necessidade de preocupar-se com as gerações futuras, mesmo que em graus diferentes, mas não enfocam nem apontam as ferramentas necessárias para tal. Efetivamente, no caso de problemas ambientais, é fácil encontrar exemplos de ações atuais que resultam em vantagens para as gerações futuras, mas a idéia principal seria conceber uma colaboração ao longo de muitas gerações e não somente as mais próximas, dentro de um esquema comum de justiça. Apesar de atualmente se observar muitas injustiças, não se pode pensar que as pessoas têm somente um interesse egoísta ou que só pensam no seu bem-estar. Esses não são os únicos motores das ações humanas, as pessoas se movem impulsionadas por uma pluralidade de motivações, elas levam em conta as considerações éticas que nos fazem ampliar o conceito de bem-estar mais longe do que sua própria satisfação ou felicidade.

Ainda para a autora, o uso sustentável dos recursos naturais pode ser prejudicado por posturas como as que foram mencionadas; a democracia se vê questionada. A degradação ambiental deixa vulnerável a qualidade de vida das gerações atuais e também das futuras. Isso em vários sentidos afeta as possibilidades coletivas de sobrevivência, os projetos individuais de levar uma vida longa e saudável, a possibilidade de afirmar nossa interdependência com outras espécies e, o mais importante, as gerações futuras de seres humanos.

A autora ressalta ainda que os recursos naturais são bens públicos. Quem tem posse desses recursos exerce dominação sobre os demais. É a liberdade que está em jogo e, por isso, essa deveria ser uma questão de estado. Os governos deveriam ser os primeiros a se preocupar com a preservação ambiental e a apoiar a criação de instituições que inibissem a dominação e exploração desordenada e indiscriminada dos recursos naturais por alguns indivíduos, diminuindo, por consequência, a degradação ambiental.

 ISSN 1679-8902

Castellanos (2004) coloca que a ideia de comunidade e a relação comunidade-natureza está sendo destruída pelo mercado e pela ganância. Na visão dele a criação de leis que orientariam a conduta humana com a finalidade de evitar o esgotamento dos recursos naturais por meio da exploração insana seria uma boa opção. As leis gerariam resultados práticos, pois as pessoas sentem o dever de cumprir ordens, elas temem ser julgadas por desobedecer algo que foi pré-estabelecido, independente de concordar ou não com elas. Em contrapartida, uma ética poderia ser trabalhada em pessoas que se supõe ter valores intrínsecos. Esta ética tem que estar enraizada em sentimentos. Apesar de ser a melhor forma de pensar a natureza, é muito difícil de ser implementada na sociedade atual, onde a palavra "ética" anda meio esquecida. A ética só funciona com aqueles que possuem dignidade e a compaixão como valores muito importantes. O indivíduo compassivo vive dolorosamente o sofrimento dos mais fracos, ele também o sente, seu sentido de justiça gira em torno do princípio de igualdade e o mesmo pode se pensar em relação à natureza, pois esta passa a ser vista como "seu semelhante". Porém, ele afirma que para os casos onde os agentes principais não possuem esses valores intrínsecos, para quem a moral não tem valor, é necessário a implantação das leis.

A pertinência de que a ética seja aplicável e realmente possa ser atuante obriga ao reconhecimento de que ela está estritamente relacionada nos movimentos sociais ascendentes, em uma nova cultura, como, por exemplo, a que se manifesta no fórum social mundial de Porto Alegre, onde precisamente confluem, sem choques, numerosas correntes sociais que, apesar de terem metas diversas, têm como principal característica o sentido de justiça e de piedade juntamente com a vontade de arriscar-se por eles.

O autor destaca ainda que estes novos movimentos se organizam de forma muito diferente. Parece que estão traçando as coordenadas de uma nova ética, de modo que os princípios e valores ambientais se confundem com os referentes a outros âmbitos da atividade humana.

Considerações finais

É fundamental pensar constantemente sobre como esta reorientação deve ser aplicada na prática. A noção de sustentabilidade precisa estar clara e ela só poderá acontecer se for implementada simultaneamente em diversas áreas.

É certo que a importância da preservação dos elementos naturais para a construção de um meio ambiente saudável é imprescindível. Para tanto, deve-se lançar mão de técnicas, métodos e ideologias que possibilitem chegar a este estado de harmonia entre a humanidade e o planeta. A ética ecológica é, sem dúvida, um dos caminhos mais rápidos e eficientes para atingir este objetivo. Ela deve ser o suporte basilar desse projeto.

Os seres humanos devem compreender que a vida não surgiu no planeta pela competição, mas através da cooperação, de parcerias e formação de redes interdependentes. Os sentimentos de disputa e de individualismo têm que ser substituídos pelos sentimentos de cooperatividade e coletividade. A continuidade da vida, a coexistência pacífica entre as espécies e o bem estar coletivo são mais importantes do que o poder e a acumulação de capital a qualquer custo. Oxalá que isso ocorra em breve, enquanto a situação é reversível, e não somente no momento em que o homem perceber que não pode nem comer, nem beber nem respirar dinheiro.

Referências

CASTELLANOS, E. M. Una etica ambiental igualitarista y compasiva In: *Jorge Riechmann (coord)*. *Ética ecologica: propuestas para una reorientación*. Nordan Comunidad, Montevideo, 2004, pp.53-58.

LA VALLE, M. T. Quién representa a las generaciones futuras? In: Jorge Riechmann (coord). Etica Ecologica: Propuestas para una reorientación. Nordan Comunidade, Montevideo, 2004, pp. 77-82.

REVISTA CHICO MENDES, CNS, Xapuri, 2005. p. 12.

RODRIGUES, A. M. Problemática ambiental: Agenda política, espaço, território e classes sociais. Boletim Paulista de Geografia, nº 83, São Paulo, Dez. 2005.

UNA ÉTICA PARA LA SUSTENTABILIDAD. MANIFESTO POR LA VIDA. Bogotá, 2002.

PROPOSTA DE UM CONJUNTO DE BOAS PRÁTICAS PARA A UTILIZAÇÃO E CONSTRUÇÃO DE SERVIÇOS WEB BASEADOS EM REST

Proposal for a set of good practice for the use and construction of Web service Rest based

ANDRADE, Guilherme Afonso
Faculdade Politécnica de Campinas

SILVA, Neimar Gustavo Lopes da
Faculdade Politécnica de Campinas

DIAS, Mateus Pereira Dias
Faculdade Politécnica de Campinas

Resumo*:* A fim de facilitar a implementação dos serviços web e utilizar ao máximo os recursos consagrados no HTTP, tem sido sugerido como alternativa o estilo arquitetural Representational State Transfer (REST). Neste artigo, serão apresentados os conceitos necessários para o desenvolvimento de uma arquitetura baseada no estilo REST e um conjunto de boas práticas para tornar a implementação dos serviços bem sucedida.

Palavras-chave*:* REST, Serviços Web, SOAP.

Abstract*:* In order to facilitate the implementation of web services and use the maximum of devoted resources in HTTP, it's been suggested as alternative the architectural style Representation State Transfer (REST). In this article, will be presented the necessary concepts to develop an architecture based on REST style and a set of good practices to turn services implementation successful.

Keywords*:* REST, Web Services, SOAP.

1. Introdução

A busca de soluções para integração de sistemas e comunicação entre diferentes aplicações incentivou a popularização dos serviços web, que são

definidos como sistemas de software com o objetivo de prover um serviço de interoperabilidade entre sistemas distintos, que funcionam, ou não, em mesma rede. [1].

A comunicação com os serviços web é possibilitada por meio da Internet em um estilo cliente/servidor e, sua utilização, objetiva a troca de informações entre aplicações. Este conceito pode ser chamado de web programável que é muito parecida com os sites convencionais que retornam páginas amigáveis e atraentes, com conteúdos que servem para o consumo humano. A web programável tem como principal objetivo disponibilizar representações para uso programático, geralmente por outras aplicações. [2].

Para a disseminação e a adoção dos serviços web surgiram padrões para prover integração entre diferentes aplicativos de software em diversas plataformas [3]. Esses modelos fornecem definições comuns de um serviço web, destacando-se, entre os principais: SOAP[1], WSDL[2], UDDI[3].

Apesar dos muitos padrões em torno dos serviços web, a maior parte deles negligenciou os conceitos implementados no protocolo atual da web (HTTP[4]). Este fato torna difícil a implementação dos serviços web.

Uma alternativa para implementação de serviços web, utilizando ao máximo os recursos que consagraram o HTTP, é o estilo arquitetural Representational State Transfer (REST), sugerido por Roy T. Fielding em sua pesquisa de doutorado [4], onde é apresentado um modelo para o desenvolvimento de sistemas de hipermídia distribuídos

Pretende-se demonstrar neste trabalho, que a construção e a utilização de serviços web baseados em REST é mais eficaz, e seu entendimento, é claro, diferenciado de outros padrões, como o SOAP que é de difícil compreensão e uso.

[1] Simple Object Access Protocol
[2] Web Services Definition Language

2. Objetivo

O objetivo deste trabalho é apresentar um conjunto de boas práticas para a utilização do estilo de arquitetura REST, visando à utilização fácil e eficaz da arquitetura para a implementação e utilização de serviços web.

3. Procedimentos metodológicos

Para a construção de um conjunto de boas práticas no uso de REST, foram realizadas as seguintes etapas:

- Levantamento teórico sobre o estilo de arquitetura REST;
- Análise do funcionamento de serviços web implementados utilizando tal tecnologia e seus resultados;
- Elaboração de um conjunto de boas práticas, baseado nos resultados obtidos na etapa anterior.

4. Justificativa

Existem vários artigos que explicam os conceitos e as definições de REST, segundo o modelo apresentado por Roy Fielding em [4]. Contudo, o pouco material que é encontrado contendo implementações de serviços baseado no modelo, não apresenta um conjunto de boas práticas, como é proposto por este trabalho.

5. O estilo arquitetural REST

O estilo arquitetural REST tem como princípio utilizar os próprios recursos existentes no protocolo HTTP como meio para prover serviços

[3] Universal Description, Discovery and Integration
[4] Hypertext Transfer Protocol

distribuídos. Tem como base as estruturas definidas no HTTP Object Model [8] e possui uma série de restrições que levam um sistema a possuir determinadas propriedades que não violam os princípios da WEB.

Uma afirmação sobre como o modelo REST se comporta com a WEB pode ser encontrada em [5] página 116: *"The name "Representational State Transfer" is intended to evoke an image of how a well-designed Web application behaves: a network of Web pages forms a virtual state machine, allowing a user to progress through the application by selecting a link or submitting a short data-entry form, with each action resulting in a transition to the next state of the application by transferring a representation of that state to the user."*. Em resumo, REST representa um modelo de como a Web deveria funcionar.

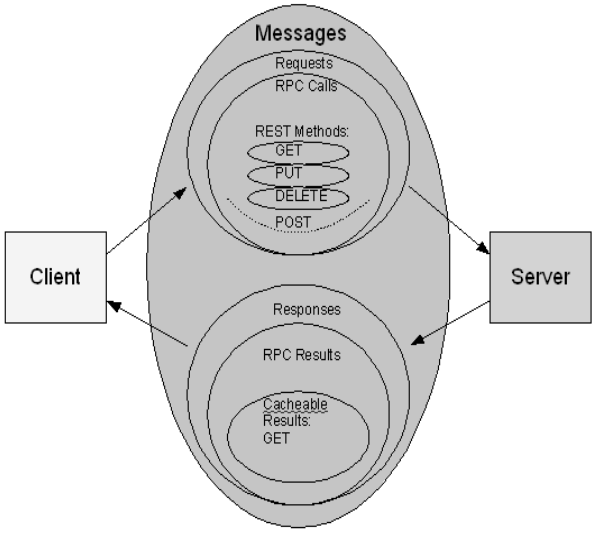


Figura 1 - Ciclo de comunicação REST [13]

A seguir serão apresentados os conceitos e restrições que uma arquitetura de serviços REST deverá atender:

a) Recursos

O recurso é um importante conceito dentro do modelo, caracterizando-se como uma abstração de um elemento de informação dentro do sistema, que pode representar qualquer objeto que possa ser nomeado, seja físico, seja

abstrato. Um recurso é um mapeamento conceitual para um conjunto de entidades [4]. Alguns exemplos de possíveis recursos são:

- Um documento;
- Uma imagem;
- A relação entre dois recursos.

Todo recurso deve possuir um nome e um endereço, representado por uma URI[5], que é uma cadeia de caracteres usada para identificar, de modo simples, todo item disponível na web [6]. Por pertencer a um namespace global, toda URI possui uma identificação única e universal [7].

É recomendável que toda URI possua uma estrutura previsível e descritiva do recurso que está representado. Não é uma regra absoluta, mas já é entendida como uma boa prática no desenvolvimento de aplicativos web, que facilita a sua leitura e compreensão por usuários comuns. Alguns exemplos de URI:

http://www.policamp.edu.br/alunos/<ra>

http://www.policamp.edu.br/materias/<id>/alunos

Todo recurso deve possuir um endereço intuitivo na obtenção dos dados de um recurso. Em outras palavras, o endereço deve significar o que o serviço faz.

b) Falta de Estado

Toda iteração HTTP deve ocorrer em um nível de isolamento completo, ou seja, quando é realizada uma requisição, esta deve possuir todas as informações necessárias para o processamento no servidor e este, por sua vez, não pode depender de informações de solicitações anteriores. Se alguma informação do estado anterior for importante para a nova solicitação, o cliente deve mencionar na URI esses dados a serem enviados para o servidor.

[5] Uniform Resource Identifier – entende-se como um endereço web

Por exemplo, ao realizar a solicitação de uma lista de objetos, esta não deve retornar todo seu conteúdo e sim, os cinco primeiros registros para facilitar a exibição. Na primeira requisição, é necessário realizar uma chamada como: http://www.policamp.edu.br/materias/<id>/arquivos. Para consultar os próximos registros, o cliente deve informar ao servidor o estado atual da aplicação, realizando uma solicitação para a URI: http://www.policamp.edu.br/materias/123/arquivos?start=5. Ou seja, o cliente "avisa" o seu estado ao servidor, informando que é necessário listar as representações apenas a partir do sexto registro. É uma solicitação sem estado, pois cada uma é desconectada das outras. O cliente pode fazer solicitações para páginas distintas, mesmo não seguindo uma ordem, que o servidor não se importará.

Para construir o estado no lado do servidor, poderiam ser utilizadas técnicas como sessões e cookies, porém a característica da arquitetura obriga que o estado do recurso seja mantido na máquina cliente e transmitido para o servidor em toda solicitação [2].

c) Representações

A representação é o formato específico enviado pelo serviço, cuja finalidade é transmitir a ideia do recurso, que pode conter qualquer informação útil sobre seu estado, sejam dados reais, sejam metadados.

d) Link e encadeamento

A utilização de hipermídia como mecanismo de aplicação do estado [4] é a restrição mais obscura e discutida no estilo REST [9]. Muitas vezes sua utilização é negligenciada e não implementada.

Algumas representações possuem dados que são extraídos e, depois, descartados. Mas muitos dos recursos possuem representações com documentos de hipermídia, isto é, não possuem apenas dados, mas links com outros recursos.

Com isso, o estado atual da aplicação não é armazenado no servidor como um estado do recurso, mas controlado pelo cliente como estado da aplicação. O estado é apenas dirigido pelo servidor, ao informar ao cliente os caminhos dos links, fornecendo à hipermídia.

Esta restrição ajuda na evolução independente dos sistemas, pois quando é alterada a estrutura de navegação do servidor, este deve fornecer as novas URIs em seus links, e o cliente continuará operando sem sofrer adaptações.

e) Interface Uniforme

Todos os métodos necessários para a comunicação com o servidor estão presentes na interface uniforme do HTTP e devem ser usados para lhe enviar o estado do recurso. Os métodos utilizados são:

- HTTP HEAD
- HTTP OPTIONS
- HTTP GET
- HTTP DELETE
- HTTP PUT
- HTTP POST

* HTTP HEAD

O método HEAD é usado para obter os detalhes dos metadados do recurso, sem realizar o download dos dados da entidade. Ele é útil para verificar a existência do recurso ou descobrir detalhes das informações do escopo do serviço.

* HTTP OPTIONS

O método OPTIONS permite descobrir as operações que são permitidas para um determinado recurso solicitado, transmitidas pelo servidor por meio de uma resposta com um cabeçalho de permissões: *Allow*. Por exemplo:

 ISSN 1679-8902

Allow: GET, HEAD, PUT, DELETE

* HTTP GET

O método GET permite recuperar as informações de um recurso, retornando este os metadados no cabeçalho de resposta e a representação no corpo da entidade.

* HTTP DELETE

O método DELETE permite apagar as representações de um recurso, enviando uma solicitação para sua URI. Esta operação deve retornar o status HTTP do resultado da ação.

* HTTP PUT

O método PUT permite realizar a modificação ou a criação de um recurso. O corpo da entidade de solicitação deve conter os dados que serão enviados para o servidor.

A alteração desses dados ocorre quando é realizada uma solicitação para um recurso já existente, como, por exemplo, a URI http://www.policamp.edu.br/alunos/<RA>. Neste caso, o registro do aluno será alterado com dados que estão no corpo da entidade.

Para a criação um novo recurso com um PUT, deve ser realizada uma solicitação para uma URI não existente, e o endereço solicitado será o caminho para o novo recurso. Esta ação obriga o conhecimento prévio do endereço do novo recurso.

* HTTP POST

O POST é o mais complexo dos métodos existentes na interface HTTP [2]. Maiores detalhes sobre este método podem ser encontrados em seu texto original, o RFC 2616 [10], entretanto serão apresentadas apenas as finalidades que se encaixam no estilo REST. A ação real que o servidor irá executar sobre uma solicitação POST depende da URI solicitada. Pode ser utilizada para criar

um novo recurso ou simplesmente anexar dados ao estado de um recurso já existente.

Partindo das perspectivas do REST, pode ser usado para criar um recurso que seja subordinado a outro, chamado recurso "pai". Isto se torna útil quando não se conhece a nova URI, pois depende de dados processados no servidor. Neste caso, o cliente precisa apenas ter ciência da URI do recurso pai. Também é possível utilizar uma solicitação POST para anexar as informações enviadas para o estado de um recurso já existente. Neste caso, não é criado um novo recurso, e sim a adição dos dados. Além das utilizações apresentadas, é possível realizar uma implementação que foge dos conceitos sugeridos para estilo REST, o chamado POST sobrecarregado, quando utiliza apenas um método HTTP para representar qualquer quantidade de métodos não HTTP. Esta implementação não é recomendada, pois a informação do método não se encontra na interface HTTP.

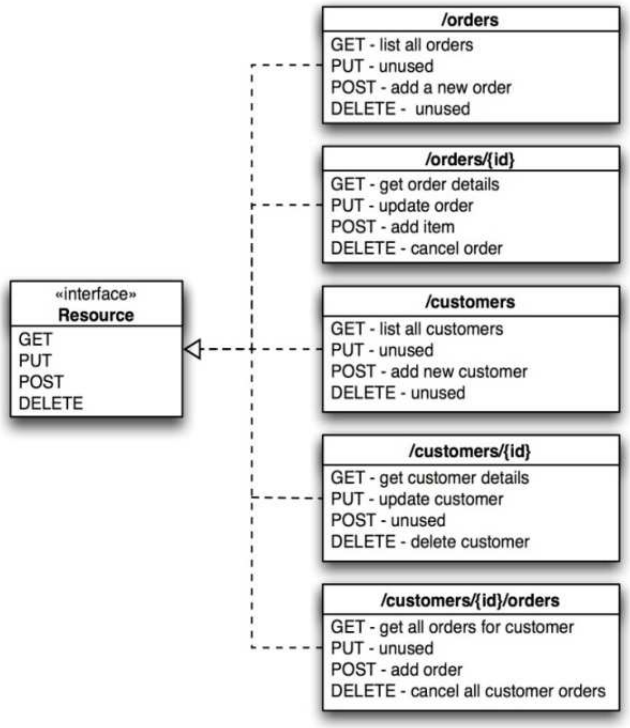


Figura 2 - Exemplos de Recursos e o retorno de cada um de seus métodos [7]

 ISSN 1679-8902

6. Contribuição: conjunto de boas práticas dos serviços baseados em REST

As restrições já apresentadas são peças fundamentais para uma base sólida nos princípios do estilo. Algumas práticas melhores serão indicadas para tornar a implementação dos serviços bem sucedida. Este conjunto de práticas foi possível pelo trabalho experimental em laboratório.

a) Nomeação dos recursos

Os nomes dos recursos devem ser divididos de forma a conter e a suportar todas as partes móveis de que o sistema tratará [2]. A divisão será realizada pelos substantivos [11] que compõem o conjunto de dados desse sistema, como, por exemplo, “Aluno”, “Matéria” e “Curso”, que representam um recurso dentro da aplicação; para acessá-los, devem possuir um endereço intuitivo, claro e descritivo sobre o conjunto de dados que retornará ao cliente, contendo todas as informações necessárias ao escopo do serviço.

Quando for necessário representar outros níveis dentro de um determinado recurso, usando a barra para separar as partes das informações do escopo, devem ser utilizadas hierarquias, que representam os vários níveis da informação dentro de um diretório [2]. Para representar as notas ou matérias de uma determinada classe de alunos, podem ser utilizados níveis hierárquicos dentro do recurso desse aluno, como nos exemplos a seguir:

http://www.policamp.edu.br/alunos/notas

http://www.policamp.edu.br/alunos/materias

b) Construção dos dados aceitos pelo serviço

Em muitos casos, é necessário o envio de informações do estado para o serviço no momento de uma chamada. É desejável que todas as informações do escopo sejam enviadas ao endereço do serviço, garantindo o princípio de endereçabilidade do REST [4]. Quando for necessário o envio de uma representação em conteúdo binário, pode se utilizar o cabeçalho para este fim.

Quando são conhecidos os valores a serem transmitidos no escopo, devem ser usadas variáveis de diretório dentro dos endereços dos recursos [2]. Como exemplo para esta abordagem, a consulta de um determinado aluno, dentro do diretório de alunos: www.policamp.edu.br/alunos/<RA>. É possível notar como se fosse uma relação todo parte, ou seja, um aluno pertence a um conjunto maior: alunos.

Outra abordagem possível é a utilização de variáveis de consulta, para enviar parâmetros ao servidor em recursos algorítmicos. Uma consulta dentro do acervo de livros de uma biblioteca pode ser implementada utilizando este conceito: www.policamp.edu.br/biblioteca/livro?filtro=<parâmetros do filtro>.

c) Representações retornadas pelo serviço

Os serviços podem retornar uma variedade de tipos de dados que devem conter todas as informações úteis sobre o recurso. É importante que os dados de retorno satisfaçam os objetivos esperados pelo cliente para poder ser utilizado adequadamente.

Devido à facilidade de implementação e de integração entre diferentes linguagens de programação, a utilização do formato XML[6] para retorno dos dados é um padrão adotado. Se algum outro formato for mais útil ao consumidor do serviço, deve ser usado, pois não infringirá os princípios REST.

No conteúdo de retorno, é imprescindível fornecer os links para os recursos vizinhos da representação, os quais são os possíveis novos estados da aplicação, tendo como objetivo promover o encadeamento entre serviços, o que corresponde à capacidade de ir de um recurso para outro, utilizando esses links.

Uma representação em XML de um aluno com links para outros recursos:

[6] eXtensible Markup Language

```
<?xml version=”1.0” standalone=”Yes”>
<aluno>
    <nome>...</nome>
    ...
    <curso href=“/cursos/SI”/>
    <notas href=“/alunos/<RA>/notas”/>
</aluno>
```

d) Tratamento das condições

Os serviços de leitura e gravação devem tratar de todas as condições de sucesso e falha para a chamada dos recursos, importantes para assegurar que as solicitações do cliente sejam transformadas corretamente em respostas. O tratamento do status de retorno deve utilizar os códigos de respostas do HTTP.

O status padrão de sucesso para os serviços de leitura e gravação, é o código de retorno 200 (“OK”), com as representações no corpo da entidade e possíveis dados no cabeçalho HTTP.

Na criação de um novo recurso, sugere-se retornar ao status 201 (“Criado”), com um cabeçalho de resposta *Location*, com a URI do novo recurso.

Quando for solicitado um recurso inexistente dentro do sistema, deve-se retornar a um código de status 404 (“Não Encontrado”), não sendo necessário enviar o corpo da entidade na resposta.

Se forem informados valores inválidos para os parâmetros do serviço, ou a obrigatoriedade de parâmetros, deve ser indicado o status 400 (“Requisição Incorreta”). É adequado enviar no corpo da solicitação, informações sobre os valores incorretos para um possível ajuste.

Para serviços que implementam autenticação e forem solicitados com credenciais incorretas, o sistema deve retornar ao código de resposta 401 (“Não autorizado”).

Caso o serviço não seja capaz de satisfazer a solicitação devido à sobrecarga no servidor, deve ser enviado o status 503 (“Serviço Indisponível”). Todos os status de erro pertencentes à família 5xx representam erros ocorridos no servidor, quando o cliente fica incapacitado de obter as representações do serviço.

Outros problemas podem ocorrer durante o consumo de um serviço, porém os erros apresentados acima são suficientes para tratar da grande parte dos casos típicos.

e) Segurança

Toda solicitação GET e HEAD deve ser segura, não alterando o estado do servidor [12]. Se o software cliente invocar o recurso uma ou N vezes, o seu estado deve ser o mesmo, como se nunca existisse a solicitação. Este conceito é importante por se tratar de métodos confiáveis dentro do protocolo HTTP. Quando solicitado um recurso com estes métodos e o servidor não retornar uma resposta, é seguro fazer uma nova solicitação.

f) “Idempotência”

As operações “idempotentes” são aquelas que têm o mesmo efeito sempre que são executadas uma ou mais vezes. Os métodos GET, HEAD, PUT e DELETE devem ser idempotentes [12]. Se um recurso for alterado com PUT, o estado deste será alterado no servidor. Realizando novas solicitações PUT para o mesmo recurso, a representação do estado será igual à da primeira solicitação realizada.

g) GET Condicional

A utilização de GET condicional permite que o cliente e o servidor trabalhem juntos para economizar largura de banda. Quando o cliente executa

uma consulta a um determinado recurso e o servidor verifica que o recurso do cliente é exatamente igual ao do servidor, ele retorna apenas uma resposta ao agente do usuário, informando que esse recurso é o mesmo e que o cliente pode se utilizar de seu cache para devolver o recurso ao usuário, economizando assim, na transferência de dados.

h) Compactação

Outro mecanismo utilizado para a economia de dados na rede é a compactação de dados. Um cliente HTTP pode requisitar uma versão compactada das representações e a descompactação ocorre de modo transparente. Para requisitar dados compactados, o cliente envia um cabeçalho *Accept-Enconding*, informando os tipos de compactação compreendidos. Se o servidor entender algum dos formatos enviados, ele pode transmitir os dados compactos, economizando largura de banda. O cabeçalho *Content-Encoding* deve ser enviado na resposta, indicando o padrão de compactação do documento. Exemplo de uma solicitação e resposta com compactação de dados:

Solicitação:

GET /aluno/<RA> HTTP/1.1

Host: www.policamp.edu.br

Accept-Encoding: gzip, compress

Resposta:

200 OK

Content-Type: text/XML\

Content-Enconding: gzip

7. Conclusões

A Transferência de Estado Representacional (REST) é uma tecnologia promissora para o desenvolvimento de sistemas web distribuídos. O estilo possui uma fácil implementação e funciona de modo a aproveitar todos os recursos já existentes no protocolo HTTP, possibilitando, com isso, a utilização de uma forma simples nos mais diversos tipos de equipamentos que suporte o HTTP – protocolo padrão da Internet.

Outro ponto importante do modelo é a quantidade de dados trafegados na rede. Por não implementar protocolos adicionais como o SOAP, durante o transporte da solicitação e da resposta, são trafegados apenas os dados que agregam valor para o serviço. Técnicas de compactação e de resposta condicional são facilmente implementadas por serem nativas do protocolo HTTP. Esta abordagem é muito eficiente para clientes que possuem um alto custo de consumo de banda, como celulares e serviços com grande número de acessos, evitando, assim, a transferência de dados que não foram solicitados pelo software cliente. Mesmo para os problemas que os serviços web tradicionais tentam resolver, como aplicações de negócios e governamentais, a utilização de serviços REST mostra-se eficiente, tornando uma alternativa real para a implementação dos serviços. Com a utilização dos modelos apresentados, todo o esforço é na implementação do recurso, não nos protocolos e regras adicionais impostos pelos serviços tradicionais.

Referências

[1] W3C, *Web Services Glossary*, Fevereiro 2004. [Online]. Disponível em: http://www.w3.org/TR/ws-gloss. Último acesso em: 28/11/2009.

[2] L. Richardson and S. Ruby, RESTful Serviços Web. Rio de Janeiro: Alta Books, 2000.

[3] W3C, *Web Services Architecture*, Fevereiro 2004. [Online]. Disponível em: http://www.w3.org/TR/2004/NOTE-ws-arch-20040211. Último acesso em: 30/11/2009.

[4] R. T. Fielding, *Architectural Styles and the Design of Network-based Software Architectures*. Tese (Doctor of Philosophy in Information and Computer Science, Chapter 5) - University of California, Irvine, 2000.

[5] R. T. Fielding and R. N. Taylor, *Principle Design of the Modern Web Architecture*. ACM Transactions on Internet Technology, pp 115–150, Maio 2002.

[6] W3C, *Universal Resource Identifiers - Axioms of Web Architecture*, Dezembro 1996. [Online]. Disponível em: http://www.w3.org/DesignIssues/Axioms.html. Último acesso em: 30/11/2009.

[7] S. Tilkov, *"A Brief Introduction to REST"*, Dezembro 2007. [Online]. Disponível em: http://www.infoq.com/articles/rest-introduction. Último acesso em: 30/11/2009.

[8] S. Nunes and G. David, *"Uma Arquitectura Web para Serviços Web"*. [Online]. Disponível em: http://www.fe.up.pt/si/publs_web.show_publ_file?p_id=12085&pv_nocache=20091129234207. Último acesso em: 28/11/2009.

[9] *REST intro slides*. Maio 2007. [Online]. Disponível: http://tech.groups.yahoo.com/group/rest-discuss/message/8367?var=1. Último acesso em: 30/11/2009.

[10] Network Working Group, *Hypertext Transfer Protocol - HTTP/1.1*, Junho 1999. [Online]. Disponível: http://www.ietf.org/rfc/rfc2616.txt. Último acesso em: 30/11/2009.

[11] R. L. Costello, "*Building Web Services the REST Way*". [Online]. Disponível em: http://www.xfront.com/REST-Web-Services.html. Último acesso em: 30/11/2009.

[12] D. Gourley and B. Totty, *HTTP: The Definitive Guide*. O'Reilly Media, 2009.

[13]http://www.innoq.com/blog/st/2006/06/30/rest_vs_soap_oh_no_not_again.html Ultimo acesso em: 17/12/09

SOLUÇÃO PROPOSTA DE AUDITORIA DE SEGURANÇA EM FIREWALLS CISCO PARA EMPRESAS COM GRANDE QUANTIDADE DE EQUIPAMENTOS DE SEGURANÇA EM REDE

Proposed solution in safety audit firewalls Cisco for companies with large amount of equipment networking security

MACIEL FILHO, Marcus Antonius Gadelha
Faculdade Politécnica de Campinas

MATTOS, Amarildo Martins de
Faculdade Politécnica de Campinas

Resumo*:* Auditoria de Segurança para *firewalls* é algo realmente importante que precisa ser feito em todas as grandes empresas. Este trabalho mostra como fazer um processo automático de Auditoria de Segurança para *firewalls*, os conceitos de segurança, ameaças e vulnerabilidades envolvidas e como é realizado esse processo.

Palavras-chave: auditoria, Cisco, firewall, segurança.

Abstract: Security Audit for firewalls is a really important activity that need to be performed by all big companies. This work shows how to do an automated Firewall Security Audit and explain the concepts of security, threats and vulnerabilities and how is the process for a Firewall Security Audit.

Keywords: audit, Cisco, firewall, security.

1. Introdução

Com o passar dos anos, a segurança de redes e sistemas se tornou uma grande necessidade para todas as empresas de grande porte. Com a expansão das atividades ilegais envolvendo acessos não autorizados à sistemas e redes de terceiros, tornou-se indispensável o uso de equipamentos

conhecidos como *firewalls* em quaisquer redes de empresas de grande, médio e pequeno portes.

Como definição um *firewall* é uma parte de uma rede ou sistemas de computadores desenvolvidos para bloquear acessos não autorizados, ao mesmo tempo em que permite o acesso de comunicações autorizadas no meio. O mesmo pode ser descrito como um dispositivo ou conjunto de dispositivos, configurados para permitir, negar, criptografar, decriptografar, ou analisar o tráfego de entrada e saída de dados dos computadores entre diferentes domínios de segurança, sempre baseados em um conjunto de regras específicas (Figura 1).

Seria muito difícil garantir a segurança de qualquer rede sem o uso de um sistema de *firewall*. Uma rede protegida por um *firewall* bem configurado permitirá que apenas os pacotes de dados legítimos (i. é: previamente aprovados pelo mesmo) possam trafegar pela rede. Além da confirmação periódica do fluxo de pacotes, o sistema precisa efetuar o registro das conexões e assim garantir o funcionamento dos diversos fatores relacionados à segurança da rede.

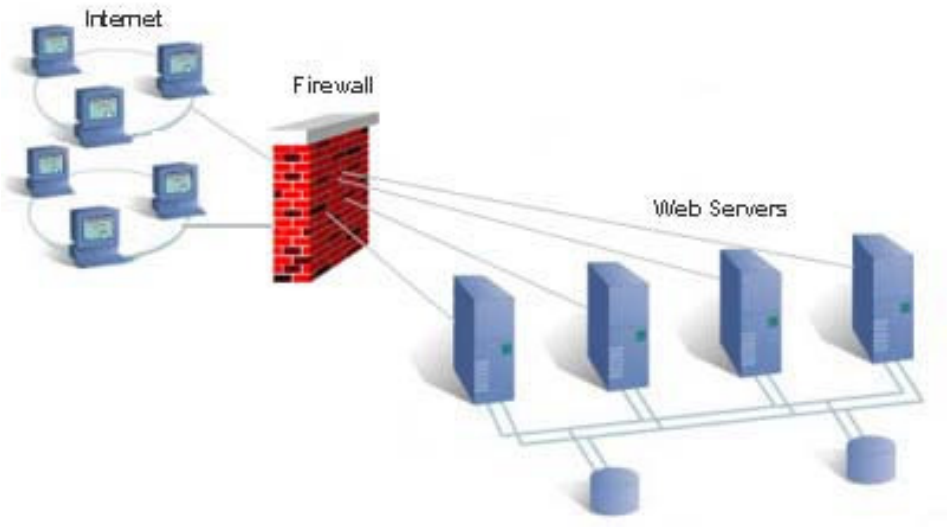


Figura 1 – Representação esquemática de um Firewall em execução em uma rede (ilustração do fastserve.net).

A. Motivação

Grande parte do trabalho realizado em processos de auditoria de segurança de *firewalls* é feito de forma manual. Este trabalho pode até ser aceitável caso seja feito em uma empresa de pequeno porte que possua poucos equipamentos de rede e pouquíssimos *firewalls* implementados. Mas, para empresas de grande porte, que possuem milhares de equipamentos de rede e *firewalls* ativos (e muitas das vezes em redes continentais), o processo manual de auditoria é completamente inviável, pois exige um grande número de profissionais realizando verificações manuais nos sistemas, a todo o momento.

O uso de profissionais para esse tipo de trabalho contribui consideravelmente para o aumento das taxas de erro nos processos de controle e manutenção de uma rede, além de ser o responsável pela redução da produtividade de um setor ou mesmo da empresa. O desvio de profissionais qualificados para uma única função rotineira acarreta em problemas de gerenciamento, inflacionamento de quadro funcional, e a consequente perda de produtividade de todo um setor estratégico. A automatização dos processos de auditoria de redes de computadores, reduz consideravelmente as taxas de erros humanos, otimiza o uso de profissionais no setor e, garante a rapidez e a precisão com que as verificações são realizadas, e os resultados para análise são obtidos.

B. Objetivos

O objetivo deste projeto é demonstrar a possibilidade de automação de grande parte dos processos de auditoria de *firewalls* Cisco[7], com o uso da ferramenta apresentada neste documento – o DBPortal. O DBPortal é um sistema de automação voltado para a auditoria de *firewalls* Cisco, que foi inteiramente desenvolvido pelo autor deste trabalho. O uso dessa ferramenta em grandes redes empresariais aumenta a produtividade dos funcionários da

[7] A Cisco, ou *Cisco Systems Inc*. é uma empresa que atua no mercado no desenvolvimento e

área de segurança, permitindo que os mesmos possam executar em paralelo outras atividades de igual importância, nas quais seja necessária uma maior interação humana. Esses profissionais também poderão estar mais envolvidos com a apresentação dos referidos estudos de processos de auditoria, analises de vulnerabilidade e de ameaças, além de um breve estudo no conceito de segurança setorial e global nas empresas em que trabalham.

C. Contribuições

O DBPortal torna a atividade diária das equipes de segurança um processo mais rápido, preciso e dinâmico, além de garantir uma grande redução nas taxas de erros humanos em atividades de auditoria. Essas ações permitem um aumento na qualidade das informações usadas em auditorias de segurança em *firewalls*, além de permitir que as mesmas possam ser obtidas em um menor intervalo de tempo.

2. Segurança da Informação em firewalls

A Segurança da Informação é um tema muito discutido e de extrema importância para a nossa sociedade. No mundo em que vivemos, encontram-se pessoas mal intencionadas (indivíduos, empresas ou mesmo governos), que utilizam de meios e métodos ilegais para adquirir todo tipo de informações. Na maioria das vezes, a intenção dos criminosos é o lucro, através do roubo de informações sigilosas, ou projetos de tecnologia, que possuam grande valor econômico e/ou estratégico, para uma empresa ou mesmo uma nação. Cada empresa precisa estar preparada para poder se defender de forma adequada. Entretanto, devido à capacidade dos *firewalls* – de permitir ou negar qualquer tipo de conexão independente de sua origem – a segurança das informações se tornou um processo um pouco mais fácil de ser administrado.

---

comercialização de equipamentos de rede como roteadores, *switches* e *firewalls*.

Quando se fala em Segurança da Informação a mesma refere-se à tomada de ações necessárias para a garantia da confidencialidade, integridade, disponibilidade, e a todos os demais aspectos de segurança da informação dentro das necessidades do cliente [2]. Devido ao conceito de segurança ser considerado global, o mesmo pode ser adaptado as necessidades de segurança em *firewalls*. Sendo assim, os seguintes itens são definidos:

1) Confidencialidade: refere-se à capacidade que um *firewall* tem em permitir que os usuários acessem determinadas informações, sem que o mesmo conteúdo seja interceptado por outros usuários.
2) Integridade: refere-se à capacidade de um *firewall* em garantir a integridade e veracidade dos dados recebidos.
3) Disponibilidade: refere-se à capacidade dos *firewalls* em relação a disponibilidade de acesso. Acesso esse realizado por todos que precisem do dispositivo para a realização dos objetivos da empresa. Sendo mais específico, a disponibilidade refere-se a capacidade de permitir ou de bloquear um acesso em uma rede.

Alem desses três aspectos principais de segurança em *firewalls*, ainda existem os seguintes pontos [2]:

1) Autenticação: o objetivo da autenticação é garantir que um indivíduo confirme sua identidade como usuário na rede.
2) Não-repudio: ter uma prova de que toda ação executada por qualquer usuário possa ser verificada posteriormente.
3) Legalidade: o *firewall* deve seguir as regras definidas pelo órgão responsável pela segurança na empresa.
4) Privacidade: o *firewall* deve garantir que os tráfegos autorizados possam ser executados de forma anônima, a fim de garantir a privacidade do usuário. Este processo envolve o anonimato do tráfego de informações referentes a avaliações de funcionários, troca de informações entre setores, e os serviços prestados pela empresa.
5) Auditoria: o *firewall* deve ser capaz de auditar todo tipo de ação executada por um usuário em uma rede, detectando tentativas de ataque, ou mesmo fraudes realizadas.

3. Fundamentos em auditoria de segurança

As empresas possuem grande necessidade de ter e de administrar o fator segurança em seu ambiente de trabalho, além de serem obrigadas a manter o correto funcionamento de seus *firewalls* dentro das redes de suas próprias instalações. Por isso, é imprescindível a implementação de um processo de verificação e confirmação de toda a estrutura de transmissão de dados nas suas redes corporativas.

A função da auditoria de sistemas é promover a adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos nos sistemas de informações da empresa, bem como avaliar a utilização dos recursos humanos, materiais e tecnologias envolvidas em seu processamento [1].

A. Processos em auditoria de firewalls

Em empresas de grande porte, a auditoria de segurança em *firewalls* geralmente é dividida em processos que devem ser constantemente verificados. Abaixo são apresentados os processos que estão relacionados com a auditoria de *firewalls* baseados em [2, 3, 4, 5].

1) Verificação de alterações de senhas de sistema a cada X dias: A alteração de senha de sistema é um processo muito importante em auditoria de *firewalls*. O mesmo garante que os usuários com o péssimo hábito de possuir senhas iguais para todos os sistemas da empresa sejam obrigados a alterar suas senhas em períodos determinados pela própria companhia. Além de forçar a alteração de senhas, as empresas ainda podem utilizar métodos de verificação de caracteres, forçando o usuário do sistema a adotar um conjunto de dígitos variados, como o uso de maiúsculas, minúsculas, caracteres especiais, números, além de uma quantidade mínima de caracteres envolvidos na construção de suas

senhas. O sistema pode, inclusive, verificar se a nova senha é igual às X ultimas senhas usadas neste sistema, evitando que o usuário utilize senhas repetitivas na rede da empresa. Obviamente esta verificação só será possível através do uso de determinados métodos de criptografia para as devidas autenticações.

2) Verificação de existência de *logs*[8] para cada usuário em uma faixa de X dias: O registro de *logs* é a parte mais importante em uma auditoria, pois com eles é possível verificar todas as tentativas de ataque que possam ser realizadas no sistema, obter alertas de mau funcionamento do hardware do *firewall* e, ainda, ajudar na solução de problemas referentes ao tráfego. Afinal, a maior parte do trafego de determinados setores das empresas passam por meio de *firewalls,* tornando possível a visualização dos *logs* dessas conexões, e assim, facilitar a analise dos problemas de rede.
3) Analise da configuração básica do *firewall*: Geralmente, a configuração básica dos *firewalls* possui vários serviços habilitados, sendo que grande parte desses mesmos serviços nunca serão utilizados. Para garantir que apenas os serviços que sejam necessários e seguros estejam habilitados é necessário efetuar uma analise inicial de serviços, registrando assim quais poderão ser desabilitados em um *firewall*. Alguns exemplos de serviços que são normalmente encontrados em uma configuração de *firewall*: Telnet (devido a problemas de segurança é recomendado o uso exclusivo do ssh v2, para qualquer conexão realizada ao firewall), http (que geralmente não é usado) e várias outras configurações que podem, de forma desnecessária, afetar a segurança do *firewall*.

Serviços habilitados no *firewall*, mas que estejam inativos como serviços nas empresas, possuem um potencial de risco e de vulnerabilidade muito grande. Serviços habilitados, mas em desuso, não são monitorados, e muito menos atualizados como pacotes, caso uma brecha de segurança seja descoberta pelos seus desenvolvedores. Ao serem descobertas brechas de segurança nestes serviços, o perigo passa de potencial para real. Através de uma vulnerabilidade exposta e não monitorada, atacantes podem se beneficiar

não somente da vulnerabilidade do serviço, mas também da vulnerabilidade da administração de toda a rede da empresa. Pense em serviços não utilizados em seu *firewall* (a exemplo, VoIP). Uma brecha descoberta para este recurso em uma rede sem monitoramento adequado de serviços inativos, pode se tornar um pesadelo. Isso faz com que o *firewall* esteja vulnerável a um serviço que ele não deveria ter. Esse tipo de situação é considerado uma falha no processo de validação da configuração básica de qualquer *firewall*, e em uma auditoria, isso é um sério problema.

4) Analise de regras de acesso do *firewall*: Quando um *firewall* entra em produção em uma rede, o mesmo deve receber as regras de acesso adequadas para a permissão de determinados tipos de tráfegos. Estes tráfegos geralmente são aprovados pelos responsáveis envolvidos no projeto de implantação deste *firewall*, garantindo que apenas o necessário seja permitido trafegar pela rede. Desta forma, a cada auditoria, torna-se necessário a verificação de todas as regras de acesso do *firewall*, a fim de confirmar que apenas o que foi previamente acordado, é o que esta sendo permitido trafegar na rede.
5) Validação de usuários cadastrados no *firewall*: É normal em qualquer empresa a rotatividade de funcionários, seja na contratação, na demissão, ou na transferência de setor na mesma empresa ou unidade. Desta forma, a validação de usuários é fundamental para garantir que apenas os usuários registrados, e em atividades nos seus devidos setores, tenham acesso coordenado ao sistema e a rede. Esta validação impede o acesso de pessoal não-autorizado aos *firewalls* e, consequentemente, garante que não sejam efetuadas alterações nos mesmos, que possam ocasionar impactos de magnitude incalculável dentro da empresa.
6) Gerar e analisar relatórios a partir de *logs*: É muito improvável que uma analise de *log* seja efetuada sem que esteja acontecendo um problema gerador de impacto dentro da empresa. Sendo assim, a geração automática de relatórios – sempre sumarizando os *logs* de forma a facilitar a identificação e analise de problemas – é algo extremamente necessário em uma auditoria de *firewall*. Sem esses relatórios a análise diária de

[8] *Logs* são registros de eventos relevantes que podem ocorrer no firewall.

milhares (ou até mesmo milhões) de linhas de *log*, tornaria o processo impossível para qualquer ser humano (um indivíduo ou mesmo uma equipe inteira).

7) *Backup* de configurações: Assim como um sistema precisa de um *backup* para garantir que qualquer tipo de alteração possa ter um retorno, o *firewall* também necessita de um *backup* – porém apenas de suas configurações. Através da realização de *backups*, todas as alterações feitas nas configurações podem ser analisadas e, em caso de uma falha, as versões podem ser facilmente comparadas entre si, facilitando assim a identificação do problema.

8) Verificação de versão e modelo do *firewall*: Os fabricantes de dispositivos de segurança disponibilizam com freqüência alertas de segurança informando as possíveis vulnerabilidades que podem permitir ataques do tipo DoS[9] ou DDoS[10]. Inclusive, essas vulnerabilidades podem até mesmo garantir acessos não autorizados ao próprio *firewall*. Normalmente esses alertas vêm sempre acompanhados da solução do problema, podendo ser desde a necessidade da desabilitação de um determinado comando, ou até mesmo uma indicação de urgência para uma atualização no sistema operacional do próprio *firewall*. Sendo assim a verificação de versões destes dispositivos deve ser um procedimento freqüente, para assim garantir a segurança da rede como um todo.

4. Vulnerabilidades e ameaças

Um dos motivos pelo qual existem os processos de auditoria em empresas é garantir que os *firewalls* da rede estejam sempre seguros contra qualquer tipo de vulnerabilidade e, assim, possam garantir maior segurança para setores potencialmente vulneráveis da empresa.

Vulnerabilidades são falhas de segurança que podem afetar o sistema operacional do *firewall*. Através dessas falhas é possível que o *firewall* seja

[9] DoS é a sigla para Denial of Service, que é um ataque que visa a negação de serviço de um servidor na rede.
[10] DDoS é a sigla para *Distributed Denial of Service*, que é um ataque que visa a negação de serviço de um servidor

afetado a ponto de gerar um mau funcionamento do sistema. O resultado pode ser um grande risco para toda empresa. Essas vulnerabilidades devem ser analisadas como grandes fatores de risco para a segurança de qualquer companhia.

A. Ataques de negação de serviço

Os ataques de negação de serviço conhecidos como DoS ou DDoS são ataques que possuem o objetivo de tornar a rede ou serviço indisponível. Normalmente, os ataques do tipo DoS e DDoS são realizados através do envio de uma grande quantidade de pacotes UDP para determinados endereços de Internet, sobrecarregando assim toda a disponibilidade de memória e requisição de resposta para os chamados desses dispositivos. Isso faz com que os equipamentos de redes e serviços fiquem indisponíveis para seus usuários. Os pacotes utilizados para esse tipo de ataque são geralmente via protocolo UDP, por não serem orientados à conexão. Isso facilita o mascaramento do endereço de origem em um ataque.

Muitos se perguntam como é possível ocorrer um ataque DDoS. Muito provavelmente ninguém nunca se perguntou sobre o real motivo da existência dos *malwares*. Boa parte desses *malwares* foi feita com o objetivo de criar *Botnets*. Os Botnets são redes de computadores infectados por *malwares*. Estes computadores passam a possuir comportamento de zumbis, aceitando comandos de seus “mestres” (os criadores dos *malwares*). Normalmente os computadores zumbis se conectam a salas de bate-papo em redes de IRC (*Internet Relay Chat)* controladas por senha, em que o “dono” desta rede de computadores infectados é capaz de executar comandos de ataque.

Esses ataques, nada mais são que o disparo de milhares de pacotes provenientes de todos esses computadores infectados, visando um único alvo (um ou mais servidores ou dispositivos em uma rede), com o intuito de sobrecarregá-lo.

---

na rede, só que de forma distribuida.

Mesmo com todos esses recursos, os ataques nem sempre são efetivos. Os ataques do tipo DoS mais complexos envolvem profundo conhecimento dos equipamentos de rede por parte do atacante, muitas vezes por técnicas de engenharia reversa, permitindo assim a exploração de falhas no processamento de protocolos por parte desses dispositivos. Equipamentos como *firewalls* costumam efetuar a analise de pacotes até a camada de aplicação (camada 7 do modelo OSI), o que tornam esses equipamentos mais suscetíveis aos ataques que se beneficiam da má formatação de pacotes. Tudo isso com o intuito gerar indisponibilidade de serviços em uma rede.

B. Sniffing

Boa parte dos protocolos que trafegam pela *Internet* não utilizam criptografia, o que os torna mais suscetíveis a ataques do tipo *Sniffing*. O *Sniffing* é um método para analise de redes que envolve o recebimento de pacotes de todas as origens possíveis, e consequentemente, a formatação dos mesmos em um formato legível para o ser humano (*human-readable*). O *Sniffing* é naturalmente uma técnica utilizada para a análise de funcionamento de redes, ou seja, ela é originalmente uma técnica de uso licito. Dentre os diversos serviços que podem ser “sniffados” destacam-se: telnet, ftp, http, pop, smtp e imap. Porém, nem todos os serviços existentes podem ser “sniffados”, basicamente por trabalharem com conteúdo criptografado. Exemplos são: ssh, sftp, https, pop over ssl, smtp over ssl, imap over e ssl. Explicando de uma forma mais simples, através do uso de técnicas de *sniffing* é possível visualizar dados de usuários em trânsito (a ex.: login e senha) numa rede local, para todos os serviços que utilizam de métodos de autenticação sem criptografia.

C. Man-in-the-Middle

Este tipo de ataque permite que o atacante seja capaz de visualizar em tempo real todas as atividades que estão sendo executadas pelo cliente responsável por iniciar uma conexão. Literalmente é poder estar no meio do

caminho em uma rede e saber tudo o que acontece em todo o trânsito de pacotes a sua volta. Um exemplo prático desse tipo de ataque é a conexão via cliente a um site de banco. Enquanto um usuário efetua a conexão com seu banco via *Internet*, um atacante realiza um *dns spoofing*[11] e um *arp spoofing*[12], fazendo com que os pacotes que deveriam ir para o site do banco sejam re-direcionados para a maquina do próprio atacante, que fica entre o cliente e o banco.

Na maioria dos casos, o usuário acaba aceitando um certificado gerado pelo atacante, permitindo ao criminoso estabelecer a conexão com o site do banco, via conta da própria vítima. Obviamente, o certificado gerado pelo atacante será reconhecido como inválido, ou não confiável, pelo navegador de Internet da vítima (Firefox, Opera, IE, etc.). Porém, a maioria esmagadora dos usuários que utilizam recursos bancários via Internet não possuem (ou não se preocupam em ter) o mínimo de conhecimento para reconhecer uma ação criminosa deste nível. Mesmo com o certificado inválido aparecendo em sua tela, poucos serão os usuários que suspeitarão estarem sendo vítimas de criminosos e, consequentemente, darão continuidade ao engodo a que estão se submetendo.

Dentre os protocolos mais utilizados para esse tipo de conexão, o ssh versão 1 é considerado bastante vulnerável a este tipo de ataque. Por este motivo, é recomendado apenas a instalação e o uso do protocolo ssh versão 2 em todos os servidores de rede, assim como nos próprios *firewalls* das empresas. O ataque do tipo *man-in-the-middle* pode ser detectado facilmente por sistemas de IPS[13], sendo os mesmos capazes de efetuar o bloqueio da porta utilizada para este ataque. Porém, esse ponto não será abordado neste trabalho.

D. Port Scan

[11] Ataque usado para direcionar o dns de um host para um destino falso.
[12] Ataque usado para enviar um endereço de hardware falso ao requisitante.
[13] IPS é a sigla em inglês para Intrusion Prevention System.

Este ataque tem como objetivo procurar portas que possam estar abertas em determinados servidores, a fim de gerar algum tipo de ataque em alguns dos serviços encontrados. Em *firewalls* bem configurados, esses ataques podem ser reconhecidos através da análise dos *logs*, pela grande quantidade de acesso negado a determinadas portas para um mesmo endereço IP de origem.

5. O Projeto

Devido à ausência de softwares que atendam este ramo de automação, o projeto em discussão, denominado DBPortal, foi desenvolvido com o intuito de automatizar a maior parte dos processos de auditoria de *firewalls*. O DBPortal é um sistema *Web* capaz de realizar, de forma automatizada, grande parte dos processos de auditoria de *firewalls* existentes nas grandes empresas, que normalmente são realizados de forma manual pelo corpo funcional destas mesmas companhias.

O sistema foi desenvolvido e implementado em um servidor DUAL Intel® Xeon™, com CPUs de 3.20GHz, possuindo discos SCSI de alta performance. O sistema operacional instalado é o Red Hat Enterprise Linux (RHEL) AS release 3 (Taroon Update 9). Como ferramentas de desenvolvimento foi utilizado o PHP versão 4.3.2 como linguagem de script para *Web*, e o banco de dados relacional de código aberto MySQL versão 4.1.22. Também foram utilizadas como ferramentas de integração, *scripts* em *Shell* usando Expect, Bash, e AWK, além de diversas outras ferramentas de código aberto disponíveis para o projeto.

O DBPortal conta com uma interface *Web* desenvolvida através de técnicas de IHC[14], facilitando seu aprendizado e uso por parte dos usuários. Toda a tela apresentada pelo sistema é resultado de 2 anos de pesquisa com a colaboração de diversos usuários-testes do sistema, incluindo testes de

[14] IHC é a sigla para Interação Humano Computador.

posicionamento de menus e formulários, além da escolha das cores utilizadas, representado o resultado de funções do sistema.

Apesar do DBPortal já estar em uso, seu desenvolvimento continua com a criação de novos recursos de automatização de processos de segurança, os quais ainda estão sendo efetuados de forma manual nas empresas e, com isso, consumindo uma quantidade desnecessária de tempo e recursos em seus processos. Para que o sistema pudesse efetuar todas suas atividades atualmente implementadas foram criados *scripts* especializados com capacidade de interação com os *firewalls* na rede. Esses *scripts* especializados possuem a função de processamento do retorno de informação gerada pelos *firewalls*, em complemento a já mencionada interface *Web* do sistema.

O DBPortal possui diversas funcionalidades que foram implementadas de forma modular, visando sempre a automatização de um processo de auditoria de *firewalls* dento de uma empresa de grande porte. Para facilitar o completo entendimento de sua estrutura e funcionalidades, primeiro serão apresentados todos os processos independentes de interação com cada dispositivo registrado no sistema. Posteriormente serão abordados os módulos funcionais e o processo de *backup* dos arquivos de configuração dos dispositivos:

A. Script de captura de configuração

Este *script* é responsável pela captura da configuração dos *firewalls* que estejam em atividade na rede. Essa captura envolve dados como numero serial, versão de software e modelo do *firewall*. Este *script* foi totalmente escrito em uma linguagem de *script* não muito conhecida – o Expect[15].

A linguagem de *script* Expect é uma ferramenta de teste e automação do Unix, escrita por Don Libes[16], para ser uma extensão da linguagem de *script*

[15] Saiba mais sobre a linguagem de script Expect em `http://expect.nist.gov/`
[16] `http://en.wikipedia.org/wiki/Don_Libes`

Tcl[17]. O expect é destinado para a realização de interação com aplicações como telnet, ftp, passwd, rlogin, tip, ssh, e muitas outras. O *script* criado na linguagem Expect, possui a capacidade de interpretar os resultados recebidos dos outros *scripts* de interação com os *firewalls*. A partir desses dados, o Expect é capaz de descobrir qual comando utilizar no sistema. Esse processo garante a interação do DBPortal com *firewalls* de diferentes modelos e fabricantes, que estejam em funcionamento em uma mesma rede. Esses *scripts* são capazes de acessar o *firewall* independente do tipo de protocolo utilizado (a ex.: ssh ou telnet). Os mesmos possuem um recurso de *time-out* junto ao sistema de investigação, o que lhes permite tentar outros protocolos caso o primeiro não esteja disponível. Os *scripts*, por padrão, sempre procurarão primeiro pelo protocolo ssh em uma rede, sendo capazes de acessar *firewalls* que utilizem os protocolos jumpbox [18] ou mesmo socks[19] para suas conexões. No entanto, para que possam funcionar corretamente, estes métodos de acesso dependem da sua configuração na interface *Web* do DBPortal.

B. Script de alteração de senhas de console

Independente de seus modelos ou fabricantes, os *firewalls* possuem senhas de emergência que geralmente são utilizadas para os processos de reparação via console, ou mesmo no caso do servidor de autenticação não estar funcionando. O processo de troca de senhas do DBPortal também inclui as senhas de emergência, o que tornou necessário a criação deste *script* para automatizar esta atividade. Tente imaginar um operador (ou mais de um) precisando trocar as senhas de forma manual para todos os *firewalls* das redes que administra, quando esse número ultrapassa a casa do milhar. Esta tarefa hercúlea seria uma atividade que tomaria tempo em demasia, deslocaria muitos funcionários para essa atividade, além de ocasionar a perda de produtividade do setor e, consequentemente, da empresa como um todo. Para

[17] Tcl é uma linguagem de programação para scripts maiores informações em http://pt.wikipedia.org/wiki/Tcl
[18] *Jumpbox* é uma palavra em inglês usada para representar uma máquina que é utilizada para acessar outra máquina.
[19] Socks é um protocolo que facilita o roteamento de pacotes entre cliente e servidor.

tentar otimizar ao máximo essa atividade, foi criado este *script*, que possui as mesmas capacidades do *script* de captura de configuração, porém com o objetivo de trocar as senhas de emergência de todos os dispositivos em análise nas redes.

C. Scripts de interpretação de retorno dos scripts de coleta de dados

Para que seja possível a interpretação dos resultados recebidos pelos *scripts*, e que estes mesmos resultados possam ser administrados via interface *Web* do DBPortal, foram criados para o sistema diversos outros *scripts* em Bash e AWK. Estes *scripts* extras são capazes de analisar o retorno recebido pelos *scripts* de coleta de dados, além de serem capazes de classificar o processo de captura de configuração, ou alteração de senhas de emergência. Ao avaliar o processo (se foi bem sucedido ou não), a informação é posteriormente armazenada em banco de dados.

D. Script de controle de processos

Para que seja possível a execução simultânea do sistema para as capturas de configuração, e para a viabilidade das diversas trocas de senha dos dispositivos, foi criado um *script* que controla a inicialização de vários processos simultâneos, sempre limitados por um numero máximo definido em configuração. Desta forma, executando 20 instâncias simultâneas via DBPortal, foi possível efetuar a captura de configuração de 150 *firewalls* por minuto, o que é uma quantidade muito expressiva.

E. Script de controle de alteração de configuração

No DBPortal cada captura de configuração deve ser classificada quanto a possíveis alterações efetuadas na configuração. É importante para o sistema gerenciar esse tipo de informação, além de ser apto a informar ao operador se

a configuração foi alterada ou não. Para que isso seja possível, o *script* de controle de alteração de configuração recebe o retorno do comando md5sum[20] que efetua a comparação entre a configuração atual e a configuração anterior. Caso ambas sejam idênticas, a nova configuração é descartada. Caso sejam diferentes, o sistema irá registrar a nova configuração, e irá gerar um arquivo com as diferenças entre as duas versões mostrando em vermelho o que foi removido e em azul o que foi adicionado.

Caso a nova configuração recebida seja diferente da configuração anterior, e na configuração da interface *Web* do DBPortal seja informado um email de notificação, será enviado para esse destinatário a nova configuração do *firewall*.

F. Interface Web

A interface *Web* foi criada utilizando basicamente a linguagem de script PHP e o banco de dados relacional de código aberto MySQL. Para otimizar o sistema com a recarga localizada de novas informações em tela foram implementados alguns recursos em AJAX (*Assincronous JavaScript and XML*). Essa implementação também contribuiu para a melhoria da interface do usuário, tornando-a mais amigável e intuitiva. Através da interface *Web*, o usuário (também chamado de operador) poderá ter o controle total das informações sobre os dispositivos cadastrados. Também poderá efetuar modificações globais ou isoladas nos dispositivos, assim como manter o monitoramento em uma rede global de computadores, tudo isso visando o processo de auditoria de *firewalls*.

Atualmente o DBPortal apresenta os seguintes recursos implementados e completamente funcionais: inventário de equipamentos, *backup* de configurações, alteração de senhas de sistema, controle de quantidade de *logs*, geração de arquivo com diferença entre as configurações, geração de relatório

[20] `md5sum` é um programa capaz de calcular os *hashes* de 128-bits em MD5, como descrito da RFC 1321.O hash MD5 (ou *checksum*) funciona como uma assinatura digital compacta de um arquivo. Por ser uma assinatura de 128-bits será muito difícil encontrar dois md5sum iguais para arquivos diferentes.

de analise de configuração básica, controle de troca de senhas, controle de *healthchecking,* e pesquisa por comandos em configurações:

1) Inventario de equipamentos: Através do inventário de equipamentos, o operador pode obter de forma imediata todas as informações referentes aos dispositivos cadastrados no sistema. Nele é possível encontrar informações como endereço de IP, *hostname*, saber qual cliente que utiliza o equipamento, além de diversas outras informações úteis. As informações contidas no inventário de equipamentos podem ser encontradas pelo sistema de busca criado para o DBPortal. Por exemplo, uma busca por 192.168 no campo de IP, irá retornar todos os endereços de IP que começam com 192.168 (ex.: 192.168.0.1, 192.168.0.2). O sistema de busca ignora capitulação (não reconhece a diferença entre maiúsculas e minúsculas entre os caracteres digitados). Essa implementação favorece encontrar o mesmo alvo em diferentes formatos (a ex.: CISCO, Cisco ou cisco).
2) *Backup* de configurações: O *backup* de configurações é realizado para todos os equipamentos que tenham configurações específicas para a realização de *backup*, como pode ser visto na Figura 2. Este procedimento está implementado no sistema via cron. O mesmo realiza *backups* simultâneos a cada minuto, iniciando diariamente à zero hora (0:00). Todos os equipamentos com a configuração de *backup* habilitada são imediatamente adicionados à fila de execução de *backup*. Além do *backup* diário de todos os *firewalls*, também é possível realizar um *backup* a qualquer momento por intermédio do operador (vide Fig. 3. e Fig. 4).

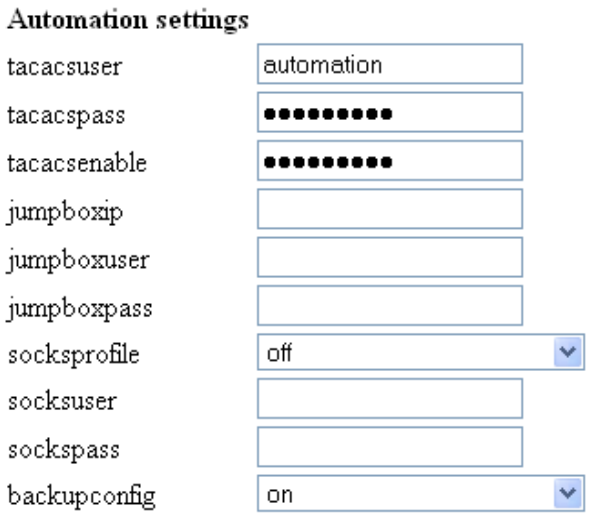


Figura 2 - Demonstra como são os campos de automação no DBPortal.

3) Alteração de senhas de sistema: Esta opção permite que todos os equipamentos com a opção de *backup* de configuração ativa, possam ter suas senhas alteradas pelo DBPortal. Esta opção é muito útil quando se faz necessário efetuar a troca de todas as senhas de sistema de vários equipamentos ao mesmo tempo. Essa automatização contribui para reduzir a zero o problema de erro humano, muito freqüente em tarefas repetitivas. Por ser automatizada, esta tarefa é incomensuravelmente mais rápida que um ser humano. Para se ter uma ideia da performance do sistema de troca de senha, é possível efetuar a troca das senhas de aproximadamente 150 equipamentos por minuto, executando 20 processos simultâneos. O numero de processos deve ser registrado na configuração do *script* de alteração de senhas.

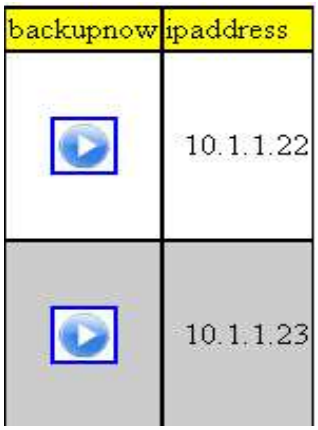


Figura 3 - Demonstra a função de execução de *backup*, sem necessariamente estar na fila de execução.

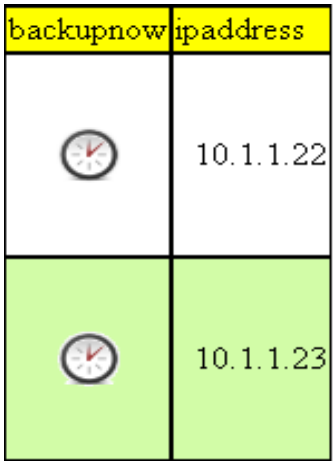


Figura 4 - Demonstra a função de execução de *backup* já inscrita na fila de execução.

4) Controle de quantidade de *logs*: O controle de quantidade de *logs* é um dos processos automatizados que mais beneficiam a infraestrutura local de administração de equipamentos para auditoria. Além de ser automatizada, esta ação exime o operador de possuir conhecimentos avançados em administração de sistemas UNIX via linha de comando, além de tornar desnecessário que o operador efetue o acesso ao servidor de *syslog* do *firewall* de forma manual. Sendo assim, o controle de quantidade de *logs* é executado pelos *scripts* de sistema do próprio DBPortal, que possui chaves RSA com todos os servidores de *syslog* ativos, permitindo assim que o sistema acesse outros servidores no intuito de obter informações específicas como, quantidade de *logs*, tamanho dos *logs*, cabeçalho do primeiro *log* e rodapé do ultimo *log*.

5) Geração de arquivo com diferença entre configurações: Esta função é gerada automaticamente pelo processo de *backup* de configuração, ajudando o operador do sistema saber qual foi a última alteração na configuração de determinado equipamento. Um exemplo pode ser visto na Figura 5.

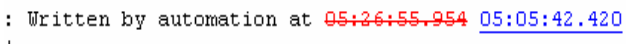
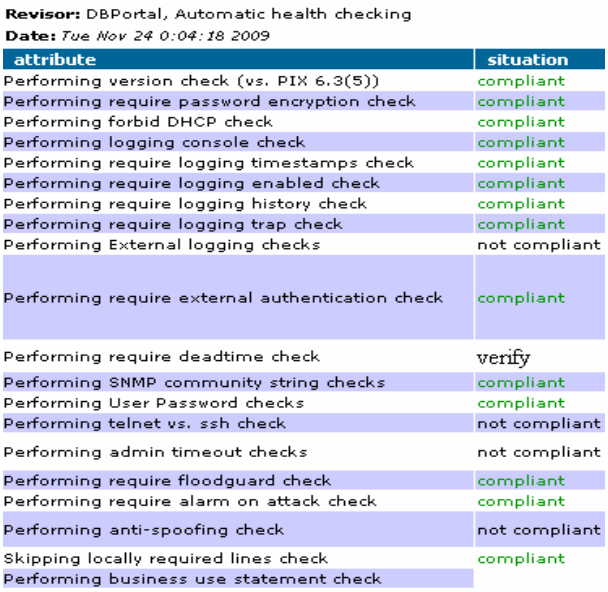


Figura 5 - Demonstra o funcionamento do arquivo de diferença de configurações, gerado pelo processo de *backup* de configurações, sendo vermelho o removido e azul o adicionado na configuração.

6) Geração de relatório de analise de configuração básica: O relatório de configuração básica é executado no momento em que o *backup* de configurações é completado. Este processo é responsável por analisar a configuração básica do equipamento, tornando possível saber se o mesmo está configurado e funcionando de acordo com o que foi previamente estabelecido. Um exemplo deste relatório pode ser visto na Figura 6.



Revisor: DBPortal, Automatic health checking
Date: *Tue Nov 24 0:04:18 2009*

attribute	situation
Performing version check (vs. PIX 6.3(5))	compliant
Performing require password encryption check	compliant
Performing forbid DHCP check	compliant
Performing logging console check	compliant
Performing require logging timestamps check	compliant
Performing require logging enabled check	compliant
Performing require logging history check	compliant
Performing require logging trap check	compliant
Performing External logging checks	not compliant
Performing require external authentication check	compliant
Performing require deadtime check	verify
Performing SNMP community string checks	compliant
Performing User Password checks	compliant
Performing telnet vs. ssh check	not compliant
Performing admin timeout checks	not compliant
Performing require floodguard check	compliant
Performing require alarm on attack check	compliant
Performing anti-spoofing check	not compliant
Skipping locally required lines check	compliant
Performing business use statement check	

Figura 6 - Demonstra o relatório de verificação de configuração básica.

7) Controle de troca de senhas: A troca de senhas de sistema é uma atividade que faz parte de qualquer auditoria. Porém a periodicidade da troca de senhas pode variar de acordo com a definição da política de segurança de cada empresa. Sendo assim, o DBPortal possui um campo específico para o cadastro da data de alteração de senha para cada dispositivo, ou conjunto de dispositivos. As senhas podem ser alteradas manualmente, ou de forma automática, através do *script* de alteração de senhas. Este campo possui 3 (três) opções de filtro: vermelho, amarelo e verde. Dependendo do tempo em que foi feita a ultima alteração de senha, o campo recebe uma cor diferente. Os prazos que influenciam a marcação por cores, variam de empresa para empresa e das suas respectivas políticas de monitoramento e auditorias.
8) Controle de *healthchecking*: O *healthchecking* é um processo de confirmação, voltado para a verificação da correta funcionalidade do equipamento em monitoramento. Seu funcionamento é planejado conforme as políticas de segurança de cada empresa. A verificação da configuração básica dos equipamentos faz parte desta atividade, assim como o processo de verificação de quantidade de *logs*. Porém, alguns processos ainda precisam ser executados de forma manual, como a verificação das regras permitidas e negadas pelo equipamento. O DBPortal possui um campo para o cadastro da data em que foi realizado este processo, e também permite que o mesmo seja filtrado em vermelho , amarelo ou verde, facilitando assim saber quais equipamentos tiveram seus *healthchecks* efetuados no período acordado.
9) Pesquisa por comandos em configurações: A função de pesquisa por comandos de configurações é uma das funções que mais facilita a vida das pessoas responsáveis pelas auditorias. Esta função permite que os alertas de segurança dos fabricantes de equipamentos possam ser verificados em todos os dispositivos que possuem o *backup* de configuração ativo. Tudo isso em poucos segundos. Caso este processo fosse efetuado de forma manual, o tempo para sua realização poderia ser contabilizado em dias, meses, ou até anos – tudo dependendo da

quantidade de equipamentos a serem verificados. O funcionamento desta característica é bem simples. Devemos apenas informar o comando a ser procurado, e o retorno será de todos os equipamentos que possuem este comando ativo, além do seu modelo e sua versão de software em uso. A obtenção das informações sobre modelo e versão de software é de extrema importância, visto que nem todos os problemas de segurança registrados atingem (ou podem atingir) todos os modelos e/ou versões de software destes equipamentos.

Agregando todas essas nove funcionalidades, podemos expor a estrutura de operação do DBPortal em três módulos funcionais distintos: inventário, controle e backup (Figuras 7, 8, 9 e 10):

1) Inventário: inventário de equipamentos, alteração de senhas de sistema e, pesquisa por comandos em configurações.
2) Backup: backup de configurações, geração de relatório de analise de configuração básica e, geração de arquivo com diferença entre as configurações.
3) Controle: controle de quantidade de logs, controle de troca de senhas e, controle de *healthchecking.*

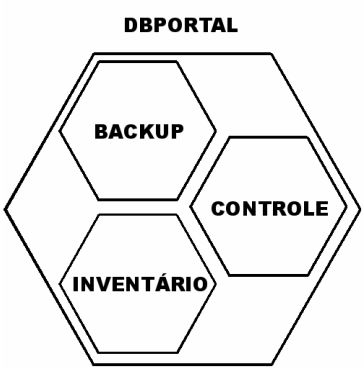


Figura 7 - Apresentação dos três módulos principais do DBPortal.

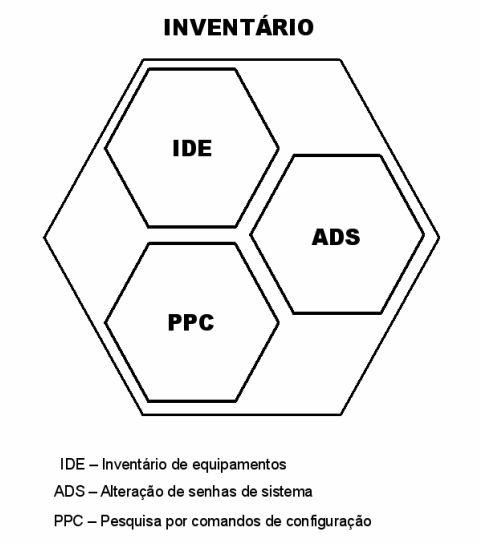


Figura 8 - Módulo de inventário expandido, apresentando seus sub-módulos IDE, ADS e PPC.

G. Entendendo o processo de Backup

Um dos processos mais interessantes que o DBPortal possui é o *backup* de arquivos de configuração de *firewalls*. Cada dispositivo cadastrado no sistema precisa que um conjunto de duas variáveis estejam ativas para assim permitir que o processo de gravação dos arquivos ocorra. A primeira é a variável backupconfig e a segunda é a variável runnow. Por padrão, ambas as variáveis sempre estarão inativas para o dispositivo cadastrado.

O primeiro passo é ativar a variável backupconfig de cada dispositivo. Por padrão, ao cadastrar qualquer dispositivo no DBPortal, essa variável é marcada como OFF. A marcação desta variável para ON deve ser feita sempre de forma manual por um operador no sistema. O segundo passo é ativar a variável runnow, de 0 (zero) para 1 (um). Esse procedimento pode ser feito tanto de forma manual, quanto de forma automática.

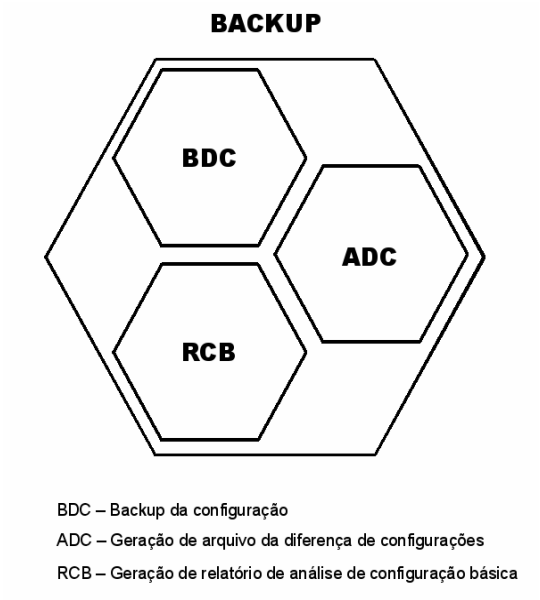


Figura 9 - Módulo de *backup* expandido, apresentando seus sub-módulos BDC, ADC e RCB.

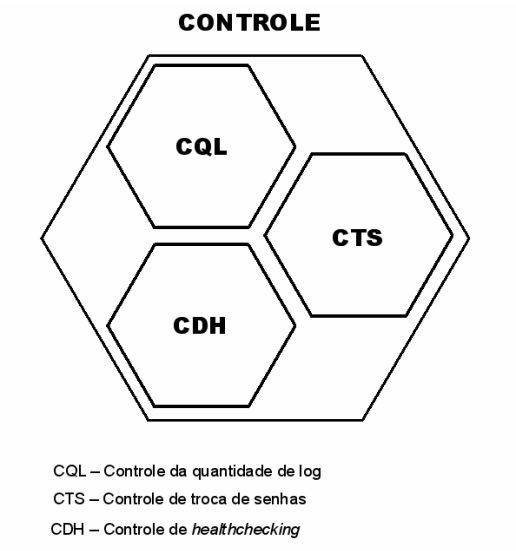


Figura 10 - Módulo de controle expandido, apresentando seus sub-módulos CQL, CTS e CDH.

O DBPortal possui um sistema ativo de *backup* de arquivo de configuração de dispositivos, que é executado de 01 em 01 minuto, de forma contínua e ininterrupta. Mas para que o dispositivo possa ser acessado pelo sistema de *backup*, além da variável backupconfig, a variável runnow também precisa estar ativa.

O processo automático se inicia toda zero hora (0:00) de cada dia, quando o sistema força todos os dispositivos cadastrados que possuam a variável backupconfig em ON, a ter sua variável runnow em 1 (veja Fig. 11)

O processo manual pode ser feito por intermédio de um operador. Um usuário com permissão de alteração das configurações do dispositivo no sistema, pode alterar o valor da variável runnow para 1, de forma manual, efetuando sua ativação. Após essa etapa, o sistema de verificação de dispositivos prontos para *backup* (que está sempre pronto para efetuar *backups* de dispositivos de 01 em 01 minuto) irá identificar o mesmo como READY, iniciando imediatamente o processo de gravação dos seus arquivos de configuração.

A cada minuto o sistema consegue efetuar o *backup* de até 150 dispositivos, de forma simultânea. A quantidade de processos simultâneos através do DBPortal depende exclusivamente da capacidade do servidor onde o sistema está instalado. Basicamente, a capacidade do hardware e a largura de banda da rede.

Após efetuar o *backup*, a variável runnow para aquela máquina voltará a ser marcada como 0. Esse mesmo dispositivo, enquanto estiver com sua variável backupconfig ativa (ON), só poderá passar por um novo processo de *backup*, caso o ciclo de zero hora (0:00) se repita, ou caso neste intervalo de tempo, um operador resolva ativar novamente a variável runwon para esse dispositivo. E durante um dia, de forma manual, uma mesma máquina pode sofrer vários *backups*, se os operadores do sistema assim o desejarem. Tudo depende de seus operadores e da necessidade da empresa com relação aos dados de seus dispositivos em um processo de auditoria padrão.

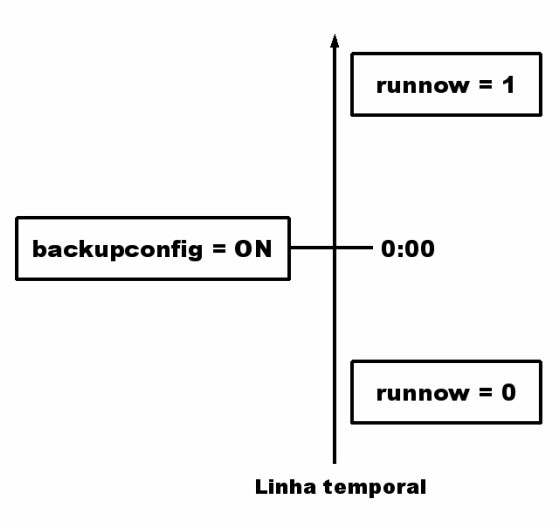


Figura 11 - Sistema automático de *backup* em andamento toda zero hora (0:00) para todos os dispositivos com a variável backupconfig marcadas como ON.

O motivo principal da realização constante de *backups* de arquivos de configuração de dispositivos no sistema está na necessidade de se ter uma cópia dos mesmos para cada equipamento monitorado. Todos os dados são armazenados em disco através do DBPortal. Esse é um procedimento comum em qualquer auditoria de *firewalls*. Em uma auditoria, a companhia sempre precisa conhecer o *status* temporal de todas as alterações nas configurações de seus dispositivos em monitoramento.

Ao ser acionado para realizar o *backup* de um dispositivo, duas situações distintas podem ocorrer durante o processo: o *backup* do dispositivo: ocorrer normalmente, ou acontecer uma falha no processo de *backup*. Se esse foi um *backup* bem sucedido, o sistema irá avaliar se o arquivo de configuração recebido é igual a gravação anteriormente registrada. Através do comando md5sum, o sistema tem como comparar os arquivos entre si – o já registrado no sistema e o recém adquirido pelo procedimento de *backup*.

É importante informar que, antes mesmo de executar quaisquer desses procedimentos de *backup*, a primeira ação tomada pelo sistema é a desativação da variável runnow do dispositivo em interação. Caso os arquivos sejam idênticos, o sistema irá descartar o arquivo mais recente e irá manter o arquivo mais antigo, que já está registrado em disco no DBPortal (veja a Figura

12). O sistema, então, irá registrar a data e a hora da ação na variável lastconfigbackup.

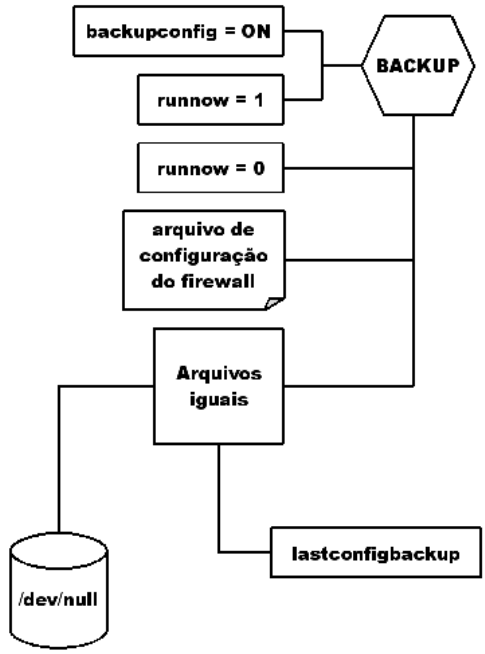


Figura 12 - Procedimento de *backup* onde os arquivos de configuração são idênticos.

Caso os arquivos sejam diferentes, será realizado um DIFF pelo sistema, onde as informações novas serão registradas em azul, e as informações descartadas, serão registradas em vermelho. O sistema então registra a nova configuração em disco. Após o procedimento, o DBPortal registra na variável lastbackupchange, a data e a hora do último *backup*. A data e a hora do processo também são registrados na variável lastconfigbackup (ver Figura 13).

Caso o processo de *backup* falhe, o sistema irá registrar a data e a hora do processo da tentativa de *backup*, tanto na variável lastconfigbackup quanto na lastbackupfailure (veja a Fig. 14). Para este dispositivo, mesmo com a falha no processo de realização de *backup*, o sistema só tentará efetuar um novo procedimento, caso ocorra uma intervenção manual do operador, sinalizando novamente a variável runnow do dispositivo para 1, ou de forma automática no

próximo ciclo de zero hora (0:00), caso o dispositivo ainda possua a sua variável backupconfig ativada.

Todos os dispositivos registrados no sistema possuem uma variável chamada backupfailures. Para todos, ela começa com o valor zero. A cada falha registrada no processo de *backup*, é adicionado 1 ao valor já encontrado nesta variável para esse dispositivo em questão. Esse valor só poderá ser resetado (i. é, voltar a ser zero) caso ocorra um procedimento de *backup* bem sucedido em uma próxima interação.

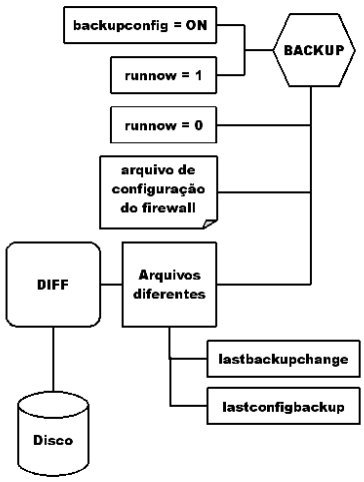


Figura 13 - Procedimento de *backup* onde os arquivos de configuração são diferentes.

Um dos problemas mais comuns para a ocorrência de uma falha no procedimento de *backup* é a falha na comunicação com o dispositivo. As formas mais comuns de ocorrência desse problema são: falha na resposta pelo dispositivo alvo, ou problemas de caminho da rede até o dispositivo. E essas situações são plenamente previstas pelo DBPortal. Veja a Figura 14 para maiores detalhes sobre o procedimento de *backup* quando ocorre uma falha.

Um dado importante a informar é que, independente do processo de *backup* falhar ou não, serão registradas a data e a hora da tentativa de gravação realizada pelo sistema. Essas informações sempre serão registradas no DBPortal, na variável lastconfigbackup. Para interromper os backups diários que se iniciam toda zero hora (0:00), os operadores precisam marcar

manualmente a variável backupconfig para OFF, para cada dispositivo onde a mesma se encontre ativa (ON).

Dentro do sistema DBPortal as variáveis backupconfig e runnow são consideradas variáveis booleanas no sistema de verificação de *backup*. Por segurança, as mesmas são representadas como colunas no banco de dados, dispensando qualquer interação flutuante, apenas em variáveis de memória do sistema em execução.

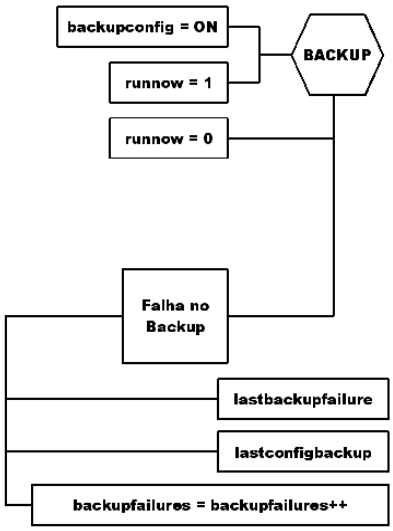


Figura 14 - Procedimento de *backup* não concluído.

O DBPortal é capaz de monitorar milhares de *firewalls* simultaneamente. O sistema permite mostrar todo o seu poder quando instalado para uso em grandes empresas. Nas grandes companhias, cada uma de suas unidades físicas (as mesmas, contendo milhares de *firewalls* cada) poderá estar espalhada por todo o planeta. Nesse tipo de cenário, a administração dos equipamentos no DBPortal é realizada por equipes de trabalhos distintas, separadas por área. Essa logística de operação permite que as equipes de trabalho criadas possam associar grupos de equipamentos para monitoramento local, otimizando assim todo o trabalho de auditoria em empresas desse porte.

A instalação do DBPortal é realizada em um único servidor, e as equipes cadastradas em todo o mundo acessam sua interface gráfica via *Web* para

realizarem suas tarefas. Como mencionado anteriormente, as únicas limitações do DBPortal são: sua capacidade de hardware, e a largura de banda associada para sua operação. Uma empresa de grande porte que queira utilizar o DBPortal para a automatização de seus processos de auditoria deve avaliar essas características físicas para poderem implementar o sistema de forma otimizada, atendendo assim as suas necessidades.

H. Níveis de usuários

O DBPortal possui uma interface desenvolvida para uso com três níveis de usuários distintos: super-administrador, administrador e operador (Tabela 1):

1) Super-administrador: este usuário possui acesso completo as configurações do DBPprtal. O super-administrador é capaz de cadastrar equipamentos, criar grupos de trabalho por área de atuação (envolvendo um grupo regional de equipamentos a serem monitorados), pode criar novos administradores e operadores para o sistema, dentre diversas outras funções.
2) Administrador: o administrador possui poder de gerência local no grupo ao qual é designado para administrar, podendo cadastrar e descadastrar equipamentos para uso local em sua equipe. O mesmo é capaz de adicionar operadores para trabalhar no sistema em sua equipe.
3) Operador: O operador pode trabalhar com o monitoramento de equipamentos locais associados a sua equipe de trabalho. O mesmo é capaz de agendar *backups* para os equipamentos em monitoramento por sua equipe de trabalho.

Tabela 1: Quadro de usuários do DBPortal

	super-administrador	administrator	Operador
Criação de usuários	SIM	SIM*	NÃO
Cadastro de equipamento	SIM	SIM	NÃO
Busca por equipamentos	SIM	SIM	SIM**
Monitoramento de equipes	SIM	SIM***	NÃO

* Capacidade apenas de criar usuários em nível de operador.
** Busca por equipamentos apenas em sua equipe de trabalho.
*** O monitoramento só pode ser realizado em sua equipe de trabalho.

É importante informar que, diante da relação de sigilo contratual existente entre a empresa e o desenvolvedor, o projeto apresentado não permite a divulgação de dados de qualquer natureza neste trabalho.

I. Visão Geral do Funcionamento do DBPortal

O DBPortal possui grande parte dos recursos necessários para o trabalho diário de seus operadores, para a administração, monitoramento e auditoria de *firewalls*. Para facilitar a compreensão de seu funcionamento, será apresentada uma visão geral das principais funcionalidades do DBPortal e sua interface gráfica de operação. Após o operador acessar o DBPortal via login e senha, será carregada na mesma janela, a tela principal do sistema (Figura 15) evidenciando todos os recursos disponíveis para cada tipo de usuário (sendo mais específico, baseado na hierarquia de usuário). No exemplo abaixo a janela mostrará todas as funcionalidades do DBPortal disponíveis já que o *login* foi efetuado por um super-administrador do sistema.

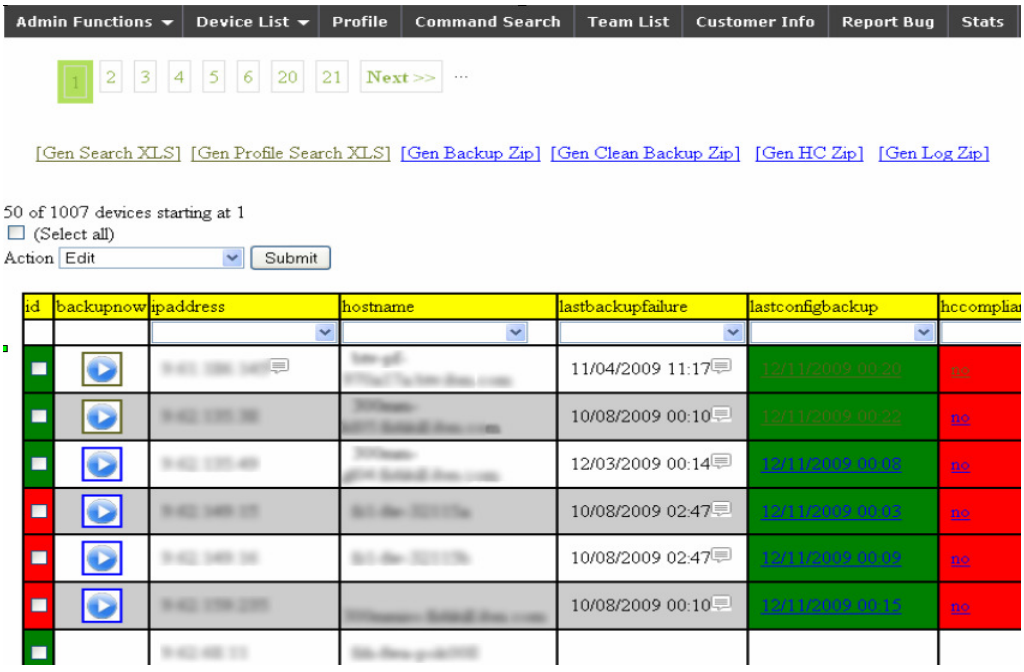


Figura 15 – Janela principal do DBPortal (algumas partes foram omitidas devido à necessidade de sigilo das informações)

No topo da janela encontramos o Menu Principal do DBPortal, com os itens *Admin Functions* (Funções do Administrador), *Device List* (Lista de Dispositivos), *Profile* (Perfil), *Command Search* (Busca por Comandos), *Team List* (Lista das Membros das Equipes, apresentando todas as informações referentes aos membros de cada equipe cadastrada), *Customer Info* (Informações sobre o Cliente), *Report Bug* (Relatório de Bugs) e *Stats* (Estatísticas). Abaixo do menu principal o operador encontra o sistema horizontal de navegação por páginas, onde a primeira página se encontra ativa e as demais navegáveis pelo operador. Por padrão, o DBPortal lista 30 (trinta) dispositivos cadastrados por página. Esse número pode ser facilmente alterado nas configurações de usuário de cada operador através do item de menu *Profile* do sistema. Logo abaixo encontra-se o segundo menu horizontal do DBPortal, com funções específicas de geração de conteúdo e arquivos de interesse para o sistema corrente de auditoria de cada empresa (será explicado em maiores detalhes mais abaixo). A seguir, identificamos a contagem total de dispositivos cadastrados no sistema, e quantos deles estão sendo apresentados na primeira página (*50 of 1007 devices starting at 1*).

Um dos recursos interessantes da interface do DBPortal é a caixa de marcação *Select All*, onde o operador do sistema poderá selecionar todos os dispositivos simultaneamente. Esse tipo de operação, não muito frequente, é uma funcionalidade extra para casos onde o operador precisa trabalhar com todos os dispositivos cadastrados de forma simultânea. Posteriormente, o DBPortal apresenta o seu menu de ação principal para os dispositivos cadastrados que estejam marcados para processamento (será explicado em maiores detalhes mais abaixo) e a listagem dos dispositivos em visualização, no formato de tabela. O sistema de apresentação dos dispositivos apresenta todas as ações e resultados cotidianos que cada operador precisa ter acesso sobre os dispositivos que esteja monitorando em sua equipe. A seleção de cada dispositivo para produção se encontra na coluna *id*. O DBPortal permite o processamento simultâneo de múltiplos dispositivos. Tudo o que o operador necessita é selecionar todos os dispositivos de interesse na coluna *id*. Na tabela de dispositivos destacamos as primeiras colunas:

1. *backupnow*, é apresentada como botões para cada dispositivo, onde o operador poderá ativar o *backup* do arquivo de configuração de cada dispositivo apresentado.
2. *ipaddress*, identifica o endereço de IP de cada dispositivo cadastrado no DBPortal.
3. *hostname*, identifica o nome de host de cada dispositivo cadastrado no DBPortal.
4. *lastbackupfailure*, informa a data e hora da última falha de backup para cada dispositivo.
5. *lastconfigbackup*, informa a data e a hora do último *backup* realizado do arquivo de configuração do dispositivo em questão.

O item *lastconfigbackup* para cada dispositivo é representado na forma de um link. Ao clicar nesse link, o operador poderá acessar o diretório respectivo desde dispositivo (Figura 16).

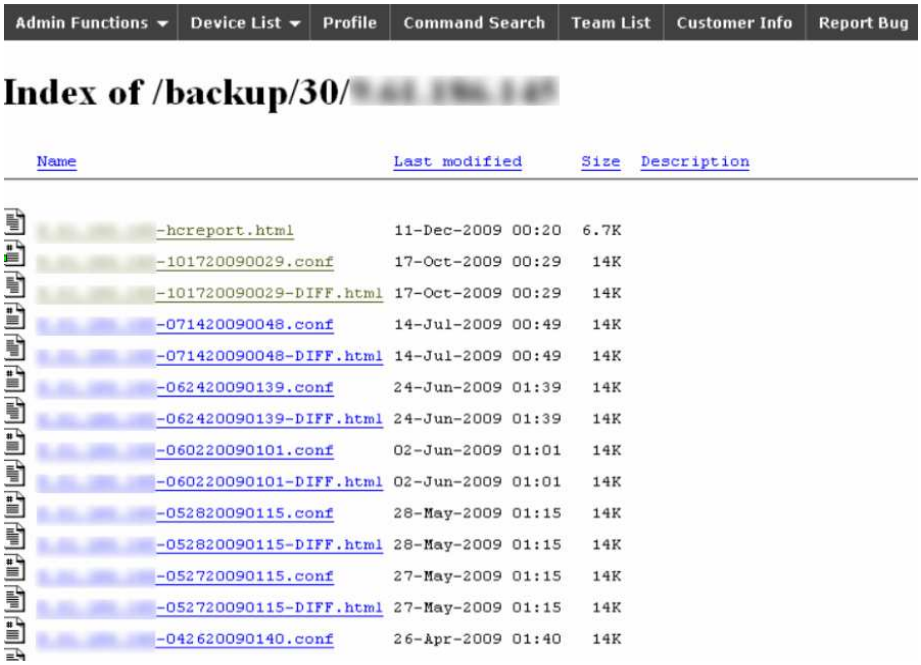


Figura 16 – Acesso ao diretório do dispositivo através do link apresentado para cada dispositivo na coluna *lastconfigbackup* do DBPortal *(algumas partes foram omitidas devido a necessidade de sigilo das informações).*

Nesta listagem de arquivos apresentada pelo diretório do dispositivo selecionado, destacamos os três primeiros. O primeiro arquivo é o HCREPORT (*healthchecking report*). Em formato HTML, esse é o arquivo de *healthchecking*

do dispositivo em questão (Figura 17). O segundo arquivo (*.conf*) é o último arquivo de configuração armazenado como *backup* para esse mesmo dispositivo (Figura 18). E o terceiro e último arquivo em destaque, é o arquivo que efetua o DIFF entre os arquivos de configuração dos dispositivos, caso os mesmos tenham sua configuração alterada ao longo do processamento via operador, durante os processos de *backup* realizados no sistema (Figura 19).

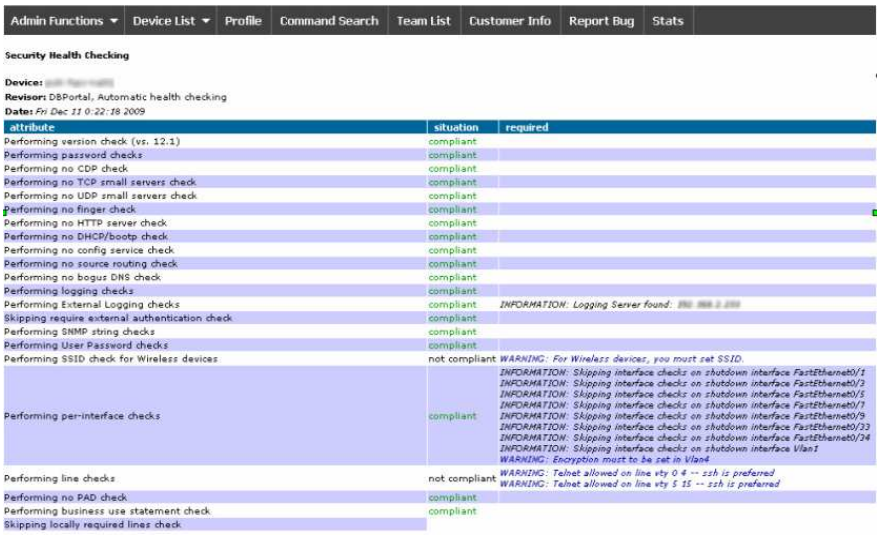


Figura 17 – Arquivo HCREPORT do dispositivo, apresentado em formato HTML o seu healthchecking (algumas partes foram omitidas devido a necessidade de sigilo das informações).

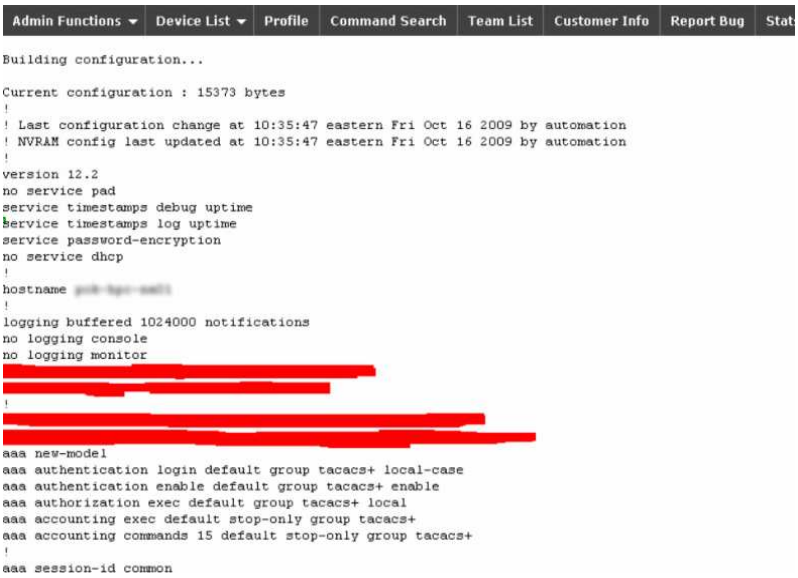


Figura 18 – Arquivo de configuração (formato texto) da última configuração válida do dispositivo cadastrado no DBPortal (algumas partes foram omitidas devido a necessidade de sigilo das informações).

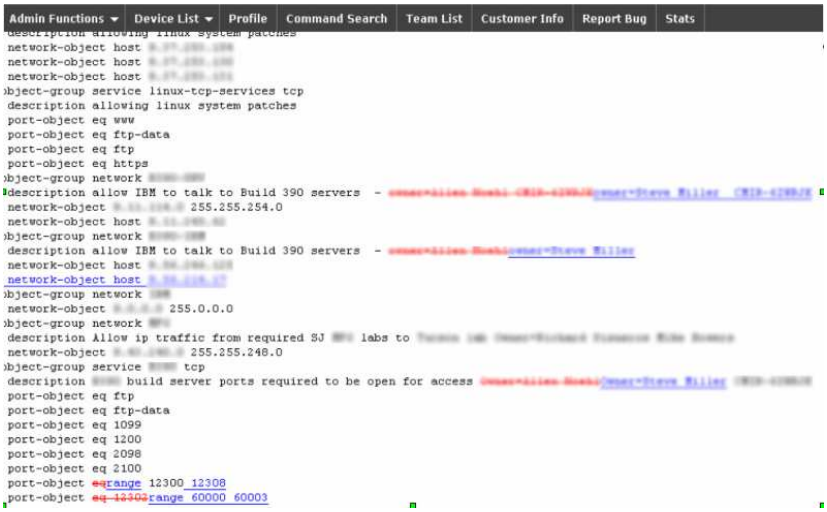


Figura 19 – Arquivo DIFF das configurações registradas em backup do dispositivo cadastrado no DBPortal (algumas partes foram omitidas devido a necessidade de sigilo das informações).

Para atender a todos os requisitos de uma auditoria destaca-se no DBPortal o cadastro do número de dias de *log* necessários para registro no sistema. O operador poderá processar e administrar esse recurso através da coluna *loggingdays* na tabela de dispositivos da tela principal do DBPortal (Figura 20). Como exemplo ilustrativo, o dispositivo registrado nesta figura possui a atividade de manter os seus últimos 05 (cinco) *logs* armazenados. Para acessar maiores informações sobre esses *logs*, o operador poderá clicar no balão de texto que se segue ao registro numérico de dias cadastrados para o armazenamento de *logs.*

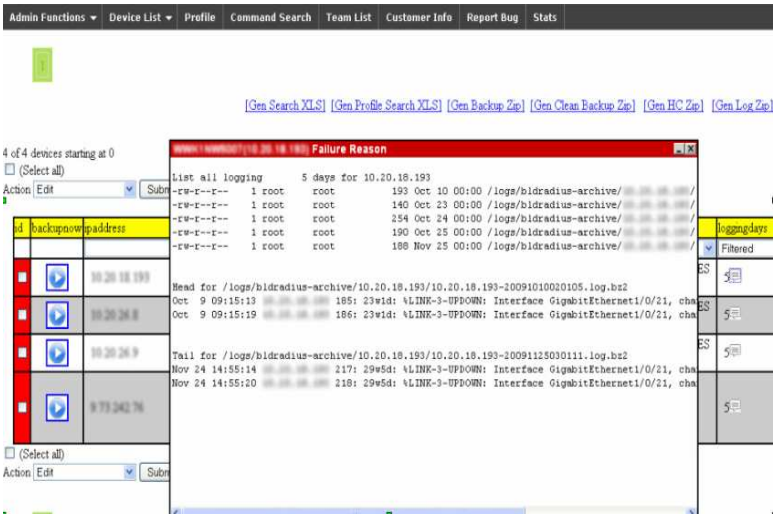


Figura 20 – A coluna loggingdays apresentando a caixa de registro expandida com a quantidade de dias de log para o dispositivo selecionado (algumas partes foram omitidas devido à necessidade de sigilo das informações).

Nesta nova janela, o operador poderá visualizar as informações derivadas da listagem dos últimos cinco *logs* desse dispositivo, o *head* (ou cabeçalho) do primeiro dos arquivos de *log*, e o *tail* (ou rodapé) do último arquivo de *log* do mesmo dispositivo. Esse é um padrão de apresentação de informações referentes à *logs* de dispositivos requeridos em uma auditoria de *firewalls*.

Outro item muito importante em uma auditoria é a exportação de informação em diversos formatos de arquivos. Formatos esses que estão a escolha de cada empresa. O atual DBPortal trabalha com a exportação de arquivos e informações em vários formatos diferentes, dependendo da tipo de informação especificada. Para auxiliar a automação dessa parte de um processo de auditoria extremamente necessária, foi criado o item de menu horizontal secundário. O primeiro item deste menu é o *Gen Search XLS*. O mesmo, efetua a exportação das informações dos dispositivos selecionados via coluna *id*, para o formato XLS da Microsoft™. O arquivo XLS gerado poderá ser utilizado na maioria das versões do aplicativo de planilha da Microsof™, o Excel® (Fig. 21).

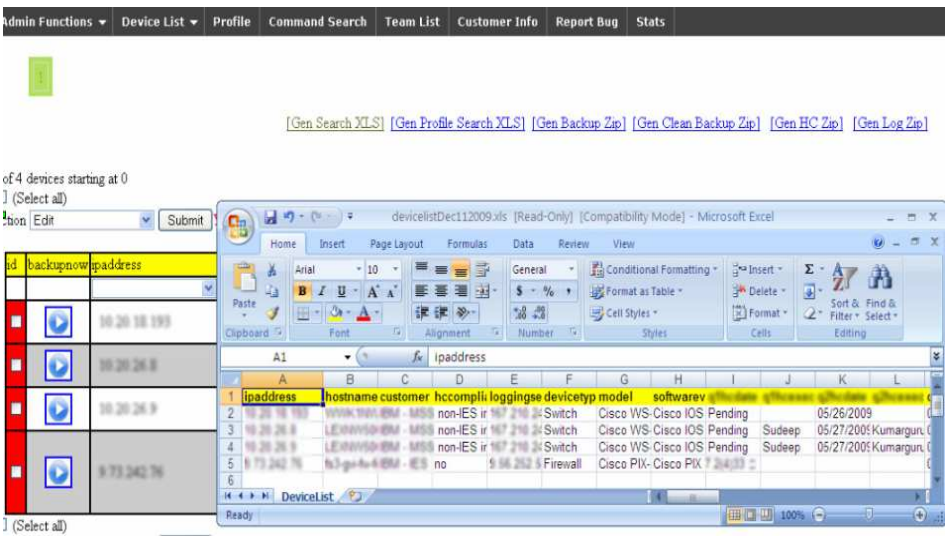


Figura 21 – Uso do item de menu Gen Search XLS, permitindo exportar as informações sobre os dispositivos selecionados para um arquivo no formato XLS (algumas partes foram omitidas devido a necessidade de sigilo das informações).

O exemplo apresentado, mostra a exportação e uso do arquivo XLS contendo todas as informações previamente listadas na tela principal do DBPortal, dos quatro primeiros dispositivos visualizados em tela pelo operador.

O segundo item de menu de importância (em análise) a ser citado é o *Gen Backup Zip*. Esse item é capaz de gerar um arquivo compactado no formato ZIP, dos últimos arquivos de backup para cada dispositivo selecionado (Figura 22).

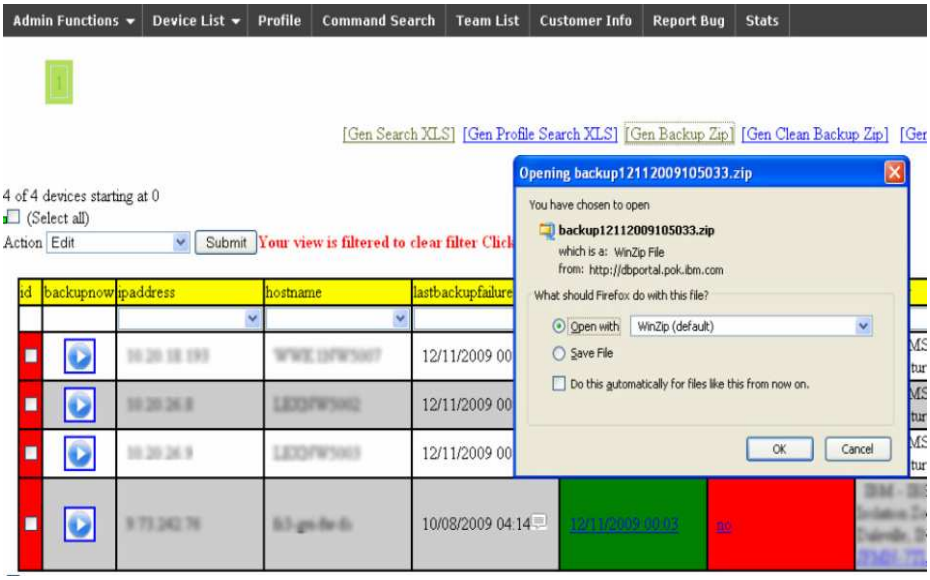


Figura 22 – Através do item de menu Gen Backup ZIP o DBPortal é capaz de gerar um arquivo compactado no formato ZIP, contendo o último arquivo de configuração de backup para cada dispositivo selecionado na tela de operação do sistema (algumas partes foram omitidas devido a necessidade de sigilo das informações).

O exemplo abaixo foi obtido através da seleção dos primeiros quatro dispositivos em tela. A figura mostra inclusive uma janela popup, sob o título *Opening backup12112009105033,zip*, para que o arquivo gerado possa ser salvo pelo operador do sistema.

Ao abrir o arquivo compactado no formato ZIP, é apresentado seu conteúdo constando de quatro arquivos de backup de configuração dos respectivos dispositivos selecionados (Figura 23). Inclusive é demonstrado a abertura de um dos arquivos de configuração e apresentado o mesmo em formato TXT via aplicativo NotePad® da Microsoft™. A seção distorcida da imagem refere-se as senhas desse dispositivo, que por motivos de sigilo, não podem ser apresentadas a público.

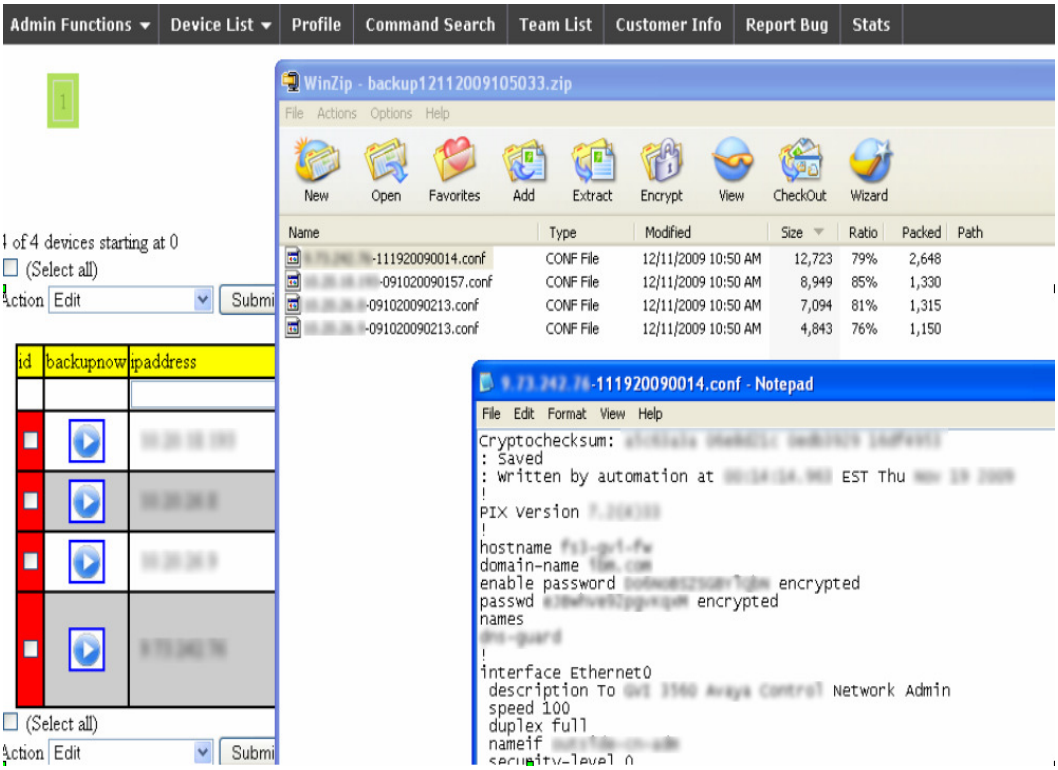


Figura 23 – Apresentação do conteúdo do arquivo compactado contendo os arquivos de configuração, gerados pelo Gen Backup ZIP, dos dispositivos selecionado. Inclusive é exibida a apresentação do conteúdo textual de um dos arquivos de configuração (algumas partes foram omitidas devido a necessidade de sigilo das informações).

A seguir é apresentado o item conjunto de ações do DBPortal através do menu de seleção vertical *Action* (Figura 24), localizado na tela principal da interface do sistema. O menu é composto das seguintes ações:

1) *Edit*, permite a edição das configurações de um dispositivo selecionado (edição individual para cada dispositivo selecionado).
2) *Bulk Action*, permite a edição de mais de um dispositivo selecionado de forma simultânea. É a versão de edição múltipla do item *Edit*.
3) *Copy*, permite a cópia de configuração entre os dispositivos cadastrados no DBPortal, facilitando o processo de administração dos dispositivos com configurações idênticas ou mesmo, semelhantes.
4) *Run Backup Now*, assim como presente na tabela de apresentação de dispositivos cadastrados, esse item permite a execução dos backups dos dispositivos selecionados. A vantagem desta ação é permitir a inicialização de backup de dispositivos simultâneos.
5) *Change Password*, permite a alteração da senha de usuário de acesso

(*access*) e de falha (*failsafe*) dos dispositivos cadastrados. A vantagem desse item no *Action* é a possibilidade de efetuar a alteração simultânea de senhas para todos os dispositivos cadastrados. Funciona como o sistema de *backup*, com o foco na troca de senhas dos dispositivos.

6) *Delete*, permite a deleção de um dispositivo do DBPortal, retirando-o da lista de dispositivos cadastrados no sistema.

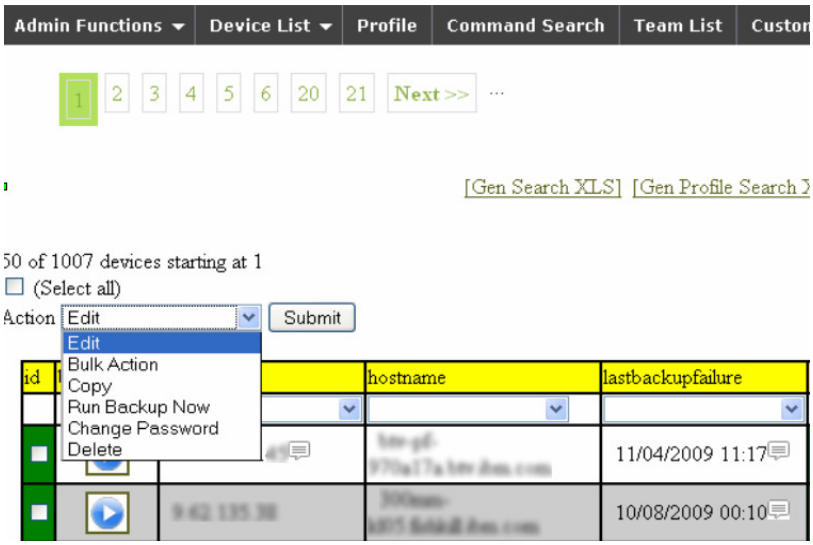


Figura 24 – Exposição dos itens de menu do Action, facilitando o processo de configuração global de dispositivos (algumas partes foram omitidas devido a necessidade de sigilo das informações).

No item *Edit* do menu *Action* o operador pode ter acesso a uma miríade de itens de configuração, todos de extrema importância para uso em auditoria de *firewalls* em grandes empresas (Figura 25). A primeira coluna de itens é a configuração global do dispositivo, onde pode-se ver a equipe responsável pelo equipamento, o IP do dispositivo, seu *host*, cliente, e diversos outros itens de igual importância. A título de sigilo de informação, algumas informações nesta figura foram camufladas.

A edição de configuração do dispositivo é extensa e separada por vários grupos de itens de configuração, como o *Healthchecking*, *Physical Location* (localização física), *Authentication* (Autenticação) e *Automation Settings* (Configurações de Automação).

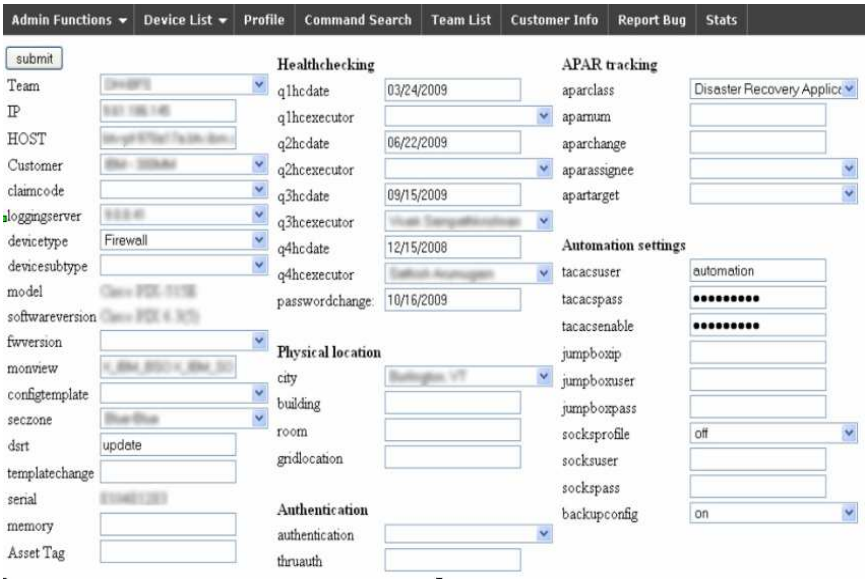


Figura 25 – Exemplo de edição de dispositivo cadastrado (ou a cadastrar) via item Edit do menu Action (algumas partes foram omitidas devido a necessidade de sigilo das informações).

Voltando ao menu principal do DBPortal, temos o item *Profile* (Figura 26). O Profile é onde o operador, independente de seu nível de usuário poderá configurar quais colunas quer ver (primeira coluna da esquerda para a direita) e qual a ordem em que elas aparecerão (segunda coluna). O que o operador estipular no *Profile* refletirá na tela principal do DBPortal. No Profile o operador também poderá atualizar e manter suas informações pessoais como nome, ID, telefone, dentre outros.

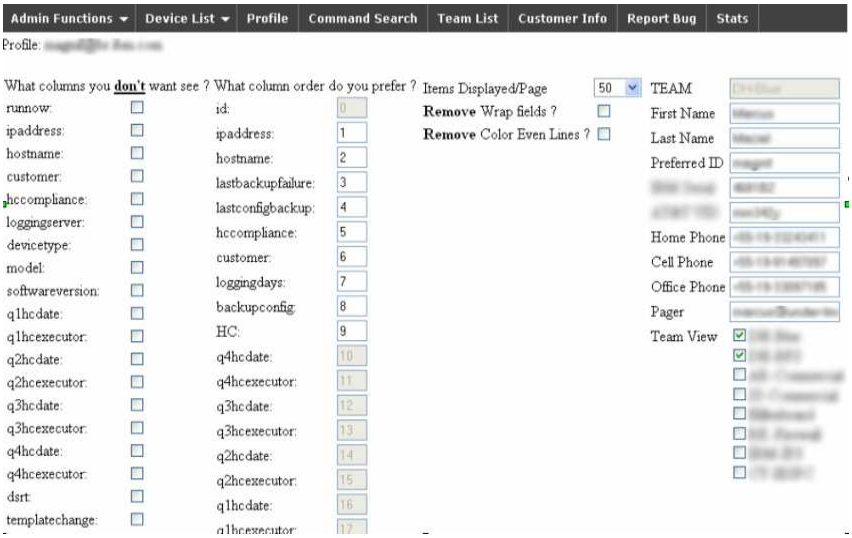


Figura 26 – Item de menu Profile sendo acessado, onde o operador poderá escolher e ordenar as colunas de apresentação dos dispositivos no DBPortal. Ele também poderá atualizar e manter os dados pessoais.

O operador também poderá escolher visualizar as outras equipes registradas no DBPortal, além da sua própria. Para trabalhos que envolvem mais de uma equipe esse recurso é essencial.

O item *Command Search* do menu principal do DBPortal é um dos recursos mais utilizados pelas equipes registradas no sistema (Figura 27). Através desta ferramenta o operador poderá efetuar buscas por comandos dentro dos últimos arquivos de configuração de todos os dispositivos registrados no sistema que estejam sob monitoramento por sua equipe. Essa funcionalidade facilita o trabalho dos operadores em encontrar dispositivos com configurações semelhantes dentro de seu universo de *firewalls* administrados, saber quais possuem determinados serviços habilitados, além de identificar suas vulnerabilidades.

No caso de vulnerabilidades, o operador poderá chegar ao dispositivo-alvo através da busca por comandos. Por exemplo: caso um dispositivo, de um modelo de fabricação e versão de sistema operacional específico possua uma vulnerabilidade na versão 1 do ssh, o operador poderá listar todos os dispositivos que utilizam o ssh versão 1, ao digitar no campo de busca "*ssh version 1*" e clicar no botão *Submit*. Dentre os resultados apresentados (Figura 28) o operador poderá localizar qual dispositivo que ainda utiliza a versão 1 do ssh de determinado modelo e versão de sistema operacional.



Figura 27 – Ferramenta Command Search do menu principal do DBPortal em atividade.

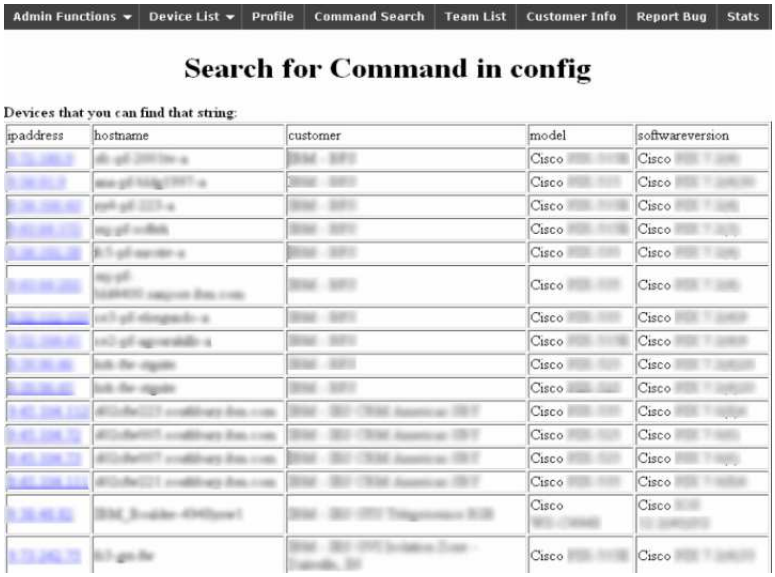


Figura 28 – Resultados da busca pela ferramenta Command Search.

6. Conclusão

O processo de auditoria de segurança em *firewalls* é um procedimento complexo e extenso, que certamente exige muito trabalho de toda uma equipe bem treinada. Este processo envolve a verificação periódica de todos os itens que fazem parte do procedimento de segurança da empresa. Com a utilização do sistema DBPortal estas atividades se tornam muito mais simples e rápidas, além de serem capazes de obter dados mais seguros e precisos, pois diminuem consideravelmente a possibilidade de erro humano em todo o processo. Através do uso do DBPortal a equipe responsável pelas auditorias é capaz de obter respostas em um curto intervalo de tempo, se comparado a um processo de intervenção manual.

O DBPortal, aparentemente, é uma ferramenta única no que se propõe. Suas funcionalidades não foram encontradas em nenhum outro software no mercado ou mesmo em projetos de software livre disponíveis ao público. Essa ferramenta pode ser utilizada para inventário de equipamentos de rede, monitoramento de alterações de modelo, versão, nº. Serial e configurações desses dispositivos, além de auxiliar as auditorias com um repositório de

informações afins. em uma rede empresarial. Porém seu foco atual é a auditoria de segurança de *firewalls* Cisco.

Referências

[1] SCHMIDT, P.; SANTOS, J. L.; ARIMA, C. H. Fundamentos de auditoria de sistemas. São Paulo: Atlas, 2006.

[2] LYRA, M. R. Segurança e auditoria em sistemas de informação. Rio de Janeiro: Ciência Moderna, 2008.

[3] MITNICK, K. D.; SIMON, W. L. The art of deception: controlling the human element of security, ISBN: 85-346-1516-0, Pearson Makron Books, 2003.

[4] COOK, B. Fortigate-60 Firewall Security Audit: An Auditor's Perspective, https://it-audit.sans.org/community/papers/fortigate-60_firewall_security_audit:_an_auditors_perspective_178, Acessado em 16 de nov. 2009.

[5] YUEN, R. W. Auditing a Cisco PIX firewall: An Auditor Perspective, https://it-audit.sans.org/community/papers/auditing_a_cisco_pix_firewall:_an_auditor_perspective_70, Acessado em 16 de nov. 2009.