ISSN 2238-2011

MUNDO TECNOLÓGICO

Faculdade Norte Capixaba de São Mateus – UNISAM
v. 1 n. 1 julho/dezembro – 2011 - Semestral

Endereço para correspondência
Rod. Othovarino Duarte, s/nº, Bairro Park Washington,
São Mateus-ES, CEP.: 29930-000
e-mail: oliviad@unisam.edu.br

M965 Mundo Tecnológico/ Faculdade Norte Capixaba de São Mateus – v.1, n.1, 2011 – São Mateus:UNISAM, 2011.

Semestral
ISSN 2238-2011

1. Pesquisa acadêmica – periódicos. 2. Gestão. 3. Exatas. I. Faculdade Norte Capixaba de São Mateus

CDD 001.891
CDU: 001.891(05)

EDITORIAL

A revista científica Mundo Tecnológico é uma iniciativa da Faculdade Norte Capixaba de São Mateus que possibilita a divulgação de artigos e resumos de contribuições relevantes para a comunidade científica das diversas áreas de estudo que abrange a Instituição. Portanto, trata-se de um veículo de publicação acadêmica semestral, cujo público-alvo são professores e alunos de graduação e pós-graduação.

Diante disso, a Instituição almeja que a revista científica Mundo Tecnológico contribua para o fomento contínuo da prática da investigação, e promova o crescimento educacional.

MUNDO TECNOLÓGICO

SUMÁRIO

A R T I G O S

ISSN 2238-2011

ERP – ENTERPRISE RESOURCE PLANNING
UMA ABORDAGEM AOS SISTEMAS DE GESTÃO INTEGRADA

Alessandro José Ventorin [1]

RESUMO

Um mundo turbulento, em constante mutação, tem exigido dos administradores uma postura cada vez mais estratégica e preparada. A falta de informações consolidadas e com agilidade trazem grande defasagem às empresas com relação à disputa existente no mercado, problemas estes, que afetam a agilidade do processo decisório e empobrecem o embasamento do planejamento estratégico de uma organização. O avanço da tecnologia tem trazido muitas oportunidades e desafios aos administradores. O surgimento dos sistemas ERP (Enterprise Resource Planning) ou sistemas de gestão integrada que hoje são a coqueluche das grandes corporações têm surgido como uma forma de resolver tais problemas e integrar de vez todos os diversos processos de uma empresa. O estudo em questão apresenta uma série de resultados positivos e benefícios a serem obtidos com a adoção desses sistemas. Porém, as dificuldades a serem enfrentadas e a profundidade das mudanças a serem realizadas levantam dúvidas com relação à sua adoção, principalmente por parte de pequenas empresas, que não possuem tantos recursos para investimentos em tecnologia. Este artigo teve por objetivo fazer uma revisão de literatura abordando o conceito e as principais características de um sistema de gestão integrada.

PALAVRAS-CHAVE: Software, informação, automação empresarial.

ABSTRACT

A turbulent world, in constant mutation, has required from administrators a strategic and prepared behavior. The lack of agile and consoled information causes great loss to companies with agile process and gets poor the strategic planning of a organization. The technological advance has caused much opportunity and challenge to administrators. The appearance of ERP systems (Enterprise Resource Planning) or systems of integrated management that nowadays are a model of the great corporations has appeared like a way to solve the problems and to integrate the different processes of a company. This study shows some positive results and benefits that can be obtained with the adoption of these systems. However, the next difficulties and the important changes causes doubts with relation to the adoption, mainly to short companies that don't have so many resources to invest in technology. This article had as objective to do a review of literature, dealing with concepts and mainly characteristics of a system of integrated management.

Keywords: Software, Information, Business Automation.

[1] Tecnólogo em Processamento de Dados, Especialista em Administração de Sistemas de Informação e Docência do Ensino Superior, Coordenador do Núcleo de Processamento de Dados e Professor das Disciplinas de Análise de Sistemas, Linguagem e Técnicas de Programação e Sistemas de Informações Gerenciais do Grupo UNIVIX.

1 INTRODUÇÃO

O mundo atual contracena com um cenário sob constante mutação, de grandes avanços e descobertas, alavancado principalmente pela globalização e pelas novas tecnologias de telecomunicações, acarretando uma forte competição, que tem forçado as pessoas e organizações a assumirem novas posturas perante tais inovações.

Uma das mudanças mais importantes e significativas para as organizações nas últimas décadas foi a transição de uma economia industrial para uma economia baseada na informação. Afinal, estamos na "era da informação". Nunca o mundo produziu ou teve a sua disposição tanta informação como nos últimos anos, a maior parte, devido ao avanço da tecnologia.

De acordo com MCGEE, a informação passou a ser o principal fator criativo de riquezas e prosperidade, e que, nesse tipo de economia, o sucesso é determinado pelo que você sabe e não pelo que você possui. Gates (1999) também destaca o alto valor estratégico da informação e diz que a forma como uma empresa reúne, administra e utiliza a informação determina se vencerá ou perderá.

A informação é matéria-prima básica para algumas das funções do administrador, como a tomada de decisão, o planejamento, a verificação das estratégias, dentre outras. Tomar uma decisão sem baseá-la em informações é não ter "nenhuma" chance de obter êxito. A necessidade de informações exatas, consolidadas e com maior agilidade fica então evidente, para que organizações e administradores possam responder às exigências cada vez maiores de seus clientes e fornecedores, e com capacidade de competir em igualdade de condições com seus concorrentes.

Portanto, o administrador tem buscado alternativas que otimizem o desempenho empresarial, com ênfase na agilidade da seleção e disponibilização das informações necessárias ao planejamento estratégico e à tomada de decisões. Dentro desse contexto, destaca-se o papel da tecnologia, que auxilia no armazenamento, processamento e disponibilização de grandes volumes de informações, se tornando uma importante e necessária aliada no dia a dia das organizações.

As organizações têm utilizado cada vez mais a tecnologia como apoio para enfrentar o desafio de captar, filtrar, armazenar, processar e disponibilizar tais informações com velocidade para municiar o processo decisório de seus administradores e gerentes.

Os sistemas de informações, que de acordo com Alves (2004), são sistemas que utilizam processos de coleta e tratamento de dados, gerando e disseminando as informações necessárias aos diversos níveis e processos organizacionais, e consistem em organizar esforços para prover informações que permitam a uma empresa decidir e operar, surgiram para resolver o problema da informação dentro das organizações.

Mas tais sistemas levaram todos a um problema típico, que é a fragmentação de informações. Diversos pequenos sistemas (softwares) que compõem um sistema de informação tornam muito difícil uma consolidação de informações, pois cada aplicativo tem suas características e seu banco de dados isolado dos demais. A gestão moderna de

uma empresa exige cada vez mais informações consolidadas para uma análise global da situação organizacional e respectivamente uma reação fundamentada sobre os fatores implicativos ao desempenho produtivo, financeiro, de relacionamento com o cliente, dentre outros.

Uma solução para esse problema, que as grandes corporações utilizam a algum tempo e que vem crescendo também entre as pequenas empresas do mundo moderno são os chamados Sistemas de Gestão Integrada, mais conhecidos como ERP (Enterprise Resource Planning).

Estes sistemas são mais robustos que os atuais sistemas de informação, e têm o objetivo de integrar todas as funções da empresa num único grande sistema que utiliza um banco de dados que armazena todas as informações captadas. Isso possibilita aos administradores obterem informações consolidadas e centralizadas, em tempo real, de todas as atividades da empresa, o que possibilita uma gestão mais eficiente e uma capacidade maior de responder às mudanças constantes. Eles também modificam completamente a cultura organizacional, transformando todas as atividades e processos de negócios.

Este artigo tem com objetivo conceituar e detalhar melhor as características do ERP. Fazer uma revisão de literatura que esclareça e descreva todos os benefícios e problemas encontrados durante seu ciclo de vida e sua adoção. Que descreva melhor suas vantagens e facilidades, e mostre realmente qual a verdadeira função do ERP dentro do contexto empresarial.

Um outro ponto que motivou este trabalho é que há uma forte tendência para um crescimento da utilização de sistemas de gestão integrada pelas pequenas empresas, visto que a tendência de seu custo é cair, pois o mercado do ERP entre as grandes corporações já começa a saturar. Outro motivo que eleva a possibilidade de utilização do ERP é essa tendência natural de integração que cresce a cada dia e faz com que empresas e pessoas tenham que se atualizar. Os sistemas isolados evoluíram para sistemas de informações, e estes, consequentemente evoluirão ou serão substituídos, se tornando futuros ERP’s.

2 REFERENCIAL TEÓRICO

De acordo com Alves, Zambalde e Figueiredo (2004, p. 25) Enterprise Resource Planning (ERP) ou sistema integrado de gestão empresarial “é a tentativa de integrar todos os departamentos e funções de uma organização num único sistema informatizado, que consiga servi-los de forma eficaz”.

Um outro conceito, apresentado por Bogui (2002, p. 35) diz que um ERP é um “conjunto de soluções que possibilita o planejamento e acompanhamento financeiro, logístico e produtivo de uma empresa, de forma integrada e interativa”.

Pode-se dizer então que “ERP” representa um grande sistema composto por diversos módulos que automatizam as mais diversas tarefas de uma organização. É um pacote de

softwares de negócios que permite a uma empresa automatizar e integrar a maioria de seus processos de negócios.

O ERP pode auxiliar o gestor de uma empresa nas principais fases de seu negócio, como desenvolvimento de seus produtos, manutenção de seus estoques, ligação com seus fornecedores, nos serviços oferecidos aos seus clientes ou até mesmo na gestão de recursos humanos (SOUZA, 2004).

A ênfase principal do ERP é prover aos administradores uma gestão integrada de todas as áreas da empresa, com foco principal no fluxo de informações necessárias à tomada de decisão e ao planejamento estratégico. A utilização de um ERP, de acordo com Souza (2004, p. 85) "otimiza o fluxo de informações e facilita o acesso aos dados operacionais, favorecendo a adoção de estruturas organizacionais mais achatadas e flexíveis". Completa ainda dizendo que os sistemas de gestão integrada favorecem a tomada de decisão com base em dados, que refletem a real situação da empresa, por estarem centralizados num único banco de dados.

Um sistema ERP utiliza ou está integrado a uma base de dados relacional (banco de dados). O seu conjunto de softwares emprega a tecnologia cliente/servidor, que indica que um usuário (cliente) utiliza um software que acessa os dados que estão centralizados em uma única base de dados (servidor). Isso evita inconsistências e redundância de informações, assegurando a integridade dos dados e facilitando o trabalho de gerenciamento do banco de dados, além de prover informações atualizadas em tempo real a qualquer parte da organização.

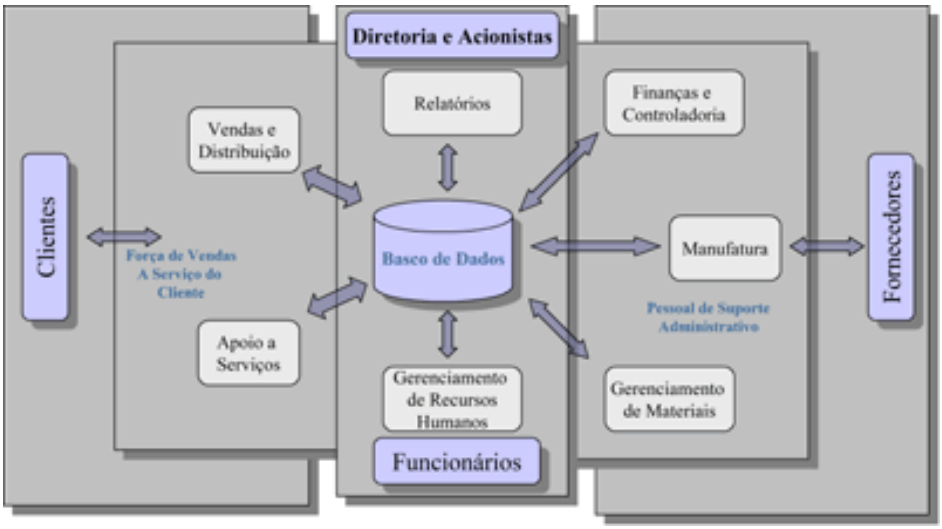


Figura 1 - Estrutura típica de um sistema ERP
Fonte: Adaptado de Souza, 2004.

Mas o que leva uma empresa a adotar um ERP? De acordo com Souza (2004. p. 92) os principais motivos que levam uma empresa a usar o ERP são os seguintes:

- Permanecer competitivas;
- Melhorar a produtividade e a qualidade dos serviços oferecidos aos clientes;
- Reduzir custos, estoques;
- Melhorar o planejamento e alocação de recursos.

Alvesm Zambalde e Figueiredo (2004) também relacionam três principais razões para a empresa recorrer a este tipo de solução:

- Para integrar dados financeiros – os dados sobre receita, fornecidos pelos diversos setores da empresa, apresentam sempre divergências. O departamento financeiro tem seus dados relativos às receitas, a seção de vendas possui dados diferentes. Isso dificulta um entendimento por parte da administração. O ERP pode resolver esse problema;
- Para padronizar processos de produção – as empresas possuem diversos sistemas em seus setores que possuem quase a mesma função. Utilizar um único sistema poderia integrar os processos, poupando tempo e aumentando a produtividade;
- Para normalizar a informação sobre recursos humanos – em empresas que possuem diversas unidades de negócios, ocorre a falta de um método padronizado para acompanhar os empregados e fornecer-lhes informações sobre eventuais serviços e benefícios.

De acordo com Souza (2004), os componentes típicos de um sistema ERP, ou seja, suas principais áreas de automação por seus módulos, são as seguintes:

- Finanças;
- Contabilidade;
- Planejamento e controle de produção;
- Recursos humanos;
- Custos;
- Vendas;
- Marketing;
- Dentre outros.

Para se ter uma idéia, de acordo com Bogui (2002), o ERP gerencia: contas a pagar e receber, ativos fixos, gestão de recursos disponíveis, controle de custos, cria cronogramas de produção, automatiza a entrada e o processamento de pedidos, gerencia estoques, monitora custos de projetos, administra acordos, contratos, clientes, dentre outros.

Bogui (2002) aponta também, algumas descobertas no ERP identificadas por empresas que já aderiram ao sistema:

- Traz benefícios estratégicos e táticos significativos;
- Traz benefícios inesperados;
- Permite decisões melhores e mais rápidas;
- Funciona como espinha dorsal para novas funcionalidades;
- O foco de preocupações muda após a entrada em produção;
- Um projeto de ERP é principalmente um projeto de pessoas;
- Empresas bem sucedidas aceleram, maximizam e mantêm os benefícios do ERP.

Mas então por que todas as empresas não adotam um ERP para gerir seus negócios? A resposta é a seguinte: o alto custo das soluções existentes no mercado aliado à complicada tarefa da radical mudança na cultura organizacional de forma geral fazem com que uma empresa tenha a necessidade de pensar muitas vezes e se planejar muito bem antes de partir para a implantação de um sistema de gestão integrada.

De acordo com Oliveira (2000), para se investir em um ERP, antes de mais nada, é preciso saber exatamente qual a verdadeira necessidade que a empresa possui e delimitar muito bem quais os objetivos a serem atingidos com a nova ferramenta. Apenas empresas que planejam adequadamente um sistema complexo como este vão conseguir ser bem sucedidas. Para as empresas que se aventurarem sem planejamento, metas, prazos e investimentos bem dimensionados, a chance de insucesso é bem grande.

Oliveira (2000) afirma que um projeto de implementação de um sistema de gestão integrada afeta todas as áreas da organização para que se tenha seu objetivo atingido. Para muitas empresas, talvez esse seja o maior projeto em que já se envolveram. Elas devem ser apoiadas por consultores, pessoas da área com experiência em projetos desse nível, que possam dar segurança e conselhos aos investidores.

De acordo com Souza (2004, p. 101), "a decisão de implantação de um sistema ERP só deve ser tomada, após uma análise detalhada dos processos da empresa e das funcionalidades dos sistemas ERP". Isso é necessário porque, na implantação de um ERP, a customização é evidente, entre ambas as partes, os requisitos da empresa e as funcionalidades do sistema, ou seja, é necessária uma mudança de cultura organizacional para que esta adapte seus processos de negócios ao novo sistema, caso contrário, a experiência não será bem sucedida. "Na maioria das vezes, os processos de negócios das empresas precisam ser redefinidos para que seus requisitos se aproximem das funcionalidades do sistema". Outro fator decisivo na implantação é o custo de um ERP, que ainda é muito alto, sendo acessível a poucas empresas.

Assim, antes de iniciar um projeto de implantação de um ERP, a empresa deve estar consciente da necessidade de mudança e da dificuldade e esforços para que tais mudanças aconteçam. Oliveira (2000) comenta: "Não estamos falando de implementar um simples pacote de aplicativos, mas de afetar significativamente todos ou quase todos os processos de negócios".

Portanto, a primeira fase da implantação seria definir quais módulos seriam instalados. Por estar justamente divido em módulos, a empresa tem a facilidade de escolher somente as áreas que necessite automatizar, podendo posteriormente continuar com o projeto em outras áreas ou atividades, possibilitando uma implantação gradativa.

Oliveira (2000) expõe alguns fatores críticos para se obter sucesso na implantação de um ERP:

- Ter visão dos negócios e comprometimento da alta administração;
- Selecionar cuidadosamente um sistema que mais se encaixe às necessidades da empresa;
- O software de gestão empresarial será a base dos sistemas aplicativos;

- Prazos condizentes com a realidade;
- Quanto menos rebuliço na organização, melhor;
- Comprometimento da empresa com a solução;
- Equipe altamente qualificada;
- Não fazer tudo ao mesmo tempo, implementar gradualmente;

De acordo com Oliveira (2000), existem muitas questões sobre a implantação de um ERP a serem discutidas, como infra-estrutura tecnológica, metodologia de desenvolvimento dos trabalhos, ferramentas de suporte ao projeto, estratégia de implementação, o problema da migração de dados dos aplicativos antigos, dentre outros pontos. Mas umas das questões mais importantes sem dúvida nenhuma é a equipe do projeto. Ela é formada por consultores e especialistas externos, pessoal de informática e usuários internos. Veja na figura a seguir, como funciona a estrutura organizacional do projeto:

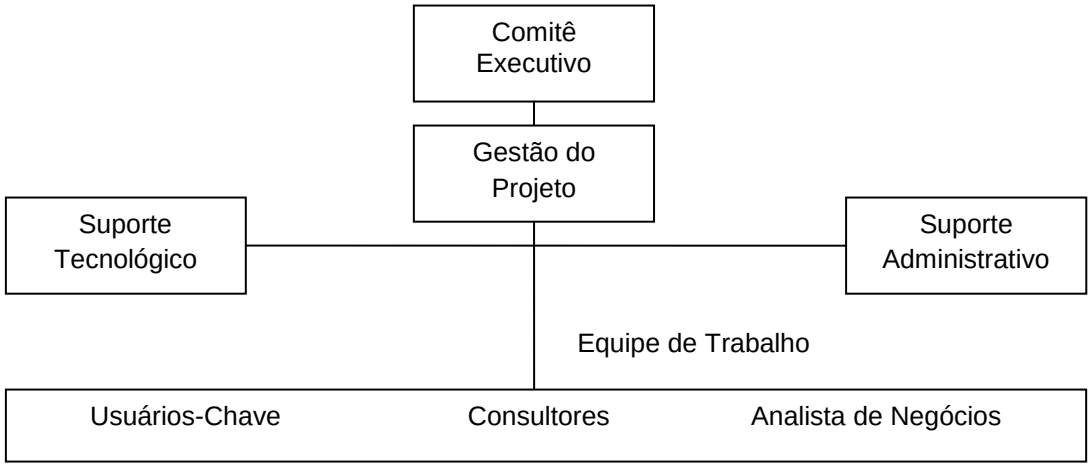


Figura 2 - Implementação de um sistema de gestão integrada – Organização Básica
Fonte: Oliveira, 2000.

- Comitê executivo – representantes da alta administração da empresa, responsável por avaliar o andamento do projeto, aprovar os resultados intermediários, prover recursos necessários para a execução dos trabalhos, etc.;
- Gestão do projeto – formada por profissionais de consultoria e um "coordenador interno" que será responsável pela condução dos trabalhos programados;
- Equipe de trabalho – pessoas que vão trabalhar diretamente mas tarefas previstas no programa de trabalho, desde levantar informações com os usuários até acompanhar o início do processamento com o novo sistema;
- Usuários-chave – são os usuários do futuro sistema e vão definir como o sistema vai funcionar em todos os seus detalhes;
- Analista de negócios – são profissionais de informática da empresa que podem facilitar o trabalho dos consultores no levantamento e entendimento da situação atual;
- Suporte tecnológico – ambientes de processamento de dados que ajudam a desenvolver aplicativos e sistemas para redução de custos e auxílio na migração dos dados dos aplicativos.

Oliveira (2000, p. 76) diz que a implementação de um ERP pode ser problemática. “Leva-se muito tempo, é cara e não traz os benefícios de competitividade e redução de custos que promete”. Ele diz que 70% dos casos não atingem as metas corporativas estabelecidas.

Mas em algumas empresas o ERP funcionou. A Chevron Corporation conseguiu reduzir seus custos de compras em 15% e promete mais 10% num futuro próximo. Houve redução de tempo necessário para atualizar os cálculos de preços dos produtos da International Business Machines Storage Products. Com redução de estoques a Autodesk Inc. conseguiu economizar o suficiente para pagar toda a implementação do sistema (OLIVEIRA, 2000)

Então qual são os problemas do ERP? De acordo com Oliveira (2000), as dificuldades do ERP se dividem em duas questões: a primeira diz que a empresa não faz as escolhas estratégicas necessárias para configurar os sistemas e os processos e a segunda diz que o processo de implementação escapa do controle da empresa de forma natural. “Isso é inerente ao processo de implementação do ERP”.

3 METODOLOGIA

As informações para realização deste trabalho foram obtidas através de pesquisa bibliográfica, baseando-se nas literaturas citadas no capítulo 6.

O foco principal foi voltado para informações que esclarecessem o conceito dos sistemas de gestão integrada (ERP), suas características, seus problemas e demais informações que fossem encontradas.

Partindo desse ponto, o estudo foi desenvolvido com base nas dificuldades para se implantar tal sistema, nos benefícios trazidos com a implantação do ERP, na implantação propriamente dita, dentre outros.

4 RESULTADOS E DISCUSSÃO

Com a crescente necessidade pelo controle de métodos e de informações, os ERP´s surgiram como soluções aplicáveis para suprir a necessidade das organizações.

Diante do estudo feito, nota-se que o ERP é uma importante ferramenta para o processo decisório, para automação da produção, para centralização e disseminação do conhecimento, para redução de custos, dentre outros.

Mas cabe ressaltar também, que a empresa deve estabelecer um planejamento para a implantação de um sistema de gestão integrada, e verificar se há realmente necessidade de se adquirir um ERP ou há apenas a necessidade de um sistema de informação em determinada área. A empresa deve estar consciente sobre a mudança organizacional e a quebra de paradigmas que está para acontecer.

O alto custo de um ERP também deve ser levado em consideração, analisando o custo/benefício e qual a chance de sucesso na implantação e na obtenção do resultado esperado. É necessário alinhar os objetivos da organização ao novo sistema em questão.

Mas diante de tudo isso, a primeira coisa a rever, é que o software tem que ser encarado como solução e não como premissa. E depois devemos refletir que sua utilização não será responsável por todas as operações necessárias para o funcionamento da empresa, mas a deixará preparada para novas funcionalidades e que, essas sim, trarão diferenciais competitivos.

Talvez uma existência de resposta para a implantação de um sistema ERP, esteja no alinhamento dos objetivos da empresa. Estabelecer regras que garantam que o ERP deva reduzir custos, aumentar o fluxo de caixa ou incrementar o faturamento pode ser uma solução para a aceitação destes sistemas como preparadores do diferencial competitivo.

5 CONCLUSÃO

Através deste estudo, pode-se concluir que um ERP, ou sistema de gestão integrada, é um pacote de softwares que vai automatizar de forma integrada todos os processos de negócios de uma empresa. Por ter um banco de dados que centraliza todas as informações, favorece a consolidação, confiança e agilização na disponibilização das informações úteis ao processo decisório, podendo ser acessadas de qualquer nível da hierarquia organizacional.

O ERP também favorece a reengenharia dos processos organizacionais e a disseminação da informação e do conhecimento a quem deles precisar.

O seu alto custo e a sua exigência de modificação na cultura das organizações são características que dificultam sua adoção, principalmente por empresas de pequeno porte.

Mas quando existe planejamento e dinheiro para se investir, verificamos que o ERP realmente traz benefícios incalculáveis.

REFERÊNCIAS

1. ALVES, R. M; ZAMBALDE, A. L; FIGUEIREDO, C. F. **Sistemas de informação**. Lavras: UFLA/FAEPE, 2004.

2. BOGUI, Cláudio; SHITSUKA, Ricardo. **Sistemas de informação**: um enfoque dinâmico. São Paulo: Érica, 2002.

3. GATES, Bill. **A empresa na velocidade do pensamento:** com um sistema nervoso digital. São Paulo: Companhia das Letras, 1999.

4. OLIVEIRA, Jayr Figueiredo de. **Sistemas de informação**: um enfoque gerencial inserido no contexto empresarial e tecnológico. São Paulo: Érica, 2000.

5. SOUZA, Reginaldo Ferreira. **Sistemas integrados e comércio eletrônico**. Lavras: UFLA/FAEPE, 2004.

A PRODUÇAO DE ETANOL NO BRASIL E SUAS OSCILAÇOES

Ana Carolina Rocha Dos Santos Ferri[2]
Cecilia Ferraz Dos Santos[3]
Dalvaci Quirino Santos[4]
Mayara Vargens Cardoso[5]
Melanie Nicco Marchiori[6]

RESUMO

A crise do petróleo na década de 70 provocou uma instabilidade e insegurança no mercado energético do país e do mundo. Desde então a busca por fontes alternativas de energia vem se tornando cada vez mais necessária. Nesse cenário, o Brasil se destaca pelo domínio da produção de etanol, utilizando o caldo da cana de açúcar, chamada de bicombustível de primeira geração, obtido através do processo de fermentação. E ainda existem estudos para a obtenção do álcool através da celulose (bagaço da cana de açúcar),chamado de segunda geração. No entanto ainda existe toda uma especulação em torno dessa produção de etanol e destino final desse produto, seja pela questão da crise dos alimentos em 2008, onde especialistas apontaram a produção de etanol como uma das principais causas ao comprometimento da produção de alimentos ou as oscilações no preço do etanol. Visto toda essa problemática esse artigo propõe uma discussão para essas oscilações no mercado alcooleiro do país.

Palavra-chave: Álcool, preço, produção.

ABSTRACT

The oil crisis in the 70s led to instability and insecurity in the energy market of the country and the world, since the search for alternative energy sources is becoming increasingly necessary. In this scenario, Brazil stands out for the field of ethanol production using sugar cane juice, called first-generation biofuel obtained through the fermentation process. And there are studies to obtain alcohol through the pulp (bagasse from sugar cane), called the second generation. However there is still all speculation around that ethanol production and disposal of this product, is the issue of food crisis in 2008, where experts identified the production of ethanol as a major cause of impairment to the production of food or the oscillations the price of ethanol. Since all these problems this paper proposes an argument for these oscillations in the alcohol market in the country.

Keyword: Alcohol, price, production.

[2] Aluna do curso de Petróleo e Gás da Faculdade Norte Capixaba de São Mateus
[3] Aluna do curso de Petróleo e Gás da Faculdade Norte Capixaba de São Mateus
[4] Aluna do curso de Petróleo e Gás da Faculdade Norte Capixaba de São Mateus
[5] Aluna do curso de Petróleo e Gás da Faculdade Norte Capixaba de São Mateus
[6] Aluna do curso de Petróleo e Gás da Faculdade Norte Capixaba de São Mateus

1 INTRODUÇÃO

O Brasil utiliza energia de várias fontes. Aproximadamente 20% delas são oriundas da cana de açúcar e outras fontes renováveis. Como as consequências do aquecimento global de fato já estão ocorrendo e o petróleo, além de ser o grande vilão na emissão de gases para atmosfera, se torna cada vez mais escasso ou até pode terminar em curto espaço de tempo, não resta alternativa a não ser buscar distintas soluções para questão energética (NODARI, 2010, p 51).

A produção acontece em duas linhas: o álcool hidratado, usado nos veículos que utiliza como o combustível o etanol e álcool anidro, que é utilizado na gasolina. Em decorrência disso tem ocorrido um aumento no preço do diesel de petróleo, quando o álcool está em alta, acarretando uma inflação nos preços dos combustíveis.

Este trabalho visa à discussão do preço do etanol em decorrência das oscilações no mercado alcooleiro no Brasil e os efeitos causados por estas, bem como o aumento do preço da gasolina em função do etanol e as desvantagens do abastecimento do carro a álcool.

2 METODOLOGIA

Este artigo trata de uma pesquisa exploratória onde foram analisados dados históricos e interpretações de gráficos. Onde realiza descrições precisas da situação e quer descobrir as relações existentes entre seus elementos componentes. Este tipo de pesquisa requer planejamento bastante flexível para possibilitar a consideração dos mais diversos aspectos de um problema ou de uma situação. (CERVO; BERVIAN; DA SILVA, 2006)

3 REVISAO BIBLIOGRÁFICA

3.1 A PRODUÇÃO DE ÁLCOOL NO BRASIL

A cana de açúcar foi introduzida no Brasil pelos portugueses em 1532, no entanto a produção de álcool ocorreu no inicio do século XX, a princípio era utilizado com subproduto, só mais tarde que houve a incorporação deste a gasolina para barateá-la.

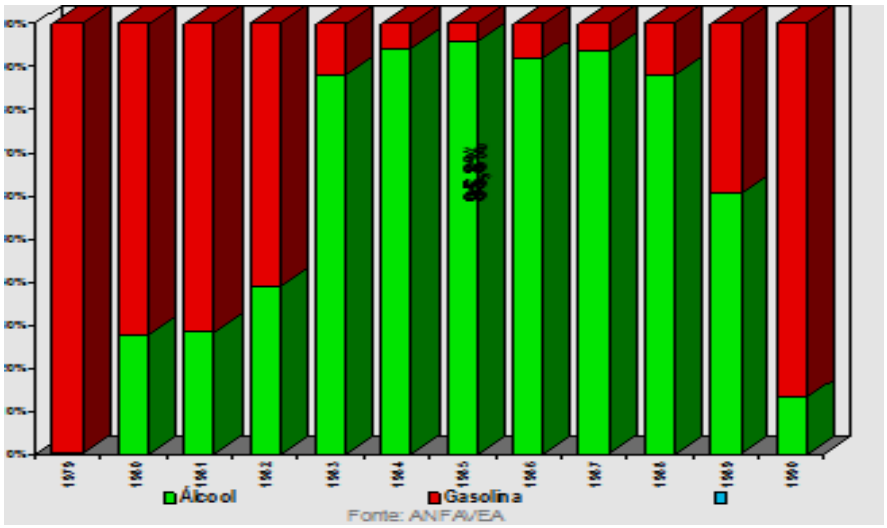
A crise do petróleo na década de 70, trouxe uma insegurança e instabilidade ao mercado energético que levou o país a criar estratégias para ampliar sua produção e incentivar o consumo de bicombustíveis. O governo brasileiro criou então o decreto federal de nº: 76.593 de 1975, como objetivo de tornar obrigatória a adição do álcool anidro à gasolina e estimular a conversão de veículos para usar álcool hidratado, o chamado Proálcool (programa nacional do álcool).

O Proálcool é considerado o maior programa do mundo de utilização Comercial da biomassa para produção e uso de energia, demonstrando a viabilidade técnica da

produção em larga escala de etanol a partir da cana de açúcar e do seu uso como combustível automotivo. (LA ROVERE apud THIAGO OROSZ, 2011).

Nesse período compreendido entre a primeira e segunda fase do Proálcool, a demanda por veículos adaptados a álcool cresceu significativamente. Como mostra o gráfico abaixo.

FIGURA 01

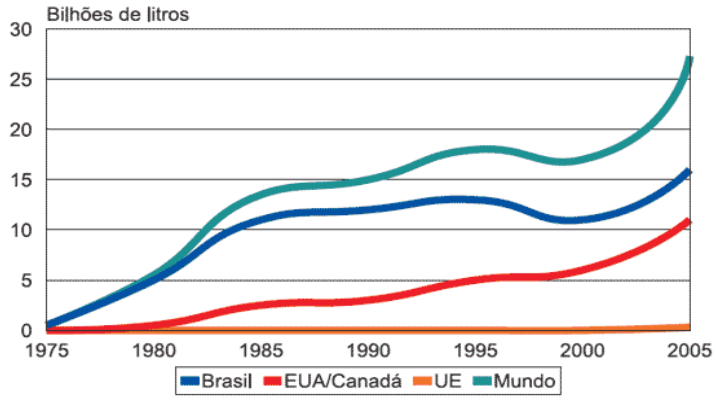


Fonte: ANFAVEA, 2011

O incentivo dado pelo governo consistia principalmente num aumento da produção de álcool hidratado, para atender a demanda da frota de veículos que usavam esse combustível. É importante ressaltar que a produção destes se deve também ao incentivo oferecido pelo governo, proposto no segundo decreto do Proálcool decreto de nº: 83.700 de 1979.

Nesse contexto, é importante destacar as tecnologias que foram desenvolvidas para a produção de etanol no país, como as instalações de novas refinarias e ampliações de algumas já existentes. Tudo isso contribuiu para que o país ganhasse destaque no mundo na produção de etanol, conforme destacado no gráfico abaixo.

Figura 02 – Produção Mundial de Etanol



Fonte: Gazzoni apud Silveira, Silva e Silva Junior, 2011

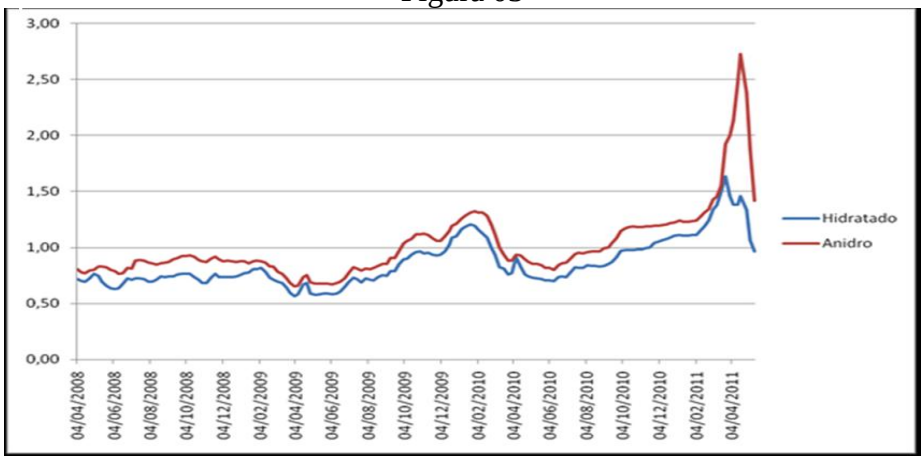
3.2 PREÇOS DO ETANOL NO BRASIL

Notoriamente o mercado alcooleiro no país tem ganhado destaque tanto pela produção quanto pela tecnologia agregada que proporcionaram o crescimento desse combustível no país. Porém o custo da produção bem como o preço do produto vem se desenhando um mercado instável.

Segundo Riveras (2011) os preços de etanol estão disparando com o forte aumento da demanda, colocando mais pressão sobre a inflação e elevando temores sobre uma possível falta de combustível em algumas partes do país.

O aumento da percentagem do álcool na gasolina, fez com que elevasse o preço do álcool anidro, conforme a figura abaixo.

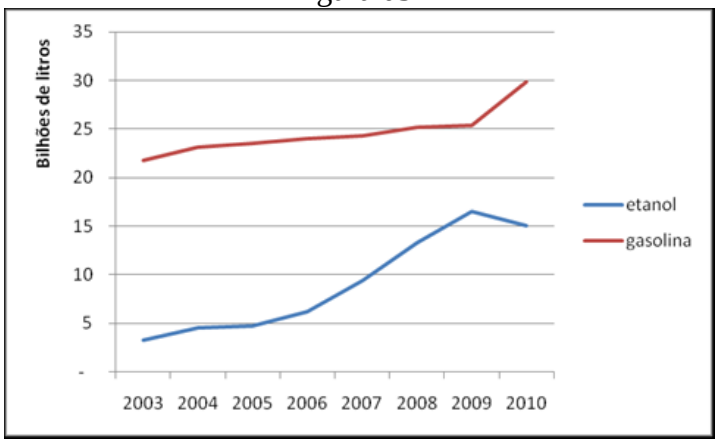
Figura 03



Fonte: CEPEA/ESALQ/USP

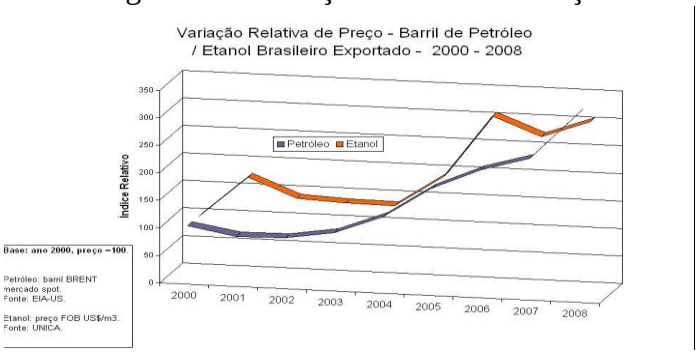
Com a alta do preço, o etanol passa a não ser tão mais atrativo, levando os consumidores a optarem pela gasolina. Esse decréscimo deu-se graças ao preço elevado do etanol, como podemos constatar no gráfico abaixo: no segundo semestre de 2009 e início de 2010 houve uma queda no consumo do etanol em relação à gasolina, na figura 05, na figura 06 o preço do etanol demonstra maior que o da gasolina entre 2006/2007.

Figura 05



Fonte: ANP, 2011

Figura 06 - Variação Relativa do Preço



Fonte: ANP, 2011

Enquanto o preço da gasolina se manteve estável durante cinco anos, o preço do álcool apresentava oscilações, no mesmo período compreendido entre 2005 a 2010, no entanto no primeiro semestre de 2011 os consumidores puderam sentir no bolso o aumento da gasolina que chegou a R$ 3,19 nas bombas dos postos de combustíveis em função do aumento do preço do etanol, que na opinião de especialista se deve ao período de intersafra da cana de açúcar que ocorre entre os meses de dezembro a abril. Porém o que se vê é um mercado ainda imaturo na administração da produção e/ou consumo do etanol.

3.3 CRISES DOS ALIMENTOS

O tema crise alimentar ganhou grande destaque nas mídias durante o ano de 2008, quando alguns especialistas apontavam a produção de bicombustíveis como a principal causa da crise de alimentos, pois argumentavam que o incentivo à produção levou os agricultores a desenvolverem uma monocultura atraída pela oferta oferecida do mercado. Todavia a crise dos alimentos não se deve apenas a um fator isolado, mas a um conjunto de fatores como condições climáticas e crescimento populacional, etc.

O Brasil é um dos maiores produtores de alimento para consumo interno e também para exportação, graças às condições climáticas favoráveis ao cultivo de diversas plantas de gênero alimentício. Em decorrência dessa posição, o país foi alvo de críticas na produção exagerada do plantio para produção de bicombustível. Como o país utiliza a cana de açúcar para produção do açúcar e também o etanol, essa crise ficara mais evidente.

Dentro desse contexto alimentos, ainda é importante salientar que a área de cultivo para bicombustível, na opinião de alguns especialistas fomentaria a perda da biodiversidade e em conseqüência disso o aumento de gases de efeito estufa provocado pelo desmatamento de áreas para cultivo que impediria o efeito esponja desempenhado pelas florestas em absorver as emissões de carbono (VON DER; ROSENTHAL apud LEITE, 2010)

4 CONCLUSAO

Diante dos dados analisados percebe-se uma fragilidade da produção assim como preço e desenvolvimento sustentável no mercado sucroálooleiro no país. Muito embora todo avanço tecnológico obtido nesses últimos anos, não se pode menosprezar a analise de alguns fatores; como por exemplo, o cultivo da cana de açúcar ainda desestruturado necessitando nortear limite a esse cultivo para assegurar que áreas florestais não sejam desmatadas, garantindo assim um controle ambiental no que tange aos gases de efeito estufa o que acrescentaria uma maior credibilidade, aceitação e consumo desse biocombustível, pois já se sabe que ele é menos poluente em relação aos demais (MACEDO, 2006).

Outro fator relevante é a mão de obra empregada, pois não convém esquecer os problemas sociais sofridos pelos cortadores de cana que trabalham em condições desumanas que contribuem riscos para sociedade que podem tornar esses benefícios em malefícios. É verdade que os incentivos do governo proporcionaram um avanço excepcional no mercado alternativo de energia, todavia é notório que houve um decréscimo no consumo do álcool hidratado produzido para atender veículos com motores fabricados para tal. Isso se deve a uma insatisfação dos usuários seja como o preço do etanol ou poder calorífico dele em relação ao combustível do petróleo. O que se sugere é um maior investimento em tecnologias para melhoramento e/ou desenvolvimento de motores que sobressaiam a esses problemas.

Enfim, em decorrência de todos os fatos descritos acima se notifica um grande desafio para que se tenha um desenvolvimento sustentável para produção, aceitação/consumo e estabilidade no preço tanto para o etanol como demais biocombustíveis.

REFERENCIAS

1. ANFAVEA - **Anuário Estatístico da Indústria Automobilística Brasileira**, 2011.

2. ANP – Associação Nacional do Petróleo, 2011

3. LEITE, Jose Rubens Morato et al.**Bicombustível fonte de energia sustentável?** São Mateus, 2010.

4. MACEDO, Isaias C. **Situação atual e perspectivas do etanol**. Disponível em:<http://www.scielo.br/pdf/ea/v21n59/a11v2159.pdf.html>. Acesso em: 18 jun 2011.

5. MAFUD, Marina Darahem; **Uma reflexão sobre a produção de alimentos e de etanol no Brasil**. Disponível em: <http://www.favaneves.org/.../doc-vii-2.84-uma-reflexao-sobre-a-produção-de-alimentos.pdf.html>. Acesso em 17 jun 2011

6. MENDONCA, Marcos Aurélio Alves de; COSTA, Ricardo Cunha de et al; **Expansão da produção de álcool combustível no Brasil uma análise baseada**

nas curvas de aprendizagem. Disponível em: <htpp://www.sober.org.br/9/189.pdf.html>. Acesso em:17 jun2011.

7. OROSZ, Thiago. **Tecnologias Utilizadas para Desidratação de Etanol.** Disponível em: www.mta.ufscar.br/araras-i/tecnologias_utilizadas...etanol/at.../file. Acesso em 17 jun 2011

8. RAMOS, Pedro; **A evolução da agroindústria canavieira e os mercados de açúcar e álcool carburante no Brasil:a necessidade de planejamento e controle.** Disponível em: http://www.sober.org.br/palestras/9/35.pdf.html>.Acesso em: 17 jun 2011

9. RIVERAS, Inaê. **Preço do etanol sobre ameaça.** Disponível em: <http://www.globo.globo.com.br/...preço-do-etanol-sobe-ameaça-oferta-de-combustivel no brasil.html>. Acesso em: 18 jun 2011

10. SILVEIRA, John Herbert Maciel Diamantino da; SILVA, Scarlet Barcelos; SILVA JÚNIOR, Vicente Souza da. **Energia renovável e impacto ambiental.** Disponível em: *www.essentiaeditora.iff.edu.br/index.php/BolsistaDeValor/.../975. Acesso em 18 jun 2011*

11. TAVOR, Fernando Lagares**;Historia e economia dos bicombustíveis no Brasil**. Disponível em :<http://www.senado.gov.br/senado/conleg/textos.../td89-fernando lagares.pdf.html>.Acesso em 17 jun 2011

PRINCIPAIS AMEAÇAS À SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

Diogo Farias Mota[7]

RESUMO

Nos últimos anos, houve um crescimento exponencial na utilização da tecnologia da informação por parte das empresas em todo o mundo, o que vem levando as empresas a se tornarem cada vez mais dependentes dos sistemas de informação para a execução de suas atividades diárias. Este artigo tem como objetivo analisar as principais ameaças aos sistemas de informação das empresas. Também é objetivo deste trabalho apresentar algumas das principais práticas e ferramentas utilizadas para garantir um nível de segurança da informação aceitável para as organizações. Propõe-se uma reflexão sobre a necessidade das empresas em investir na segurança da informação em seus sistemas de informação.

Palavras-Chave: Segurança, Tecnologia, Informação e Sistemas de Informação.

ABSTRACT

In the last years, there has been an exponential growth in the use of information technology by companies in all over the world, which is leading companies to become increasingly dependent of information systems to perform their daily activities. This article aims to analyze the main threats to information systems companies. It is also aim of this paper present some of the leading practices and tools used to ensure a level of information security acceptable to the organizations. It proposes a reflection on the need for companies to invest in information security in their information systems.

Keywords: Security, Technology, Information and Information Systems

1 INTRODUÇÃO

Presenciamos todos os dias avanços tecnológicos em diversas áreas do saber humano. Ao selecionarmos as áreas que têm causado um alto impacto no dia a dia das empresas, destacamos a tecnologia da informação e telecomunicações. Diante deste cenário de avanços tecnológicos constantes, observa-se que a carga de conhecimento está se tornando cada vez maior e mais complexa de ser gerida.

[7] Formado em Administração de Empresas com Habilitação em Análise de Sistemas. Especialista em Engenharia de Sistemas pela ESAB , Docência do Ensino Superior pela Faculdade Norte Capixaba de São Mateus e Logística Empresarial pela UFES. Professor da Faculdade Norte Capixaba de São Mateus.

Presente em um ambiente mutável e incerto, as empresas convivem em um meio hostil em suas redes locais e na Internet, onde diversos fatores ameaçam seus sistemas de informação, o que pode acarretar prejuízos e até decretar o desaparecimento da empresa no mercado.

Esse artigo foi desenvolvido com o objetivo precípuo de apontar as principais ameaças a que os sistemas de informação estão sujeitos e apresentar soluções disponíveis no mercado para corrigir ou minimizar as ameaças existentes.

2 METODOLOGIA

Para a elaboração do presente artigo, foram coletadas informações através de uma pesquisa bibliográfica, buscando identificar as principais ameaças à segurança das informações presentes nos sistemas de informação existentes. Por fim, foram apresentas as principais ferramentas disponíveis no mercado que visam a contribuir para a segurança dos sistemas.

3 CONTEXTO DA SEGURANÇA DA INFORMAÇÃO

A humanidade sempre conviveu com uma preocupação, como salvaguardar informações importantes de inimigos e ameaças naturais? Com o advento do surgimento dos primeiros computadores, notou-se um processo de valorização da questão da segurança das informações. Podemos ressaltar que desde que o homem começou a gerar conhecimento, o mesmo está constantemente correndo riscos pelas ameaças existentes de cada época da humanidade.

Nas últimas décadas, registram-se mudanças que vêm causando impactos cada vez maiores para a sociedade, levando as organizações a reverem a importância da segurança da Informação para o bom funcionamento de seus processos. Mudanças significativas na tecnologia são apresentadas:

> Nas décadas de 70 e 80, a informática fazia parte da retaguarda dos negócios das organizações, nas quais o enfoque principal da segurança era o sigilo dos dados. Entre as décadas de 80 e 90, com o surgimento dos ambientes de rede, a integridade passou a ser de suma importância, e a proteção era feita não tendo em mente os dados, mas sim as informações. A informática fazia parte da administração e da estratégia da organização. A partir da década de 90, o crescimento comercial das redes baseados em *Internet Protocol* (IP) fez com que o enfoque fosse mudado para a disponibilidade. A informática, agora, tornou-se essencial nos negócios, e o conhecimento é que deve ser protegido. (NAKAMURA; GESUS, 2007, p.50).

Percebemos que a revolução da informática nas décadas de 80 e 90 exerceu forte influência sobre o desenvolvimento da tecnologia da informação e nos processos que estão relacionados à segurança dos dados presentes nos sistemas das organizações. Ressaltamos que as preocupações com segurança da informação não são privilégio de empresas do presente século, mas entendemos que os riscos e falhas sempre coexistiram e continuarão existindo em conjunto com as informações.

3.1 CENÁRIO DA SEGURANÇA DA INFORMAÇÃO NO BRASIL

Em todos os ambientes organizacionais, encontramos os computadores e demais aparatos da tecnologia como Iphones, Ipads e celulares. Em um passado recente, a questão da segurança da Informação era simples de ser gerenciada, pois bastava trancar os papéis em locais seguros como gaveteiros com chave ou até mesmo em cofres e pronto. Entretanto, os avanços tecnológicos como a Internet e suas facilidades, trouxeram também uma carga elevada de problemas relacionados à segurança dos dados.

Podemos afirmar que não existe segurança da informação absoluta em nenhuma parte do mundo, o que torna intrínseca a necessidade das organizações tomarem medidas para tratar os pontos vulneráveis aos quais estão expostas, ou seja, providenciar para que a segurança dos dados da empresa seja feita de forma eficaz. Esta crescente utilização dos computadores é evidenciada,

> Os computadores tomam conta dos ambientes de escritório, quebram o paradigma e acesso local à informação, e chegam a qualquer lugar do mundo através dos – cada vez mais portáteis notebooks e da rede mundial de computadores: a Internet. (SEMOLA, 2003, p.3).

O Brasil conta atualmente com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br), um dos serviços disponibilizados pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), que divulga estatísticas de relatos enviados espontaneamente por administradores e usuários envolvendo redes brasileiras, além de desenvolver atividades de pesquisa sobre Segurança de Sistemas.

Entender o grau de importância em se proteger contra as ameaças torna-se importante devido ao fato de que qualquer cidadão ou organização está exposto a riscos de segurança da informação. O problema que não deve ser visto apenas do ponto de vista técnico é um problema cultural e social, que precisa ser tratado.

3.2 PILARES DA SEGURANÇA DA INFORMAÇÃO

Para compreender de forma mais eficaz do que se trata a informação, primeiro deve-se elucidar e diferenciar Dado e Informação, entender como a informação se movimenta e de que forma a mesma influi dentro de uma organização.

O dado pode ser definido como:

> Pode-se definir os dados como um conjunto de bits armazenados, como os nomes, endereços, datas de nascimento, números de cartões de créditos ou histórico financeiros. Um dado é considerado uma informação quando ele passa a ter um sentido, como as informações referentes a um cliente especial. O conhecimento é o conjunto de informações que agrega valor ao ser humano e à organização, valor este que resulta em uma vantagem competitiva, tão importante no mundo atual. (NAKAMURA e GESUS, 2007, p.50).

Compreende-se que a formatação de vários dados resulta em uma informação, que traz significado e gera vantagem competitiva para quem a detêm. Portanto uma informação é

> Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas operações que envolvam, por exemplo, a transferência de valores monetários). (SEMOLA, 2003, p.45).

Podemos ainda definir informação, como sendo um conjunto de dados, imagens, textos ou quaisquer formas de representação dotadas de um significado dentro de um contexto. Dentre um amplo universo, podemos classificar como exemplos de informação: relações de clientes, marcas de produtos, contas pessoais, extrato de banco.

A informação não é apenas um fator isolado a ser considerado dentro das organizações, visto que a informação deve ser considerada como um ativo da empresa, devendo ser protegida e zelada como quaisquer outros bens tangíveis. Podemos considerar a informação como um ativo:

> Todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada. (SEMOLA, 2003, p.45).

Percebe-se que a informação, por ser um ativo, deve ser tratada com extrema importância e cuidado nas empresas, sendo necessário pensar em como protegê-la desde a sua geração até o seu descarte, pois há uma grande quantidade de ameaças que podem comprometer a segurança das informações. Entretanto, para poder assegurar de forma mais eficaz a segurança das informações, extremamente importante é entender o seu ciclo de vida e gerenciar todas as etapas vividas pela mesma.

A segurança deve estar presente em todo o ciclo de vida da informação, desde a criação, passando pelo armazenamento até o seu descarte. Uma informação que é acometida por alguma ameaça no decorrer do seu ciclo, pode causar sérios danos ao seu proprietário. Todo o ciclo de vida da informação deve ser protegido,

> O ciclo de vida, por sua vez, é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa (SEMOLA, 2003, p.9).

Existe uma necessidade premente de proteger a informação durante o seu ciclo, sendo de vital importância para o bom andamento dos processos organizacionais que não ocorram alterações indevidas nas informações, haja vista que a informação mantém processos da organização operantes.

Os estágios do ciclo de vida da informação são os seguintes:

> **Manuseio:** Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma

> aplicação internet, ou, ainda, ao utilizar sua senha de acesso para autenticação, por exemplo;
> **Armazenamento:** Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda, em uma mídia de disquete depositada na gaveta da mesa de trabalho, por exemplo;
> **Transporte:** Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico (email, ao postar um documento via aparelho de fax, ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo;
> **Descarte:** Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CD-ROM usado que apresentou falha na leitura. (SEMOLA, 2003, p.10)

De acordo com Semola (2003), garantir o sucesso de todo tratamento da informação no seu ciclo de vida depende de uma série de fatores, como medidas de segurança, programas de conscientização aos colaboradores sobre o procedimento correto a ser adotado durante o clico seja no seu manuseio, armazenamento, transporte ou descarte.

Proteger as informações significa adotar medidas e procedimentos para evitar a concretização das ameaças que podem afetá-las, corrompendo-as, tendo acesso de forma indevida e eliminando-as ou furtando-as. A segurança da informação visa a preservar ativos de informação levando em conta três objetivos fundamentais: integridade, confidencialidade e disponibilidade da informação.

Segundo Beal (2005), o princípio da legalidade da informação visa garantir que a informação foi produzida em conformidade com a lei. Outro objetivo que a segurança da informação garante, é o do não-repúdio, garantindo que os envolvidos no processo de criação, alteração e exclusão das informações sejam devidamente identificados, sem a possibilidade de repudiar o acesso que foi realizado.

Além dos objetivos da segurança da informação, alguns aspectos adicionais emergem quando a informação precisa ser transmitida num processo de comunicação. Problemas como a alteração fraudulenta de documentos no seu processo de comunicação, nos leva a estabelecer objetivos relativos à segurança da comunicação.

Segurança da informação significa, "área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" (SEMOLA, 2003, p.43).

Para que a informação possa ser utilizada, ela deve estar íntegra. Quando ocorre uma alteração não-autorizada da informação em um documento, dizemos que o documento perdeu sua integridade. A quebra da integridade ocorre quando a mesma é corrompida, falsificada ou indevidamente alterada.

O alvo da integridade da informação pode ser definido "objetivo da integridade é garantir que toda a informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais"(SEMOLA, 2003, p.45).

Quando garantimos a integridade da informação, asseguramos que somente pessoas autorizadas possam realizar alterações em uma informação, ou que as alterações causadas por acidente ou defeitos não ocorram ou pelo menos que sejam minimizadas.

Segundo Beal (2005), outro pilar da segurança da informação a confidencialidade, tem como objetivo garantir que apenas as pessoas autorizadas tenham acesso à informação. Ter confidencialidade na comunicação é ter segurança de que o que foi dito a alguém ou escrito em algum lugar só será escutado ou lido por quem tiver autorização para tal. As informações têm diferentes graus de confidencialidade relacionados aos seus valores. Dependendo do tipo de informação e do público para o qual se deseja colocar à disposição a informação, define-se um grau de sigilo.

Segundo Semola (2003, p.48), podemos afirmar que a confidencialidade foi violada quando a informação é acessada por pessoas não autorizadas, quer seja propositalmente ou acidentalmente ou fora da organização.

Para que uma informação possa ser utilizada, ela precisa estar disponível a quem desejar acessá-la. A disponibilidade é o terceiro princípio da segurança da informação. Refere-se à disponibilidade da informação e de toda estrutura física e tecnológica que permite o acesso, o trânsito e o armazenamento da informação.

Segundo Semola (2003, p.45), para proteger a disponibilidade, muitas medidas são levadas em consideração, entre elas: configuração segura do ambiente tecnológico, realizar cópias de segurança e definir estratégias para situações de contingência.

4 VULNERABILIDADES E AMEAÇAS AOS SISTEMAS

Uma vulnerabilidade é considerada uma falha que expõe o sistema sob algum dos aspectos da segurança. Uma vulnerabilidade pode comprometer um sistema como um todo ou parte dele. Existem vários tipos de vulnerabilidades como exemplo podemos citar: vulnerabilidade humana, falta de treinamento, compartilhamento de informações confidenciais, desobediência ou não execução de rotinas de segurança, falta de comprometimento dos funcionários.

As ameaças são agentes ou condições existentes que causam incidentes que comprometam as informações, muitas das vezes consequências das vulnerabilidades existentes, provocando assim perdas de confidencialidade, integridade e disponibilidade.

Exemplos de vulnerabilidades que afetam a disponibilidade da informação são definidos,

> Físicas: instalação predial fora do padrão, salas mal planejadas, falta de extintores, detectores de fumaça, riscos de explosões, vazamentos ou incêndios
> Naturais: computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades e outros.
> Hardware: falhas nos recursos tecnológicos ou erros de instalação

> Software: erros na instalação ou na configuração podem acarretar acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário.
> Mídias: discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
> Humanas: falha de treinamento, compartilhamento de informações confidenciais, não execução de rotinas de segurança, erros ou omissões; ameaças de bomba, sabotagens, distúrbios civis, greves, vandalismo, roubo, destruição da propriedade ou dados, invasões ou guerras. (SEMOLA, 2003, p.48)

Segundo Beal (2005), os riscos são as possibilidades das ameaças explorarem as vulnerabilidades, ocasionando dados e perdas de dados o que acaba impactando os princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

As ameaças à segurança da informação sempre existiram. A principal diferença é que hoje o inimigo se tornou muito mais veloz, mais difícil de detectar e muito mais criativo em seus ataques. As violações de segurança afetam as pessoas e organizações de várias maneiras. Normalmente essas violações resultam em prejuízos financeiros, danos à reputação da organização, perda ou comprometimento de dados, interrupção do processo de negócios, danos à confiança do cliente entre outros.

Devemos sempre lembrar que quando falamos segurança da informação, todos envolvidos direta e/ou indiretamente com a empresa como: Funcionários, Terceiros, Visitantes, Prestadores de Serviço e outros devem estar envolvidos, devem zelar para manter a segurança das informações.

O mundo virtual está repleto de vilões que podem comprometer a informação das empresas caso obtenham sucesso em sua investida. A cada dia surgem novas tecnologias e com elas, novas ameaças antes inexistentes. A popularização do computador e a dependência das empresas por parte dos mesmos para uma harmoniosa execução de suas atividades, vem contribuindo para um aumento exponencial de métodos e técnicas de ataques contra as informações das empresas.

Segundo Nakamura e Gesus (2002, p.39-51), denomina-se de atacantes as pessoas que atacam um sistema computacional, explorando uma vulnerabilidade, podendo ou não obter êxito. Dentre os atacantes que são mais conhecidos encontramos os *hackers*, mas existe uma vasta gama e atacantes. Podemos classificar como exemplos de atacantes:

> Preackers: responsáveis por fraudes em telefonia, sendo atualmente o principal alvo deste tipo de atacante o telefone celular.
> Script Kiddies: atacantes com pouco conhecimento técnico utilizam ferramentas encontradas na Internet.
> Crackers: tem um conhecimento avançado, são capazes de quebrar segurança de sistemas de grande porte como bancos e instituições governamentais.
> Carders: realizam compras com cartões de crédito roubados ou clonados através de um software especifico.
> Insiders: funcionários insatisfeitos ou ex-funcionários que usam os acessos que possuem para praticar delitos dentro das empresas. (NAKAMURA; GESUS, 2002, p.40-47).

Segundo o CERT.br (2011), o total de notificações de incidentes no primeiro trimestre de 2010 foi superior a 28 mil, representando um decréscimo de 8% em relação ao trimestre anterior e de 87% em relação ao mesmo período de 2009. As notificações sobre ataques a servidores Web cresceram 13% em relação ao trimestre anterior e 42% em relação ao mesmo período de 2009.

Uma técnica de ataque que vem ganhando espaço é a Engenharia Social. Esta técnica é utilizada visando a obter acesso às informações importantes ou sigilosas de organizações/pessoas ou sistemas por meio da enganação ou exploração da confiança das pessoas. Para realizar o ataque, o indivíduo pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc. Os cidadões que não possuem treinamento básico em segurança da informação, são alvos que podem ser facilmente manipulados pelo atacante.

A técnica de ataque engenharia social é definida:

> Engenharia social, dentro da área de segurança de sistemas computacionais, é um termo utilizado para qualificar os tipos de intrusão não técnica, que coloca ênfase na interação humana e, freqüentemente, envolve a habilidade de enganar pessoas objetivando violar procedimentos de segurança. (MENDES, 2004,)

A engenharia social pode ser caracterizada por um método de ataque no qual alguma pessoa faz uso da persuasão, para obter informações que poderão ser utilizadas para ter acesso não autorizado a computadores ou a informações da empresa. Um ataque de engenharia social pode ser executado através de qualquer meio de comunicação que o atacante possua como disponível: telefone, e-mails e conversas através da Internet.

Uma ameaça há tempos conhecida por todas as empresas é o vírus de computador, que analogamente ao vírus que ataca os seres vivos, atua infectando os sistemas e causando prejuízos imensuráveis.

Segundo Brookshear (2005), os vírus são programas desenvolvidos para alterar nociva e clandestinamente softwares instalados em um computador. Os vírus se disseminam ou agem por meio de falhas ou limitações de determinados programas, como ocorrem com os vírus de macro que são embutidos em ferramentas de utilização diárias nas empresas como editores de texto. Uma medida importante é disseminar a cultura da prevenção nas empresas, evitando que a ameaça seja concretizada para posteriormente tomar uma medida corretiva.

Considerado por muitos como sendo uma evolução do conceito de vírus de computador, os *worms* (vermes) são um tipo de vírus com maior poder de propagação, ou seja, mais inteligente que os demais existentes na atualidade. A principal diferença entre eles e os vírus está em sua forma de propagação: os *worms* podem se propagar rapidamente para outros computadores.

Um tipo de *Worm* que está causando grandes prejuízos é o BOT, um tipo de *Worm* capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes, além de permitir que o programa seja controlado remotamente.

Comumente um tipo de ameaça desprezada pelas empresas é o Spam, abreviação em inglês de “spiced ham” (presunto condimentado), que sendo uma mensagem eletrônica não-solicitada enviada em massa pode inundar os sistemas de e-mail de uma ou mais organizações.

Não menos destrutivo do que as ameaças já mencionadas, os Cavalos de Tróia ou Trojans são programas executáveis, que transformam o computador hospedeiro em um terminal de internet "aberto" possibilitando que seu criador tenha acesso ao equipamento da pessoa ou empresa infectada.

Os cavalos de tróia são programas que são entregues para o usuário de forma legítima, mas sem o conhecimento do mesmo. Realiza ações maliciosas como capturar informações e enviar para o atacante. Os Trojans geralmente são instalados quando se executam anexos desconhecidos ou instalamos um programa de origem duvidosa.

Os Sistemas de Informação são facilmente propensos a danos se as medidas apropriadas não forem tomadas para minimizar o risco. Em alguns casos, é possível que haja desastres e as calamidades naturais como os tremores terrestres, vulcões, fogo, furacões etc. Assim como o ser humano está inserido em um macro sistema, os sistemas de informação sofrem a influência do ambiente externo, sendo necessário um plano para manter tais sistemas protegidos contra essas ameaças.

As principais perdas acidentais de dados são:

> [...] fenômenos naturais: incêndios, enchentes, terremotos, guerras, motins ou ratos roendo fitas ou discos flexíveis;
> Erros de hardware ou software: discos ou fitas com problemas de leitura, erros de telecomunicações e erros de programas;
> Erros humanos: entrada incorreta de dados, má montagem do disco ou fita, execução do programa errado, perda do disco ou fita ou algum outro erro (TANENBAUM, 2003, p.441).

Embora proteger dados contra perda acidental pareça bobagem se comparando a proteger as mesmas de invasores inteligentes e ágeis, na prática, provavelmente mais danos sejam causados por acidentes do que por invasores. O agravante em relação às ameaças é o grau de exposição das empresas e até mesmo do Governo na Internet sem as devidas ferramentas e técnicas para proteção dos sistemas de informação.

4.1 POLÍTICAS E FERRAMENTAS DE SEGURANÇA

Devido ao acréscimo no estudo do tema segurança da informação, foram desenvolvidas técnicas, ferramentas e metodologias que visam a garantir a salvaguarda das informações. Hoje se tornou comum encontrarmos empresas e até usuários domésticos que compram equipamentos buscando garantir a sua segurança. Há de se ressaltar que um sistema nunca estará totalmente seguro, pois à medida que os sistemas de segurança se aprimoram, por outro lado verifica-se que as técnicas de invasão também evoluem. As informações estão cada vez mais valiosas,

> A cada dia e cada vez mais as empresas possuem informações sigilosas em seus computadores, exigindo cuidados, a fim de protegê-las.Limitar o acesso físico e lógico aos computadores, principalmente para ambientes computacionais compartilhados ou que utilizem algum meio de comunicação público, é o ponto de partida de uma política de segurança de informações. Estes cuidados podem ser aplicados através da implantação de um conjunto de mecanismos de segurança para a proteção de arquivos e de outras informações armazenadas, inclusive com a automatização de processos e ferramentas de segurança. (GUEDES, 2006, p.110).

Uma política de segurança pode ser vista como a formalização dos desejos da empresa quanto à questão da proteção de suas informações e a sua criação concretiza e formaliza que a empresa deseja documentar e normatizar os processos que geram e manipulam informações. A ideia de uma política de segurança é servir como balizadora de toda a atividade que manipula informações,

Podemos definir uma política de segurança como:

> A Política de Segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação. (FERREIRA, 2008, p.36).

Existe uma grande dificuldade de entender a importância da segurança da informação para a empresa. Muitas delas somente iniciam a implantação de medidas de segurança depois de sofrerem ataques que causaram algum prejuízo.

Cada empresa possui particularidades em seu ambiente, o que torna a criação de uma política de segurança uma tarefa não muito fácil de ser executada. Neste documento devem constar propósitos e orientações para toda a força de trabalho abrangendo desde funcionários, parceiros e demais envolvidos nos processos da empresa desde o nível operacional até o estratégico.

Uma política de segurança da informação deve atender aos seguintes propósitos dentro de uma organização:

> Descreve o que está sendo protegido e por quê;
> Define prioridades sobre o que precisa ser protegido em primeiro lugar;
> Permite estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança;
> Fornece ao departamento de segurança um motivo válido para dizer "não" quando necessário;
> Proporciona ao departamento de segurança a autoridade necessária para sustentar o "não";
> Impede que o departamento de segurança tenha um desempenho fútil (WADLOW, 2000, p.40).

Tendo como principal objetivo o uso adequado dos recursos de informática e informação, o sucesso ou não da implantação de uma política de segurança depende de inúmeros fatores que variam em cada empresa. Os obstáculos à sua implementação são grandes e os principais podem ser evidenciados na figura abaixo:

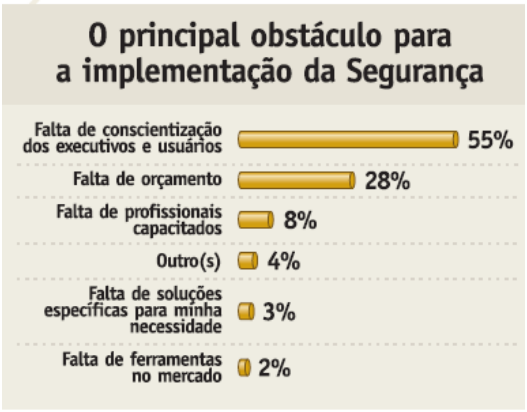


Figura 1: Principais obstáculos para a implementação da Segurança nas empresas.
Fonte: (Módulo Security, 2010, p.7)

Dentre os controles existentes na norma NBR ISO 17799, os controles considerados como melhores práticas para a segurança da informação incluem:

> Documentação da política de segurança da informação;
> Definição das responsabilidades na segurança da informação;
> Educação e treinamento em segurança da informação;
> Relatório de incidentes de segurança;
> Gestão de continuidade do negócio. (NBR ISO 17799, 2001, p.3)

Pode-se observar que a política de segurança da informação é um documento abrangente e que necessita de ser escrito com muito critério. Para uma empresa criar, implantar e monitorar uma política recomenda-se a contratação de empresas especializadas no assunto, pois o sucesso da implantação de um sistema e uma política de segurança na empresa depende em grande parte do profundo conhecimento dos processos envolvidos nessa implantação além das particularidades de cada empresa. Após a criação e implementação de uma Política de Segurança da Informação, a empresa almeja colher os frutos do trabalho realizado.

Entre os principais benefícios alcançados por empresas que implementam uma Política de Segurança configuram:

> Benefícios de curto prazo
> Formalização e documentação dos procedimentos de segurança adotados pela organização;
> Implementação de novos procedimentos e controles;
> Prevenção de acessos não autorizados, danos ou interferências no andamento dos negócios, mesmo no caso de falhas ou desastres;
> Maior segurança nos processos do negócio
> Benefícios de médio prazo
> Padronização dos procedimentos de segurança incorporados na rotina da empresa;
> Adaptação segura de novos processos do negócio;
> Qualificação e quantificação dos sistemas de resposta a incidentes;
> Conformidade com padrões de segurança, como a NBR ISO/IEC 27002(antiga NBR ISO/IEC 17799)
> Benefícios de longo prazo
> Retorno sobre o investimento realizado, por meio da redução de problemas e incidentes de segurança da informação;

> Consolidação da imagem corporativa associada à Segurança da Informação; (FERREIRA, 2008, p.46)

4.2 NORMAS ISO PARA SEGURANÇA DA INFORMAÇÃO

Devido ao aumento do grau de importância da questão da segurança da informação, foram criadas normas visando à regulamentação desta temática. A ISO "International Organization for Standartization" é uma organização que tem sede na Suíça (ABNT ISO 27001, 2006). No Brasil, o papel da ISO é desenvolvido pela Associação Brasileira de Normas Técnicas - ABNT.

As normas de segurança da informação permitem às organizações implantar os requisitos de Segurança da Informação e de qualidade para com os envolvidos nos processos, respectivamente, garantindo a confidencialidade e a integridade dos dados.

Para compreendermos melhor a situação atual das pesquisas em segurança da informação, apresentamos um breve histórico sobre a evolução das normas:

> 1995: publicada a primeira versão da BS 7799-1
> 1998: publicada a primeira versão da BS 7799-2;
> 1999: publicada a revisão da BS 7799-1;
> 2000: publicada a primeira versão da ISO/IEC 17799;
> 2001: publicada a primeira versão da norma no Brasil, NBR ISO/IEC 17799;
> 2002: publicada a primeira versão da norma BS 7799 parte 2;
> 2005: Agosto: publicada a segunda versão da no Brasil, NBR ISO/IEC 17.799;
> Outubro: publicada a norma ISO 27.001;
> 2006: publicada a norma no Brasil; NBR ISO/IEC 27.001;
> 2007: Julho: alterado apenas o nome da norma NBR ISSO/IEC 17.799 para a NBR ISO/IEC 27.002; (FERREIRA, 2008, p.53).

Sempre que uma empresa decide implantar uma norma de segurança em sua empresa, a mesma deve procurar equipes de auditores experientes e que possam certificar a empresa na referida norma.

Segundo Ferreira (2008) existe no Brasil empresas com equipes de auditores e consultores com conhecimento nas normas de segurança. Esses profissionais preparam as empresas para obterem a certificação desejada. No Brasil diversas organizações já foram certificadas na norma NBR ISO/IEC 27001:2006, entre elas instituições bancárias, empresas de telecomunicações e organizações governamentais.

4.2.1 Normas ISO/IEC 27001 e ISO /IEC 27002

Segundo Aragon (2008), a origem de praticamente todas as normas internacionais na questão da segurança da informação em sua origem no Governo Britânico. As normas existem para regulamentar e auxiliar as organizações no gerenciamento de seus processos relativos à segurança da informação. As normas de segurança são especialmente aplicáveis onde a proteção da informação é crítica, assim como finanças, saúde, setores público e de TI.

A norma ISO/IEC 27001 é um padrão para sistema de gestão da segurança da informação (ISMS - Information Security Management System) publicado em outubro de 2005 pela ISO e pelo International Electrotechnical Commision.

Segundo ARAGON (2008), a ISO/IEC 27002 estabelece diretriz e princípios gerais para iniciar, manter e melhorar a gestão da segurança da informação em uma organização, provendo diretrizes sobre as metas geralmente aceitas para a gestão da segurança da informação. A implantação dos objetivos de controle e dos associados da norma tem como finalidade atender aos requisitos identificados por meio da análise/avaliação de riscos.

4.3 FERRAMENTAS PARA ASSEGURAR A SEGURANÇA DA INFORMAÇÃO

Diante de inúmeros avanços tanto de ferramentas quanto de normas e procedimentos para garantir a segurança da informação, existem empresas que negligenciam algumas práticas que devem ser executadas para garantir um bom nível de segurança. Essas organizações estão cada vez mais dependentes de seus sistemas de informação e por isso aumentam o grau de importância em se implementar as melhores práticas de segurança e as principais ferramentas disponíveis no mercado atualmente.

Chamamos de ferramentas para a segurança da informação o conjunto de software, hardware e técnicas que têm como principal objetivo combater os ataques. No mercado de tecnologia da informação, existem inúmeras ferramentas e fabricantes de soluções para a segurança dos dados, sendo necessário que cada empresa avalie com cautela cada ferramenta visando checar se é aplicável a sua realidade.

Alguns serviços são utilizados pelas empresas para manterem suas informações seguras, os principais serviços são:

> Privacidade - Serviço que permite acesso à informação apenas a pessoas autorizadas, limitando o acesso às informações geralmente através do uso de criptografia.
> Autenticidade - esse serviço trata de assegurar que a comunicação seja autêntica.
> Integridade - esse serviço assegura que os dados não serão alterados durante a transmissão sem o conhecimento do receptor.
> Não-repúdio - este serviço é uma etapa posterior à autenticidade, podendo também ser um atributo desse serviço.
> Controle de acesso- este serviço limita e gerencia o acesso, a utilização de recursos, sistemas e hosts apenas por pessoas autorizadas
> Disponibilidade - este serviço tenta evitar a perda de disponibilidade dos elementos de um sistema distribuído, mesmo em caso de ataques. (GUEDES 2006, p.14 e 15).

Além dos serviços citados, as empresas podem valer-se de tecnologias tanto de hardware quanto de software para se manterem seguras. Dentre as mais utilizadas por empresas que possuem inter-relação com fornecedores e clientes através da Internet encontramos o Firewall. O Firewall é,

> Os firewalls são apenas uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Este recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas. (TANENBAUM, 2003, p.776).

Segundo Nakamura e Gesus (2007), um firewall pode também ser definido como um sistema ou um grupo de sistemas que tem o objetivo de reforçar a segurança de controle de acesso entre duas redes.

Este tipo de software pode ser dividido em categorias, mas que possui sempre o mesmo objetivo principal que é o de permitir somente a entrada de pacotes de dados que sejam confiáveis.

Segundo Parihar (2002), podemos ainda definir um firewall como um mecanismo de controle de acesso que busca tornar as redes das empresas mais seguras. Essa tecnologia auxilia as organizações a protegerem suas informações dos perigos da Internet. Logo abaixo podemos visualizar um exemplo típico do funcionamento deste tipo de ferramenta.

Mesmo implantando um firewall, a empresa ainda não está segura. Na busca por manter-se protegida, iniciou-se o desenvolvimento de uma nova ferramenta que tivesse a capacidade de prevenir e detectar intrusos surgiu então os softwares de detecção de intrusos e prevenção de intrusos.

Segundo Nakamura e Gesus (2007), um sistema de detecção de intrusos é essencial para manter a segurança em um ambiente corporativo, pois com sua capacidade de detectar intrusos auxilia na proteção do ambiente dos dados da organização.

Um sistema de detecção de intrusão pode ser definido como:

> O Intrusion Detection System(IDS) ou sistema de Detecção de intrusos(SDI) tem como principal objetivo analisar o tráfego a fim de detectar tentativas de invasões, como atividades de reconhecimento ou tentativas de se explorar alguma vulnerabilidade. Este tipo de software é muito utilizado por grandes empresas, devido a seu funcionamento ocorrer de uma forma não assistida, ela notifica uma ameaça somente quando encontra algo de errado, realizando todo o trabalho sozinho. (GUEDES, 2006, p.25)

Geralmente este tipo de ferramenta trabalha em conjunto com o firewall, a fim de aumentar a segurança na comunicação dos dados dentro das organizações. Através desse tipo de ferramenta, todo o tráfego de informações é verificado e checado para verificar a sua validade. O nível de importância desta ferramenta,

> Assim, um sistema de detecção de intrusos (Intrusion Detection System-IDS, que tem como objetivo detectar atividades suspeitas, impróprias, incorretas ou anômalas, é um elemento importante dentro do arsenal de defesa da organização. Além de ser crucial para a segurança interna, o IDS pode detectar ataques que são realizados por meio de portas legítimas permitidas e que, portanto, não podem ser protegidas pelo firewall. (NAKAMURA ; GESUS , 2007, p.265)

Uma ferramenta crucial na luta por manter as informações a salvo de ameaças é a cópia de segurança ou backup. Este tipo de ferramenta permite às organizações manter seus dados armazenados de forma segura.

Segundo Furtado (2002), toda empresa deve criar sua própria política de backup, um documento onde seja mencionada a periodicidade, a forma como serão realizados os backups bem como a forma como serão testados periodicamente. Empresas que possuem cópias de segurança de seus dados, podem retornar à operação normal em suas atividades com maior rapidez após uma catástrofe ou ataque de alguma ameaça do mundo virtual.

Na busca por manter as informações seguras, as organizações podem além das ferramentas citadas anteriormente, fazer uso da criptografia de dados. Para a criptografia pode ser definida como:

> A criptografia em função e importância cada vez mais fundamentais para a segurança das organizações; é a ciência de manter as mensagens seguras. A cifragem (encryption) é o processo de disfarçar a mensagem original, o texto claro(plaintext ou cleartext, de tal modo que sua substância é escondida em uma mensagem com o texto cifrado (ciphertext, enquanto a decifragem (decryption) é o processo de transformar o texto cifrado de volta em texto claro original. (NAKAMURA ; GESUS ,2007, p.301).

Segundo Nakamura e Gesus (2007), os processos de cifragem e decifragem são realizados através da utilização de algoritmos com funções matemáticas que alteram os textos claros, que podem ser lidos, em textos cifrados, que são transformados em inteligíveis. A criptografia é utilizada atualmente em muitas das soluções do nosso dia-a-dia, dentre as aplicações onde a criptografia se faz presente podemos citar: celulares, compras através da Internet, transações de bancos, redes privadas virtuais e certificados digitais.

Uma ferramenta muito utilizada por parte das empresas é o antivírus, este programa pode ser instalado nas máquinas das empresas com o único objetivo de detectar e eliminar as pragas virtuais. No mercado encontramos uma infinidade de opções de softwares de antivírus e, portanto as empresas devem pesquisar um bom antivírus antes de comprar.

Os softwares de antivírus que são caracterizados como completos devem possuir as seguintes características:

> Identificar e eliminar a maior quantidade possível de vírus e outros tipos de Malware;
> Analisar os arquivos que estão sendo obtidos pela Internet;
> Verificar continuamente os discos rígidos (HDs, flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e pen drives, de forma transparente ao usuário;
> Procurar vírus, cavalos de tróia e outros tipos de Malware em arquivos anexados aos e-mails;
> Criar, sempre que possível, uma mídia de verificação (disquete ou CD de boot) que possa ser utilizado caso um vírus desative o antivírus que está instalado no computador;

> Atualizar as assinaturas de vírus e Malwares conhecidos, pela rede, de preferência diariamente.
> Alguns antivírus, além das funcionalidades acima, permitem verificar e-mails enviados, podendo detectar e barrar a propagação por e-mail de vírus, Worms, e outros tipos de Malware. (CERT.BR ,2006, p. 18).

Um tipo de IDS que vem ganhando notoriedade entre as empresas é o Honeypot, que significa "pote de mel", este recurso é criado para ser sondado, atacado e comprometido.

Segundo Hoepers (2007) existem dois tipos de honeypots: os de baixa interatividade e os de alta interatividade.Como exemplos de honeypots de alta interatividade temos as honeynets e as honeynets virtuais

Para Hoepers (2007), uma honeynet pode ser:

> Uma *Honeynet* é uma ferramenta de pesquisa, que consiste de uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes.
> Uma *Honeynet* nada mais é do que um tipo de *honeypot*. Especificamente, é um *honeypot* de alta interatividade, projetado para pesquisa e obtenção de informações dos invasores. É conhecido também como "*honeypot* de pesquisa".

A soma das ferramentas aplicadas em conjunto contribuem para a prevenção e eliminação de ameaças à segurança da informação que comprometem os sistemas de informações. Proporcionalmente ao investimento realizado por uma empresa quanto à segurança de suas informações, melhor será o gerenciamento de risco de ameaças e consequentemente menor será o número de ataques aos sistemas.

5 CONSIDERACÕES FINAIS

Através deste estudo, pude concluir que, os principais problemas relacionados à segurança dos sistemas possuem forte influência das mudanças constantes na tecnologia, crescimento do número de atacantes, o avanço e popularização da Internet e na falta de preparo de algumas organizações em realizar o devido gerenciamento de ameaças, que inevitavelmente acompanham e evoluem junto com as mudanças.

As inúmeras falhas de segurança causam prejuízos no Brasil e no mundo, o que nos leva a pensar sobre a necessidade que as empresas possuem de investir de forma adequada na segurança de seus sistemas. O fato de uma organização destinar ou não investimentos anuais para a área de segurança da informação pode decretar a sua permanência no mercado.

A correlação investimento versus segurança ainda é um paradigma a ser gerenciado por inúmeras empresas, o que torna este assunto em alguns termos muito particular a cada gestor local dos sistemas de informação. Contudo, observa-se que grandes corporações

começaram a despender a devida importância à prevenção e correção das ameaças existentes às informações presentes em seus sistemas de informação.

Acreditamos que com investimentos em segurança da informação, podemos diminuir o tempo de resposta a ameaças ou até mesmo prevenir as mesmas. Através de um monitoramento e gerenciamento de todos os processos envolvidos na manipulação da informação, uma organização possuirá melhores condições para enfrentar as ameaças que inevitavelmente estão presentes nos sistemas de informação.

REFERÊNCIAS

1. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Código de prática para a gestão da Segurança da informação** (NBR ISO/IEC 17799). Rio de Janeiro: s.ed., 2001.

2. ARAGON, Aguinaldo Fernandes. **Implantando a governança de TI**: da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.

3. BEAL, Adriana. **Segurança da Informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

4. BROOKSHEAR, J.GLENN. **Ciência da Computação - uma visão abrangente**. 7. ed. São Paulo: Bookman, 2005.

5. HOEPERS, Cristine; STEDING-JESSEN, e Marcelo H. P. C. Chaves **Honeypots e Honeynets: Definições e Aplicações.** v.1.1,2007. Disponível em <http://www.cert.br/docs/whitepapers/honeypots-honeynets/> **.** Acesso em: 21 Jan. 2011.

6. COMITÊ GESTOR DE INTERNET NO BRASIL. Centro de Estudos,Resposta e Tratamento de Incidentes de Segurança no Brasil: **Cartilha de segurança para Internet**. V. 3.1, 2006. Disponível em: <http://cartilha.cert.br/download/cartilha-02-prevencao.pdf>. Acesso em: 10 de Jan. 2011.

7. COMITÊ GESTOR DE INTERNET NO BRASIL. Centro de Estudos,Resposta e Tratamento de Incidentes de Segurança no Brasil: **Incidentes Reportados ao CERT.BR**. 2010. Disponível em: <http://www.cetic.br/seguranca/index.htm>. Acesso em :10 de Jan. 2011.

8. COMITÊ GESTOR DE INTERNET NO BRASIL. Centro de Estudos,Resposta e Tratamento de Incidentes de Segurança no Brasil: **Práticas de segurança para administradores de redes Internet**. 2010. Disponível em: <http://www.nbso.nic.br/docs/seg-adm-redes>. Acesso em:21 de Jan. 2011.

9. FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu. **Política de segurança da informação**: guia prático para embalagem e implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

10. GUEDES, Alexandre Guimarães et al. **Segurança com redes privadas virtuais VPN`s**. Rio de Janeiro: Brasport, 2006.

11. MENDES, Antonio. **A era da Informação**. 2001. Disponível em: <http://www.espacoacademico.com.br/002/02col_mendes.htm>. Acesso em: 5 Fev. 2011.

12. MENDES, Antonio. **Entendendo e evitando a engenharia social**: protegendo sistemas e informações. 2004. Disponível em: <http://www.espacoacademico.com.br/043/43amsf.htm>. Acesso em: 22 Jan. 2011.

13. Módulo Security Brasil. **Pesquisa nacional Segurança da Informação.** 2010. Disponível em: <http://www.nbso.nic.br/docs/seg-adm-redes>. Acesso em: 21 de Jan. 2011.

14. NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de redes em ambientes cooperativos.** 1. ed. São Paulo: Novatec, 2007.

15. PARIHAR, Mridula et al. **TCP/IP**: a Biblia. Rio de Janeiro: Elsevier, 2002.

16. SEMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. São Paulo: Campus, 2003.

17. TANENBAUM, Andrews S. **Sistemas operacionais modernos**. 2. ed. São Paulo: Pearson, 2003.

18. TANENBAUM, Andrews S. **Redes de computadores**. 4. ed. São Paulo: Campus, 2003.

19. FURTADO, Vasco. **Tecnologia e Gestão da Informação na Gestão Pública**.Rio de Janeiro: Garamond, 2002.

20. WADLOW, Tomas A. **Segurança de redes**: projeto e gerenciamento de redes seguras.Rio de Janeiro: Campus, 2000.

A IMPORTÂNCIA DO PLANEJAMENTO PARA A PREVENÇÃO DE ACIDENTES AMBIENTAIS NAS ATIVIDADES DE PERFURAÇÃO E PRODUÇÃO OFFSHORE NO SETOR DE PETRÓLEO E GÁS

Jann Erick Possati de Moraes[8]

RESUMO

Os processos de exploração e produção de Petróleo e Gás Natural, por sua natureza, são considerados impactantes ao meio ambiente. Durante esses procedimentos são registrados diversos efeitos negativos no meio e na biota existentes onde o trabalho é desenvolvido. São necessários meios de fiscalização e políticas eficazes para um maior controle dos danos ocasionados durante essas atividades e eventuais problemas que possam surgir em decorrência dos procedimentos realizados nas operações de exploração e produção. O planejamento tem se mostrado o melhor meio de se evitar, diminuir, amenizar e recuperar a contaminação do meio pelos produtos explorados.

Palavras-chave: Gestão ambiental; Petróleo; Gás Natural; Meio ambiente; Exploração; Impacto; Fiscalização; Planejamento.

ABSTRACT

The process of exploration and production of Oil and Natural Gas, by their nature, are considered impacting the environment. During these procedures are reported several negative effects on the environment and biota exist where the work is developed. Resources are required for monitoring and effective policies for greater control of damage caused during these activities and any problems that may arise as a result of the procedures performed in the operations of exploration and production. The planning has proven to be the best way to avoid, reduce, mitigate and recover the contamination of the by products operated.

Keywords: Environmental management; Oil; Natural Gas; Environment; Exploration; Impact; Monitoring; Planning.

1 INTRODUÇÃO

Duas das matrizes energéticas mais valorizadas e exploradas na atualidade são o Petróleo e o Gás natural, compostos encontrados no subsolo continental e marítimo. A extração desses elementos é realizada em larga escala em todo o globo terrestre e representa uma grande fatia da economia mundial. Atualmente, é traçada uma corrida

[8] Aluno do curso de Petróleo e Gás da Faculdade Norte Capixaba de São Mateus

pelo chamado “Ouro Negro” e seus derivados e, a cada ano, tornam-se mais difíceis as condições de extração desses elementos, seja na terra ou no mar. E as dificuldades só aumentam, já que as reservas mundiais tendem a se esgotar com o acelerado ritmo de exploração.

A energia, em sua ampla concepção, é um bem quase que indispensável à sobrevivência humana. Por meio dela nos locomovemos, trabalhamos e realizamos todas as tarefas inerentes à nossa sobrevivência em meio à sociedade moderna. Os hidrocarbonetos, como o petróleo e o gás natural, são, hoje, principais fontes de energia dentro desse contexto. E sua forma de exploração aumenta a cada dia.

Apesar do avanço tecnológico e de inúmeras pesquisas e investimentos no setor, a exploração de petróleo e gás continua sendo impactante ao meio ambiente. A perfuração, por exemplo, é um dos procedimentos que geram uma grande quantidade de resíduos sólidos e ruídos prejudiciais à biota. O próprio trabalho de exploração e produção gera uma série de riscos de acidentes ambientais.

Diante da possibilidade de eventuais problemas nessa área, é preciso estar preparado para enfrentar os acidentes e os processos que impactam o meio ambiente. Nas áreas *offshore*, as etapas de exploração e perfuração se apresentam como umas das mais problemáticas, podendo interferir de forma direta não apenas nos animais e vegetais que habitam o ambiente, mas influenciando também toda a sociedade que depende desse meio para sobreviver, como é o caso de comunidades de pescadores.

Além do planejamento para amenizar os impactos, é preciso que todos estejam preparados e que haja um plano emergencial para lidar com situações de acidentes que tragam conseqüências sócioambientais, utilizando as melhores e mais modernas ferramentas para amenizar e gerenciar a situação.

Muitos encaram a atividade petrolífera como um mal necessário, já que vêm dela as fontes de energia mais usadas no planeta. A sociedade tem aprendido a conviver com os riscos que são inerentes dessa indústria. É claro que medidas são adotadas a fim de amenizar a questão. Entre as ações estão a adoção de legislação específica sobre o assunto e a cobrança de uma produção mais limpa (P+L) por parte das empresas. Aliás, esse tipo de cobrança tem ditado a sobrevivência de mercado de muitas organizações, já que, para ser um fornecedor de qualidade, é preciso atender normas ambientais que qualificam a organização e garantem a aceitação de seus produtos pela comunidade consumidora.

Pode-se perceber uma preocupação por parte de diferentes setores a respeito de uma produção menos impactante no setor petrolífero mundial. É fato que os atuais meios de exploração trazem prejuízos ao meio ambiente, mas também é verdade que a sociedade moderna ainda não conseguiu se desvincular da utilização do petróleo e do gás natural como matrizes energéticas.

É preciso pensar em um planejamento que contemple todas as ações necessárias para se evitar um acidente ambiental de graves proporções, e caso este aconteça, ter em mãos um plano de contingência para que os danos sejam os menores possíveis.

Este artigo tem por objetivo destacar a importância do planejamento ambiental, diga-se, da gestão ambiental, na tentativa de uma produção petrolífera menos impactante ao meio ambiente.

2 ENTENDENDO A CADEIA PRODUTIVA DE PETRÓLEO E GÁS NATURAL

Para entendermos a cadeia produtiva do petróleo é preciso fazer separações de etapas para melhor compreensão. A maioria dos autores separa a indústria petrolífera em seis etapas básicas. O objetivo é facilitar o entendimento de todo o complexo trabalho de extração até a chegada aos consumidores finais de combustíveis.

As seis etapas são definidas como exploração, perfuração, produção, transporte, refino e distribuição.

A etapa de exploração constitui-se na fase em que se buscam as reservas petrolíferas a fim de dar início aos procedimentos de retirada do petróleo do subsolo. Basicamente, é formada por pesquisas geológicas e sísmicas. Segundo Silveira (2009), é nesta etapa que se traduz os maiores riscos financeiros dos investimentos no setor, já que não é certo que as reservas serão encontradas, ou até mesmo possam ser encontradas, mas não apresentem uma grande potencialidade de produção, o que inviabiliza o trabalho de perfuração da área.

Descobrindo uma reserva promissora, que gere lucro a extração de petróleo ou gás, surge uma nova etapa com o início do trabalho de perfuração. Corrêa (2003) define esta etapa da seguinte forma:

> A perfuração de um poço de petróleo, em terra ou mar (*offshore*), é um trabalho contínuo e que só se conclui ao ser atingida a profundidade final programada pelos estudos geológicos. A perfuração é feita utilizando-se um estrutura metálica, torre ou mastro, de 30 a 40 metros de altura, bem com de seus equipamentos auxiliares, tais como: bombas de lama; colunas de tubos e comandos; tanques de lama, de diesel, de cimento, etc. (CORRÊA, 2003, p.21)

Depois de confirmada a viabilidade de exploração, e executada a perfuração, tem início a etapa de produção que acontece com a elevação do petróleo e do gás para seu armazenamento e tratamento, ficando os fluidos a disposição para o transporte que consiste na quarta fase da cadeia produtiva.

Resumidamente, o transporte é o caminho percorrido pelo óleo e gás até a chegada na refinaria onde será feito o beneficiamento da produção. Esse caminho pode ser feito por oleodutos, gasodutos, estradas de ferro e navios petroleiros.

Na refinaria, a produção é beneficiada e segue para a distribuição até o consumidor final, consistindo esta etapa como a última etapa da cadeia produtiva.

> Por fim, tem-se a distribuição que é o encaminhamento do derivado do petróleo para o consumo final. É o conjunto de transporte, estocagem, comercialização e entrega do derivado final. Cabe destacar que dependendo da arquitetura e disposição dos elementos dessas etapas existirá um preço final, ou seja, é interessante que as refinarias estejam perto dos consumidores, contudo também se sugere que a refinaria esteja próxima a unidade de produção, além da influência de onde se encontra a reserva, em um deserto, alto mar e demais áreas. (SILVEIRA, 2009, p. 27)

Silveira (2009) chama a atenção ainda para uma conceituação, que o autor caracteriza como interessante, em que o setor petrolífero padroniza as atividades em *upstream* e *downstream*. O primeiro faz referência à exploração, perfuração e produção; já o segundo faz menção às atividades de transporte, refino e distribuição. No caso deste trabalho, abordaremos as atividades de *upstream*, mais especificamente a perfuração e a produção.

3 ATIVIDADES DE *UPSTREAM* (PERFURAÇÃO E PRODUÇÃO)

Como vimos no capítulo anterior, as atividades de *upstream* se dividem em exploração, perfuração e produção. Para este trabalho, iremos nos atar aos dois últimos processos, pelas suas relevâncias e riscos de acidentes ambientais, inerentes à atividade.

3.1 OPERAÇÃO DE PERFURAÇÃO

Durante a perfuração de um poço, que se caracteriza pela aplicação de peso e rotação na broca, enquanto circula o fluido de perfuração para a remoção de cascalhos, uma série de outras operações também desempenha um papel importante dentro do processo. Podemos destacar alguns desses trabalhos como o Alargamento e Repassamento, a Conexão, Manobra e Circulação, o Revestimento e a Cimentação. A seguir detalharemos esses processos.

3.1.1 ALARGAMENTO E REPASSAMENTO

O alargamento consiste em se reperfurar o poço com uma broca de diâmetro maior que a utilizada para sua perfuração. É possível, para se economizar tempo, que as operações de perfuração e alargamento sejam feitas simultaneamente com um alargador posicionado acima da broca.

3.1.2 CONEXÃO, MANOBRA E CIRCULAÇÃO

Quando o topo do Kelly (ou, o motor, no caso de top drive) atinge a mesa rotativa, é necessário acrescentar um novo tubo de perfuração à coluna. Esta operação é chamada de conexão e, no caso de uma perfuração normal, se realiza do seguinte modo:

O tubo a ser acrescentado é colocado em local apropriado junto à mesa rotativa. Eleva-se o Kelly até o primeiro tubo de perfuração aparecer e colocado a cunha na coluna para que o seu peso fique sustentado pela mesa rotativa. Desconecta-se o Kelly da coluna e o conecta ao tubo de perfuração adicionado. Eleva-se o conjunto Kelly-tubo de perfuração e o conecta novamente à coluna. Retira-se a cunha e desce-se a coluna até o Kelly encaixar na mesa rotativa e volta-se a perfurar. No caso de perfuração com *top drive* a operação é semelhante. A manobra completa consiste na retirada e descida de toda a coluna de perfuração para a substituição da broca, por exemplo.

A circulação consiste em manter a broca pouco acima do fundo do poço e apenas circular o fluido de perfuração para remover os cascalhos do espaço anular. É normalmente feita antes da manobra, perfilagem ou descida do revestimento.

3.1.3 REVESTIMENTO DE UM POÇO DE PETRÓLEO

Durante a perfuração de poços atravessamos várias formações, o fluido de perfuração deve ser dimensionado de acordo com as características das formações com que ele entra em contato. Assim, pode ocorrer que um fluido dimensionado para as formações perfuradas não atenda os requisitos de uma zona perfurada e não possa ser modificado em função das zonas atravessadas. Então, o que fazer nestas situações?

Em situações como esta é necessário proteger as formações já atravessadas para que o fluido possa ser modificado e ao mais entre em contato com elas. Para conseguir este objetivo, devemos revestir o poço.

Os tubos de revestimento são tubos de aço especial, de diâmetro variando comumente entre 30” e 51/2” com o comprimento de 9 a 10 metros e espessura da parede variando entre ¼” e 1” . Estes tubos podem ser conectados uns aos outros através das roscas soldadas ou encaixe, sendo estas duas últimas conexões mais comuns em tubos de maior diâmetro. E a conexão destes tubos que formará a coluna de revestimento necessária para revestir o poço perfurado, sendo a quantidade de tubos utilizado variando de acordo com o comprimento final da coluna de revestimento a ser descida.

O revestimento, além de isolar as formações através de sua cimentação, serve para suportar as paredes das formações não cimentadas e possibilitar a circulação pelo seu interior, conduzindo o fluido de perfuração e cascalhos até a superfície e permitir a produção de óleo, gás e/ou água do poço. Assim que atinge a profundidade predeterminada, eles devem cimentar o revestimento, ou seja: colocar seções da tubulação de revestimento no poço para prevenir que ele desmorone. A tubulação de revestimento possui espaçadores em volta do lado externo, para ficar centralizada no poço. A equipe de revestimento coloca a tubulação de revestimento no poço.

O poço é perfurado em fases, cujo numero depende das características das zonas a serem perfuradas e da profundidade final prevista. Geralmente o numero de fases de um poço é de três ou quatro, podendo chegar a oito, em certo casos. Cada uma das fases é concluída com a descida de uma coluna de revestimento e sua cimentação.

3.1.4 CIMENTAÇÃO

A cimentação possui dois objetivos básicos dentro de um projeto de perfuração de um poço de petróleo: o 1º é o de fixar a tubulação de revestimento no interior do poço e o 2º é o de evitar que haja migração de fluidos para a parte interna da cavidade.

O procedimento é realizado por meio de bombeio de pasta de cimento e água, que são deslocadas através da própria tubulação de revestimento. Após essa etapa, é preciso verificar se a pasta ficou fortemente aderida à superfície externa do revestimento e à parede de poço, nos intervalos previamente definidos (THOMAS, 2004).

O cimento usado durante esse processo é composto, basicamente, de uma mistura de argila e calcário na proporção de 60 a 67% de Cal (CaO), 17 a 25% de Sílica (SiO2), 3 a 8% de Alumina (Al2O3) e de 0,5 a 6% de Óxido de Ferro (Fe2O3).

Existem dois tipos de cimentação nas fases de exploração, a primária e a secundária. A 1ª é considerada a principal. Ela serve para fixar o revestimento à parede do poço e evitar que ocorra a entrada de fluidos no espaço anular. Já a 2ª é feita para corrigir eventuais falhas da cimentação primária. Esta, só é realizada quando existe a necessidade de uma eventual correção da cimentação feita na 1º etapa (cimentação primária).

O procedimento de cimentação pode ser usado ainda para a vedação de canhoneios abertos e também para fechar poços que serão abandonados, o chamado abandono de poço, por meio do uso de “tampões” de cimento.

Para que o cimento seja usado em um projeto de perfuração de poços é preciso que haja um planejamento e ensaios com o material que será utilizado. Esses testes simulam o comportamento da pasta frente as condições individuais encontradas dentro de cada projeto desenvolvido para a perfuração de um poço. Neste exame é avaliado a qualidade frente a teste padronizados para a indústria do petróleo, dentro das condições estabelecidas dentro de determinado projeto como temperatura, pressão, tempo previsto de operação e regime de fluxo durante o escoamento. Os principais testes, realizados em laboratório, medem a finura, água livre, resistência à compressão, perda de água, reologia, densidade e consistometria, sendo este último o mais importante, por indicar o tempo em que a pasta tem fluidez para ser bombeada (THOMAS, 2004).

Para que a cimentação seja feita é necessário o uso de determinados equipamentos que tornam a operação mais segura e precisa. Esses “acessórios” são colocados na coluna de revestimento para garantir a qualidade durante o procedimento.

3.2 OPERAÇÃO DE PRODUÇÃO

O objetivo de se perfurar poços de petróleo é o de conseguir a produção de hidrocarbonetos. Para se obter isso, não basta perfurar até o reservatório. É preciso todo um aparato para que haja produção controlada de petróleo e gás.

O poço perfurado serve de duto, até a superfície, para o fluido que será extraído do subsolo. Para que isso ocorra é preciso a instalação de uma série de equipamentos que garantam o fluxo e a segurança dos operadores que trabalham no local. Alguns equipamentos são instalados dentro do próprio poço, e outros na área logo acima da cavidade (CORRÊA, 2003).

"Este equipamento e qualquer procedimento ou itens necessários para instalação, são, coletivamente, denominados de 'completação de poço'". (CORRÊA, 2003, p. 51).

Nos dias de hoje, a maioria dos poços, em produção, são cimentados. Isso significa que são revestidos com cimento a fim de evitar o desmoronamento das paredes e de evitar vazão do fluido entre o poço e a coluna de produção.

Para que o fluido passe da rocha para o tubo de produção é preciso fazer furos no cimento. Esse trabalho é feito com o uso da técnica de canhoneio.

> Os tiros, originados por este equipamento, perfuram o revestimento, o cimento e penetram pela formação adentro, abrindo canais para a produção de fluidos. Após este "canhoneio", perfis a cabo são descidos para verificar se as perfurações tiveram êxito. (CORRÊA, 2003, p.51)

Com o passar do tempo, o poço começa a perder pressão e a produção cai vertiginosamente. Nesses casos, é preciso adotar mecanismos de produção para que o fluxo seja recuperado.

Entre os vários mecanismos de produção temos a surgência, quando a pressão do reservatório é suficiente para empurrar o fluido para cima, sem a necessidade de equipamentos. Este tipo de mecanismo é chamado surgência natural. Temos também a surgência artificial, onde são adotados meios, com a intervenção do homem, para que o fluxo volte a atingir a superfície. Entre os mais conhecidos e utilizados estão: o bombeio mecânico, a elevação por gás, o bombeio elétrico submerso convencional, o bombeio elétrico a pistão, o bombeio hidráulico a jato, a elevação a embalo, e outros. "A finalidade de qualquer sistema de elevação artificial é criar uma determinada pressão na entrada do *tubing*, de maneira que o reservatório possa responder e produzir à vazão esperada" (CORRÊA, 2003, p. 56).

4 ATIVIDADES DE *UPSTREAM* E OS RISCOS

As atividades de *Upstream* são as que mais impactam o meio ambiente. O termo *Upstream* é comumente usado na indústria do petróleo e gás natural para designar as atividades de exploração e produção, sendo aquela a atividade inicial nesse processo.

Com relação aos riscos de acidentes com consequências ambientais, as etapas de perfuração e de transporte de hidrocarbonetos são as mais preocupantes, já que caso haja acidentes, os prejuízos serão maiores por se tratar de grandes quantidades de petróleo e gás natural sendo despejados no meio ambiente. Nesses casos, o dano à natureza pode ser irreversível, ou na melhor das hipóteses, levar anos para ser sanado.

Uma das maiores preocupações durante o processo de perfuração de poços, referentes a questões ambientais, é o controle de kicks, que significa controlar a pressão no interior do poço para que não ocorra um *blowout*, termo designado quando o fluido da formação jorra sem controle trazendo graves consequências como prejuízos financeiros, ambientais, representando riscos de acidentes com trabalhadores e a perda parcial ou total do reservatório de petróleo e/ou gás natural.

Segundo Thomas (2004), para evitar esse tipo de acidente é preciso um controle rigoroso sobre as operações a serem realizadas nos poços. Entre as ações está o monitoramento do fluido de perfuração.

> Uma das principais funções do fluido de perfuração é exercer pressão hidrostática sobre as formações a serem perfuradas pela broca. Quando esta pressão for menor que a pressão dos fluidos confinados nos poros das formações e a formação for permeável, ocorrerá influxo destes fluidos para o poço. Se este influxo for controlável diz-se que o poço está em *kick*; se incontrolável, diz-se em *blowout*. (THOMAS, 2004, p. 102)

Há riscos também durante o processo de produção do poço, como o rompimento de tubulações e consequentemente o vazamento de petróleo no mar. Durante esta etapa, existem também os efluentes que podem representar a contaminação do meio, já que os resíduos da produção petrolífera são altamente tóxicos. Entre os principais resíduos estão:

- Água de produção (água das formações e de injeção salina);
- Lamas de perfuração usadas na retirada dos cascalhos no fundo do poço;
- Cascalhos de perfuração;
- Efluente de processamento do óleo e do gás;
- Outros.

Caso ocorra qualquer um incidente de vazamento de um desses produtos, é preciso que sejam adotadas medidas rápidas para amenizar o impacto gerado no meio ambiente, e garantir uma possibilidade de recuperação da biota.

Diante do que foi exposto, pode-se perceber os riscos inerentes da atividade. Não existe uma garantia de que todos os processos serão bem executados, resultando em índice zero de falha. Notamos um alto grau de periculosidade que faz parte da própria cadeia produtiva do petróleo.

O controle e o planejamento de todas as etapas das operações são de fundamental importância para a garantia de uma atividade com menor poder de impacto sobre o meio ambiente.

5 OS DANOS PROVOCADOS AO MEIO AMBIENTE PELAS ATIVIDADES DE *UPSTREAM*

As simples atividades de perfurar e produzir petróleo geram danos ao meio ambiente, independente de eventuais acidentes que venham a ocorrer. No caso da perfuração, há

formação de muitos dejetos nesse processo, como os cascalhos que se desprendem das rochas no contato com as brocas de perfuração. O descarte correto desses materiais é fundamental para amenizar o impacto no meio ambiente.

> Os cascalhos são separados das lamas e limpos em separadores especiais. A quantidade de óleo residual presente nos cascalhos é bastante maior quando são utilizadas lamas à base de óleo. As lamas separadas e os fluidos de limpeza dos cascalhos são parcialmente reciclados para o sistema. Os cascalhos e a lama restante são descarregados no mar ou transportados para a terra para serem corretamente dispostos, a depender da situação e das exigências ambientais concernentes, sendo mais comum a primeira forma de descarte. Os cascalhos cobertos por óleo e, freqüentemente, por fluidos de perfuração tóxicos são a maior fonte de poluição das operações de perfuração. Por outro lado, sabe-se hoje que a disposição dos cascalhos, próximo ao leito marinho, ao invés de seu lançamento na superfície da água, pode limitar a dispersão dos poluentes suspensos, e, conseqüentemente, reduzir a magnitude de seu impacto potencial sobre o meio ambiente. (MARIANO, 2007, p. 163)

O grande perigo no uso dos fluidos de perfuração está em sua composição química. "Os fluidos de perfuração são misturas complexas de sólidos, líquidos, produtos químicos e, por vezes, até gases." (THOMAS, 2004, p. 80). Caso esse material tenha contato direto com o meio, os riscos de uma grave contaminação são iminentes, e o trabalho de recuperação é complicado, demorado, e representa alto custo para a empresa responsável, podendo até gerar a falência da mesma. Destacando que durante a ação de recuperação de uma determinada área pelo fato de um acidente ambiental, todas as operações de perfuração e produção realizadas na localidade são suspensas, o que agrava ainda mais os prejuízos financeiros.

A presença de materiais lubrificantes nos fluidos de perfuração são, sem dúvida, um dos fatores mais preocupantes em caso de acidentes ambientais nas atividades de *upstream*. Esses compostos são formados por hidrocarbonetos que asseguram a eficácia do processo de perfuração de poços, principalmente os direcionais, e são bastante utilizados em formações com rochas mais duras.

> Os lubrificantes são adicionados nos fluidos de perfuração desde o início, com parte das formulações originais ou no decorrer do processo, quando as necessidades operacionais aparecem. Em ambos os casos, as lamas utilizadas e os cascalhos cobertos por esses fluidos contêm consideráveis quantidades de hidrocarbonetos estáveis e tóxicos, assim como de um grande espectro de muitas outras substâncias. (MARIANO, 2007, p. 164, 165)

Por causa do alto grau de toxidade dos fluidos, é preciso que haja um planejamento para o descarte correto do material gerado pelas operações de *upstream*, para que ocorra a menor interferência possível com a biota marinha. O que norteia esse descarte são legislações específicas que abordam o assunto, com a finalidade de criar parâmetros, regras, para que o meio ambiente não seja tão prejudicado com esse procedimento.

Apesar da contaminação com hidrocarboneto ser considerada uma das mais graves no meio marinho, é preciso destacar que as atividades de produção de petróleo e gás natural *offshore* geram também outras formas de agressão ao meio ambiente, influenciando, inclusive, nas atividades pesqueiras. Durante a exploração, é alto o nível

de ruído provocado pelo uso constante da broca e pelo tráfego de embarcações de apoio no local. Estes são aspectos que também geram impacto ao meio. O ruído persiste durante a fase de exploração, o que representa transtorno à biota marinha, causando em algumas espécies, o afugentamento para outras regiões.

6 ACIDENTES QUE PODEM OCORRER NAS ATIVIDADES DE *UPSTREAM*

Durante as atividades de perfuração e produção de petróleo e gás natural existe o risco de eventuais acidentes que podem significar danos ao meio ambiente. A própria atividade em si gera impactos à biota e à estrutura marinhas, mas nada se compara aos danos provocados pelos acidentes ambientais decorrentes do trabalho de *upstream*.

Os acidentes, por sua natureza, geram graves consequências, já que, quase sempre, estão ligados a grandes reservatórios, ou então de enormes quantidades sendo transportadas por navios petroleiros.

Um agravante disso é que os desastres envolvendo o setor petrolífero afetam diretamente as pessoas que vivem na localidade atingida, transformando a questão em, também, um problema social, já que muitas famílias dependem do meio ambiente, em equilíbrio, para sobreviver.

Analisaremos, agora, alguns desses acidentes que podem representar danos ao meio ambiente e à sociedade no entorno da área atingida.

6.1 DERRAMAMENTOS DE ÓLEO, DE COMBUSTÍVEIS, GÁS, MATERIAIS PERIGOSOS E SUBSTÂNCIAS QUÍMICAS

O derramamento de óleo pode ser originado por diversas fontes nos locais de produção e perfuração: vazamentos em linhas de transferências de fluidos, vazamentos em válvulas, medidores de pressão ou juntas de conexão. Vazamento de óleo diesel pode acontecer durante as operações de perfuração, descarga de lama de perfuração à base de óleo. De acordo com técnicos do setor, os vazamentos são os tipos mais comuns de acidentes, e nesses casos as quantidades liberadas são relativamente pequenas.

6.2 *BLOWOUTS*

É considerado um dos acidentes mais graves, quando a pressão de dentro do poço é maior do que a pressão exercida pelos equipamentos e pela lama de perfuração. O resultado é a saída descontrolada de hidrocarbonetos de dentro do poço, gerando um grave dano ao meio ambiente, aos equipamentos, e representando riscos de acidentes com trabalhadores. A maior chance de acontecer é durante o processo de perfuração, mas nada impede que o incidente também ocorra durante a fase de produção do poço.

6.3 INGERÊNCIA NO DESCARTE DE RESÍDUOS

A falta de controle no descarte dos resíduos derivados da perfuração e produção de petróleo também pode ser considerada um acidente ambiental, mesmo que o motivo seja uma ingerência por parte da empresa que deveria cumprir o regulamento que dita as regras para o descartes de substâncias nocivas à biota. Esses resíduos possuem componentes tão contaminantes quanto o do próprio petróleo, o que os faz serem demasiadamente perigosos para qualquer espécie de vida marinha, no caso *offshore*.

7 QUÍMICA DOS FLUIDOS

Segundo Mariano (2007, p.174), "o espectro de substâncias químicas que penetra no ambiente marinho em conseqüência das diferentes atividades de perfuração e produção é bastante amplo e inclui centenas de compostos e de suas combinações". Essa afirmação é feita devido a gama de compostos utilizados no processo de *upstream* que podem ser naturais ou artificiais, e a existência dos hidrocarbonetos existentes nas formações, em forma de óleo ou gás.

A composição dos fluidos de perfuração varia de acordo com diversos fatores, entre eles o tipo de trabalho que será realizado e o tipo de rocha a ser cortada. Quanto maior o grau de dificuldade de perfuração, maior a utilização de fluido à base de óleo, que facilita o desgaste da formação rochosa. Entretanto, nos últimos anos, tem sido bastante difundido o uso de fluido à base de água. Um dos motivos é o baixo grau de toxidade deste frente ao fluido à base de óleo, que continua sendo usado em poços direcionais e em rochas mais rígidas. Ainda não há tecnologia para suprimir totalmente o uso desde tipo de componente.

> Originalmente, os fluidos à base de óleo incluíam o diesel na sua composição como componente básico, devido à sua ampla disponibilidade e baixo custo. Entretanto, após o início da década de 80, especialmente após muitos países terem proibido o uso do diesel nas lamas de perfuração, as companhias de petróleo começaram a desenvolver novas formulações, com o objetivo de substituir o óleo por substâncias menos perigosas. Os fluidos de perfuração alternativos são compostos principalmente por moléculas de baixo peso molecular, menos tóxicas e com maior solubilidade em água, de natureza parafínica e aromática, e, além disso, continuam sendo desenvolvidas pesquisas neste campo. (MARIANO, 2007, p. 175)

Estudos recentes têm trazido à baila fluidos de perfuração à base de compostos químicos, que garantem tanta eficácia quanto os fluidos à base de óleo, só que com uma vantagem, um grau menor de toxidade. O problema desses produtos é o alto custo para a sua produção, mas já são considerados como uma solução ambiental e tecnológica para a área de produção de petróleo e gás.

O petróleo e o gás natural representam a presença de hidrocarbonetos em sua forma mais densa. Os principais componentes desses produtos são os hidrocarbonetos saturados, os hidrocarbonetos aromáticos, as resinas e os asfaltenos.

Thomas (2004, p. 10, 11), explica que os hidrocarbonetos saturados constituem o maior grupo, formado por alcanos normais (n-parafinas), isoalcanos (isoparafinas) e cicloalcanos (naftenos). No petróleo são encontradas parafinas normais e ramificadas, que vão do metano até 45 átomos de carbono. As parafinas normais representam cerca de 15% a 20% do petróleo, variando, no entanto, entre limites bastante amplos (3% e 35%). A tabela 1 mostra a composição química de um petróleo típico.

TABELA 1 – COMPOSIÇÃO QUÍMICA DE UM PETRÓLEO TÍPICO

Substâncias	Concentrações
Parafinas Normais	14%
Parafinas Ramificadas	16%
Parafinas Cíclicas (Naftênicas)	30%
Aromáticos	30%
Resinas e AsfaltenosLítio	10%

Fonte: Thomas, 2004

O gás natural é uma composição também formada de hidrocarbonetos. Sua composição pode se estender desde o metano até o hexano. Ele é encontrado na forma livre ou associado ao petróleo nos reservatórios naturais. A tabela 2 mostra as faixas de composição dos gases extraídos a partir de reservatórios de gás natural e a partir de reservatórios de óleo.

TABELA 2 – COMPONENTES DO GÁS NATURAL (% EM MOL)

Substâncias	Campos de gás natural	Gás liberado do óleo
Nitrogênio	Traços – 15%	Traços – 10%
Dióxido de Carbono	Traços – 5%	Traços – 4%
Gás Sulfídrico	Traços – 3%	Traços – 6%
Hélio	Traços – 5%	Não
Metano	70 – 98%	45 – 92%
Etano	1 – 10%	4 – 21%
Propano	Traços – 5%	1 – 15%
Butanos	Traços – 2%	0,5 – 2%
Pentanos	Traços – 1%	Traços – 3%
Hexanos	Traços – 0,5%	Traços – 2%

Fonte: Thomas, 2004

Como mostrado nas tabelas, os hidrocarbonetos são compostos altamente tóxicos e prejudiciais se colocados em contato como meio ambiente. Por isso é preciso uma série de cuidados para evitar riscos de acidentes ambientais.

8 LEGISLAÇÃO PARA AS ATIVIDADES DE *UPSTREAM* E ACIDENTE EM DECORRÊNCIA DOS PROCEDIMENTOS DE PERFURAÇÃO E PRODUÇÃO

A legislação brasileira reserva um grande número de leis, decretos e resoluções que tratam do meio ambiente e dos danos ambientais que possam ser provocados em decorrência das atividades de *upstream*. Apesar de existir um grande número de normas, as regras nem sempre são cumpridas por problemas que afetam diversos órgãos da Administração Pública, como a falta de aplicação e fiscalização das leis por déficit de pessoal na estrutura pública.

Segundo Bezerra (2005, p. 3), o arcabouço jurídico brasileiro guarda uma riqueza de textos legais que tratam da proteção ambiental nas atividades de exploração e produção de petróleo e gás no Brasil, garantindo aos culpados as responsabilidades penais e criminais.

Os principais órgãos do Ministério do Meio Ambiente que atuam na proteção ambiental no país são o Conselho Nacional do Meio Ambiente (CONAMA) e o Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA). O primeiro é um órgão consultivo e deliberativo e o segundo um órgão executor e fiscalizador das políticas voltadas para a área.

A resolução 293/2001 dispõe sobre o conteúdo mínimo do plano de emergência individual para incidentes de poluição por óleo originado em portos organizados, instalações portuárias ou terminais, dutos, plataformas, bem como suas respectivas instalações de apoio. Há ainda legislações internacionais das quais o Brasil ratificou adesão como convenções que tratam da responsabilidade civil em danos causados por óleo no mar e a que trata da prevenção, resposta e cooperação em caso de poluição por óleo.

> O petróleo é responsável por uma percentagem enorme da energia consumida no mundo, e a indústria de petróleo é grande geradora de receita e empregos para a sociedade brasileira, participando com fatia considerável, e a cada ano crescente, no PIB do País. Sua não utilização como fonte de energia, hoje, é algo inimaginável. A única alternativa é buscar o equilíbrio entre o desenvolvimento e a mínima degradação ambiental, o que convenhamos é algo bastante complexo. Com relação à proteção ambiental das atividades de E & P, os atores, estudiosos e interessados da indústria petrolífera brasileira já chegaram a algumas conclusões de como contribuir para se atingir o desenvolvimento sustentável. Deve-se exercer as atividades de E & P com o mínimo de impactos ambientais quanto seja possível, a partir de medidas que destacamos a seguir [...] Com relação à proteção ambiental das atividades de E & P, os atores, estudiosos e interessados da indústria petrolífera brasileira já chegaram a algumas conclusões de como contribuir para se atingir o desenvolvimento sustentável. Deve-se exercer as atividades de E & P com o mínimo de impactos ambientais quanto seja possível, a partir de medidas que destacamos a seguir [...] Outra medida de grande valia e que já se torna consenso na indústria é a utilização da chamada Avaliação Ambiental Estratégica – AAE [...] Várias outras medidas podem aqui ser enumeradas como: o incentivo à efetiva participação populacional nos procedimentos de licenciamento, já que as comunidades e instituições locais devem ter um papel importante na execução das normas ambientais na E & P de petróleo e gás; utilização de estratégia e política amplamente integrada no uso dos recursos naturais e da energia; inclusão da licença de desativação, a ser requerida após o término da produção, visando ao escomissionamento/desinstalação da atividade e; maior participação da indústria do petróleo no CONAMA, interferindo na elaboração de resoluções de seu interesse. (BEZERRA, 2005, p. 6, 7)

Ao longo dos anos, a legislação brasileira vem editando normas para melhor adequação da questão ambiental ao funcionamento da indústria petrolífera, uma maneira de permitir o funcionamento e minimizar os impactos gerados pela produção de petróleo e gás no País.

Britto (2009) destaca que o aumento com a preocupação ambiental, referente à atividade de exploração de hidrocarbonetos no Brasil, teve início com a Emenda Constitucional nº 09, de 09 de novembro de 1995, quando houve a flexibilização da forma de execução do monopólio pela União, para as atividades de exploração, desenvolvimento e produção de petróleo e gás natural.

Segundo a autora, a "virada" na legislação ocorreu, de fato, em 1997 com a criação da lei do petróleo e com a edição de normas mais rigorosas para a liberação de atividades e fiscalização por parte de órgãos de proteção ambiental.

> Mas foi com a criação da Lei Federal nº 9.478, de 06 de agosto de 1997, também conhecida como "lei do Petróleo", que foram estabelecidas as bases para a abertura do mercado e a flexibilização do monopólio da União. Essa lei dispõe sobre a política energética nacional, as atividades relativas ao monopólio do petróleo, e também institui o Conselho Nacional de Políticas Energéticas (CNPE) e a Agência Nacional do Petróleo (ANP). Neste mesmo ano (1997) foi regulamentado o sistema nacional de licenciamento ambiental, através da Resolução CONAMA nº 237, de 09 de dezembro. Esta resolução determina que todas as atividades e empreendimentos que utilizem recursos ambientais e/ou sejam passíveis de degradação ambiental dependerão de prévio licenciamento do órgão ambiental competente. Anteriormente a esta norma, o CONAMA já havia estabelecido os procedimentos específicos para licenciamento ambiental visando o melhor controle e gestão ambiental das atividades relacionadas a exploração e lavra de jazidas de combustíveis líquidos e gás natural. Através da Resolução CONAMA nº 23, de 7 de dezembro de 1994, as atividades relacionadas a sperfuração e produção de petróleo e gás natural ficam condicionadas ao licenciamento pelo IBAMA ou pelos órgãos ambientais estaduais. (BRITTO, 2009, p. 26)

Ainda segundo Britto (2009), com a abertura das nossas jazidas para capital estrangeiro, houve um aumento significativo na quantidade de empresas atuantes tanto em terra (*onshore*), quanto no mar (*offshore*), isso fez com que a cobrança por normas de garantia à proteção ambiental fossem intensificadas par a preservação do meio ambiente, como garante a própria Constituição Federal de 1988. "Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao poder público e à coletividade o poder de difundi-las e preservá-la para a presente e futuras gerações" (CF, art. 225).

Com a promulgação da nossa Carta Magna, uma série de regras passou a ser formalizada, a fim de garantir e promover a melhoria das condições ambientais do nosso País. Com a indústria do petróleo não foi diferente. A legislação e instrumentos normativos que tratam do assunto preveem penas de ordem administrativa, civil e criminal para autores e co-autores de condutas que prejudiquem o meio ambiente.

9 CONCLUSÃO

O petróleo e o gás natural ainda são considerados uns dos principais meios de energia e são usados em larga escala no cenário mundial. Imaginar o fim da exploração e produção desses compostos é uma utopia, já que a sociedade se tornou dependente dessas fontes energéticas. O setor petrolífero é um dos maiores empregadores mundiais, representando a base econômica de muitos países no mundo.

O que deve ser feito é associar a exploração ao menor impacto ao meio ambiente. Tentar buscar um desenvolvimento do setor com a mínima degradação ambiental possível, já que as atividades *offshore* representam um grande impacto ao meio ambiente se não houver concordância com as políticas públicas voltadas para o setor.

No entanto, percebe-se que na última década, as empresas exploradoras de petróleo têm se preocupado com uma gestão sustentável do setor. O mercado internacional tem exigido o respeito às normas legais tanto dos países onde ocorre a exploração quanto das convenções internacionais. Atualmente, um acidente ambiental não traz prejuízos apenas para o meio ambiente e as pessoas que dependem dele, mas também as consequências podem atingir o faturamento da empresa, tanto na forma de multas, aplicadas pelos órgãos ambientais, como na queda da valorização dos papéis dessa empresa.

É preciso colocar em prática ações que minimizem os impactos ambientais e garantam a produção, sem prejuízos financeiros ou ambientais. Para isso, algumas ações precisam ser efetivadas antes, durante e depois das etapas de perfuração e produção de poços de petróleo e gás. Uma das medidas que devem ser adotadas e a avaliação dos riscos inerentes à atividade em relação à localidade em que serão realizadas as operações. Dessa forma podemos traçar estratégias de contenção, em casos de acidentes, e de monitoração para evitar qualquer sinistro.

Durante as operações de perfuração e produção, os derramamentos de óleo são considerados a maior ameaça em potencial, já que o óleo pode contaminar a água, no caso da extração *offshore*, de diferentes maneiras como um *blowout*, ou mesmo vazamentos vindos de equipamentos e tubulações. Para evitar qualquer imprevisto é preciso um gerenciamento para evitar a probabilidade de qualquer acidente ambiental. Fundamental é ter em mãos um planejamento de medidas adotadas caso ocorra um vazamento de hidrocarboneto. Neste caso, é preciso um estudo prévio para prever o comportamento do óleo no mar, sabendo a direção que poderá migrar e o tempo de dispersão.

Outro perigo são os resíduos sólidos que podem partir da própria plataforma, como plásticos e outros derivados tóxicos que comprometem a vida de animais marinhos. É preciso uma fiscalização eficiente, a fim de que esse tipo de dejetos não seja jogado ao mar.

Os efluentes de perfuração, como cascalhos e lama de perfuração, precisam também de cuidados especiais. É preciso cumprir as regras de descarte dos efluentes no mar para a preservação da biota marinha. Para tanto, são necessários diversos mecanismos de controle da qualidade da água que devem ser comprovados por meio de documentos apresentados aos organismos de controle e fiscalização.

Outra maneira de tornar a produção marítima mais sustentável é diminuindo as emissões atmosféricas. É preciso desenvolver tecnologias para armazenamento e reutilização de todos os gases gerados no processo de produção petrolífera, evitando o seu descarte por meio da queima em *flaires*.

Essas são apenas algumas maneiras de diminuir o impacto gerado pela exploração petrolífera em áreas *offshore*.

Aliar a exploração ao menor dano possível ao meio é fundamental para garantir uma exploração sustentável e respeitando as normas exigidas pelas políticas ambientais. Para colocar em prática toda a legislação vigente, é preciso investimento pelo poder público para reforçar as ações de fiscalização e monitoramento das atividades de perfuração e produção *offshore* de petróleo e gás natural.

REFERÊNCIA

1. AFFONSO, Fernando Luiz. **Metodologia para implantação de sistema de gestão ambiental em serviços de engenharia para empreendimentos petrolíferos:** Um estudo de caso. Tese de Mestrado em planejamento estratégico – UFRJ. Rio de Janeiro, 2001, 218 p.

2. BEZERRA, Luiz Gustavo Escorcio. **A Indústria Brasileira de Petróleo Upstream e a Proteção Ambiental** – Arcabouço Jurídico e Breves Reflexões. Anais do 3º Congresso Brasileiro de P&D em Petróleo e Gás: UERJ, 2005.

3. BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF, Senado, 1988.

4. BRITTO, Mariana de Karam e. **Mamíferos marinhos, a atividade de prospecção sísmica e o uso do sistema de monitoramento de animais marinhos – SIMMAM**. Tese de mestrado em em Ciência e Tecnologia Ambiental: Universidade do Vale do Itajaí. Itajaí, 2009, 106 p.

5. CORRÊA, Oton Luiz Silva. **Petróleo:** Noções sobre exploração, perfuração, produção e microbiologia. Rio de Janeiro. Interciência: Petrobras, 2003.

6. MANÇU, R. J. de S; MONTEIRO, A. O. M; BRUNI, A. L. **A gestão ambiental na produção de petróleo no Estado da Bahia:** um comparativo entre a aderência das práticas de gestão ambiental de uma empresa nacional e uma estrangeira às normas internacionais. In: 5ème colloque de l'IFBAE, 2009, Grenoble.

7. MARIANO, Jacqueline Barboza. **Proposta de Metodologia de Avaliação Integrada de Riscos e Impactos Ambientais para Estudos de Avaliação Ambiental Estratégica do Setor de Petróleo e Gás Natural em Áreas Offshore**. Tese de Doutorado em Ciências de Planejamento Energético: COOPE/UFRJ, 2007.

8. SILVEIRA, Thiago Gomes da. **Uma análise da exploração petrolífera no Sul do Estado do Espírito Santo:** Estudo de caso. Monografia de Graduação para o título de Bacharel em Ciências Econômicas: UFES. Vitória, 2009, 68 p.

9. THOMAS, José Eduardo. **Fundamentos da Engenharia do Petróleo**. 2ª ed. Rio de Janeiro. Interciência: Petrobras, 2004.

OTIMIZAÇÃO NO USO DO PROTOCOLO IPV4

Lucas Costa Jardim[9]

RESUMO

Nos tempos atuais a utilização da internet e das redes de computadores cresce de forma exponencial a cada dia. Para cada dispositivo ou computador conectado em uma rede é necessário que ele tenha configurado um endereço lógico (protocolo IP) para que o mesmo possa ser enxergado na rede e assim trocar informações com demais dispositivos conectados. Neste artigo abordaremos a estrutura deste protocolo, bem como a sua utilização de forma que não ocorram certos desperdícios de endereços, pois com a quantidade atual de dispositivos conectados à rede a quantidade disponível de endereços IPV4 já não está sendo mais suficiente para atender a demanda de usuários.

Palavras Chave: Otimização; Protocolo; Redes

ABSTRACT

In modern times the use of the Internet and computer networks grows exponentially each day. For each computer or device connected to a network it needs to have configured a logical address (IP protocol) so that it can be discerned in the network and to exchange information with other connected devices. In this article we discuss the structure of this protocol as well as its use so that there are no certain address waste, because with the current number of devices connected to the network the amount of available IPv4 addresses is no longer being longer sufficient to meet demand users.

Keyword: optimization; protocol, network.

1 INTRODUÇÃO

As redes de computadores têm um papel fundamental e essencial nos dias atuais, elas nos mantêm conectados e através delas são oferecidos uma infinidade de serviços aos seus usuários, de forma direta ou indireta. Um usuário comum faz o uso das redes de computadores, de forma direta, para se manter conectado a internet e acessar seus e-mails, redes sociais, mensagens instantâneas, jogar on-line, pesquisar, entre outras atividades. Outro usuário pode também estar utilizando as redes de computadores, de forma indireta, quando se paga uma conta em um banco, quando acessa o seu saldo em um caixa eletrônico entre outros serviços essenciais que só são disponibilizados aos usuários graças às redes de computadores. Nos dias atuais a quantidade de dispositivos que estão conectados em rede e conectados à internet cresce de forma exponencial e para que cada um desses dispositivos esteja conectado em uma rede de computador é

[9] Graduado em Sistemas da Informação.

necessário que cada um deles tenha um endereço lógico, este endereço lógico é chamado de IP (Internet Protocol).

Com o crescente crescimento da quantidade de dispositivos conectados à internet a disponibilidade de endereços lógicos existentes não está sendo mais o suficiente para conectar tantos dispositivos disponíveis nos tempos atuais. Existem algumas soluções que podem ser aplicadas ao protocolo IP de forma que haja um melhor aproveitamento dos mesmos pelas empresas de Telecom ou empresas que possuem uma infra-estrutura de médio porte. Este artigo mostrará a estrutura do endereço Lógico versão 4 e as soluções que podem ser utilizadas para um melhor aproveitamento dos endereços disponíveis em uma estrutura de rede.

Como objetivo geral o presente artigo busca fornecer um entendimento no que se refere a estrutura do protocolo IP versão 4, tais como suas classes, máscaras de sub-rede, porção de rede e porção de host.

Para atender ao objetivo geral tem-se os seguintes objetivos específicos: Mostrar como utilizar técnicas nos endereços lógicos disponíveis para uma infra-estrutura a fim de aproveitar melhor a quantidade de endereços lógicos disponíveis, fazendo um melhor uso do protocolo de modo que as necessidades da rede sejam atendidas.

2 PROTOCOLO IP VERSÃO 4

Em qualquer rede de computador ou em um único computador conectado à internet se faz necessário a atribuição de um endereço IP à esses computadores. O endereço IP, também conhecido como endereço lógico, é quem vai identificar um computador, ou outro dispositivo conectado à rede, de forma única. Para todo computador conectado à rede se faz necessário a atribuição de um endereço IP para que o mesmo possa ser enxergado na rede e assim trocar informações com os demais dispositivos conectados.

2.1 ESTRUTURA DO ENDEREÇO LÓGICO (IPV4)

O endereço IPV4 é formado por 32 bits que estão divididos em 4 octetos. A representação do endereço lógico para um usuário final não será exibida em um formato binário e sim em formato decimal. Como cada octeto possui 8 bits cada octeto poderá variar de 0 até 255. O sistema numérico de base 2, ou binário, representa valores utilizando apenas os algarismos 0 e 1, portanto se todos os bits de um octeto assumirem o valor zero teremos 8 bits contíguos com valor zero e transformando-os para o sistema numérico base 10 teremos o valor zero. Caso os 8 bits do octeto assumirem o valor 1, que é o valor máximo que um bit pode assumir, teremos uma sequência de 8 bits com valor um, convertendo este valor de base 2 (binário) para base 10 (decimal) teremos o valor 255. Na figura 02 temos uma rede local e seus respectivos endereços lógicos utilizados em cada dispositivo.

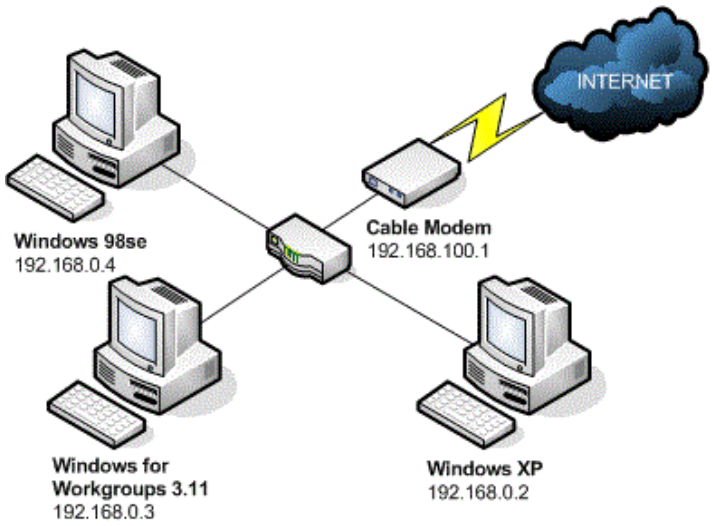


Figura 1 - Rede Local

O protocolo IP possui uma quantidade de bits que é utilizada para identificar qual é a rede a qual aquele endereço pertence e existe outra porção de bits que é utilizada para identificar qual é o identificador único do computador ou do dispositivo conectado à rede. Somente utilizando o endereço lógico em um computador não é suficiente para identificar qual é rede a qual o computador pertence e qual é a porção de bits que é usada para identificar o computador em uma rede, para que a representação seja feita por completa se faz necessário o uso da máscara de sub-rede. A máscara de sub-rede é quem vai mostrar para a rede qual é o identificador de rede, em um endereço ip, e qual é o identificador do computador ou dispositivo conectado a rede. Inicialmente os endereços IPs de versão 4 foram divididos em 5 classes diferentes, onde cada classe comporta uma quantidade diferente de redes distintas que podem ser formadas e cada rede comporta uma certa quantidade de computadores ou dispositivos, dependendo da classe a qual a rede pertence. A máscara de sub-rede padrão varia de acordo com a classe de IP.

2.2 CLASSIFICAÇÃO DOS ENDEREÇOS IPV4

A classificação dos endereços IPV4 foi dividida nas classes A, B, C, D e E. Iremos mostrar apenas as classes que são utilizadas para fim de endereçamento, ou seja, as classes A, B e C. Podemos diferenciar cada classe observado o valor do primeiro octeto do endereço IP. Por exemplo, endereços de classe A podem assumir do valor 0 até o valor 127 em seu primeiro octeto.

2.2.1 Classe A

Os endereços IP’s classe A possuem como característica o fato de que o primeiro bit de qualquer endereço IP sempre será 0, com base nesta informação podemos calcular qual

será a variação do primeiro octeto da classe A. Caso todos os bits do primeiro octeto que podem variar assumirem o valor zero teremos:

0 0 0 0 0 0 0 0 . x x x x x x x x . x x x x x x x x . x x x x x x x x

Convertendo o primeiro octeto da base 2 para base 10 teremos o valor zero, ou seja, o menor valor que o primeiro octeto classe A poderá assumir é igual a zero.

Caso todos os bits que podem variar no primeiro octeto assumirem o valor 1 chegaremos ao valor máximo que um endereço IP classe A poderá assumir. Assim teremos.

0 1 1 1 1 1 1 1 . x x x x x x x x . x x x x x x x x . x x x x x x x x

Convertendo o primeiro octeto da base 2 para a base 10 teremos o valor 127, ou seja, o maior valor que o primeiro octeto de um endereço IP classe A pode atingir é 127.

O valor 127 no primeiro octeto não pode ser utilizado pelo fato de ser um endereço reservado, este endereço é usado para fazer referência à sua própria interface de rede, portanto temos que a classe A possui o seu primeiro octeto variando de 0 até 126.

A máscara padrão é responsável por esclarecer ao computador qual é a porção do IP que é referente à rede e qual é a porção do IP que se refere a identificação do computador ou dispositivo na rede. A máscara padrão é composta por 32 bits, sendo que, a porção que se refere à rede possui os bits com valor 1 e a porção do IP que é utilizada para identificar um host na rede é representado pelos bits 0.

A figura 02 mostra a representação da máscara padrão classe A.

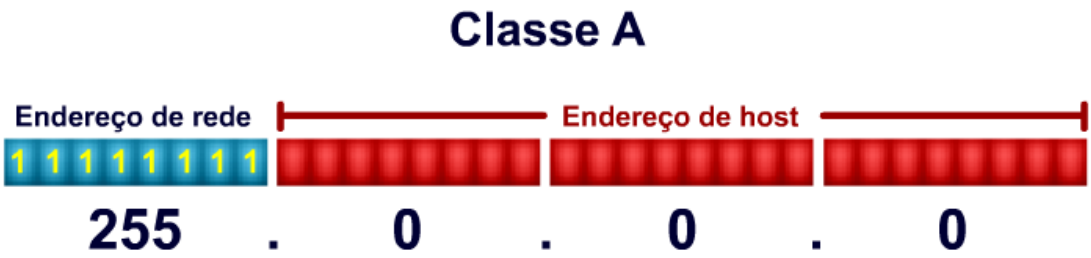


Figura 2 - Máscara padrão classe A

Com base nessas informações podemos calcular a quantidade de redes distintas que se pode formar com a classe A e podemos ainda calcular a quantidade de máquinas que podemos conectar para cada rede classe A.

Para efetuarmos estes cálculos de redes e de hosts para cada classe utilizaremos a fórmula 2^N -2, onde o significado de n muda de rede para host.

2.2.1.1 Cálculo da quantidade de redes da classe A.

Para encontrarmos a quantidade de redes distintas que podemos formar utilizando a classe A aplicamos a fórmula acima onde o valor de N será a quantidade de bits que podem variar na porção de rede da classe. Para a classe A temos:

$2^N - 2$
N = Bits da porção de rede que variam, na classe A são 7, logo temos:
$2^7 – 2 = 126$ redes distintas.

2.2.1.2 Cálculo da quantidade de hosts da classe A.

Para encontrarmos a quantidade de hosts que podemos conectar em cada uma das redes aplicaremos a mesma fórmula 2^N -2, mas o valor de N aqui será a quantidade de bits referentes à porção de host da classe. Para a classe A temos:

$2^N – 2$
$2^{24} – 2 = 16.777.214$ máquinas poderão ser conectadas em uma rede classe A.

2.2.2 Classe B

Os endereços IP's de classe B sempre terão os seus 2 primeiros bits com os valores 1 e 0, respectivamente. Com essa informação sabemos que o primeiro octeto de qualquer endereço IP classe B sempre começará com os bits 1 e 0. Com base nessa informação podemos calcular qual será o intervalo numérico que o primeiro octeto de classe B poderá assumir. Se todos os bits que podem variar no primeiro octeto de um classe B assumirem valor zero teremos o menor valor do intervalo da classe B para o primeiro octeto.

1 0 0 0 0 0 0 0 . x x x x x x x x. x x x x x x x x. x x x x x x x x

Convertendo o primeiro octeto da base 2 para base 10 teremos o valor 128. Caso os bits que podem variar no primeiro octeto da classe B assumirem o valor 1 teremos o maior valor do primeiro octeto do intervalo da classe b.

1 0 1 1 1 1 1 1 . x x x x x x x x. x x x x x x x x. x x x x x x x x

Convertendo o valor do primeiro octeto da base 2 para base 10 teremos o valor 191, logo sabemos que o primeiro octeto da classe B poderá variar entre 128 até 191.

Os endereços IP's pertencentes à classe B terão o primeiro e o segundo octetos sendo os octetos que representam o valor da rede e o terceiro e quarto octeto representarão o identificador do computador ou dispositivo conectado à rede. A figura 03 mostra a máscara padrão classe B.

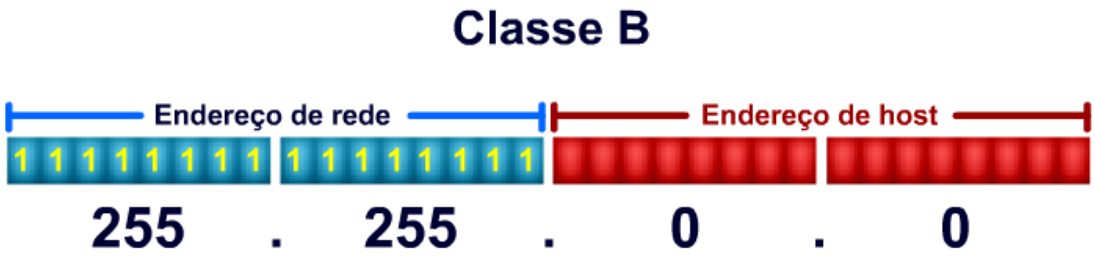


Figura 3 - Máscara padrão classe B

2.2.2.1 Cálculo da quantidade de redes da classe B.

Para encontrarmos a quantidade de redes distintas que podemos formar utilizando a classe B aplicaremos o mesmo procedimento utilizado para a classe A. Para a classe B temos:

$2^N - 2$
N = Bits da porção de rede que variam, na classe B são 14, logo temos:
$2^{14} – 2$ = 16.382 redes distintas poderão ser formadas com a classe B.

2.2.2.2 Cálculo da quantidade de hosts da classe B.

Para encontrarmos a quantidade de hosts que podemos conectar em cada uma das redes aplicaremos a mesma fórmula 2^N -2, mas o valor de N aqui será a quantidade de bits referentes à porção de host da classe. Para a classe B temos:

$2^N – 2$
$2^{16} – 2$ = 65.534 máquinas poderão ser conectadas em uma rede classe B.

2.2.3 Classe C

Todos os endereços IP's classe C terão seus 3 primeiros bits com os respectivos valores 1, 1 e 0. Com base nessa informação podemos calcular qual será o intervalo que o primeiro octeto classe C poderá assumir. Caso os bits do primeiro octeto que podem variar assumirem valor zero teremos o menor valor do intervalo.

1 1 0 0 0 0 0 0 . x x x x x x x x. x x x x x x x x. x x x x x x x x

Convertendo o valor do primeiro octeto da base 2 para a base 10 teremos o valor 192. Percebemos com esse cálculo que este será o menor valor assumido pelo primeiro octeto de um IP classe C. Caso os bits que podem variar no primeiro octeto assumirem, todos eles, o valor 1 teremos o maior valor do intervalo do primeiro octeto de um classe C.

1 1 0 1 1 1 1 1 . x x x x x x x x. x x x x x x x x. x x x x x x x x

Convertendo o valor da sequência binária do primeiro octeto para base decimal teremos o valor 223 que é o maior valor que o primeiro octeto poderá assumir dentro da classe C.

Todos os endereços IP's de classe C terão como porção de rede os 3 primeiros octetos e somente o último octeto é responsável por identificar um computador (host) ou outro dispositivo na rede. A figura 04 nos mostra a máscara padrão da classe C.

Figura 4 - Máscara padrão classe C

2.2.3.1 Cálculo da quantidade de redes da classe C.

Para encontrarmos a quantidade de redes distintas que podemos formar utilizando a classe C aplicaremos o mesmo procedimento utilizado para as classes A e B.

$2^N - 2$
N = Bits da porção de rede que variam, na classe C são 21, logo temos:
$2^{21} – 2$ = 2.097.150 redes distintas poderão ser formadas com a classe C.

2.2.3.2 Cálculo da quantidade de hosts da classe C.

Para encontrarmos a quantidade de hosts que podemos conectar em cada uma das redes aplicaremos a mesma fórmula 2^N -2, mas o valor de N aqui será a quantidade de bits referentes à porção de host da classe. Para a classe C temos:

$2^N – 2$
$2^8 – 2$ = 254 máquinas poderão ser conectadas em uma rede classe C.

3 DIVISÃO DE SUB-REDE

A máscara padrão tem um importante papel na configuração das redes de computadores, é através dela que ocorre a identificação da rede que o computador está conectado e também a identificação de um host ou outro dispositivo conectado à rede. Até agora utilizamos a máscara padrão de sub-rede de cada classe, a partir de agora iremos alterar estas máscaras de forma que possibilite novas configurações de rede de computadores e

também para que haja um melhor aproveitamento dos endereços IP's disponíveis em cada faixa de IP. Através da máscara padrão de cada classe calculamos quantos IP's válidos podemos conectar em uma rede de determinada classe. Em uma rede classe C podemos conectar, utilizando a máscara padrão, até 254 computadores, que é uma quantidade que atende a maioria das empresas de pequeno porte e ainda sobram endereços IP's válidos, ou seja, endereços que podem ser configurados em um host para endereçá-lo, provocando assim certo "desperdício" de endereços válidos.

Existem outras situações onde há a necessidade de não permitir que setores diferentes de uma organização se comuniquem entre si, por exemplo, em uma escola o setor financeiro não pode se comunicar com os computadores disponíveis em um laboratório. Uma das soluções para esse problema é criar sub-redes, assim pode-se configurar em uma mesma rede local faixas de sub-redes diferentes para setores diferentes não permitindo uma comunicação entre setores, ou melhor, entre sub-redes distintas.

3.1 CALCULANDO A QUANTIDADE DE SUB-REDES

Para encontrarmos a quantidade de sub-redes necessárias para que atenda uma determinada situação deve-se efetuar um cálculo sobre os bits da máscara padrão da faixa de IP que está sendo utilizada pela organização. Para melhor exemplificar o cálculo de sub-rede iremos criar a seguinte situação: Uma empresa possui uma matriz e com 6 setores diferentes. Cada setor possui 20 computadores. Se a empresa dispuser de um endereço de rede classe C para cada setor haverá um desperdício de endereços IP's pelo seguinte: Cada rede classe C suporta até 254 computadores, mas cada setor faz uso de apenas 20 computadores, logo temos que para cada setor haverá um desperdício de 234 endereços IP's válidos. Este problema pode ser contornado fazendo uma divisão de sub-rede onde apenas uma rede classe C daria para conectar todos os setores da empresa e não haveria comunicação entre os setores. Para calcularmos a quantidade de sub-redes ideal para solucionar o problema utilizaremos a máscara padrão da classe de IP a ser utilizada na rede, neste caso classe C.
A máscara padrão da classe C é 255.255.255.0, onde a porção de rede é representada pelos 3 primeiros octetos e o último octeto representa a porção de host. Para melhor visualização do cálculo convertemos a máscara padrão para binário, que ficaria da seguinte maneira:

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0
---------- Porção de Rede ----------

Para encontrarmos a quantidade de sub-redes utilizaremos a fórmula 2^N -2, onde o valor de N será os bits que serão "emprestados" da porção de host para a porção de rede. Para o problema em questão serão necessários 3 bits a mais na porção de rede da máscara.

2^N -2
2^3 -2 = 6 Sub-redes.

Como foram utilizados 3 bits da porção de host na porção de rede a máscara padrão foi alterada e o seu novo valor é:

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 0 0 0 0 0
---------- Porção de Rede ----------

Note que a porção de rede agora está alterada, foram adicionados 3 bits à porção de rede e a porção de host foi diminuída em 3 bits, agora basta converter os valores dos octetos da base 2 para base 10 para termos o valor da nova máscara de rede.

O valor da nova máscara é **255.255.255.224**

3.2 CALCULANDO A QUANTIDADE DE HOST

Agora se faz necessário verificar se a quantidade de endereços IP's válidos disponíveis com a nova máscara serão o suficiente para atender a necessidade da organização. O cálculo é realizado com a mesma fórmula que utilizamos para calcular a quantidade de sub-rede. 2^N -2, onde o valor de N agora será a quantidade de bits que restaram na porção de host, no caso em questão sobraram 5 bits.

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 **0 0 0 0 0**

2^N - 2
2^5 -2 = 30 IP's válidos para cada uma das 6 sub-redes disponíveis com a nova máscara. 30 endereços são mais que suficiente para o problema em questão, já que cada setor possui 20 computadores, ainda restaram 10 endereços IP's válidos que não serão utilizados de imediato, mas poderão ser aproveitados no futuro para conectar novos computadores.

Os dois endereços IP's que são excluídos na fórmula são o primeiro IP de cada sub-rede que é utilizado para representar o endereço da sub-rede, portanto o mesmo não poderá ser utilizado para fins de endereçamento, e o último endereço IP de cada sub-rede que é o endereço de Broadcast, que também não poderá ser utilizado para fins de endereçamento.

3.3 FAIXA DE IP PARA CADA SUB-REDE

Para concluir a configuração da rede deve-se identificar qual será a faixa de endereço IP válido para cada uma das 6 sub-redes. Para cada uma das sub-redes válidas existe um endereço que é utilizado para representar o endereço da sub-rede, que é sempre o primeiro IP de cada sub-rede, e outro endereço IP que é utilizado como o endereço de Broadcast da sub-rede, que é o último endereço IP de cada sub-rede. O endereço de broadcast é o endereço que permite que uma determinada informação seja enviada para todos os dispositivos da rede. Entre o endereço de ID da sub-rede e o endereço de broadcast da sub-rede temos a faixa de endereços válidos para a sub-rede, que é a quantidade de endereços encontrados no cálculo, no problema em questão são 30. A figura 5 mostra a faixa de endereços válidos para cada sub-rede válida.

#	ID	Range	Broadcast
1	192.100.100.32	192.100.100.33 - 192.100.100.62	192.100.100.63
2	192.100.100.64	192.100.100.65 - 192.100.100.94	192.100.100.95
3	192.100.100.96	192.100.100.97 - 192.100.100.126	192.100.100.127
4	192.100.100.128	192.100.100.129 - 192.100.100.158	192.100.100.159
5	192.100.100.160	192.100.100.161 - 192.100.100.190	192.100.100.191
6	192.100.100.192	192.100.100.193 - 192.100.100.222	192.100.100.223

Figura 5 - Sub-redes válidas

4 MÁSCARA DE SUB-REDE DE CUMPRIMENTO VARIÁVEL

O termo VLSM significa máscara de sub-rede de cumprimento variável, o que consiste em criar sub-redes que comportem diferentes quantidades de hosts, ou seja, utilizar a máscara mais adequada para cada setor da organização a fim de evitar desperdícios de endereços IP. O conceito de VLSM se resume em fazer a "sub-rede da sub-rede", ou seja, a idéia é quebrar uma sub-rede em outras sub-redes menores para que ela se adéqüe ao número de hosts e de redes que a empresa necessita. A necessidade de se aplicar o VLSM vem da escassez de endereços IPV4 exigindo que as operadoras de telefonia distribuam melhor os endereços disponíveis de modo que o cliente tenha a quantidade que realmente necessite.

Em redes wan ponto a ponto são necessários apenas 2 endereços IP's para a configuração das interfaces dos dispositivos que conectam dois pontos, os roteadores. A figura 6 mostra como seria a estrutura de uma rede WAN ponto a ponto.

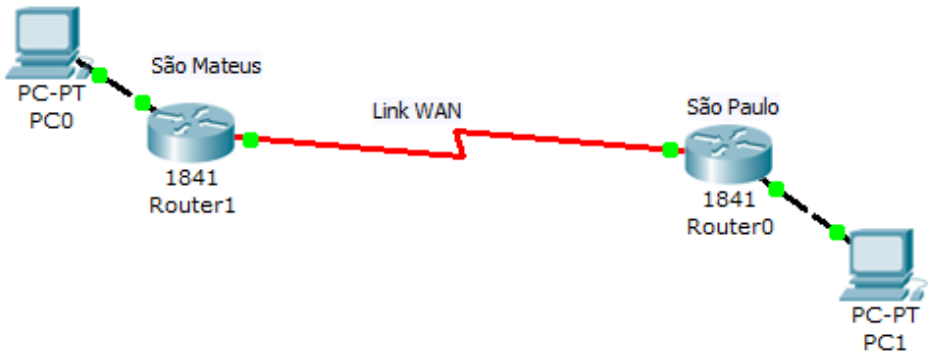


Figura 6 - Exemplo de rede WAN Ponto a Ponto

Pelo fato das redes WAN ponto a ponto utilizarem apenas 2 endereços lógicos a aplicação de VLSM nesta ocasião seria viável, pois evitaria um desperdício de endereços IP's. Imagine se para a configuração destas interfaces estivéssemos utilizando endereços IP's classe C, dos 254 disponíveis estaríamos utilizando apenas 2, deixando de utilizar 252 endereços válidos. Portanto, o ideal para a rede WAN ponto a ponto seria uma máscara de sub-rede que tivesse apenas 2 endereços válidos. Bom, vamos para um exemplo prático considerando a rede wan da figura acima. Suponha que a LAN do roteador São Mateus necessite de 126 endereços válidos, a LAN do roteador São

Paulo precisa de 60 endereços válidos e para as interfaces seriais dos roteadores necessitamos de 2 endereços válidos.

A. Partindo do pressuposto que estamos utilizando um endereço de classe C utilizaremos uma máscara adequada para cada situação acima. Para a rede LAN do roteador São Mateus precisamos de pelo menos 7 bits 0 na máscara de sub-rede, portanto a máscara ficaria 255.255.255.128. Pois para a LAN teremos 2^7 - 2 = 126 endereços disponíveis. Neste caso temos 2 sub-redes disponíveis, 2^1 = 2 sub-redes. As sub-redes disponíveis são 192.168.100.0/25 e 192.168.100.128/25.

B. Utilizaremos para a rede LAN do roteador São Mateus a sub-rede 192.168.100.0/25 utilizando os endereços válidos 192.168.100.1/25 até 192.168.100.126/25, o endereço 192.168.100.0 é o identificador da sub-rede e o endereço 192.168.100.127/25 é o endereço de broadcast da sub-rede.

C. Agora nos restou a sub-rede 192.168.100.128/25 para dividirmos em uma rede que comporte os 60 endereços válidos da LAN do roteador São Paulo. Para conectarmos todos os computadores da LAN de São Paulo utilizaremos 6 bits 0 na máscara de sub-rede. 2^6 – 2 = 62 endereços IP's válidos. A nova máscara ficaria 255.255.255.192. Aplicando na sub-rede 192.168.100.128 a máscara 255.255.255.192 ela terá a faixa de endereços válidos 192.168.100.129/26 a 192.168.100.190/26 e o endereço 192.168.100.191/26 é o endereço de broadcast, portanto a próxima sub-rede será 192.168.100.192.

D. Agora iremos alterar a sub-rede 192.168.100.192 de modo que consigamos obter somente 2 endereços válidos de uma mesma sub-rede. Aplicando a máscara /30 na sub-rede 192.168.100.192 teremos a seguinte situação: Endereço de identificação da sub-rede: 192.168.100.192/30, os dois endereços válidos que iremos utilizar, 192.168.100.193/30 e 192.168.100.194/30 e o endereço de broadcast 192.168.100.195/30. A máscara utilizada será a 255.255.255.252.

A figura 7 mostra a topologia da rede LAN de São Mateus, do link WAN ponto a ponto interconectando São Mateus à São Paulo e a rede LAN de São Paulo. Cada uma delas utilizando uma máscara de sub-rede diferente para que haja um aproveitamento dos endereços IP's disponíveis.

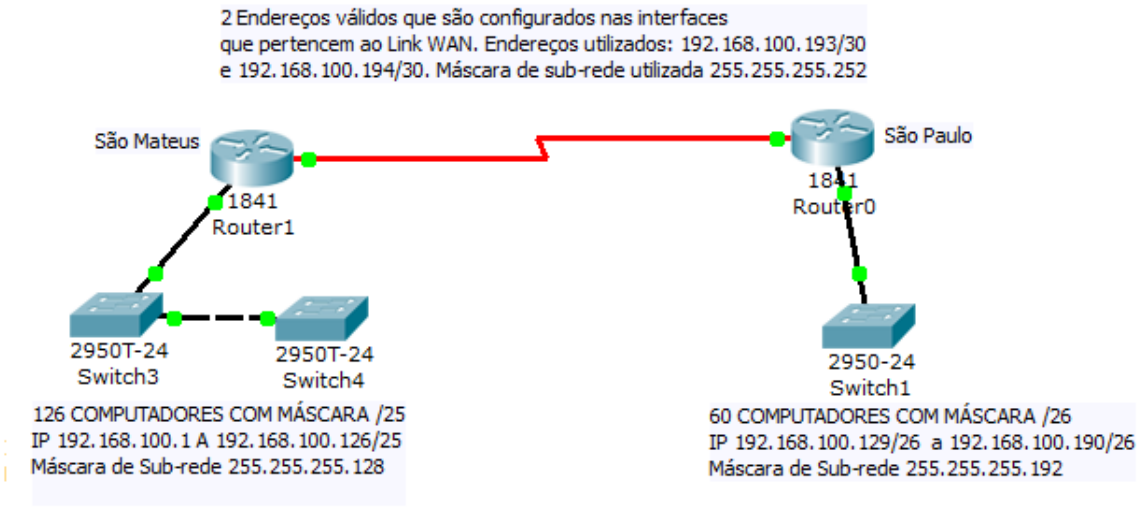


Figura 7 - Topologia

Vale ressaltar que para a utilização das VLSM, máscaras de sub-rede de cumprimento variável, é necessário que o protocolo de roteamento configurado nos roteadores tenha suporte a esse recurso. Alguns protocolos de roteamento não repassam informações referentes à máscara de sub-rede e para que a implementação das VLSM dê certo os roteadores devem conseguir interpretar e repassar as informações referentes à máscara de sub-rede.

5 ENDEREÇO FÍSICO (MAC ADDRESS)

Antes de começarmos a especificar o protocolo IP versão 4 vale ressaltar que além do endereço lógico os computadores necessitam também de um endereço físico para que o mesmo sirva de referência para transmissões realizadas para dentro de uma mesma rede local (LAN) que são chaveadas por um dispositivo de rede chamado switch. O switch é um dispositivo que conecta todos os computadores pertencentes a uma rede e trabalha na camada de link de dados do modelo OSI. O switch faz o uso do endereço físico para encaminhar os pacotes entre uma origem e um destino dentro de uma rede local. O endereço físico também chamado de MAC ADDRESS, Media Access Control, é um endereço de 48 bits que já vem especificado de fábrica na interface de rede do computador. A representação deste endereço se dá através de 12 caracteres em hexadecimal. Os primeiros 24 bits representam os caracteres que identificam o fabricante do dispositivo e os outros 24 bits restantes identificam o dispositivo, é um número de identificação única do dispositivo. A figura 8 nos mostra o formato deste endereço.

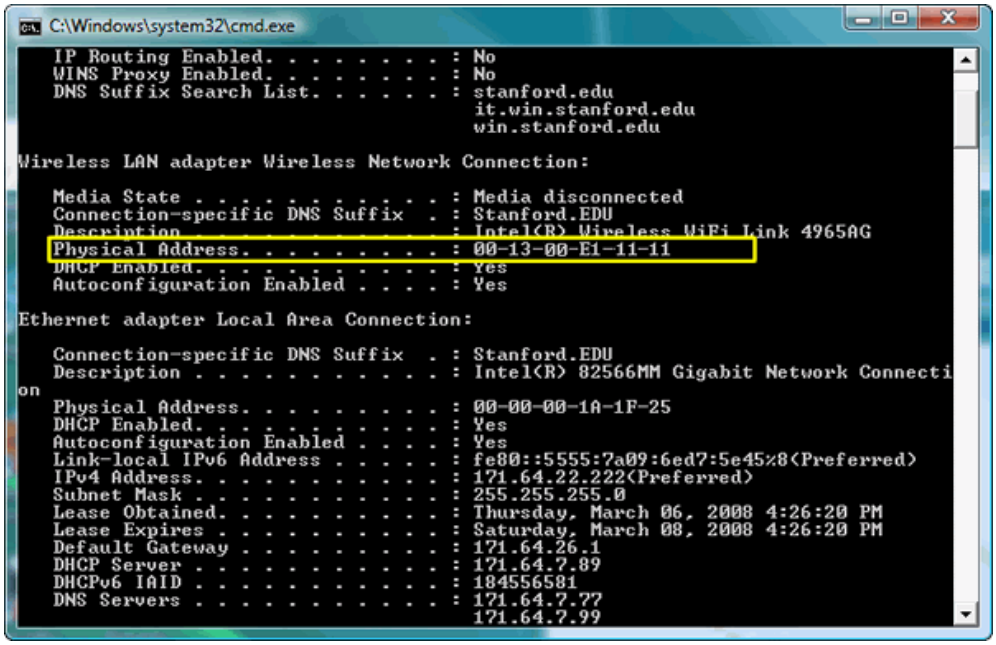


Figura 8 - Mac Address

6 CONCLUSÃO

A utilização do protocolo IPV4 está com os dias contados, mas enquanto a mudança para o protocolo IPV6 ou IP New Generation não chega para os usuários finais e para as empresas de pequeno e médio porte a solução é fazer uma melhor distribuição dos endereços utilizando técnicas de manipulação de suas respectivas máscaras de sub-rede. Neste artigo foram abordadas algumas técnicas que podem ser utilizadas para uma distribuição mais eficiente dos endereços IPV4, otimizando o seu uso e evitando assim desperdícios de endereços válidos que são utilizados para endereçamento.

REFERÊNCIAS

1. CORREA, FÁBIO XAVIER. **Roteadores Cisco**: São Paulo, Novatec 2012

2. MEETA GUPTA; MRIDULA PARIHAR; PAUL LASALLE; ROB SCRIMGER; **TCP/IP a Bíblia:** Rio de Janeiro Editora Campus 2002.

3. TCP/IP Disponível em <http://www.juliobattisti.com.br/artigos/windows/tcpip_p11.asp> Acesso em 10/2011.

4. FILIPPETTI, Marco A. **CCNA 4.1 Guia Completo de Estudo:** Editora Visual Books, São Paulo 2008.

Mundo Tecnológico

Apresentação

A revista Mundo Tecnológico publica trabalhos técnicos culturais, científicos e/ou acadêmicos, nas áreas ligadas aos cursos oferecidos de graduação, desde que atenda aos objetivos da Instituição. Admite-se, de preferência, autor pertencente à Faculdade, sem limitar, contudo, as contribuições e intercâmbios externos, julgados pelo Conselho Editorial, de valor para a Revista e, sobretudo, para a sociedade brasileira.

Normas de Publicação

Os originais entregues para publicação deverão ser assinados pelo autor e seguir as seguintes normas:

1 Texto

1.1 Os trabalhos devem ser inéditos e submetidos ao Conselho Editorial, para a avaliação e revista de pelo menos, dois de seus membros, cabendo-lhe o direito de publicá-lo ou não;

1.2 O texto deve ser apresentado em formato A4 (210x297mm);

1.3 Os trabalhos e artigos não devem ultrapassar o total de vinte laudas, em espaçamento normal; resumos de dissertação e monografia, duas laudas e resenhas e/ou relatos, não devem ultrapassar quatro laudas;

1.4 O texto deve ser entregue em CD e impresso, sendo composto no editor de texto Word for Windows, com fonte Time New Roman 12;

1.5 O trabalho deve apresentar obrigatoriamente:

- Título;
- Nome(s) do(s) autor(es)
- Breve currículo do(s) autor(es), enfocando as atividades mais condizentes com o tema trabalhado;
- Introdução;
- Corpo do trabalho;
- Resultado e/ou conclusões;
- Referências bibliográficas.

2 Referências Bibliográficas

As referências bibliográficas deverão ser listadas imediatamente após texto, em ordem alfabética, obedecendo Normas Técnicas.

3 Citações

Qualquer citação no texto deverá ter obrigatoriamente identificação completa da fonte, acrescida da (s) página (s) de onde foi retirada a citação.

Pede-se aos autores

- Seguir rigorosamente o Manual de Normas Técnicas da UNISAM, que se encontra a disposição de todos na Biblioteca e na intranet do site da Instituição;
- Linguagem condizente como produção científica, evitando abreviações, jargões e neologismos desnecessários;
- Objetividade quanto à construção do título do artigo;
- Apresentação do significado de cada sigla que conta do texto na primeira vez em que ocorre.

Considerações Finais

Os artigos são de inteira responsabilidade de seus autores e o Conselho de Editoração não se responsabilizará pelas opiniões expressadas nos artigos assinados.