JOSUÉ DAS CHAGAS MENEZES

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: ANÁLISE EM TRÊS ORGANIZAÇÕES BRASILEIRAS

Dissertação apresentada ao Curso de Mestrado Profissional em Administração, da Universidade Federal da Bahia, como requisito para a obtenção do grau de Mestre em Administração.

ORIENTADOR: Prof. Dr. José Célio Silveira Andrade

Salvador
2005

Escola de Administração – UFBA

M543 Menezes, Josué das Chagas.
Gestão da segurança da informação: análise em três organizações brasileiras. ./ Josué das Chagas Menezes. – 2005.
103 f.

Orientador: Prof. Dr. José Célio Silveira Andrade.
Dissertação (mestrado profissional) – Universidade Federal da Bahia, Escola de Administração, 2005.

1. Gerenciamento da informação - Segurança. 2. Inteligência Competitiva. 3. Capital intelectual. 4. Segurança. I. Andrade, José Célio Silveira. II. Universidade Federal da Bahia. Escola de Administração. III. Título.

CDD – 658.4

UNIVERSIDADE FEDERAL DA BAHIA
ESCOLA DE ADMINISTRAÇÃO
NÚCLEO DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO – NPGA
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO – MPA

JOSUÉ DAS CHAGAS MENEZES

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: ANÁLISE EM TRÊS ORGANIZAÇÕES BRASILEIRAS

Banca Examinadora:

Prof. Dr. José Célio Silveira Andrade
Universidade Federal da Bahia

Prof. Dr. Francisco Teixeira
Universidade Federal da Bahia

Prof. Messias Bitencourt
Universidade Federal da Bahia

Prof. Ariosto Farias Júnior
Universidade Federal da Bahia

Salvador - 2005

AGRADECIMENTOS

Em memória, a meu pai José, pelo exemplo de perseverança.

A minha mãe Eunice, pela sua habilidade conciliadora.

Aos meus filhos, Ana Fausta, Vinicius, Victor, Vicente e Pedro, forças motrizes para a superação das limitações.

Em especial, a meu filho Vicente, solidário na solidão que acompanha o trabalho de estudo e pesquisa.

Agradeço ao Prof. Dr. José Célio Silveira Andrade, meu orientador, pela simplicidade motivadora, sem a qual não seria possível superar minhas limitações.

Aos colegas, pelas possibilidades de aprendizado criadas ao longo do curso.

Ao Núcleo de Pós-Graduação em Administração da UFBA (NPGA) pelo apoio dado através de seus professores e funcionários.

Aos colegas da Petrobras, em particular da unidade Serviços Compartilhados, pela contribuição dada na construção deste trabalho.

Especial agradecimento a Petróleo Brasileiro S.A. – Petrobras, Companhia Siderúrgica de Tubarão - CST e a SAMARCO MINERAÇÃO S.A., incentivadoras de trabalhos acadêmicos.

Ariosto Farias Júnior, exemplo de determinação e visão estratégica.

José Aécio Romão, amigo nos bons momentos e nas dificuldades, por haver criado as condições para esta conquista.

Finalmente Adriana Maria Barbosa, que com seu carinho e atributos profissionais, renovou e deu nova áurea à motivação para a conclusão deste trabalho.

De Sitim enviou Josué, filho de Num, dois homens, secretamente, como espias, dizendo: Andai e observai a terra e a Jericó. Então foram, e entraram na casa de uma prostituta, cujo nome era Raabe, e pousaram ali.

Bíblia Sagrada, Josué 2.1

RESUMO

Segurança da Informação é o tema desta dissertação. Este trabalho busca conhecer a percepção dos empregados de três organizações no Brasil: duas empresas mineradoras e uma do setor petróleo, todas com atuação global, haja vista estarem mais susceptíveis à ação da concorrência internacional. Analisa o tema sob a dimensão da gestão, procurando conhecer os principais aspectos a ela relacionados, incluindo a compreensão da informação como ativo relevante para a organização e a opinião dos empregados sobre a relação entre o princípio da livre circulação da informação e a restrição imposta pelos procedimentos de segurança. Pesquisa quantitativa realizada demonstrou que o conceito de segurança da informação já é adotado nas organizações pesquisadas, que a política de segurança da informação é conhecida pelos empregados das empresas que a adota, que há compreensão quanto ao seu valor estratégico, seu diferencial competitivo e a sua importância para a manutenção do valor de mercado. Demonstrou ainda o entendimento da informação como ativo importante para a organização, juntamente com os bens físicos e financeiros. O trabalho é encerrado com duas recomendações importantes, tanto para o ambiente corporativo como para o ambiente acadêmico.

Palavras-chave: Segurança; Informação; Nova economia; Inclusão; Norma; Pesquisa; Conclusão.

ABSTRACT

Security Information is the theme of this text. This work intends to know the employees' perception of three organizations in Brazil: two mining industry and one of the sector oil, all with global performance have seen to be exposed to the action of the international competition. It analyzes the theme under the dimension of Management, trying to know the aspects to its related, including the understanding of the information as important assets for the organization and the employees' opinion about the relationship among the beginning of free circulation and the imposed restriction by procedures of security. Quantitative research demonstrates that the concept of Security Information is already adopted in the researched organizations, that the politics of security of the information is known by the employees of the companies that it adopts it, that there understanding its strategic value, its competitive differential and its importance for to keep the value of market. It still demonstrated the understanding of the information as important assets forth company, together with the physical and financial property. The work is finished with two important recommendations as much for the corporate atmosphere as for the academic atmosphere.

Keywords: Security; Information; Economics new; Inclusion; Norm; Research; Finish.

SUMÁRIO

1. INTRODUÇÃO

Ainda não se completou o tempo para a predição e já presenciamos a extraordinária evolução dos *softwares* e dos *hardwares* modificando assustadoramente o perfil das pessoas e das organizações. Presentemente, a informação é o principal bem, conseqüentemente, a sua proteção é inexorável.

No mundo contemporâneo, o cidadão comum está cada vez mais incorporando as preocupações que originariamente eram associadas às organizações. Pois segundo Bill Gates, no seu livro "A Empresa na Velocidade do Pensamento" (1999), "Os negócios vão mudar mais nos próximos dez anos do que mudaram nos últimos cinqüenta". (p.9)

Assim foi com a segurança patrimonial, com os aspectos relacionados com os sinistros, com os requisitos de saúde e meio ambiente e mais recentemente com questões relacionadas com a segurança da informação.

Pesquisa realizada por Zilda Penna Marinho[1], Diretora do *Modulo Education Center* (MEC), entre julho e setembro de 2003, nas cidades de Brasília, Rio de Janeiro e São Paulo, quando 960 pessoas foram entrevistadas, tendo como pré-requisito ser usuário da *Internet* revela preocupações do usuário comum com a segurança da informação:

- 77,77% manifesta preocupação com a segurança da informação;
- 65,97% considera crime invadir um negócio virtual;
- 61,53% considera que o filho tem direito de acesso a toda informação que busque na *Internet;*
- 56,39% toma algum tipo de cuidado quando acessa a *Internet;*
- 54,59% adota procedimentos de segurança quando está conectado;
- 52,99% já instruiu o filho sobre cuidados com o fornecimento de dados familiares;
- 50,27% considera que o anonimato estimula a realização de coisas que no mundo real não se realizaria.

[1] Não obstante o trabalho ter sido realizado sem rigor científico, segundo a própria pesquisadora, ainda assim representa a assimilação pelo usuário comum de um comportamento próprio das organizações. "A segurança da informação não é mais uma questão de tecnologia ou negócios. Hoje ela é também uma questão familiar e social. (Marinho, 2003)

Observa-se, contudo, que o "*gap"* entre as preocupações da organização com as ameaças potenciais e as preocupações do usuário comum, vêm diminuindo a cada "onda", termo cunhado por Alvin Toffler[2] para didaticamente descrever os estágios de evolução da sociedade sob a ótica da economia.

Segundo o autor, na Primeira Onda, as sociedades tinham como fundamento a agricultura e dominaram o mundo durante centenas de anos, exPlorando humanos e animais como fonte basilar de energia. Ameaças ao patrimônio se restringiam aos furtos a bens tangíveis.

Na Segunda Onda, ocorreu a revolução industrial quando a produção foi movimentada por fontes não renováveis de energia tal qual o carvão e o petróleo, passando o dinheiro a representar mola propulsora no desenvolvimento da economia. As ameaças acompanharam a própria evolução social introduzindo novas práticas delituosas como fraudes, assaltos, sabotagens, roubos e incêndios criminosos, introduzindo a vigilância que evoluiu conceitualmente passando da simPles tarefa de vigiar para se especializar e assimilar técnicas específicas quer para atender demandas no campo das instalações, quer para a proteção das pessoas nas organizações.

Com o próprio desenvolvimento da indústria, meios e dispositivos de proteção sofisticados foram desenvolvidos com o uso da mecânica e da eletrônica, transformando as organizações em casulos onde somente pessoas autorizadas têm acesso e, apesar disso, toda a movimentação interna é filmada e armazenada em sistemas digitais de gravação.

O *gap* para que o cidadão comum incorporasse tais padrões de conduta deu-se em tempo menor. Observam-se hoje as vigilâncias nas residências, os aparatos tecnológicos nas casas e condomínios, os guardas pessoais, o monitoramento remoto dos veículos particulares, inclusive com a utilização de satélite.[3]

Desde as preocupações feudais na defesa do patrimônio até as responsabilidades corporativas com a proteção da indústria contra incêndios e inundações, adotando medidas preventivas e repressivas de proteção e de seguro contra fraudes, assaltos, sabotagens, roubos e incêndios criminosos, até essa

---

[2] A Terceira Onda, publicado nos anos 80 do século XX, tornou-se um best-seller e durante algum tempo foi a "bíblia"dos intelectuais reformistas da China. (Toffler, 2003)

[3] Uma das sensações do Salão e Fórum de Inovação Tecnológica, realizado pelo Ministério da Ciência e Tecnologia (MCT) e a Finep, em Julho de 2001, em São Paulo, foi o *stand* da casa inteligente. O projeto mostrava uma casa totalmente controlada à distância: iluminação, alarmes, aquecedores, irrigação, áudio, vídeo, eletrodoméstico e fechaduras. (FINEP, 2002)

preocupação passar a ser também do cidadão comum, decorreram centenas de anos.

A Terceira Onda, descrita por Alvin Toffler como da sociedade baseada na informação e na tecnologia, traz para cena a ameaça com requinte tecnológico em busca do ativo propulsor da economia: a informação.

Não obstante a sociedade baseada na informação começar a se configurar na primeira metade do século XX, os seus reflexos na indústria já chegam também ao cidadão comum.

A ficção de George Orwell[4] no seu emblemático livro 1984 se transmuta em realidade. Philip Purpura em sua obra *Security and Loss Prevention*, (1998) sintetiza com propriedade os fatos geradores da sociedade baseada na informação.

> Nas décadas que se seguiram à segunda Guerra Mundial a segurança privada se expandiu muito mais; durante os anos 50, a Guerra da Coréia e a inacabada "Guerra Fria" criaram uma tensão mundial e uma competição entre as democracias e os regimes comunistas. O departamento de Defesa, em 1952, apoiou os requerimentos de defesa das indústrias para proteger as informações e materiais classificados. Quando os Soviéticos colocaram com sucesso o primeiro satélite em órbita (Sputinik, em 1957) e chegaram pela primeira vez à lua com um foguete dirigido (1959), os Americanos ficaram atordoados. A corrida tecnológica tornou-se mais intensa e a proteção das informações fez-se mais importante.(p.15 – tradução do autor)

Players da Guerra Fria, militares dos Estados Unidos da América, no início dos anos 60 do século passado, sentiram a necessidade de criar um sistema que mantivesse as comunicações entre as bases militares na ocorrência de um ataque nuclear que destruísse o Pentágono, Quartel General das ações de Inteligência e Contra-Inteligência.

Foi a busca incessante de troca de informações que fez florescer a *Internet*. Foram necessidades de ordem belicosa, mais uma vez na história da civilização, que levaram a natureza humana ao exercício da criação, desenvolvendo essa

[4] 1984 by George Orwell. Sumário: Obra de ficção que projeta o Mundo dividido em três países. Sociedades totalitárias governada pelo "Grande Irmão", que censura o comportamento e até mesmo o pensamento de todos os seus habitantes. Os que cometem crimes do pensamento são encaminhados para reabilitação no Ministério do Amor. (ORWELL, 1949).

extraordinária rede de comunicação que mudou comPletamente a maneira dos povos se relacionarem: a *internet*.

As distâncias deixaram de ser óbices para que o conhecimento humano se expandisse. Sob a sombra do sucesso da União Soviética com o lançamento e a colocação em órbita da Terra do primeiro satélite artificial, o *Sputnik*, o Departamento de Defesa dos EUA formou em 1957 a *Advanced Research Projects Agency (ARPA)*, com o objetivo de colocar os EUA na liderança em ciência e tecnologia aPlicáveis militarmente. O patrocínio de estudo intitulado *A Competitive Network of Time Sharing Computers* com o objetivo de desenvolver uma rede interconectada de computadores que ao mesmo tempo fosse independente em cada uma das partes, permitindo que a informação circulasse dentro dos preceitos de sigilo, disponibilidade e integridade ainda que uma das partes fosse destruída, resultou, em 1967, nas primeiras conexões entre quatro pontos fisicamente distantes: a Universidade UCLA, em Los Angeles, o Instituto de Pesquisa de Stanford (*Stanford Research Institute*), a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah. A interconexão foi batizada como *Arpanet*.

Em 1971, cerca de 24 pontos distintos já integravam a *Arpanet*, e nesse mesmo ano, foi criado o endereço eletrônico (*e-mail*) permitindo o envio e recebimento de mensagens com a identificação do remetente. Em 1972, a primeira conexão internacional foi estabelecida entre a *Arpanet*, Universidade de Londres (Inglaterra) e o *Royal Radar Estabilisment* (Noruega).

O crescimento espantoso da rede de comunicação tornou inadequado o seu protocolo original chamado de *Network Control Protocol* (NCP) e fez surgir um dos problemas iniciais que foi a incompatibilidade entre os diferentes tipos de computadores. A criação do protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*), genericamente uma linguagem comum para diferentes tipos de computadores, permitiu um acesso melhor e praticidade na transferência de informações pela rede. As crescentes conexões em diferentes partes do Planeta Terra rebatizaram a *Arpanet*, dando-lhe um novo nome: *Internet*.

Em 1990 o Departamento de Defesa dos EUA se desvinculou da *ARPANET* e criou a sua própria rede.

O desenvolvimento do *World Wide Web* (www), do *Hypertext Markup Language* (HTML), do *Hypertext Transfer Protocol* (HTTP) e do *Browser*, tornam a navegação mais fácil e atraente.

Inicialmente voltada para questões estratégicas de defesa nacional e para a comunidade científica, ampliou-se para o ambiente acadêmico e mercê da riqueza de informações e facilidades de conexões intercontinentais, novos usos foram incorporados à rede, dentre eles os interesses comerciais entre Nações, Organizações e pessoas.

As repercussões dessa nova variável no mundo dos negócios ilustram este trabalho. A opção estratégica de utilização pela indústria nacional dessa tecnologia e as vantagens comparativas e competitivas pela conseqüente criação de barreiras à concorrência, encontra na própria força de trabalho as maiores dificuldades, isto porque a convivência nesse novo cenário conduz a organização a um novo modo de pensar e agir. Assim, a constatação da existência do *peopleware*[5] como o elo mais fraco na corrente de proteção, tema central de dois eventos recentemente realizados em São Paulo-BR, *CSO Meeting* (08/2004) e 7799 *Goes Global*/*SMS International User Group* (10/2004), é o contexto delimitador deste trabalho e orientador da elaboração do problema da pesquisa:

QUAL O NÍVEL DE CONHECIMENTO DA FORÇA DE TRABALHO DE ORGANIZAÇÕES BRASILEIRAS SOBRE SISTEMAS DE SEGURANÇA DA INFORMAÇÃO?

Escolheu-se para o delineamento da pesquisa organizações com o seguinte perfil:

- Atuação global;
- Susceptíveis à ação da concorrência internacional;
- Investidoras em ciência e tecnologia;
- Inseridas no segmento das indústrias de produtos estratégicos para o desenvolvimento nacional sustentado;
- Comprometimento da alta administração com a implementação de uma cultura de segurança da informação.

[5] Usuário comum ou corporativo da Intranet e Internet desprovido de preocupação com a segurança dos seus dados pessoais e corporativos.

Assim, foi selecionada a Petrobras, a CST e a Samarco, por já haverem buscado a inclusão na aldeia global do conhecimento e da informação.

Orientado pela metodologia científica da pesquisa, suportada por Gil (1987), Levin (1987), Rudio (1992), Eco (1998) e Vieira (2004), o modelo de análise desta dissertação privilegiou a dimensão Gestão da Segurança da Informação em detrimento da dimensão Tecnológica.

Assim, foi desenvolvido um trabalho de pesquisa quantitativa com empregados com e sem função gerencial das três organizações selecionadas, além de entrevistas com consultorias especializadas e órgãos governamentais. Nesta pesquisa, optou-se por um método de amostragem não-probabilística, estabelecendo um nível de confiança de 68%, correspondente a um desvio padrão, permitindo-se erro máximo de 5%. Para o cálculo do tamanho da amostra, considerou-se a sua inserção em universo finito, permitindo-se percentual presumível de ocorrência do fenômeno igual a 50%, utilizando-se questionários via correio eletrônico e em meio físico.

2. SEGURANÇA DA INFORMAÇÃO E INTELIGÊNCIA COMPETITIVA

O conhecimento é o principal fator de produção do século XXI e a arquitetura das organizações muda por esse mister.

Nessa nova estruturação, surgem os conceitos de Nova Economia, com a sua lógica própria, introduzindo como fator de produção a *commodity* conhecimento,[6] da nova indústria, com suas mídias viajando por cabos e satélites, seus Bancos de Dados como fiéis repositórios das informações e do conhecimento explícito[7], seus *hardwares*, *softwares* e interfaces suportando toda essa estrutura, e finalmente, de Nova Organização estruturada em rede e apoiada por tecnologia da informação e comunicação como suporte ao compartilhamento do conhecimento. A inteligência empresarial, consiste agora na capacidade da organização em aglutinar a inteligência humana, e desenvolver a gestão do conhecimento para produção de produtos e de novos conhecimentos, para com isso, se posicionar competitivamente no mercado. Metodologicamente, a Gestão do Conhecimento é um conjunto de práticas cujo objetivo é identificar, selecionar, organizar, distribuir e transferir informações e conhecimentos (tácitos e explícitos) que fazem parte da memória da empresa, suportadas pela tecnologia da informação.

Vários são os modelos utilizados pelas organizações. O esquema a seguir (Figura 1), sintetiza um modelo utilizado por Elisabeth Gomes, consultora em Inteligência Empresarial.

---

[6] Não obstante a contestação de alguns economistas, cada vez mais está deixando de ser a ciência da escassez para se tornar a ciência da abundância. Nas palavras de Kevin Kelly “a informação tornou-se abundante e mesmo o conhecimento, apesar de ser mais escasso do que a informação, está se tornando abundante”. (KELLY. Entrevista portal Janelaweb. 1997)

[7] ExPlícito: expresso em palavras e números, escrito e documentado; adquirido pela educação formal. Tácito: manifestado dentro de contexto social e individual; intuições, pressentimentos, modelos mentais, sexto sentido.

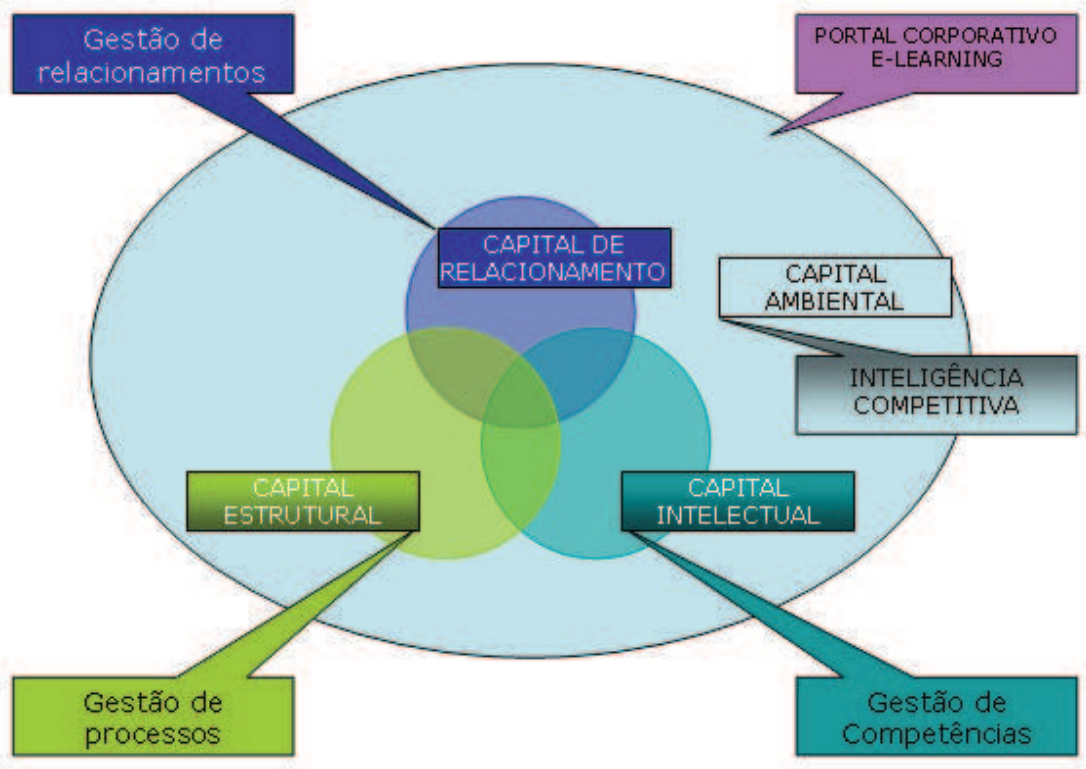


Figura 1 - Capital do conhecimento

Fonte: Universidade Petrobras. 2004

O Capital Ambiental, na definição da Professora Elisabeth, representa o ambiente externo com o qual a empresa se relaciona, semelhante ao modelo de Estratégia Competitiva desenvolvido pelo professor da *Harvard Business School, Michael E. Porter* (Figura 2) que vislumbra ameaças e oportunidades da indústria em termos econômicos e tecnológicos, com seus riscos conseqüentes e recompensas potenciais e as expectativas mais amPlas da sociedade que refletem o impacto sobre a empresa das políticas governamentais, dos interesses dos acionistas e da sociedade organizada em geral.

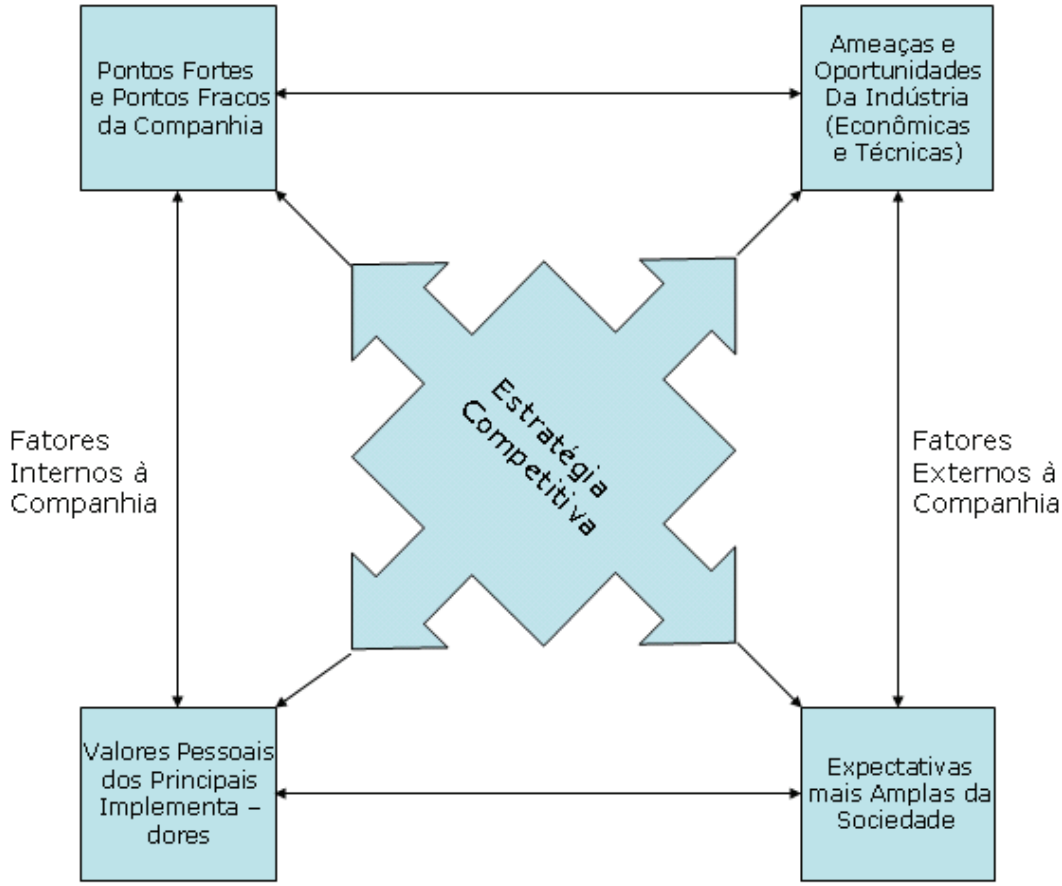


Figura 2 – Contexto onde a estratégia é formulada

Fonte: Michael Porter. (1986, p. 17)

Observa-se que tais modelos existem desde a primeira revolução industrial mudando apenas o cenário da sua manifestação. A preocupação com as ameaças potenciais aos negócios, o conhecimento das ações da concorrência, o monitoramento do mercado e a percepção para novas oportunidades, o que hoje se denomina Inteligência Competitiva, sempre foram objeto da atenção da indústria e do comércio. O que muda é o contexto. No século XXI, a velocidade com que as informações e o conhecimento fluem estabelecem a necessidade de estratégias suportadas por novos referenciais e o desenvolvimento de modelagens mentais alinhadas com os riscos desse novo ambiente de negócios.

As forças que movem a concorrência, pressionam a mudança criando, na definição de Michael Porter (1986), os processos evolutivos que conduzem a indústria à sua estrutura potencial de desenvolvimento e domínio tecnológico estabelecendo, por via de conseqüência, uma condição de liderança de mercado e

criando barreira a novos entrantes. No mundo contemporâneo, tal qual no século XIX, as estratégias precisam ser protegidas.

2.1 DIFUSÃO DE CONHECIMENTO

Sob o título “Difusão de Conhecimento Patenteado”, Michael Porter (1986) cita três mecanismos de difusão do conhecimento. Primeiro, as empresas podem aprender através da inspeção física dos produtos patenteados dos concorrentes e através de informações sobre a logística do produto obtidas de várias fontes, incluindo fornecedores e distribuidores. Fornecedores, distribuidores e clientes são todos condutos para estas informações e normalmente têm grande interesse em promover a difusão devido aos seus próprios objetivos (por exemPlo, criar outro fornecedor forte).

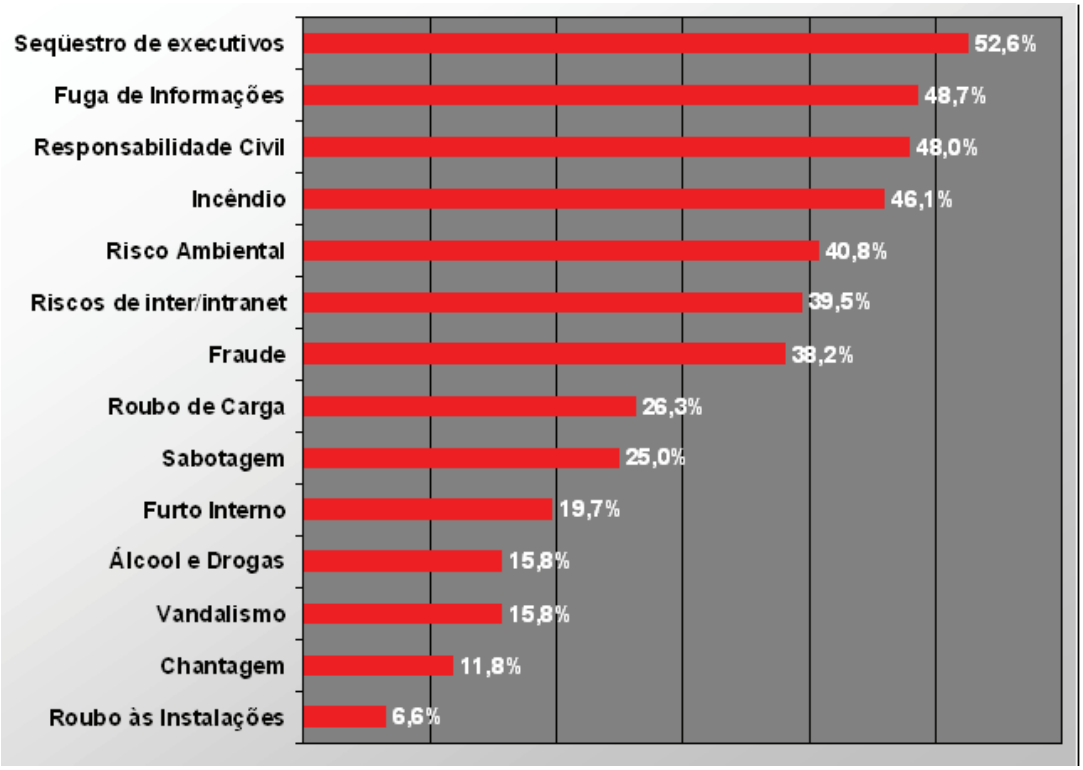
Em segundo lugar, a informação patenteada é também difundida quando se incorpora aos bens de capital produzidos por fornecedores externos. A menos que as empresas na indústria produzam seus próprios bens de capital[8] ou protejam a informação[9] que eles dão aos fornecedores, suas tecnologias podem ser adquiríveis pelos concorrentes.

Por último, destaca que a rotatividade da mão-de-obra aumenta o número de pessoas que passam a conhecer o domínio tecnológico, abrindo uma brecha de vulnerabilidade para que essas informações cheguem para outras empresas.

O Quadro 1 a seguir, demonstra a Fuga de Informações como o segundo risco mais relevante entre as empresas pesquisadas pela consultoria Brasiliano & Associados.

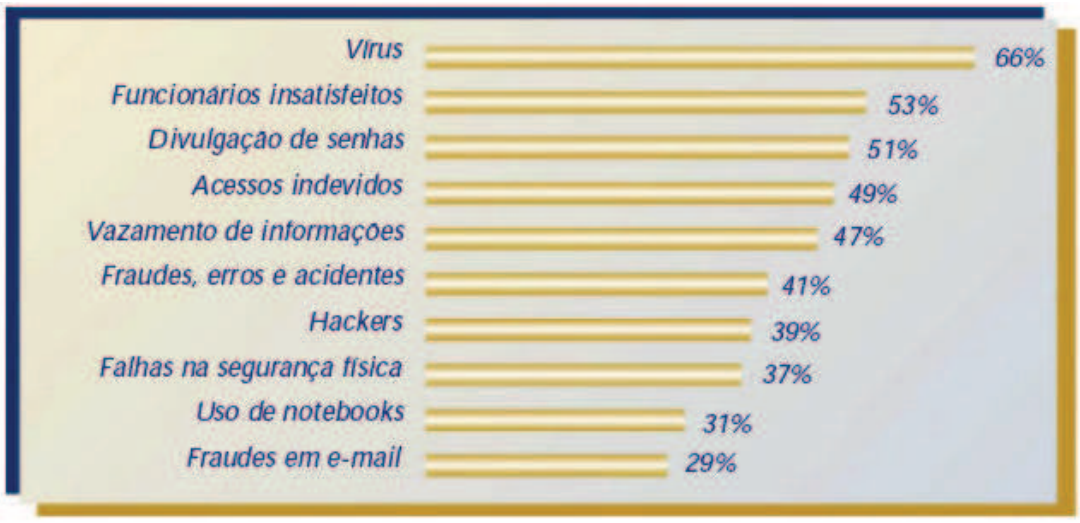
[8] Ao integrar-se a empresa pode excluir-se do fluxo de tecnologia de seus fornecedores ou clientes. A integração significa em geral que uma companhia tem que aceitar a responsabilidade pelo desenvolvimento de sua própria capacidade tecnológica.
[9] A tendência é a organização proteger o seu principal ativo: a informação.

Quadro 1 – Riscos muito relevantes



Fonte: Brasiliano & Associados. 2003

A Pesquisa Nacional de Segurança da Informação, realizada em outubro de 2003 pela empresa *Modulo Security Solutions S.A.* (Quadro 2), apresenta os funcionários insatisfeitos e vazamento de informações dentre as cinco principais ameaças à Segurança da Informação, juntamente com vírus, divulgação de senhas e acessos indevido.



Quadro 2 – Principais ameaças à segurança da informação

Fonte: Módulo Security. 2003
Obs: o total de citações é superior a 100% devido à questão aceitar múltiPlas respostas.

Podem se agrupar as estruturas de uma organização que não geram receitas, mas que minimizam perdas e maximizam lucros, tal como o segmento de segurança empresarial (patrimonial, pessoal e da informação), de saúde ocupacional, meio-ambiente e segurança do trabalho e a Inteligência Competitiva, em um único segmento ao qual denominamos Prevenção de Perdas. Na figura 3, a seguir, observa-se a representação deste conceito.

Nessa abordagem, infere-se possibilidades da mesma vir a ser inserida no contexto do sistema de Gestão Integrada, em que as organizações vêem trabalhando, baseado nos requisitos das NBR ISO 9001 – Gestão da Qualidade, 14001 – Gestão Ambiental, OHSAS 18001 – Série de Avaliação da Segurança e Saúde no Trabalho e SA 8000 – Responsabilidade Social.

.

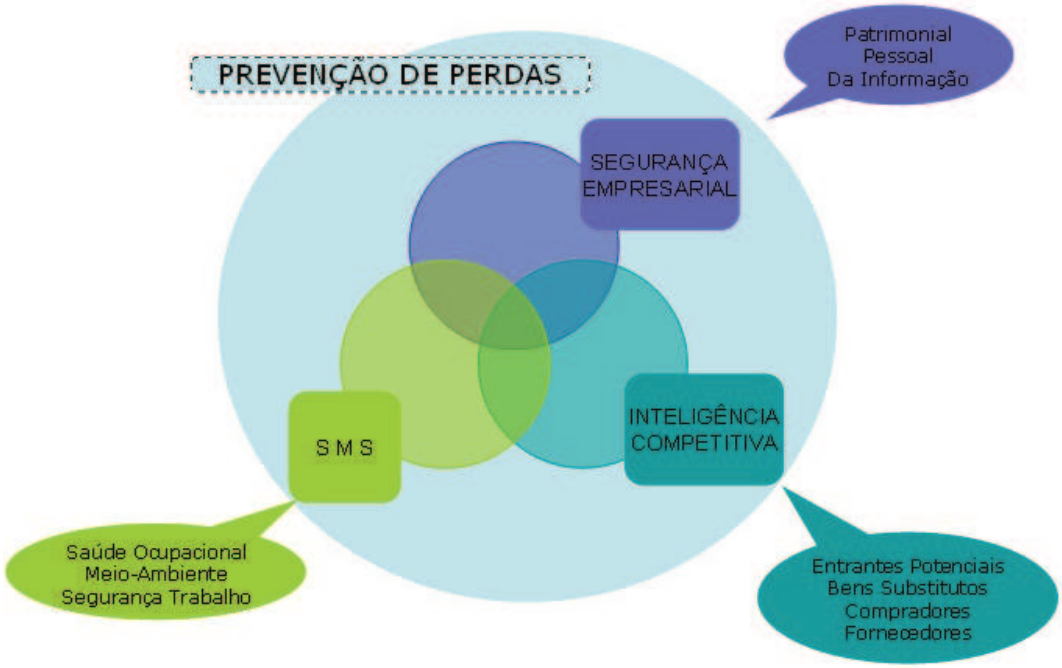


Figura 3 – Segmentos que maximizam o lucro

Fonte: Produzido pelo próprio autor do trabalho.

Sendo assim, a busca pela maximização dos lucros leva as organizações a desenvolverem mecanismos de proteção. Mais uma vez, um ator coadjuvante, a

indústria do seguro, se insere no *script* impulsionando as organizações para a prevenção de perdas potenciais.

Segundo os teóricos relatam, nos primórdios da primeira revolução industrial, os incêndios, conseqüentes de falhas estruturais nos projetos, trouxeram prejuízos significativos para as indústrias, fazendo florescer as companhias seguradoras, as quais, pela continuidade das ocorrências de sinistros, alguns até criminosos, começaram a desenvolver padrões diferenciados no seguro dos ativos, de acordo com o cuidado que cada indústria dispensava ao requisito da prevenção. Assim, quanto mais consistente fosse o projeto, aspectos ligados a treinamento, proximidade das equipes de bombeiros, ou mesmo se a indústria tivesse o seu próprio corpo de bombeiros, menor seria o custo para segurar o ativo.

Outras ameaças, contudo, passaram a existir, configurando-se nas perdas de produção conseqüente de furtos pelos próprios empregados, atos de vandalismo, perdas de materiais e equipamentos por falta de controle nas movimentações, por exemplo. Mais uma vez, as companhias seguradoras começaram a oferecer descontos na fixação do prêmio para a indústria detentora de procedimentos preventivos para o controle dessas perdas, principalmente porque as ações de sabotagem na indústria, como conseqüência do desenvolvimento industrial e a organização dos operários em sindicatos, danificavam as máquinas nas diferentes linhas de montagens, trazendo vultosos prejuízos para a indústria e também para as seguradoras. Assim, quem melhor se estruturasse para combater essa ameaça, conseqüentemente, obteria maiores reduções no custo do seguro dos ativos, representados pela terra e bens de produção.

Hoje estamos vivendo na sociedade do conhecimento e este é o ativo mais valorizado que não deprecia com o tempo como os ativos físicos, pelo contrário, se valorizam.

Artigo assinado por Patrícia Peck (2004), publicado pela *MODULO e-SECURITY*, informa que vem crescendo a tendência de aPlicação de seguro de ativos intangíveis, através de empresas americanas e européias, principalmente inglesas, como o *Chubb International*. Destaca que, para aPlicação do seguro uma série de medidas legais deve ser tomada, podendo imPlicar até em alterações societárias, com a criação de uma nova empresa hospedeira dos mesmos:

> Risco está diretamente relacionado a valor e custo de proteção do bem. Sem parâmetros de análise fica difícil para os gestores tomar a decisão de pagar por um prêmio, na medida em que precisa responder questões como o quanto pagar e o que proteger exatamente.(Peck. 2004)

Por exemplo, como avaliar informações disponíveis em um banco de dados de clientes? Qual o valor desse bem e que prejuízo ele pode causar à empresa proprietária se utilizado pela concorrência?

2.2 A GUERRA TOTAL PELA INFORMAÇÃO

Ampliando comentários sobre o tema, Alvin Toffler (2003) dedica o capítulo 14 – A guerra total pela informação, do seu livro Powershift, para chamar atenção sobre a espionagem, termo comum nos manuais militares, e que no ambiente dos negócios se apresenta sob o titulo de Inteligência Competitiva. De acordo com Toffler (2003), um novo conceito de empresa está tomando forma em resposta as infoguerras que agora estão sendo travadas em toda a economia mundial. À medida que o conhecimento se torna mais essencial para a criação de riqueza, a empresa começa a ser considerada como uma intensificadora do conhecimento, necessitando, portanto, promover mecanismos de proteção das suas informações e ao mesmo tempo desenvolver meios de obtenção de informações sobre os Planos, os produtos e os lucros de seus adversários. Por esta razão a espionagem industrial ou inteligência competitiva, vem se disseminando dramaticamente entre as organizações no mundo contemporâneo.

Ainda de acordo com Toffler (2003) muitas redes empresariais são altamente vulneráveis à entrada de determinados ladrões ou espiões, inclusive funcionários descontentes, ainda trabalhando nelas ou não, subornados por uma empresa concorrente. Conclui o capítulo, fazendo uma reflexão sobre as batalhas diuturnas que estão sendo travadas pelo mais essencial recurso da Era da Powershift: a informação. Batalhas que ora vence um lado, ora o outro, entre ataque e defesa, são o reflexo da infoguerra.

A espionagem empresarial e a contra espionagem começaram, portanto, a desenvolverem diferentes mecanismos de proteção para o tráfego das informações criando conseqüentemente um ambiente com alto grau de entropia.

A necessidade de organização do sistema, assim como a premissa da evidência confiável passou a ser cada vez mais requisito indispensável para fechamento das transações.

Gerar confiança para um potencial cliente face o inexorável compartilhamento de informações, pode ser trabalhoso para o profissional e desgastante para o contratante até que o processo de empatia se estabeleça para a consolidação da parceria.

Acredita-se que esse esforço seria minimizado pela existência de evidência confiável, credenciando o profissional junto ao contratante. É provável que por essa razão instituições internacionais estão surgindo com o propósito de preparar e certificar o profissional que atua no segmento de segurança[10]. Transmutando para o mundo dos negócios, como saber se a organização que estou estabelecendo parceria cuida das suas informações de modo a preservar o sigilo das transações? Nesse cenário, surge a importância da certificação internacional que rapidamente está se propagando no mundo dos negócios. As próprias regras sobre captação de recursos financeiros estão a exigir das organizações que apresentem evidências de controles rígidos no trato das suas informações que satisfaçam as necessidades da própria empresa, dos clientes, dos parceiros e dos órgãos governamentais.

O paradoxo nesse cenário é que, ao mesmo tempo em que as empresas buscam proteger as suas informações, criam processos estruturados para monitorar a concorrência. As Universidades já incorporam em alguns cursos a matéria Inteligência Competitiva.

Exemplo disso é a matéria Inteligência Competitiva que faz parte da grade curricular do Curso de Pós-graduação em Engenharia da Produção na Universidade Federal de Santa Catarina. No material produzido para aplicação no Curso, Dr. Ing. Neri dos Santos (2000), deixa claro que na era da economia baseada no conhecimento as empresas estão se dando conta de que as informações relevantes e oportunas sobre os concorrentes, fornecedores e clientes são necessárias para a tomada de decisão estratégica no mercado em que atuam. Segundo Santos (2000), o conceito é antigo, contudo se consolidou nos anos 90 do século passado havendo

[10] No Brasil, a Modulo Security oferece os cursos de MCSO (Modulo Certified Security Officer) e o CCSO (destinado aos profissionais que possuem o MCSO). Essas certificações contam sempre para o profissional na hora de ser contratado, especialmente se o contratante conhece essa certificação pois sabe que está contratando alguém capacitado.

nos EUA a Sociedade dos Profissionais de Inteligência Competitiva que reúnem mais de seis mil membros.

No Brasil, a Associação Brasileira dos Analistas de Inteligência Competitiva - ABRAIC, sociedade civil sem fins lucrativos, criada em 15/04/2000, realizou o 5º Workshop Brasileiro de Inteligência Competitiva e Gestão do Conhecimento (Brasília, 10/2004), aberto pelo Ministro Jorge Armando Felix, Ministro Chefe do Gabinete Institucional da Presidência da República, no qual foram tratados, dentre outros, os seguintes temas: A importância de um sistema de Inteligência Econômica no Desenvolvimento do Brasil; Introdução à inteligência Competitiva: matéria obrigatória nos cursos de Graduação em Administração; Lei da Espionagem Econômica e Industrial brasileira: uma necessidade para garantia da competitividade brasileira; e, Contra-Inteligência Competitiva: uma necessidade na manutenção da competitividade das organizações. (ABRAIC, 2004).

O Sebrae, em parceria com a ABRAIC, "está dando a pequenos produtores acesso à técnica de inteligência competitiva, termo que significa garimpar informações estratégicas para prever mudanças e definir ações (é o que fazem, por exemPlo, os serviços secretos dos países)". (EXAME, 11/2004).

Comparando a doutrina para a produção de informações estratégicas, apresentada em livro editado pela Biblioteca do Exército – Bibliex[11], em 1974, observamos similaridade com o texto de Santos (2000), intitulado Inteligência Competitiva. O Quadro 3, apresenta algumas evidências.

Quadro 3 – Semelhanças nas abordagens entre IE e IC

PRODUÇÃO DE INFORMAÇÕES ESTRATÉGICAS – IE	**FORMULAÇÃO DE INTELIGÊNCIA COMPETITIVA - IC**
DEFINIÇÃO: A produção de uma Informação sobre determinado assunto compreende a seleção e reunião dos fatos relativos ao problema (não propriamente a busca de campo), sua avaliação, seleção e interpretação, e finalmente a apresentação de forma clara e expressiva, como informação acabada, oral ou escrita.(p.25)	DEFINIÇÃO: A Inteligência Competitiva é um processo sistemático de agregação de valor, que converte dados em informação e, na seqüência, informação em conhecimento estratégico para apoiar a tomada de decisão organizacional. (fl. 1)

[11] A produção de informações estratégicas. Traduzido pelo Maj Alvaro Galvão Pereira e Cap Heitor Aquino Ferreira (Heitor foi secretário de Golbery de 1964 a 1967 e de Geisel de 1971 a 1979).

PRODUÇÃO DE INFORMAÇÕES ESTRATÉGICAS – IE	FORMULAÇÃO DE INTELIGÊNCIA COMPETITIVA - IC
FASES: 1) Levantamento Geral; 2) Definição dos Termos; 3) Coleta de Informes; 4) Interpretação dos Informes; 5) Formulação de Hipóteses; 6) Conclusões; 7) Apresentação. (p. 102-107)	FASES: 1) Estudo da posição competitiva (cap. 1); 2) Classificação em grupos (cap. 1); 3) Processo formalizado p/ coleta da informação (cap.1); 4) Interpretação com enfoque na perspectiva (cap. 2); 5) Elaboração de cenários (cap. 3); 6) Plano de apresentação (cap. 4); 7) Apresentação dos resultados (cap. 5,aula 6)

Fonte: PLATT, Washington(1974); SANTOS, Néri dos(2000).

Obviamente que os termos empregados e o direcionamento dos trabalhos são diferentes, o primeiro voltado para aplicação no campo político/militar e o segundo com foco centrado na indústria, contudo com pressupostos semelhantes.

Outro aspecto observado no livro disponibilizado para os assinantes da Bibliex em 1974, baseado na 2ª edição do original *Strategic Intelligence Producion* (1962, p. 21) vislumbra no prefácio da sua edição em português a aplicação não somente para civis e militares especialistas em informação:

> mas também a executivos de empresas e pesquisadores em outras ciências sociais, pois estes, ao lerem a presente obra, entenderão a similaridade da problemática da informação com a de suas próprias atividades, daí auferindo muitos conhecimentos, independente de constituir uma fonte de cogitações novas para os estudantes de outros campos, pelo muito de ensinamentos que contém.

3. A NOVA ECONOMIA E A SEGURANÇA DA INFORMAÇÃO

No contexto da nova economia, as relações comerciais proporcionadas pela Internet criam uma nova forma de se fazer negócios. Surge o *e-commerce* ou comércio eletrônico, expandindo rapidamente seus mercados e sedimentando as bases da Nova Economia ou Economia Digital. Essa nova percepção de transação eletrônica incorpora os conceitos de Desmaterialização (substituição do movimento e contato físico por informação), Desintermediação (eliminação de um ou mais intermediários na cadeia de venda do produto) e Grupo de Afinidades (produtos e serviços que possuem similaridades em termo de divulgação e consumo). Nas palavras de Kevin Kelly,[12] a Nova Economia possui três características distintas: é global; favorece tudo que é intangível (idéias, informação, saber e relações); e está intensivamente interligada. Esses três novos atributos estão a criar um novo tipo de mercado e de sociedade, baseado em redes eletrônicas.

Esse é o cenário de surgimento das empresas Ponto Com (.com) e sua bolsa (Nasdaq) cujas ações atingiram valores considerados altos em relação às ações das empresas tradicionais. Estamos no século XXI e os conhecimentos combinados com a velocidade são os principais produtos. As predições do guru Alvin Toffler[13] começam a se realizar.

Nesse contexto, as organizações iniciam o processo de inclusão, passando a incorporar novos paradigmas não somente no viés tecnológico, mas, e principalmente, na estratégia e na gestão dos seus negócios. As estruturas organizacionais diminuem os níveis hierárquicos, os sistemas de pagamentos tornam-se mais flexíveis, alianças estratégicas em escala mundial são criadas, os mercados comuns entre Nações são objeto de entendimentos diplomáticos, a globalização torna o mundo menor.

A redução dos custos das transações com a partilha de informações entre os *Players* do mercado global contribuiu para o desenvolvimento dos *e-marketplace* também designado de *Internet Trade Exchange*. Neste modelo de comércio

---

[12] Editor da revista “Wired”e autor dos livros Out of Control (1994) e New Rules for New Economy (1998). Entrevista concedida à janela na Web www.janelaweb.com/sociedade (KELLY, 1997)

[13] “Na terceira Onda, o conhecimento é a principal forma de capital. Você e eu podemos usar o mesmo conhecimento ao mesmo tempo. Este fato, por si só, derruba o alicerce dos pressupostos tradicionais acerca do capital e abre um rombo na própria definição de economia como a ciência da alocação de recursos escassos”. (TOFFLER, 2003)

inúmeros compradores e fornecedores interagem formando uma comunidade *Web*, em vista a comercialização de bens e serviços, a partilha de informações e a otimização de todos os processos do negócio.

Com o desenvolvimento dessas comunidades questões éticas relacionadas com confiança e transparência começaram a despertar a atenção das organizações. Confiança que necessita ser construída e fortalecida a cada dia para permitir que os processos fluam de modo dinâmico. Transparência no sentido de que cada um dos participantes do negócio saiba com quem está se relacionando e quais são as regras deste relacionamento.

Eventos na contra-mão dos negócios, contudo, começaram a surgir e a consciência da exposição a riscos de fraudes e outras ameaças se instalou no consciente dos executivos. “Hacker”, “Cracker”, “Phreaker”, “Scanner”, “Vírus”, “Trojan Horse”, ”Sniffer”, “Cookies” foram palavras incorporadas no jargão corporativo.

Diferentes usos para fins ilícitos passaram a transitar na *Internet*. Desde internautas que buscavam o preenchimento das necessidades de ordem psicológicas aos que empregavam seus conhecimentos para invadir sistemas e praticar fraudes contra instituições, a exemPlo dos arquivos de *credit card*.

> Todas as noites eu “conecto” com o intuito de poder desabafar o máximo, até me cansar para, então, o sono chegar, e levar-me para a cama. Tento imaginar o futuro todo o santo dia, e o único futuro que desejo observar, é a solução para uma dor que me consome sem pressa de acabar. A solidão realmente gostou da minha pessoa. Gostou tanto que resolveu me visitar todas as noites. E sempre muito mal educada, pois chega, sem avisar, sem pressa para terminar suas pressões psicológicas. Mas, a solidão não contava de encontrar um cara tão maluco quanto ela. Pois, sou um Hacker, e a rede me trouxe felicidade. Felicidade de saber que não conseguiria me fazer chorar de desgosto, e cair em suas tentações e infelicidades. A Rede com suas fantasias e mistério, que numa conectada me traz tesão, me faz ter desejo, me faz forte e quente, me faz chorar e rir, me faz ter vontade de correr, vontade de gritar, de amar, vontade de viver e esquecer tudo.
>
> É uma força que dificilmente conseguiríamos sozinhos, é um amigo para todos os problemas, é uma janela para o mundo quente, lento e misterioso. Todos têm os seus porque, eu tenho o meu, e com

> certeza, você deve ter o seu. Muitos acham isso uma loucura. Loucura é minha vida... Hacker. (REBITTE, 2000.p.1)

Como se não fosse suficiente, a espionagem industrial encontrou terreno fértil para se desenvolver. Em 1996, o jornalista investigativo Nicky Hager publicou na Nova Zelândia o livro *Secret Power*, denunciando ações de espionagem feitas por meio do chamado Sistema Echelon,[14] voltadas para espionar segredos industriais: de tecnologias a concorrências públicas internacionais. De acordo com Patricky S. Poole, Diretor do *Center for Technology Policy*, do *Free Congress Research and Education Fundation*, Washington, USA, em 1994, a CIA e a NSA interceptaram ligações telefônicas entre o governo brasileiro e a empresa francesa Thomson-CSF acerca do sistema de radar que o Brasil pretendia adquirir. As interceptações foram usadas em benefício da empresa americana, Raytheon.

A certeza da impunidade face inexistência de legislações para combater o delito virtual, servia de incentivo para a rápida disseminação do desenvolvimento e distribuição de vírus de computador, do *hacking*, da propagação de conteúdos e *sites* de pornografia infantil, da violação das leis de *copyright* e fraudes na *Internet*. *Is your business information secure?* Essa era a grande indagação do mundo corporativo.

Observa-se que em fins do século XX, as diferentes aPlicações comerciais que foram criadas (*business-to-business, business-to-consumer, business-to-government, e-commerce, e-procurement*), o surgimento dos sistemas integrados de gestão (ERP), o estabelecimento dos *marketPlaces* e a infra-estrutura digital[15] foram fatores determinantes para que se buscassem padrões de condutas aceitos universalmente a fim de assegurar a circulação da informação dentro dos requisitos de confiabilidade, disponibilidade e integridade, fundamentais para a velocidade das transações.

---

[14] Avançado sistema de espionagem sob controle da National Security Agency (NSA) nos Estados Unidos, que consegue interceptar e capturar informação transmitida através de telefone, satélites, e-mail, redes de comunicação óptica, microondas, etc. a Espionagem Industrial é um dos alvos do Echelon. Desde o falecimento do comunismo na Europa oriental, as agências de inteligência redefiniram a noção de Segurança Nacional incluindo interesses econômicos, comerciais e incorporados. As empresas que ajudam financeiramente a NSA no desenvolvimento do Echelon são as beneficiadas. (PATRICK S. POOLE, Deputy director, Center for Technology Policy, 2000)

[15] Capacidade de tratamento de todo tipo de informação – números, textos, som, vídeo – para uma forma digital, possibilitando qualquer computador armazenar, processar e enviar.

Encontra-se na obra de Bill Gates, A empresa na velocidade do pensamento (1999), a confirmação dessa assertiva. Referindo-se à infra-estrutura digital destaca que as empresas precisam ter a capacidade de funcionar com controle e eficácia, de reagir às emergências e oportunidades, de levar rapidamente informações valiosas às pessoas da empresa que dela necessitam, à capacidade de tomar decisões rápidas e interagir com os clientes.

Os recursos de *hardware* e *software* (*firewall*, criptografia, sistemas de detecção de intrusão) já não eram suficientes, como bem se referiu Rebitte (2000) em seu estudo com a finalidade de alertar para aspectos não considerados no desenvolvimento de sistemas de segurança.

> Um *firewall* não impede o vazamento de dados. O correio eletrônico é de fato a forma mais simPles de se enviar dados para fora da empresa, mas também é a forma mais perigosa, já que o tráfego de correio pode ser controlado e auditado. Um espião consciencioso preferirá uma fita, um disquete (razão pelos quais há quem defenda o banimento dos *drives* de disquete) ou um simPles *fax*. E não existe apólice de seguro contra estupidez se um funcionário fornecer sua senha de acesso a usuários não autorizados ou desconhecidos, não há *firewall* que resolva".
> Há empresas que gastam pequenas fortunas para montar *firewall* inexpugnáveis, mas não se preocupam em criar políticas de segurança coerentes e consistentes. Para ser eficaz, o *firewall* deve ser parte de uma política global de segurança – uma que seja realista o bastante para identificar e prevenir os riscos efetivos (máquinas que contêm dados mais confidenciais, por exemPlo, não precisam de *firewall*: elas não devem estar ligadas à *Internet*), mas que, por outro lado, não seja paranóica a ponto de impedir as pessoas de trabalhar". (p.185-186)

A questão já não era mais tecnológica, mas de conceito. Em artigo acessível em www.scua.com.br/scuanews/peopleware/scuanews02.htm, Loes (2003) comenta: "Não dá mais para pensar a partir da tecnologia mas, sim, a partir de novos conceitos". A identificação de vulnerabilidades caracterizou o *peopleware* como o elo mais fraco na corrente de proteção.

Nesse cenário, em meados da última década do século XX, começa a se sentir no ambiente dos negócios a necessidade de um padrão de relacionamento que protegesse as informações sensíveis e, ao mesmo tempo, permitisse a identificação das parcerias confiáveis através de um código de conduta que refletisse as melhores práticas de mercado relacionadas à segurança dos sistemas e informações.

4. INCLUSÃO BRASILEIRA NA SEGURANÇA DA INFORMAÇÃO

Dos livros utilizados neste trabalho, chama-se atenção pela singularidade do tema, não obstante o ano em que foi editado: 1994, o livro Segurança em Informática, de autoria do professor Antonio de Loureiro Gil, dedicado a seus alunos de 1975 a 1983 da Faculdade de Economia, Administração e Contabilidade da Escola de Comércio Álvares Penteado, além de abordar aspectos técnicos da segurança em computação, faz considerações sobre a importância da gestão da segurança da informática, destacando a necessidade de criação de "cultura organizacional própria" (Gil,1994) para continuidade operacional e lucro da empresa.

Essa pequena amostra, reflete a identificação do ambiente acadêmico brasileiro com os acontecimentos no resto do mundo, haja vista, como se tratou anteriormente nesta dissertação, que somente em 1995, quando no cenário internacional urgia no ambiente dos negócios a necessidade de um padrão de relacionamento que protegesse as informações. O *British Standard Institute*, entidade privada do Reino Unido, emissor de normas e procedimentos, criou um padrão para orientar as empresas locais a que denominou de BS 7799 – Part 1*: Code of Practice for Information Security Management* e Part 2: *Specification for Information Security Management System.*

Sem pretender ser um "código de práticas", o livro mostra caminhos para estabelecimento de uma política e propõe macro parâmetros de segurança e enfoques para sua administração.

Cultura formal, via legislação e normas, e cultura informal, via treinamento e práticas profissionais, que são a sustentação e a real formatação das atividades de segurança, portanto, é um macro parâmetro.

Definição de responsabilidades, definição de política de segurança, realização de análise de riscos e construção de normas e Planos de segurança são atividades do enfoque Planejamento na gestão da segurança.

De acordo com informações obtidas no site da Rede Nacional de Pesquisa – RNP[16], os primeiros embriões da inclusão digital do Brasil, surgiram em 1988,

[16] A RNP surgiu através do Ministério da Ciência e Tecnologia - MCT, financiada pelo Conselho Nacional de Pesquisa – CNPq, hoje Conselho Nacional de Desenvolvimento Científico e Tecnológico com apoio do Programa das Nações Unidas para o Desenvolvimento – PNUD (MCT).

ligando universidades e centros de pesquisa do Rio de Janeiro, São Paulo e Porto Alegre a instituições nos Estados Unidos. A RNP surgiu em 1989 para unir essas redes embrionárias e formar um *backbone* de alcance nacional. Inicialmente voltada exclusivamente para o meio acadêmico, em 1995, por determinação governamental, passou a fornecer conectividade a provedores de acesso comercial, contudo, o crescimento acelerado da utilização da Internet fez com que dois anos após a RNP voltasse a sua atenção exclusivamente para a comunidade científica.

Outro marco importante foi o fim da reserva de mercado em 1992 que possibilitou o acesso a tecnologias mais desenvolvidas. Ainda neste ano, durante a realização da Conferência das Nações Unidas sobre Meio-Ambiente e Desenvolvimento – ECO92, realizada no Rio de Janeiro, foi disponibilizada uma infra-estrutura de acesso à Internet para atender aos jornalistas de todas as partes do mundo que estavam presentes na cobertura do evento. A inclusão do Brasil se fazia conhecer no cenário internacional.

O crescimento geométrico de utilização da Internet a partir do último decênio do século XX alertou a área governamental para a necessidade de intervenção no sentido de coordenar e integrar todas as iniciativas de utilização da rede mundial, de modo a permitir assegurar qualidade e eficiência dos serviços ofertados.

Dados obtidos no Millennium Indicator, mostra que em 1992, apenas 0,01% da população brasileira tinha acesso a *Internet*. Nos anos seguintes os percentuais se projetaram conforme Quadro 4 abaixo.

Quadro 4 – Usuários da Internet por percentual da população

1993	1994	1995	1996	1997	1998	1999	2000	2001	2002
0,03	**0,04**	**0,11**	**0,47**	**0,82**	**1,51**	**2,08**	**2,94**	**4,66**	**8,22**

Fonte: Network Wizards

Em 2005, permanecendo a média de crescimento de usuários entre 2000 e 2002, em torno de 67%, representará a inclusão de aproximadamente 70 milhões de habitantes, tomando por base a população do Brasil de 182.508.370 habitantes, estimada pelo IBGE em 01/01/2005. O Quadro 5 a seguir, mostra as projeções com base nas estimativas de população e de crescimento de usuários.

Quadro 5 – Estimativo de usuários da Internet no Brasil

Ano	2003	2004	2005
População estimada 01/01 de cada ano[17]	**177.609.285**	**180.160.285**	**182.508.370**
% estimado	**13,72**	**22,92**	**38,28**
Usuários estimados	**24.368.084**	**41.292.737**	**69.864.204**

Fonte: Produzido pelo próprio autor do trabalho.

Em 1995, nota conjunta do Ministério das Comunicações (MC) e o Ministério da Ciência e Tecnologia (MCT) afirmaram que para efetiva participação da sociedade nas decisões envolvendo a implantação, administração e uso da *Internet*, seria constituídos um Comitê Gestor da Internet que contaria com a participação do MC e MCT, de entidades operadoras e gestoras de espinhas dorsais, de representantes de provedores de acesso ou de informações, de representantes de usuários e da comunidade acadêmica. Assim, pela Portaria Interministerial Número 147, de 31 de Maio de 1995, foi criado o Comitê Gestor da Internet no Brasil[18] com as seguintes atribuições:

- Fomentar o desenvolvimento de serviços Internet no Brasil;
- Recomendar padrões e procedimentos técnicos e operacionais para a Internet no Brasil;
- Coordenar a atribuição de endereços Internet, o registro de nomes de domínios, e a interconexão de espinhas dorsais;
- Coletar, organizar e disseminar informações sobre os serviços Internet.

O número de *hosts* crescia a cada ano. Em janeiro de 1998 o Brasil ocupava a 1ª posição na América do Sul (117.200) por número de hosts, a 3ª nas Américas, abaixo do EUA (20.623.995) e Canadá (839.141), e 19ª posição em relação aos demais Países.

Em janeiro de 2004, a sua posição na América do Sul permaneceu inalterada não obstante o incremento de 3.700% no número de *hosts* (3.163.349), nas

[17] IBGE / Diretoria de Pesquisas / Coordenação de População e Indicadores Sociais.
[18] Em 3 de Dezembro de 2003, o Comitê Gestor da Internet no Brasil – **CGIbr** assume status de pessoa jurídica através do Decreto Nº 4.829, da Presidência da República. Entre as principais medidas está a competência para administrar a arrecadação de valores de registro de nomes de domínio.

Américas continuou em 3ª abaixo do EUA (162.195.3680) e Canadá (3.210.081), e 8ª posição em relação aos demais Países. (Ver Quadro 6)

Quadro 6 – Número de Hosts. Evolução da posição do Brasil

ANO	HOSTS	CLASSIFICAÇÃO		
		MUNDO	AMÉRICAS	A. DO SUL
1998	117.200	19º	3º	1º
1999	215.086	17º	3º	1º
2000	446.444	13º	3º	1º
2001	876,596	11º	3º	1º
2002	1.644.575	11º	3º	1º
2003	2.237.527	9º	3º	1º
2004	3.163.349	8º	3º	1º

Fonte: Network Wizards

A quantidade de incidentes, em conseqüência do crescimento da *Internet* no País, sua vulnerabilidade e ausência de procedimentos de proteção, cresceu consideravelmente desde 1999, conforme tabela divulgada pelo NIC BR *Security Office* – NBSO, Grupo de Resposta a Incidentes de Segurança para a *Internet* brasileira, mantido pelo Comitê Gestor da *Internet* no Brasil. (Ver quadros 7 e 8)

Quadro 7 – Incidentes classificados por tipo de ataque

Janeiro a Dezembro de 1999

Mês	Total	AXFR (%)		AF (%)		DOS(%)		Invasão (%)		Aw (%)		Scan (%)		Fraude(%)	
jan	204	89	46.63	5	2.45	7	3.43	14	6.86	22	10.78	67	32.84	0	0.00
fev	172	75	46.60	5	2.91	1	0.58	6	3.49	31	18.02	54	31.40	0	0.00
mar	203	100	49.26	7	3.45	5	2.46	12	5.91	19	9.36	60	29.56	0	0.00
abr	151	60	39.74	8	5.30	0	0.00	2	1.32	0	0.00	81	53.64	0	0.00
mai	145	68	46.90	10	6.90	1	0.69	7	4.83	2	1.38	57	39.31	0	0.00
jun	192	76	39.58	17	8.85	2	1.04	9	4.69	8	4.17	79	41.15	1	0.52
jul	208	46	22.12	26	12.50	0	0.00	10	4.81	14	6.73	110	52.88	2	0.96
ago	385	74	19.22	167	43.38	0	0.00	35	9.09	8	2.08	100	25.97	1	0.26
set	264	97	36.74	85	32.20	1	0.38	3	1.14	4	1.52	74	28.03	0	0.00
out	269	86	31.97	34	12.64	1	0.37	7	2.60	7	2.60	134	49.81	0	0.00
nov	418	55	13.16	148	35.41	1	0.24	14	3.35	18	4.31	182	43.54	0	0.00
dez	496	19	3.83	146	29.44	2	0.40	9	1.81	50	10.08	270	54.44	0	0.00
TOT	**3107**	**845**	**27.20**	**658**	**21.18**	**21**	**0.68**	**128**	**4.12**	**183**	**5.89**	**1268**	**40.81**	**4**	**0.13**

Fonte: NIC BR Security Officer

Quadro 8 – Incidentes classificados por tipo de ataque

Janeiro a Março de 2004

Mês	Total	Worm (%)		Af (%)		Dos (%)		Invasão (%)		Aw (%)		Scan (%)		Fraude (%)	
jan	5886	3013	51	39	0	6	0	9	0	55	0	2481	42	283	4
fev	6110	2306	37	53	0	4	0	13	0	22	0	3542	57	170	2
mar	6002	2653	44	37	0	19	0	56	0	32	0	2862	47	343	5
Total	**17998**	**7972**	**44**	**129**	**0**	**29**	**0**	**78**	**0**	**109**	**0**	**8885**	**49**	**769**	**4**

Fonte: NIC BR Security Officer

Comparando os anos de 1999 e 2004, jan-mar, quadros 7 e 8, observa-se que os incidentes totais passaram de 579 para 17.998, prevalecendo os ataques tipo *worm* (264/1999 - 7972/2004) e *scan* (181/1.999 e 8.885/2004)

Estendendo essa comparação para o período abr-jun, quadros 7 e 9, os incidentes totais passaram de 488 para 16.763, continuando a prevalecer os ataques tipo worm (204/1999 – 8.508/2004) e scan (217/1999 – 7.357/2004)

Permanecendo a mesma proporção entre o primeiro semestre de 1999 e igual período de 2004, estaremos registrando no início de 2005, 1.132.450 incidentes de segurança.

Quadro 9 – Incidentes classificados por tipo de ataque

Abril a Junho de 2004

Mês	Total	Worm (%)		Af (%)		Dos (%)		Invasão %		Aw (%)		Scan (%)		Fraude (%)	
abr	4763	2496	52	36	0	2	0	14	0	81	1	1946	40	188	3
mai	5471	2260	41	38	0	2	0	19	0	58	1	2913	53	181	3
jun	6502	3752	57	24	0	3	0	6	0	26	0	2498	38	193	2
Total	**16736**	**8508**	**50**	**98**	**0**	**7**	**0**	**39**	**0**	**165**	**0**	**7357**	**43**	**562**	**3**

Fonte: NIC BR Security Officer

Segurança passou a ser preocupação dos usuários da rede. A quantidade de domínios registrados dá a dimensão do tráfego na Internet, especialmente no segmento dos negócios. Dados levantados em 17/10/2004 no site do CGIbr, figuram 685.352 domínios registrados, entre Entidades, Universidades e Profissionais Liberais. Desses, 625.317 receberam o domínio com.br, portanto aproximadamente 92% do total.

No segmento governamental (818 domínios), a preocupação com os riscos envolvendo a circulação das tarefas burocráticas e as informações restritas, tornou

necessária a criação do Comitê Gestor da Segurança da Informação (CSGI), através do Decreto nº 3.505, de 13 de junho de 2000, para assessorar a Secretaria Executiva do Conselho de Defesa Nacional nos assuntos relativos à segurança da informação. O decreto instituiu a Política de Segurança da Informação definindo como pressupostos básicos, dentre outros, "criação, desenvolvimento e manutenção de mentalidade de segurança da informação" (Art.1º, V); "conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade" (Art.1º, VII). A criação da Infra-estrutura de Chaves Públicas do Governo Federal/ICP-Gov, (Dec. 3.587, 05/09/2000, Casa Civil da Presidência da República) que contribuiu para a criação da infra-estrutura de Chaves Públicas Brasileira/ICP-Brasil (MP 2200-2, de 24/08/2001, Instituto Nacional da Tecnologia da Informação, Casa Civil da Presidência da República), consta como realização do CSGI nos seus três anos de existência (Entrevista do TC João Rufino de Sales, Modulo Security Magazine, 2004).

Fica patente, nos pressupostos definidos na Política, que deixava de predominar o entendimento na qual somente recursos da tecnologia bastavam-se para proteção das redes, passando a gestão da segurança da informação a ser considerada crucial para a minimização da exposição ao risco.

Consciente da ameaça potencial à salvaguarda de dados, informações e conhecimentos de interesse da sociedade e do Estado, o Governo Federal criou o Sistema Brasileiro de Inteligência (SISBIN), órgão vinculado ao Gabinete de Segurança Institucional, e a Agência Brasileira de Inteligência (ABIN) na posição central do SISBIN, com a missão de executar a Política Nacional de Inteligência. (Lei 9.883/1999, 07/12/1999. D.O.U., 08/12/99)

A ABIN, desenvolvendo as suas atribuições de "Planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade" (Art.4º, II, L9883), criou o Programa Nacional de Proteção ao Conhecimento – PNPC com o objetivo de "sensibilizar segmentos da sociedade brasileira sobre as ameaças ao desenvolvimento e à segurança nacionais, representadas pelas ações de espionagem em alvos econômicos, industriais e científico-tecnológicos" (ABIN, 2004).

No segmento privado nacional, a Associação Brasileira de Normas Técnicas – ABNT, fundada em 1940, entidade privada, sem fins lucrativos, reconhecida como

único Fórum Nacional de Normalização através da Resolução número 07, de 24 de agosto de 1992, do CONMETRO, órgão responsável pela normalização técnica do país, participou em outubro de 1998 de reunião realizada em Tókio pelo ISO/IEC/JTC 1, Comitê Internacional de Normalização no campo da Tecnologia da Informação, levando a sua contribuição e o seu voto para que se aprovasse uma norma internacional comprometida com a salvaguarda das informações nas organizações, quanto aos seus três componentes básicos: a confidencialidade, a integridade e a disponibilidade.

Em Agosto 2001, o Brasil adotou esta Norma ISO como seu padrão, através da ABNT, sob código NBR ISO/IEC 17799. Com essa iniciativa da ABNT, o país muniu-se de uma Norma disponível para as organizações utilizarem como referencial básico na consecução das suas demandas mercadológicas, com segurança.

A ABNT é única e exclusiva representante no Brasil das seguintes entidades internacionais:

- ISO – International Organization for Standardization
- IEC – International Electrotechnical Comission

e das entidades de normalização regional:

- COPANT – Comissão Panamericana de Normas Técnicas
- AMN – Associação Mercosul de normalização

Ainda no segmento privado nacional, em 7 de Maio de 2000 foi fundada a Câmara Brasileira de Comércio Eletrônico voltado ao comércio eletrônico como fator estratégico de desenvolvimento na era do conhecimento, reunindo 150 empresas associadas líderes dos principais setores da Economia Brasileira. Declara como Missão:

> Atuar como um *think pank*, gerando e difundindo conhecimento de vanguarda, bem como defendendo posições de consenso frente aos principais agentes públicos e privados, nacionais e internacionais, relacionados ao fomento das tecnologias da informação. Somos a inteligência e voz da Economia Digital no Brasil. (Câmara Brasileira de Comércio Eletrônico, 2004)

Assim, a sociedade brasileira, nos segmentos governamental e empresarial, está instrumentalizada na defesa do compartilhamento seguro dos recursos da informação.

O arcabouço jurídico, formado por leis aprovadas e em tramitação no Congresso Nacional, é mais um elo na corrente de proteção da segurança da informação.

5. ARCABOUÇO JURÍDICO E A SEGURANÇA DA INFORMAÇÃO

Segundo o adágio popular, sentencia: a facilidade faz o ladrão. Voz corrente no ambiente jurídico declara a falta de leis específicas para punir os crimes no ambiente digital como estimuladoras ao surgimento de quadrilhas organizadas que se locupletam através da violação desses ambientes. Não obstante, juristas e parlamentares vêm buscando dotar o arcabouço jurídico de instrumentos legais para punir tais crimes.

Promovido pelo Departamento de Polícia Federal, no período de 13 a 16/09/2004, foi realizada em Brasília a 1ª Conferência Internacional de Perícias em Crimes Cibernéticos – ICCyber' 2004, com ênfase na legislação sobre crimes cibernéticos. Das nove plenárias realizadas, cinco trataram do assunto: *E-crime in* Austrália; Legislação Brasileira sobre Crimes Cibernéticos; Terrorismo Cibernético; Crimes Cibernéticos no Âmbito Internacional e Legislação Internacional sobre Crimes Cibernéticos.

Dentre os projetos de lei em tramitação no legislativo brasileiro, figuram:

- PL[19]-4102/1993 de autoria do Senado Federal – Mauricio Correa, apresentado em 26/08/1993 com a seguinte ementa: Regula a garantia constitucional da inviolabilidade de dados; define crimes praticados por meio de computador; altera a Lei nº 7.646, de 18 de dezembro de 1987, que "dispõe sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no País, e dá outras providências". (Portal Senado Federal – Subsecretaria de Informações)
- PL-1713/1996 apresentado ao Plenário da Câmara dos Deputados em 27/03/1996 por Cássio Cunha Lima com a seguinte ementa: Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores e dá outras providências. Tal proposição foi apensada ao PL-1070/1995 do Deputado Ildemar Kussler que dispõe sobre crimes oriundos da divulgação de material pornográfico através de computadores. (Portal Câmara dos Deputados – Proposições)

[19] PL – Projeto de Lei

- PL-3235/1997 apresentada em 12/06/1997 por Osmânio Pereira que dispõe sobre crimes perpetrados por meio de redes de informação, tramitando em conjunto com o PL-1713/1996. (Portal Câmara dos Deputados – Proposições)
- PL-84/1999 apresentada pelo Deputado Luiz Piauhylino em 24/02/1999 que dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências, caracterizando como crime os ataques praticados por *hackers* e *crackers*, em especial as alterações de *home pages* e a utilização indevida de senhas. Esta matéria foi a que mais evoluiu e provavelmente se constituirá na primeira Lei específica para os crimes em informática. Encaminhada ao Senado Federal recebeu a identificação SF PLC 89 2003 de 13/11/2003 com a seguinte ementa: Altera o Decreto-Lei número 2848, de 07 de dezembro de 1940 – Código Penal e a Lei 9296, de 24 de julho de 1996, e dá outras providencias. (Dispõe sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judicial). Localizada na Comissão de Educação, que, reunida em 24/08/2004, concedeu vista ao Senador Hélio Costa, presidente da recém instalada Subcomissão Permanente de Ciência e Tecnologia-CESCT. (Portal Câmara dos Deputados – Proposições)

Ainda tramitando na Câmara dos Deputados temos o PL-3016/2000, de autoria do Deputado Antonio Carlos Pannunzio, apresentado em 16/05/2000, que dispõe sobre o registro de transações de acesso a redes de computadores destinados ao uso público, inclusive a Internet. A sua transformação em Lei será de grande importância para as autoridades empenhadas no combate aos crimes cibernéticos, uma vez que o rastreamento das mensagens na Internet é um recurso importante para o esclarecimento das ocorrências delituosas e se configura atualmente no maior entrave para uma investigação, haja vista a não obrigatoriedade dos provedores de acesso manterem cadastro de usuários ou mesmo registrarem as conexões realizadas. O art. 5º desse PL define que “para cada conexão efetuada por um usuário, o provedor de acesso registrará o endereço de rede correspondente, o horário de início e término da conexão e a origem da chamada”, estabelecendo a sua preservação mínima por três anos. Como última ação registrada na sua

tramitação, consta o seu recebimento em 15/06/2004, pela Coordenação de Comissões Permanentes (CCP). (Portal Câmara dos Deputados – Proposições)

Outro pl, desta feita tramitando no Senado Federal, é o SF PLS 2000, de 27/03/2000, de autoria do Senador Renan Calheiros, que tipifica os delitos informáticos. Atualmente se encontra com o Senador Magno Malta para emitir relatório, conseqüente de decisão da CCJ – Comissão de Constituição, Justiça e Cidadania, reunida em 13/03/2003. (Portal Senado Federal – Subsecretaria de Informações)

Apesar da falta de legislação específica, a vigente pode ser aplicada aos crimes cibernéticos, é o que entende os juristas. Segundo declaram, o que a Justiça busca demonstrar ao longo da instrução penal é certeza da autoria e elementos probatórios que comprovem que o ilícito efetivamente ocorreu. Assim, não importa se o crime foi cometido por meio eletrônico ao não, concluem.

Contudo, algumas leis têm sido alteradas ou regulamentadas para se adaptarem às especificidades do delito.

Identificou-se a Lei 9.296, de 24/07/1996, que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal: “Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa”. (PUB DOFC 25/07/1996 PAG 13757 COL 1 Diário Oficial da União)

Também a Lei 9.983, de 14/07/2000, que altera o Decreto-Lei 2.848, de 07/12/1940-Código Penal: “Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa”. “Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa”. (PUB DOFC 17/07/2000 PAG 4 COL 1 Diário Oficial da União)

Finalmente a Lei 10.764, de 12/11/2003, que altera o Art. 241 da Lei 8.069 – Estatuto da Criança e do Adolescente, de 13/07/1990, que passou à seguinte redação:

> "Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo exPlícito envolvendo criança ou adolescente: Pena – reclusão de 2(dois) a 6(seis) anos, e multa." (PUB DOFC 13/11/2003 PAG 1 COL 2 Diário Oficial da União).

Apesar da lei 10.764 não tipificar a posse da pornografia, entende-se como um grande avanço.

Certamente que a vigência das Leis específicas modificará a performance dos tribunais e influenciará a mudança de postura da sociedade como um todo.

Não se pode deixar de mencionar a responsabilidade acessória que será incorporada às preocupações dos executivos das organizações que atuam no mercado global, face principalmente o novo Acordo de Capital da Basiléia e a Sarbanes-Oxley Act, sujeitando-os a demandas cíveis pela falta de transparência na circulação de informações financeiras, em um ambiente de alta vulnerabilidade como é a *Web*, onde a essência de tais dados, via de regra, trata de estratégias de negócios. As organizações serão impelidas a proteger as suas informações, sustentadas por padrões internacionalmente reconhecidos e através de profissionais com alto grau de capacitação técnica e jurídica.

Renato Opice Blum (Módulo.2004), sócio do escritório de advocacia Opice Blum Advogados Associados, menciona as regulamentações das diversas agências reguladoras pelo mundo, que aumentam a responsabilidade da governança da Tecnologia da Informação e a gerência operacional sobre os riscos dos negócios. Cita como exemPlo a Comissão de Valores Mobiliários, o *Security and Exchange Comission* e as regulamentações mais recentes como a americana Sarbanes-Oxley[20] e o Novo Acordo de Capital da Basiléia.[21]

---

[20] Referida lei introduz regras bastante rígidas de governança corporativa, procurando dar maior transparência e confiabilidade aos resultados das empresas, instituindo severas punições contra fraudes empresariais e dando maior independência aos órgãos de auditoria" (Renata Homem de Melo e Renata Cruz Simon, Portal Societário)

[21] Consiste em um conjunto abrangente de **Princípios Essenciais** para uma supervisão bancária eficaz (Os Princípios Essenciais da Basiléia); e, um **Compêndio** (a ser atualizado periodicamente) das recomendações, orientações e normas do Comitê da Basiléia, às quais o documento dos Princípios Essenciais faz muitas referências. O Comitê de Supervisão Bancária da Basiléia *(Basle Committee on Banking Supervision)* congrega autoridades de supervisão bancária e foi estabelecido pelos Presidentes dos bancos centrais dos países do Grupo dos Dez (G-10), em 1975. É constituído por representantes de autoridades de supervisão bancária e bancos centrais da Bélgica, Canadá, França, Alemanha, Itália, Japão, Luxemburgo, Holanda, Suécia, Suíça, Reino Unido e USA.

Finalizando este tema, convém, contudo, observar o seguinte comentário de Ricardo Reis Gomes na sua monografia (2001) para o curso de Direito da UNB:

> É necessário que o legislador fique mais atento ao princípio da proporcionalidade. A aplicação de penas muito severas poderá levar a situações prejudiciais para a própria sociedade. Quando se pune uma pessoa que cometeu um ato criminoso de informática com até seis anos de reclusão, como ocorre em alguns casos no PL 84/99, levando o delinqüente a um sistema fechado ou semi-aberto corre-se o risco de se formar um novo grupo criminoso, pois serão colocados no mesmo lugar, criminosos violentos ou estelionatários perspicazes, juntamente com hackers podendo formar um grupo que unirá as habilidades dos criminosos de informática e a astúcia de criminosos comuns. Apenas relembrando a história, foi a união de criminosos políticos com bandidos comuns, no presídio da Ilha Grande, que se deu início ao Comando Vermelho, que é a maior organização criminosa do Brasil.

A pertinência da observação de Gomes (2001), nos leva a outro tema da maior relevância que é a inoperância do sistema carcerário brasileiro. Não obstante a sua temporalidade foge ao escopo deste trabalho maiores considerações a respeito.

Normalmente se reúne no Banco de Compensações Internacionais, na Basiléia, Suíça, onde se localiza sua Secretaria permanente. (Carvalheira, 1997)

6. NORMA NBR ISO IEC 17799:2001 [22]

O ISMS/IUG (*Information Security Management Systems/International User Group*), é o orientador dos negócios para a rede internacional de usuários da ISO / IEC 17799 e BS 7799 (Part 2), com o objetivo de desenvolver nas pequenas, médias e grandes organizações em todas as partes do mundo, uma *common language* para gerenciamento da segurança da informação.

Em 2004, o ISMS/IUG promoveu seis reuniões em diferentes países, inclusive no Brasil em 25/10/2004, a qual foi considerada por Ted Humphreys, seu fundador e atual Presidente, a mais importante das reuniões, haja vista ser a primeira após a consolidação da BS 7799 como Norma ISO/IEC, em encontro realizado no período de 18 a 22/10/2004 em Fortaleza-Brasil, que reuniu 130 membros da *International Organization for Standardization* - ISO, representando 25 diferentes países. Na sua palestra, *Globalisation of Information Security*, discorreu sobre a história da *Common Linguage for Information* desde a sua concepção inicial em 1986-7 quando um grupo de países incluindo Alemanha, França, Inglaterra e Estados Unidos, identificou os controles comuns por eles adotados e os catalogaram como as melhores práticas. Em 1989-91, a Inglaterra passou a adotar essas práticas em operações policiais. Em 1991-2 um grupo de industrias britânicas transformou os controles comuns em Código de Prática publicando-o em seguida. Em 1995 o *British Standard Institute*, entidade privada do Reino Unido, emissor de normas e procedimentos, criou um padrão para orientar as empresas locais a que denominou de BS 7799 – Part 1*: Code of Practice for Information Security Management* e Part 2: *Specification for Information Security Management Systems*. Tamanha foi a aceitação na Inglaterra que rapidamente passou a ser adotada por outros países da Comunidade Britânica a exemPlo da Austrália, África do Sul e Nova Zelândia. A sua propagação entre os países europeus também ocorreu rapidamente e em 1999 a International Organization for Standardization - ISO, tradicional organização sem fins lucrativos com sede em Genebra, após consulta internacional, formou comitê reunindo mais de 120 paises, incluindo o Brasil que se fez representar pelo coordenador do comitê da ABNT (Associação Brasileira de Normas Técnicas) Ariosto Farias Júnior e no ano

[22] NBR ISO/IEC 17799. Tecnologia da Informação – código de prática para a gestão da segurança da informação. ABNT. Ago 2001

seguinte adotou a primeira parte das normas inglesas, que passou a ser denominada ISO/IEC 17799:2000.

Lembra Ariosto (2004) que a sua adoção como padrão internacional para a Segurança da Informação tiveram a oposição de alguns dos paises mais ricos do mundo, a exemPlo da Alemanha, Canadá, Estados Unidos, França, Itália e Japão. Os posicionamentos contrários se exPlicavam por estes paises já possuírem as suas normas próprias e não desejarem padronizar pelas normas da Inglaterra.

Mas as normas ISO mais conhecidas no mundo, 9000 e 14000, também são britânicas na sua origem. Ressalta Ariosto(2004), que também é delegado brasileiro na ISO/IEC e membro do Grupo Internacional de Usuários (IUG), que a ISO disponibiliza apenas a Part I do padrão inglês e que por enquanto nenhuma empresa possui certificação ISO em Segurança da Informação:

> "somente depois da reunião de Varsóvia, realizada em 2002, decidiu-se que teríamos uma certificação para Segurança da Informação com padrão ISO. Já estamos trabalhando nisso e acredito que, entre dezembro de 2004 e junho de 2005, o mercado mundial tenha acesso à Certificação ISO 17799". (Entrevista concedida ao autor. 2004)

Atualmente, segundo o *Information Security Management Systems* ISO/IEC 17799 & BS 7799 Part 2, 1.104 (hum mil, cento e quatro) certificados foram concedidos de acordo com a BS 7799. (Ver quadro 10 abaixo)

Quadro 10 – Número de Certificações BS 7799 por Países

Japan	510	Norway	9	UAE	2
UK	185	Austria	5	Colombia	1
India	81	Sweden	5	Czech Republic	1
Taiwan	45	Switzerland	5	Egypt	1
Germany	36	Iceland	4	Lebanon	1
Korea	31	Poland	4	Luxemburg	1
Italy	23	Brazil	3	Macau	1
Netherlands	18	Greece	3	Macedonia	1
Hong Kong	17	Mexico	3	Morocco	1
USA	15	Saudi Arabia	3	Qatar	1
Finland	12	Spain	3	Slovakia	1
Australia	11	Argentina	2	Slovenia	1
China	11	Belgium	2	South Africa	1
Hungary	11	Denmark	2		
Ireland	11	Isle of Man	2	Relative Total	1104
Singapore	11	Malaysia	2	Absolute Total	1095

Nota: Absoluto Total representa o atual número de certificados. Relativo Total reflete o número de certificados que representam mais de uma nação ou dupla certificação.
Fonte: ISMS INTERNATIONAL User Group 2001-2005, 09/02/2005

Como se pode observar no Quadro 10, o Brasil é representado com três empresas (Ver quadro 11), contudo, em 28/10/2004, após três dias de auditoria, o auditor sênior da Det Norske Veritas (DNV) – Suécia, Birger Berggren, recomendou a Samarco Mineração, Espírito Santo – Brasil, a receber a certificação BS 7799. Assim, em 2005 o Brasil estará representado por mais uma empresa.

Quadro 11 – Empresas Brasileiras certificadas pela BS 7799

Name of Company	Certificate Number	Certification Body
Banco Matone S.A	07502-2003-AIS-LDN-UKAS	DNV
Modulo Security Solutions S.A	02154-2002-AIS-LDN-UKAS	DNV
Serasa, São Paulo	262326 IS	DQS

Fonte: ISMS INTERNATIONAL User Group 2001-2005, 09/02/2005

Segundo informação de Ariosto Farias Jr, presidente do ISMS International User Group Brazilian Chapter, é esperado que a nova norma seja publicada como ISO IEC 17799:2005, entre maio e junho de 2005. (Entrevista concedida ao autor, 2004)

6.1 PRINCIPAIS REQUISITOS DA NORMA NBR ISO/IEC 17799:2001

A Associação Brasileira de Normas Técnicas – ABNT disponibiliza para aquisição, através do seu site www.abnt.gov.br, versões eletrônica e física da referida norma técnica. Apresenta os conceitos básicos que dão sustentação ao elenco de requisitos indispensáveis para a gestão da segurança da informação. Define a segurança da informação como um ativo importante para os negócios e dá o caminho para que a organização proceda: a) à avaliação de risco dos ativos, pela identificação das ameaças, das vulnerabilidades e sua probabilidade de ocorrência; b) a análise da legislação vigente, estatutos, regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender; c) os conjuntos particulares de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

O objetivo da norma é fornecer recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações.

No título **Termos e definições,** a Norma estabelece os seguintes pilares: segurança da informação (preservação da confidencialidade, integridade e disponibilidade), avaliação de risco e gerenciamento de risco.

No título **Política de segurança** fornecem os insumos para a elaboração da documentação da política de segurança da informação, análise crítica e avaliação. O patrocínio da alta administração na elaboração e disseminação desses padrões, é de fundamental importância para o estabelecimento de um modelo de comportamento corporativo voltado para a proteção das informações.

No título **Segurança organizacional**, seus itens e sub-itens orientam a criação da Infra-estrutura da segurança da informação, o estabelecimento da Segurança no acesso de prestadores de serviços e a responsabilidade pelo processamento da informação terceirizada para uma outra organização.

Classificação e controle dos ativos de informação é outro título da Norma, que aborda a contabilização dos ativos de Segurança e o seu responsável. Estabelece recomendações para a classificação da informação, segmentando-a em níveis de sensibilidade e criticidade.

Segurança em pessoas é outro titulo de grande relevância abordado na norma, voltado para a redução de riscos de erro humano, roubo, fraude ou uso indevido das instalações. Observa-se grande preocupação dos gestores com a força de trabalho das organizações, elo mais fraco na corrente de proteção, segundo conceito por eles (gestores) estabelecido.

Segurança física e do ambiente, título que aborda aspectos de prevenção de acesso não autorizado, dano e interferência às informações e instalações físicas da organização. Estabelecem que os recursos e instalações de processamento de informações críticas ou sensíveis do negócio sejam mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso.

No título **Gerenciamento das operações e comunicações**, as recomendações buscam garantir a operação segura e correta dos recursos de processamento da informação, orientando a aPlicação, quando apropriado, do princípio da segregação de funções para reduzir o risco de uso negligente ou doloso dos sistemas.

O título **Controle de acesso**, aborda a política de controle de acessos, o gerenciamento do acesso do usuário (em particular a concessão e o uso de privilégios, as senhas dos usuários e o direito de acesso), as responsabilidades do usuário, o controle de acesso à rede, a importância da sincronização dos relógios, a computação móvel e o trabalho remoto. A aPlicação do princípio de que “tudo deve ser proibido a menos que expressamente permitido” ao invés de “tudo deve ser permitido a menos que expressamente proibido”.

O título **Desenvolvimento e manutenção de sistemas**, abordam os requisitos de segurança para o desenvolvimento de sistemas, a validação de dados de entrada, a autenticação de mensagem, a validação de dados de saída, os controles de criptografia e o controle de acesso a bibliotecas de programa fonte. Recomenda que todos os requisitos de segurança, incluindo a necessidade de acordos de contingência, sejam identificados na fase de levantamento de requisitos de um projeto e justificados, acordados e documentados como parte do estudo de caso de um negócio para um sistema de informação.

Gestão da continuidade do negócio aborda a continuidade do negócio e análise de impacto, a documentação e imPlantação dos Planos de continuidade, os testes, manutenções e reavaliações. Destaca a importância da gestão da

continuidade do negócio incluir controles para a identificação e redução de riscos, a limitação das conseqüências dos danos do incidente e a garantia da recuperação tempestiva das operações vitais.

Finalmente, o título **Conformidade** chama atenção para o cuidado com qualquer lei criminal ou civil, regulamentos ou obrigações contratuais e de quaisquer requisitos de segurança, a fim de evitar violação de qualquer natureza, haja vista que os requisitos legislativos variam de país para país e também para a informação criada em um país e transmitida para outro.

7. METODOLOGIA DA PESQUISA

Tomou-se como série de valores duas empresas mineradoras e uma do setor petróleo, todas com atuação global, haja vista estarem mais susceptíveis à ação da concorrência internacional. O mapeamento da série abrange as regiões Nordeste e Sudeste do país.

Tomando-se por base o objetivo da pesquisa, optou-se pela pesquisa exploratória descritiva, mais adequada ao que se propõe esta dissertação, ou seja, descrever as características da população selecionada quanto ao nível de conhecimento sobre segurança da informação.

As hipóteses nesta dissertação foram formuladas para medir o nível de conhecimento dos empregados das empresas pesquisadas, quanto às questões abaixo, nas quais se baseia esta pesquisa. (Quadro 12)

Quadro 12 – Formulação das hipóteses e informações pretendidas

Hipótese I – Existe conhecimento sobre Política de Segurança da Informação. Informação pretendida: conhecer as reações aos novos procedimentos de segurança e controle.
Hipótese II – Há um conflito entre o princípio de livre circulação da informação e assimilação de novos procedimentos de controle da informação nas organizações Informação pretendida: opinião dos empregados acerca do embate entre o princípio da livre circulação da informação e as restrições pelos procedimentos de segurança.
Hipótese III – Mudanças de padrões de segurança são mais rapidamente assimiladas pelos empregados quando vivenciam momentos de comprometimento da imagem da organização perante a sociedade e o mercado. Informação pretendida: verificar se existe coerência na afirmação.
Hipótese IV – O Planejamento estratégico nas organizações não leva em conta a peculiaridade do tema segurança da informação. Informação pretendida: evidências de inserção do sistema de segurança da informação no Planejamento estratégico.
Hipótese V – A relativa novidade do conceito de informação como bem econômico na sociedade em geral e nas organizações em particular, tem reflexo sobre a

disseminação dessa cultura de segurança da informação. Informação pretendida: compreensão da informação como bem econômico.
Hipótese VI – O entendimento de informação como ativo da organização, ainda é recente no mundo corporativo. Informação pretendida: compreensão da informação como ativo relevante.

7.1 SELEÇÃO DA AMOSTRA

Segundo Gil (1946), a amostragem é classificada em dois grandes grupos: probabilístico e não-probabilístico, definindo o primeiro grupo como rigorosamente científico e com forte fundamentação matemática, e o segundo como dependente unicamente de critérios do pesquisador.

Referindo-se à não-probabilística, apresenta os tipos mais conhecidos: por acessibilidade, por tipicidade e por cotas.

A amostragem por tipicidade é a mais adequada para os objetivos deste trabalho, tendo em vista haver considerável conhecimento da população e do subgrupo selecionado, assegurando a representatividade da amostra.

Assim, este trabalho determinou uma amostragem não-probabilística, por tipicidade, segmentada por grupo e subgrupo de empresa.

Seguindo a metodologia de Gil, o seu tamanho considerou a extensão do universo, o nível de confiança desejado, o erro máximo aceitável e a percentagem com o qual o fenômeno se verifica. Assim, o universo foi considerado finito – número de elementos não excedente a 100.000, o nível de confiança estabelecido por um desvio-padrão (curva de Gauss) correspondendo aproximadamente 68% do seu total, trabalhando-se com um erro máximo aceitável de 5%, e finalmente presumindo-se que a percentagem com o qual o fenômeno se verifica estivesse próxima de 50%.

7.2 FÓRMULA PARA CÁLCULO DO TAMANHO DA AMOSTRA

A fórmula básica para o cálculo do tamanho de amostras para populações finitas é a seguinte: $\mathbf{n = \sigma^2\ p.q.N\ /\ \varepsilon^2\ (N-1) + \sigma^2\ p.q}$

Onde:

n = tamanho da amostra;

σ^2 = nível de confiança escolhido, expresso em número de desvios-padrão; p = percentagem com a qual o fenômeno se verifica;

q = percentagem comPlementar;

N = tamanho da população; e

ε^2 = erro máximo permitido.

7.3 CÁLCULO DO TAMANHO DA AMOSTRA

n = ?

$\sigma^{2\,=}$ 1

p = 50%

q = 50%

N = 9.594 (Petrobras = 3.094; CST = 3.500; Samarco = 3.000)

ε^2 = 5%

n = 1.50.50.9594 / (25.9593) + 1.50.50, logo **n = 197**

7.4 INSTRUMENTO DE COLETA DE DADOS

Escalas são definidas como questionários que têm como objetivo a quantificação de fenômenos sociais, tais como opiniões e atitudes.

Por ser de elaboração mais simples optou-se pela utilização da escala de Likert. (Gil, p. 143), atribuindo-se valores a cada um dos itens, conhecidos no momento da aplicação. O procedimento para a sua validação contou com a opinião de pessoas consideradas especialistas no tema segurança da informação.

7.5 COLETA DE DADOS

A coleta de dados contou com respostas obtidas através de questionários estruturados na forma de autopreenchimento[23], enviados via correio-eletrônico corporativo e malote interno.

No total, a pesquisa quantitativa teve uma mostra de 302 questionários, compostos por nove perguntas fechadas, múltipla escolha, referentes a fatos e sobre padrões de ação, coletados no mês de novembro de 2004, constituída de empregados com função gerencial e empregados sem função gerencial, trabalhando em regime de revezamento de turno e em regime administrativo, com diferentes tempos de serviço prestado às organizações.

Os profissionais que participaram deste estudo estão distribuídos nos segmentos de siderurgia (47,5%) e petroquímica (52,5%).

Foram ouvidos empregados da Petróleo Brasileiro S.A. – Petrobras, Companhia Siderúrgica Tubarão – CST e Samarco Mineração S.A. – Samarco.

Na Petrobras, por via de conseqüência da sua estrutura organizacional, foram selecionadas unidades representativas de três segmentos: o segmento de Serviços, este representado pela unidade Serviços Compartilhados, que suporta administrativamente as áreas de produção, a fim de que estas se concentrem na sua atividade fim, portanto com atuação em todos os segmentos de negócio da Companhia, caracterizada na pesquisa pela Regional Sudeste, Regional Norte Nordeste, Regional São Paulo Sul e Regional Bacia de Campos. O outro segmento foi o de Exploração & Produção, representado pela Unidade de Negócio do Espírito Santo, por esta Unidade ainda não utilizar o segmento de Serviços. Finalmente o segmento de Abastecimento, representado pela Refinaria Landulpho Alves, localizada em Mataripe-BA,

Desta forma a amostra ficou representativa pela abrangência da população pesquisada, tanto geograficamente quanto em áreas de atuação.

Antes da sua aplicação definitiva, nos meses de setembro e outubro de 2004, foi realizada uma analise preliminar ou pré-teste, envolvendo 20 pessoas pertencentes à população pesquisada, possibilitando as correções das falhas observadas na redação.

---

[23] Ver Apêndice C – Questionário da pesquisa

As empresas selecionadas possuem políticas de segurança da informação com o patrocínio da alta direção, sendo que a Samarco foi indicada em novembro de 2004 para receber a indicação para certificação pela norma BS 7799-2:2002, obtendo o titulo de primeira mineradora no mundo e a primeira empresa do setor industrial das Américas a ser certificada pela norma inglesa.

8. APRESENTAÇÃO E ANÁLISE DOS DADOS

A análise tem como objetivo organizar e sumariar os dados de forma tal que possibilitem o fornecimento de respostas ao problema proposto para investigação. (Gil, 1987. p.166).

Os índices de retorno dos questionários enviados, tanto o geral quanto o por empresa, foram expressivos, conforme demonstra o quadro abaixo, robustecendo, dessa forma, o resultado da análise.

Quadro 13 – Índice de retorno dos questionários enviados.

EMPRESAS PESQUISADAS	QUESTIONÁRIOS ENVIADOS	QUESTIONÁRIOS RESPONDIDOS	% DE RETORNO
PETROBRAS	250	169	67
SAMARCO	100	75	75
CST	100	58	58
€ das Empresas	400	302	75

9. ANÁLISE DOS DADOS GERAIS

A Figura 4 apresenta o perfil da população pesquisada, mostrando que a maioria dos respondentes possui tempo de empresa superior a dez anos (76%), distribuídos com relativa equivalência entre as áreas operacionais (43%) e administrativas (57%) e predominando o regime administrativo de trabalho (73%).

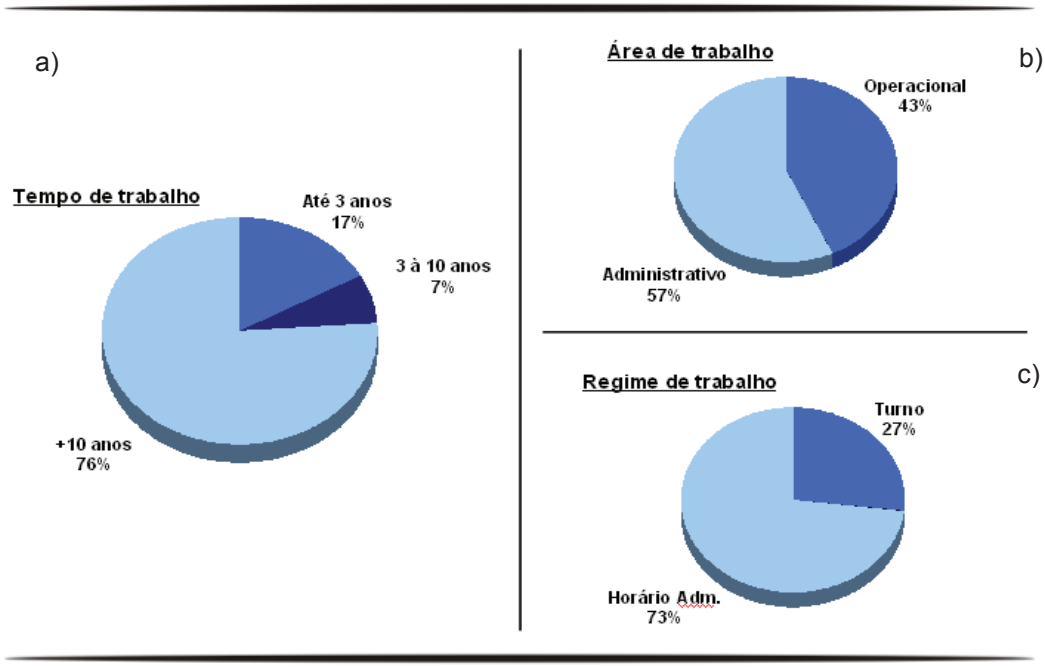


Figura 4 – Perfil de população pesquisada.
a) Tempo de trabalho. b) Área de trabalho. c) Regime de trabalho.

Os resultados apresentados nas figuras 5, 6 e 7, indicam que as empresas vêm obtendo respostas positivas na disseminação de uma cultura voltada para a segurança da informação.

Na Figura 5, a maioria (78%) tem percepção adequada sobre o conceito de segurança da informação. Apesar disso, 15% dos respondentes demonstram não possuir domínio do conceito e 6% não possuem conhecimento sobre o assunto. Em se tratando de segurança da informação, tais percentuais merecem atenção dos

gestores, considerando que esta parcela pode ser susceptível de cooptação pelo processo de Engenharia Social[24].

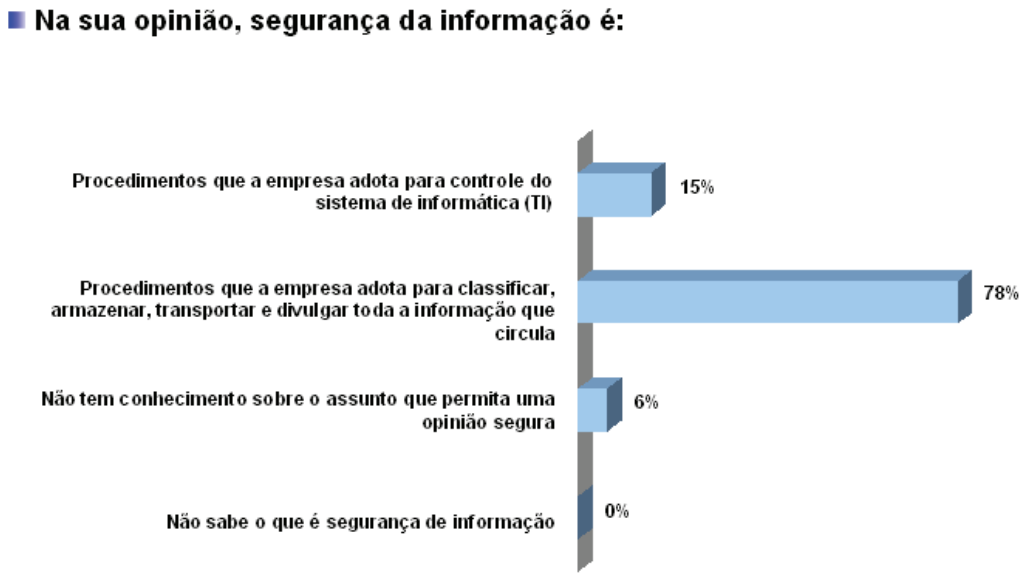


Figura 5 – Novos procedimentos. Segurança da informação.

A Figura 6 apresenta uma condição confortável para os gestores, pelo bom índice de conhecimento da Política de Segurança da Informação: concordam totalmente (57%) ou parcialmente (36%); e por considerá-la boa: concordam totalmente (48%) ou parcialmente (40%). Esta informação é importante porque sinaliza positivamente para os veículos de comunicação corporativo, indicando eficiência na tarefa de divulgar novos padrões de conduta.

[24] Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações

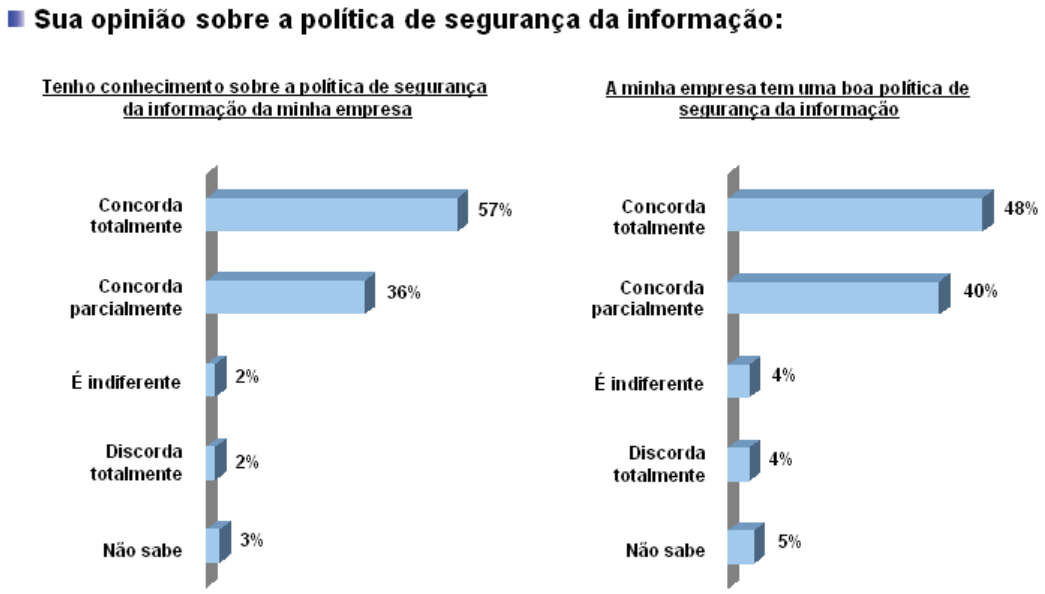


Figura 6 – Novos procedimentos. Política de Segurança da Informação.

A Figura 7 fornece dois dados importantes para os gestores. O primeiro pelo ainda expressivo percentual de empregados que concordam parcialmente (29%) com a rigidez dos controles com implicações para a rotina do trabalho, podendo provocar perda de produtividade para a organização, comprometendo a competitividade. O segundo, pela discordância total (82%), manifestada com a afirmação de que a segurança da informação é um modismo, evidenciando a formação de uma cultura voltada para a segurança da informação.

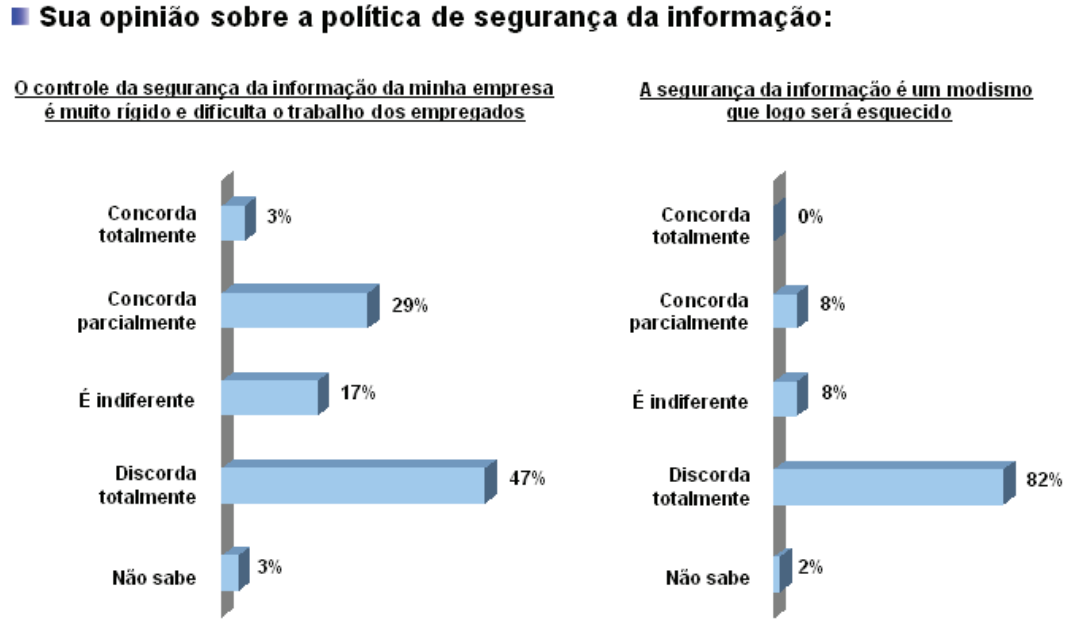


Figura 7 – Novos procedimentos. Política de Segurança da Informação. Controles.

Os percentuais apresentados na Figura 8 pressupõem que deve haver um trabalho de esclarecimento por parte dos gestores, quanto a preconização da política de segurança da informação no dia-a-dia das organizações. Apenas 48% a considera compatível com a rotina corporativa. No mesmo quadro verifica-se que o princípio da livre circulação da informação, não tem encontrado eco entre os empregados na indústria. Dentre eles, 82% são favoráveis aos controles, o que pode contribuir para o fortalecimento da competitividade.

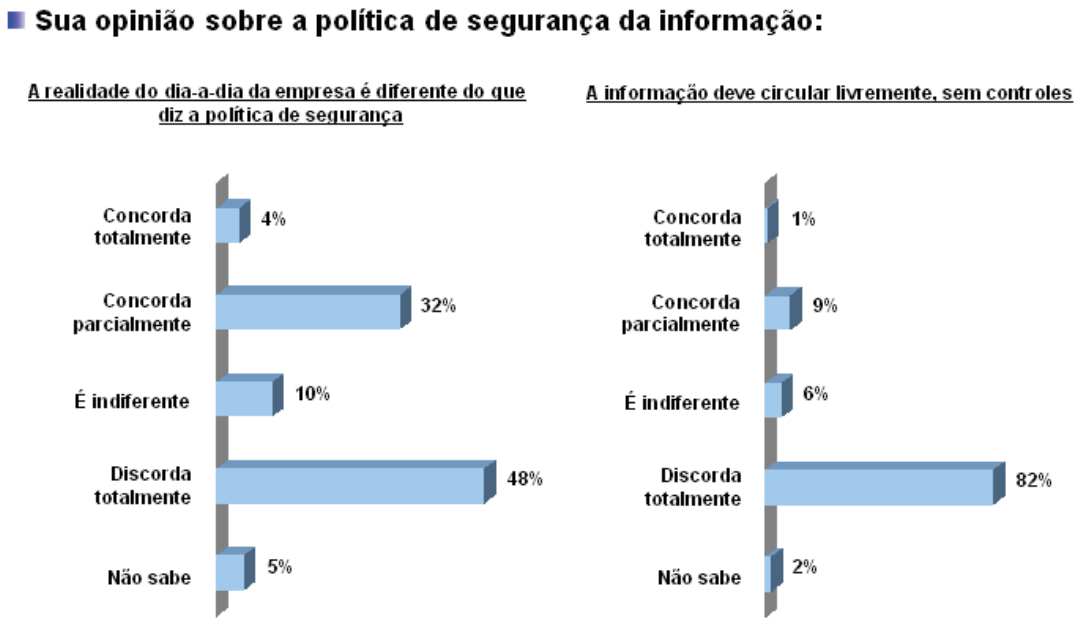


Figura 8 – Circulação da informação

Quanto à assimilação de novos padrões de Segurança, os dados da Figura 9 evidenciam que mudanças de padrões de segurança são mais rapidamente assimiladas pelos empregados quando se promove campanha educativa para esclarecimento do assunto.

Assim, pode-se inferir que as campanhas educativas continuam sendo a melhor forma de difusão de novos procedimentos (71%), todavia, permanece ainda forte (21%) a adoção de cuidados quando ocorrem situações desconfortáveis que podem comprometer a imagem da organização perante a sociedade e o mercado. É o que revela o resultado da Figura 9.

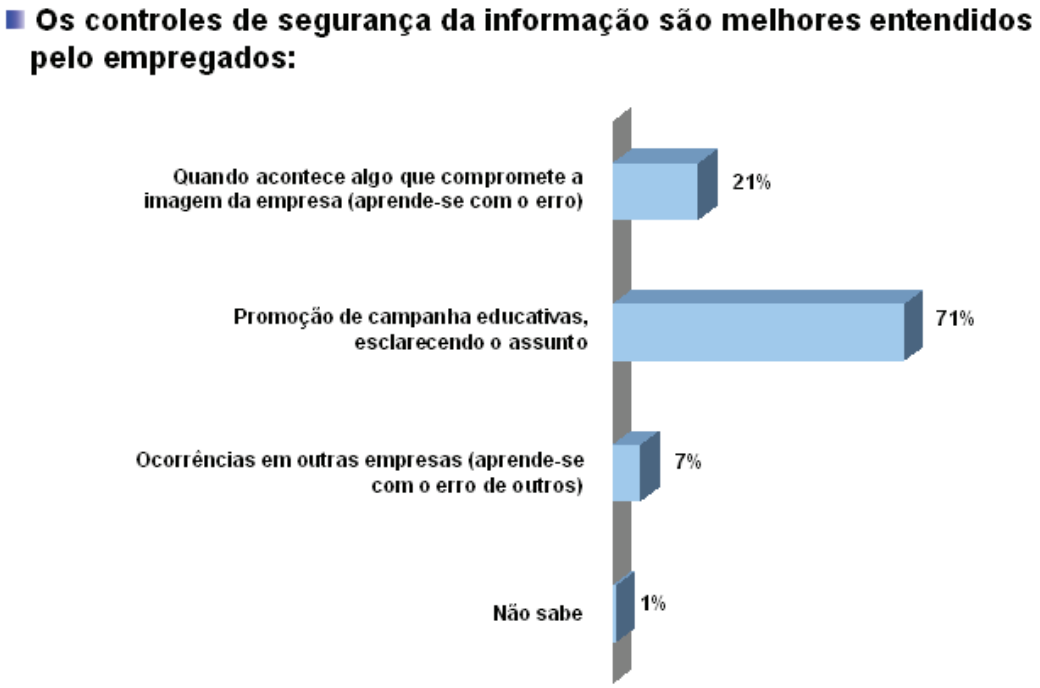


Figura 9 – Assimilação de conceitos

A Figura 10 fornece dois dados importantes: a demonstração para a organização de que 11% dos entrevistados percebem a preocupação com aspectos de segurança da informação na elaboração do Planejamento Estratégico-PE, e a compreensão de 83% que considera a segurança da informação importante para o cumprimento das metas desse mesmo Planejamento Estratégico.

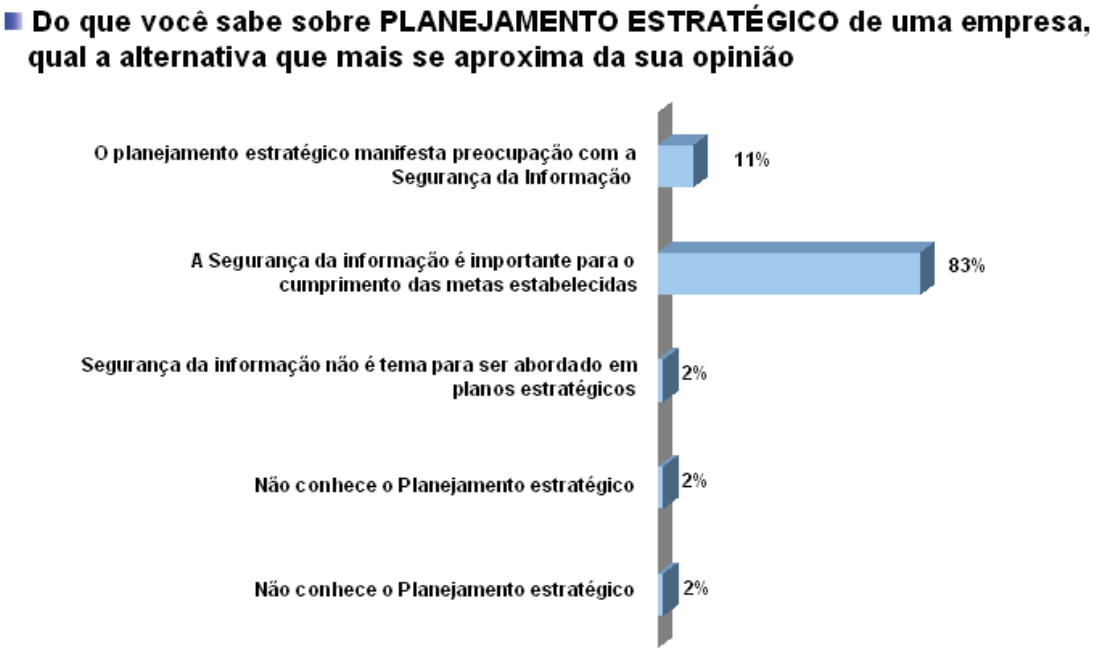


Figura 10 – Planejamento estratégico

Quanto à compreensão da informação como bem econômico, observa-se na Figura 11, que 79% dos respondentes já incorporam o conceito de informação como tal. Essa consciência repercute positivamente nas variáveis decorrentes desta compreensão. Na seqüência, a Figura 12 aponta que quanto ao entendimento a respeito dos cuidados com a segurança, 65% defende a necessidade da confidencialidade nos processos de licitação, o que assegura credibilidade perante o mercado e lhe confere competitividade. Na Figura 13, observa-se que os empregados demonstram possuir visão de longo prazo quando percebem os aspectos de confidencialidade como garantia para a continuidade do negócio: 53% concordam totalmente e 36% concordam parcialmente. Da mesma forma, ao demonstrarem preocupações com o valor de mercado como conseqüência também da preservação das informações corporativas; 42% concordam totalmente e 38% concordam parcialmente.

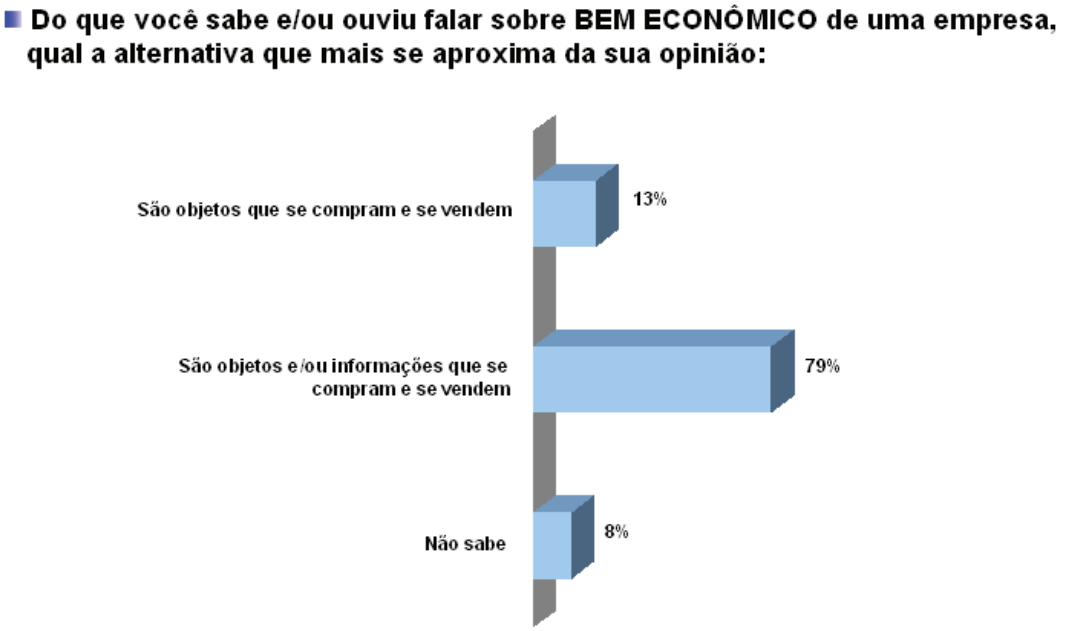


Figura 11 – Bem econômico. Conceito.

Seu entendimento quanto aos cuidados com a segurança da informação:

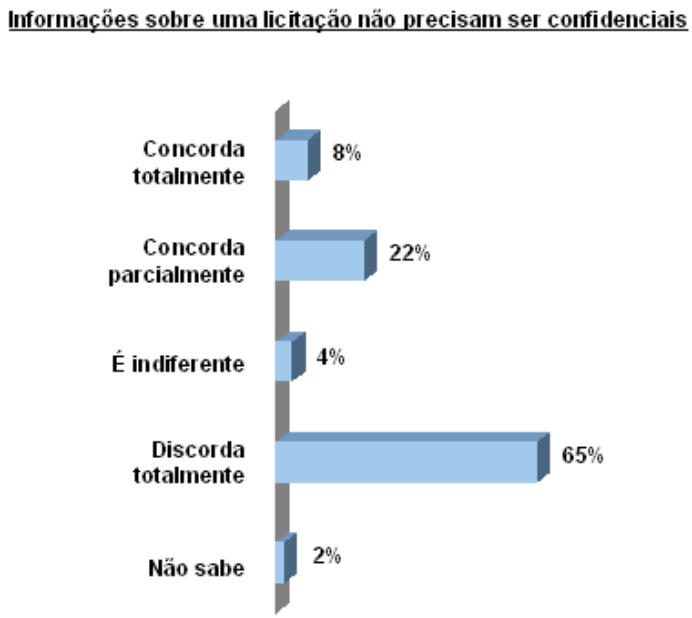


Figura 12 – Bem econômico. Licitação

Seu entendimento quanto aos cuidados com a segurança da informação:

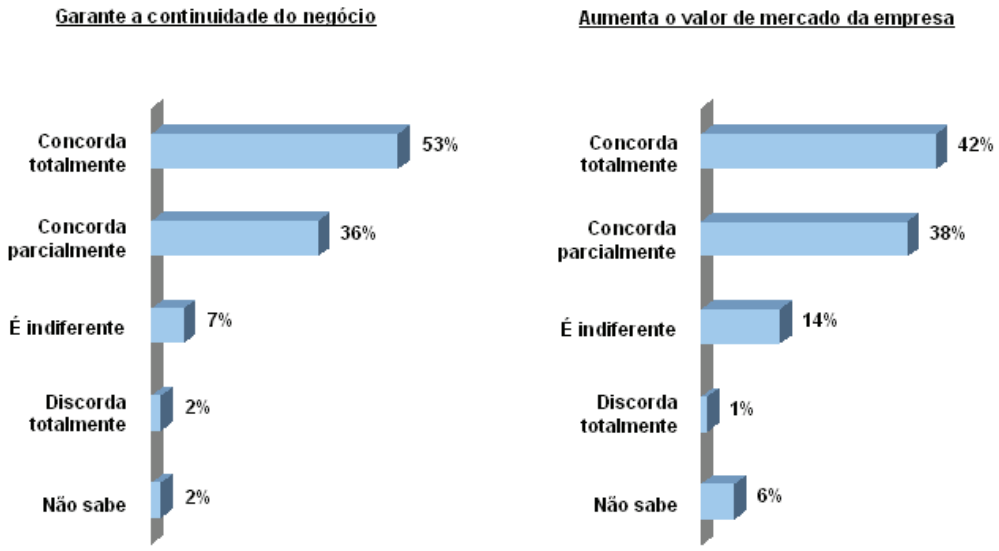


Figura 13 – Bem econômico. Continuidade do negócio. Valor de mercado

Quanto à compreensão da informação como ativo relevante, percebe-se na Figura 14 uma consistente compreensão do conceito de ativo (68%). Esta informação é de suma importância para a alta administração na medida em que incorpora os bens tangíveis e intangíveis, este de maior valor agregado no mundo dos negócios. Apesar disto, merece atenção dos gestores os percentuais dos que ainda não possuem com clareza esta compreensão: 23% compreende que são bens físicos e financeiros e 5% que são bens financeiros.

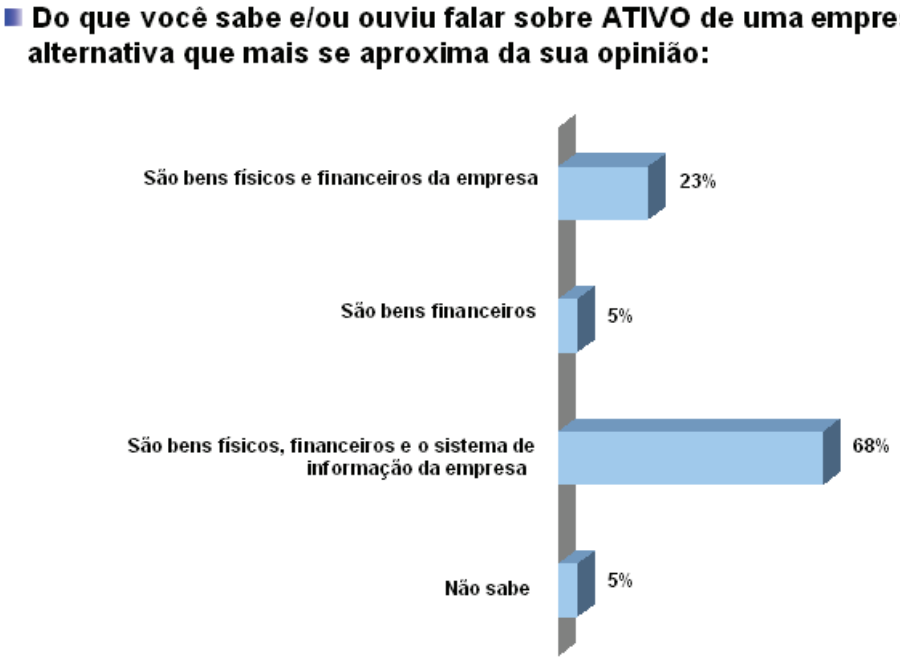


Figura 14 – Ativo. Conceito.

A Figura 15 apresenta uma ligação entre a segurança da informação e o lucro. Apesar do maior percentual (59%) situar-se entre os que concordam com a correspondência existente, observa-se uma parcela significativa (27%) sem o entendimento total ou parcial desse encadeamento. Esta parcela merece a atenção dos gestores, principalmente pelo resultado do quadro anterior.

Ainda na Figura 15 observa-se ainda um aparente desalinhamento com a média dos percentuais das questões anteriormente analisadas, quando se refere a conhecimento tecnológico. Contudo, este dado não deve preocupar os gestores, haja vista o maior percentual de respondentes (57%) trabalhar em área administrativa (Figura 4). Analisando-se sob esta ótica percebe-se até coerência nos

percentuais obtidos. Enquanto 40% (Figura 15) consideram que o conhecimento tecnológico deve ser compartilhado com todos os empregados, 57% (Figura 4) trabalham em área administrativa. Nos mesmos quadros, 51% (Figura 15) discorda total ou parcialmente do compartilhamento do conhecimento tecnológico, enquanto que na Figura 4, mostra que 43% trabalham na área operacional, portanto, com menor possibilidade de concordarem com o compartilhamento do *know-how* tecnológico da indústria.

Quadro 14 – Correspondência entre as figuras 4 e 15.

Conhecimento Tecnológico		**Área de Trabalho**	
Não deve ser divulgado	51%	Operacional	43%
Deve ser divulgado	40%	Administrativa	57%

Percebem-se, todavia, evidências do embate que se trava nos meios acadêmicos e empresariais quanto à livre circulação da informação[25].

[25] Em artigo publicado no jornal A GAZETA, Ruth Reis, Drª em Comunicação e Cultura, opinando acerca da imPlantação na Universidade Federal do Espírito Santo de programa de segurança de arquivos que selecionam assuntos que podem ser acessados na rede mundial de computadores, assim se posiciona: "A instalação de um filtro na rede de informática da Ufes evidencia a relação entre esses instrumentos e o direito de acesso à informação, princípio consagrado nas democracias de todo o mundo. O "filtro" na Ufes proibiu diversos sites a pretexto de "oferecer segurança à rede". A exPlicação pode até agradar àqueles que não chegaram a tempo de participar das lutas pelo direito à informação ou que esqueceram as lições do passado, mas não se harmoniza com os princípios da vida democrática, estampados na Constituição Federal. A informação é um bem coletivo que hoje viceja abundantemente por meio da Internet. Tentar reverter os ganhos que o exercício da comunicação obteve com ela por meio de "filtros" é retrocesso de forma condenável, pois a única forma de conter os fluxos de informação nas vias digitais é colocar estes diques tecnológicos que muito bem podem ser chamados de sensores eletrônicos. Filtrar conteúdos por critérios políticos, morais ou técnicos é praticar uma eugenia informacional que nenhum bom propósito pode justificar. O ambiente digital imita a vida, como ela, contém o bem e o mal. Não é possível admitir que hoje alguém se arrogue a autorizar ou desautorizar alguém a obter informação de qualquer natureza. Numa universidade, que se justifica pelo exercício da liberdade em busca do conhecimento, este também um bem comum, é ainda mais inaceitável que se recorra a tal mecanismo. Mais do que a velocidade das conexões da Internet, o que deve ser preservado é a liberdade"

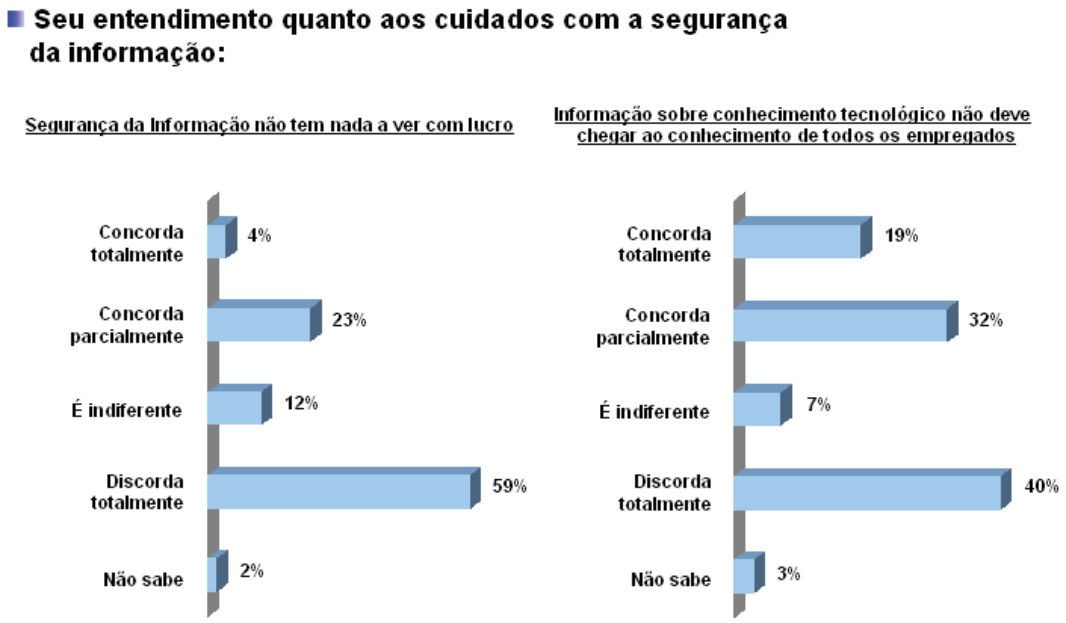


Figura 15 – Ativo. Lucro. Conhecimento tecnológico.

Na Figura 16, observam-se altos percentuais quanto ao entendimento sobre a relação entre segurança da informação versus aumentos da lucratividade: 33% concordam totalmente e 44% concordam parcialmente; e segurança da informação versus preservação da imagem: 62% concordam totalmente e 33% concordam parcialmente.

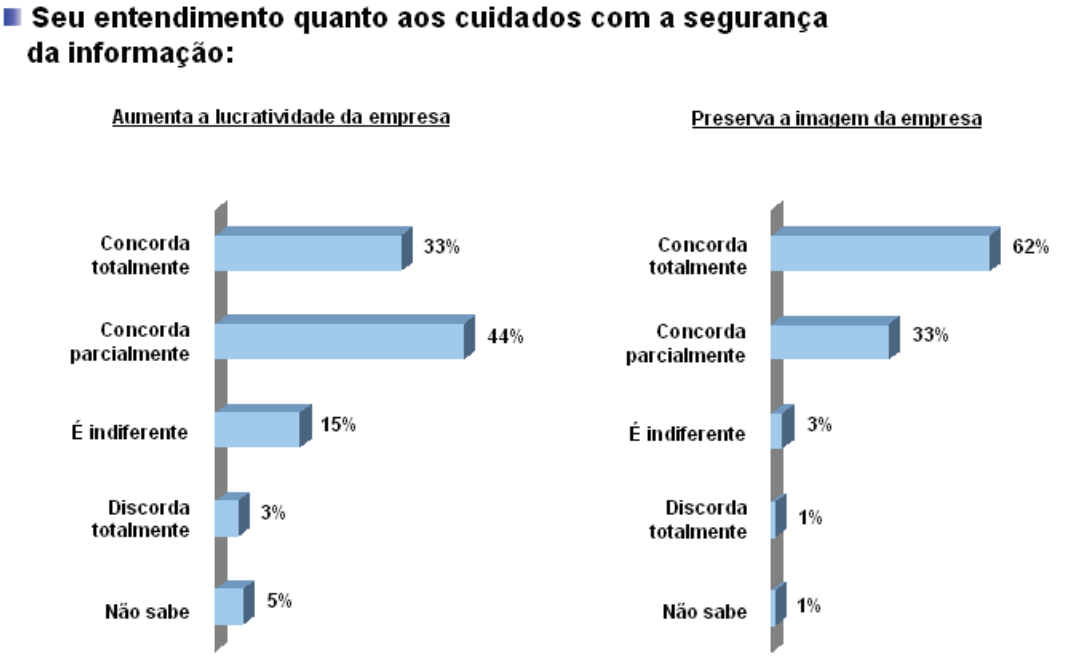
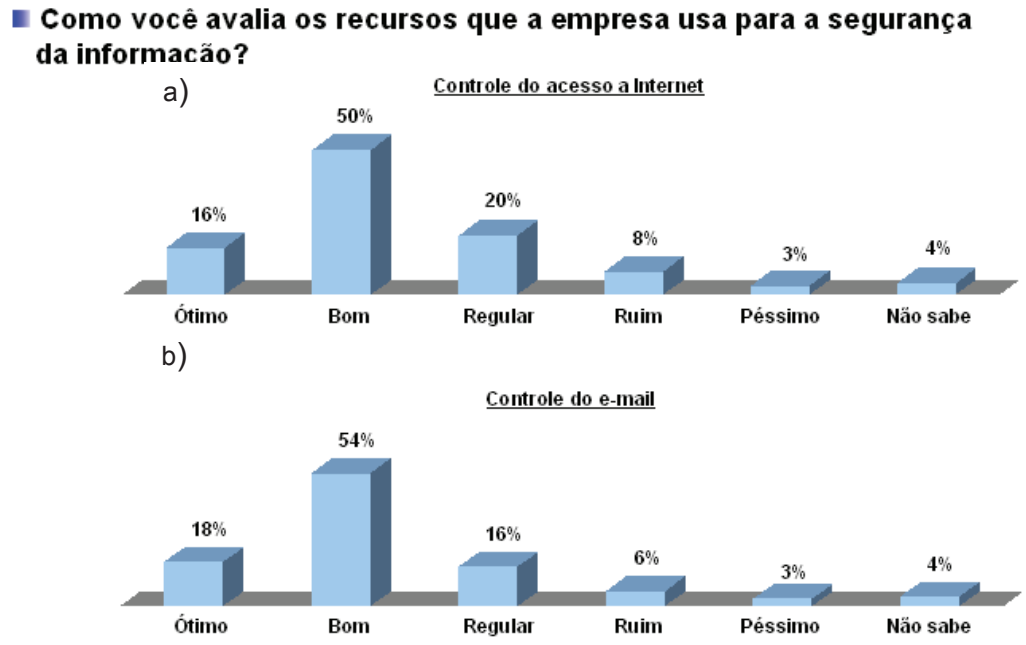


Figura 16 – Ativo. Lucratividade. Imagem.

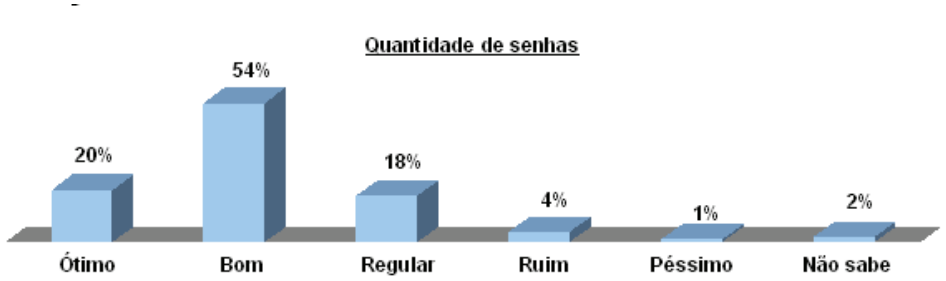
Nas Figuras a seguir, 17 e 18, são apontados indicadores de avaliação dos empregados sobre os itens de controle dos sistemas de tecnologia da informação (hardware e software) que suportam a gestão.

Na Figura 17, 66% consideram entre bom e ótimo o controle do acesso a Internet. No mesmo quadro, 72% consideram entre bom e ótimo o controle do e-mail. Ainda na Figura 17, 74% avaliam como bom e ótimo a quantidade de senhas para acesso aos sistemas corporativos, enquanto que 78% avaliam entre bom e ótimo o controle de acesso a Intranet.

Reveste-se da maior importância as considerações da Figura 18, onde os respondentes consideram os controles utilizados pela Organização para proteção dos seus ativos tangíveis e intangíveis, de fundamentais a importantes (99%).



c)



d)

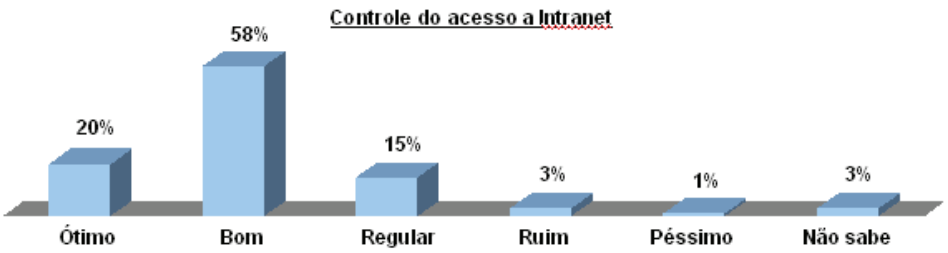


Figura 17 – Novos procedimentos.
a) Controle de acesso a Internet. b) Controle do e-mail. c) Quantidade (número) de senhas; d) Controle do acesso a intranet.

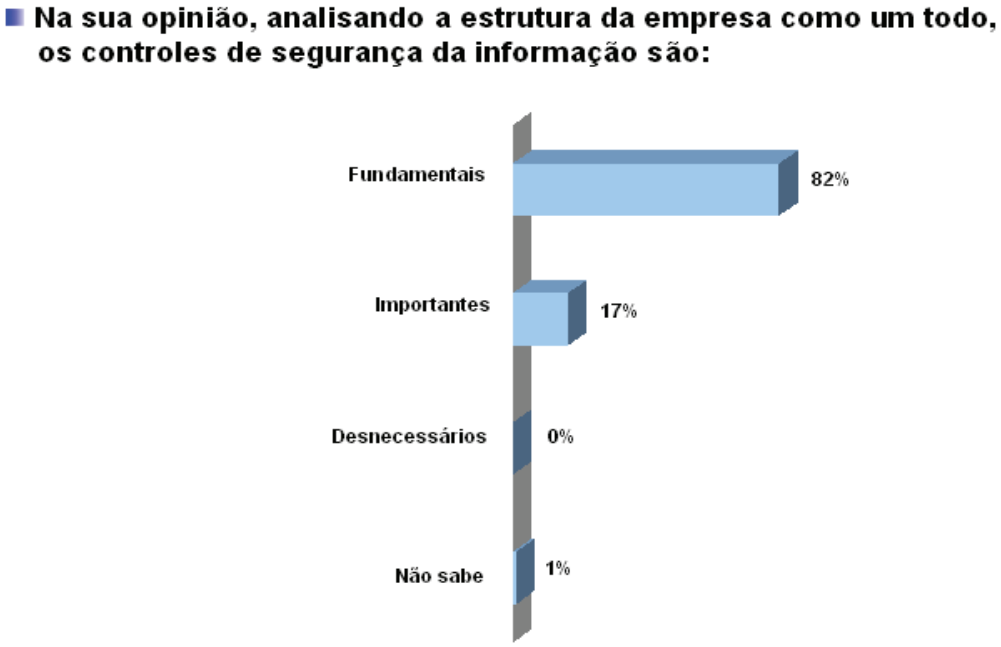


Figura 18 – Percepção dos controles.

10. ANÁLISE COMPARATIVA

O Quadro 15 sintetiza os resultados obtidos, onde se pode observar, a partir da análise comparativa entre cada empresa e a amostra pesquisada, a ocorrência dos Pontos Fortes e Pontos Fracos nas diferentes organizações, indicando que ainda há pontos de melhoria a serem observados pelas empresas para alcançarem um nível satisfatório de implementação de sistemas de gestão de segurança da informação.

Quadro 15 – Síntese dos resultados obtidos

GERAL %	PETROBRAS %	CST %	SAMARCO %	CRITÉRIOS DE ANÁLISE
78	82	57	85	Entendimento sobre segurança da informação
93 88 47 82 48 82	87 80 48 90 33 85	100 99 59 95 74 79	100 100 36 56 61 76	Sobre política de segurança: • Tem conhecimento • Considera boa • Controles são adequados • Continuidade da política • Compatibilidade entre o dia-a-dia e novos procedimentos • Restrição a livre circulação
71 21	66 24	78 14	76 21	Sobre difusão dos novos procedimentos: • Campanhas educativas • Aprendizado pelo erro
83	82	86	84	Sobre Planejamento estratégico: • Importância da segurança da informação para atingir metas preconizadas
79 89 80	76 92 85	72 92 77	92 81 70	Sobre conceito de bem econômico. • Entendimento da informação como bem econômico. • Garante continuidade negócio • Aumenta valor de mercado
68 77 95	59 79 96	53 81 95	99 65 93	Sobre informação como ativo da organização, • Entendimento da informação como Ativo • Aumenta lucratividade • Preserva a imagem da empresa
50 54 54 58	41 44 56 52	41 47 53 48	73 83 51 81	Sobre recursos utilizados para controle: • Considera Bom o controle de acesso p/ a Internet • Considera Bom o controle de e-mail • Considera Boa a quantidade de senhas • Considera Bom o controle de acesso p/ a Intranet
82	85	88	71	Consideram os controles fundamentais

Analisando o Quadro 15, constata-se que:

1. A Petrobras distingue-se da média geral no item referente à compatibilidade entre a rotina operacional do dia-a-dia e os novos procedimentos da política de segurança da informação (Ponto Fraco). No Quadro 30, observa-se um percentual elevado de usuários ainda não identificados com os padrões de controle (36%), haja vista a concordância com a afirmativa de que a realidade do dia-a-dia é diferente do que preconiza a política de segurança. Em comparação com a média geral, a posição da Petrobras está 4% acima, confirmando-se a necessidade dos gestores efetuarem um trabalho de esclarecimento.

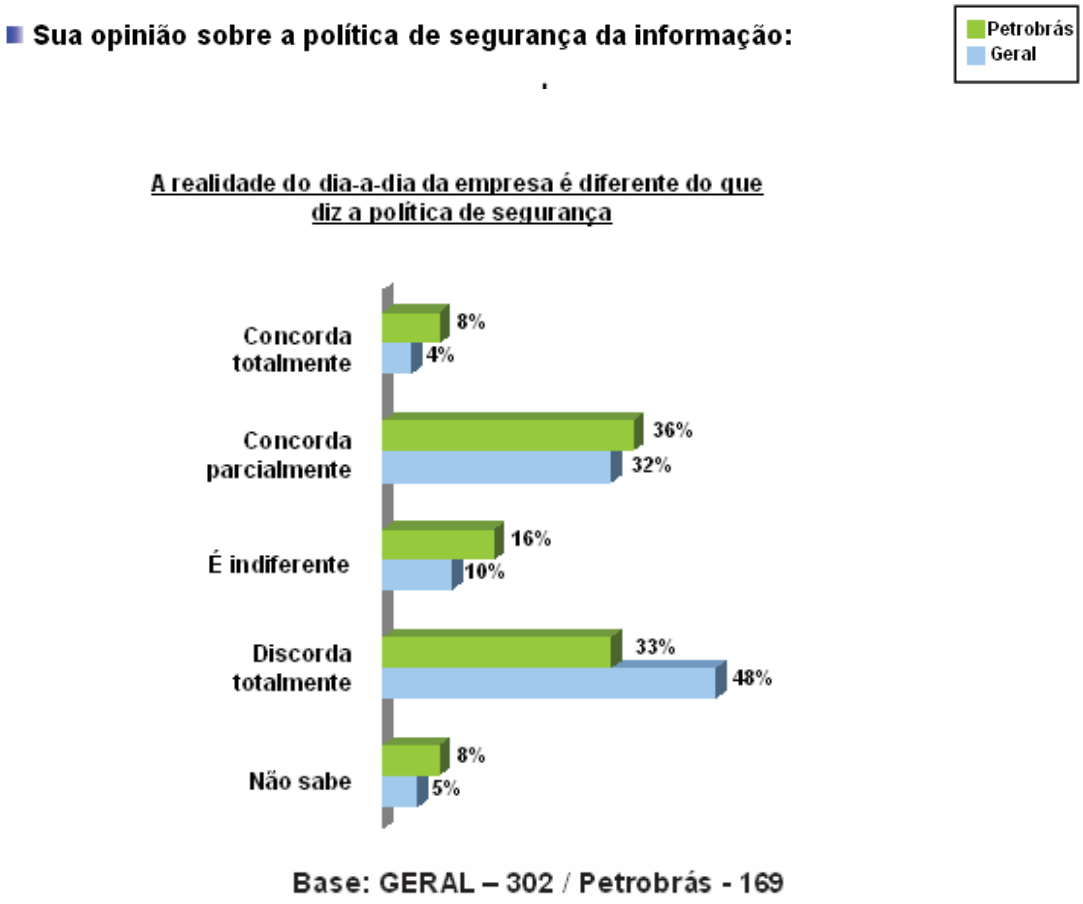


Figura 19 – Circulação da informação.

2. A CST distingue-se da média geral no que se refere ao entendimento sobre TI (Ponto Fraco) e à compatibilidade entre o dia-a-dia e novos procedimentos (Ponto Forte)

Observa-se na Figura 20, que somente 57% dos empregados da CST possuem percepção adequada do conceito de segurança da informação, enquanto que 35% necessitam de melhor compreensão. Considerando que o entendimento do conceito é de vital importância para a disseminação das práticas, para os gestores é de alta importância orientarem os esforços para este fim, sobretudo porque o site está se preparando para a obtenção da Certificação pela Norma inglesa BS – 7799. Este é um ponto fraco que merece ser cuidado.

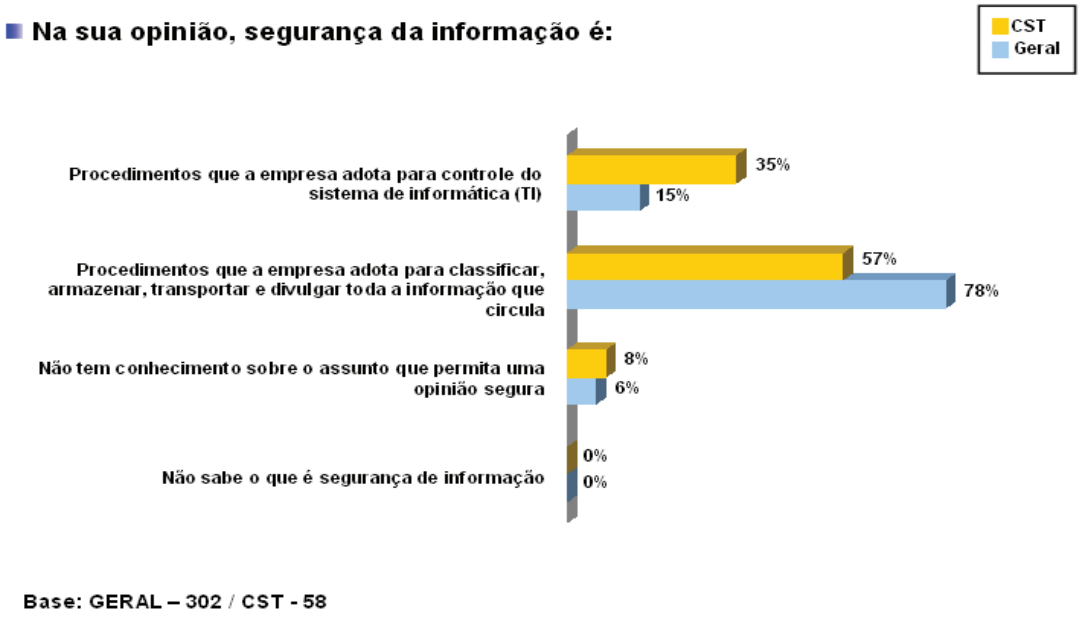


Figura 20 – Segurança da informação

Observa-se na Figura 21, a existência de coerência entre os padrões que estão sendo implantados e a rotina operacional expressa pelo percentual atingido (74%) que está bem acima da média geral dos sites pesquisados (48%). Este é um

ponto forte da organização e demonstra que o trabalho de disseminação dos conceitos está sendo incorporado na rotina da CST.

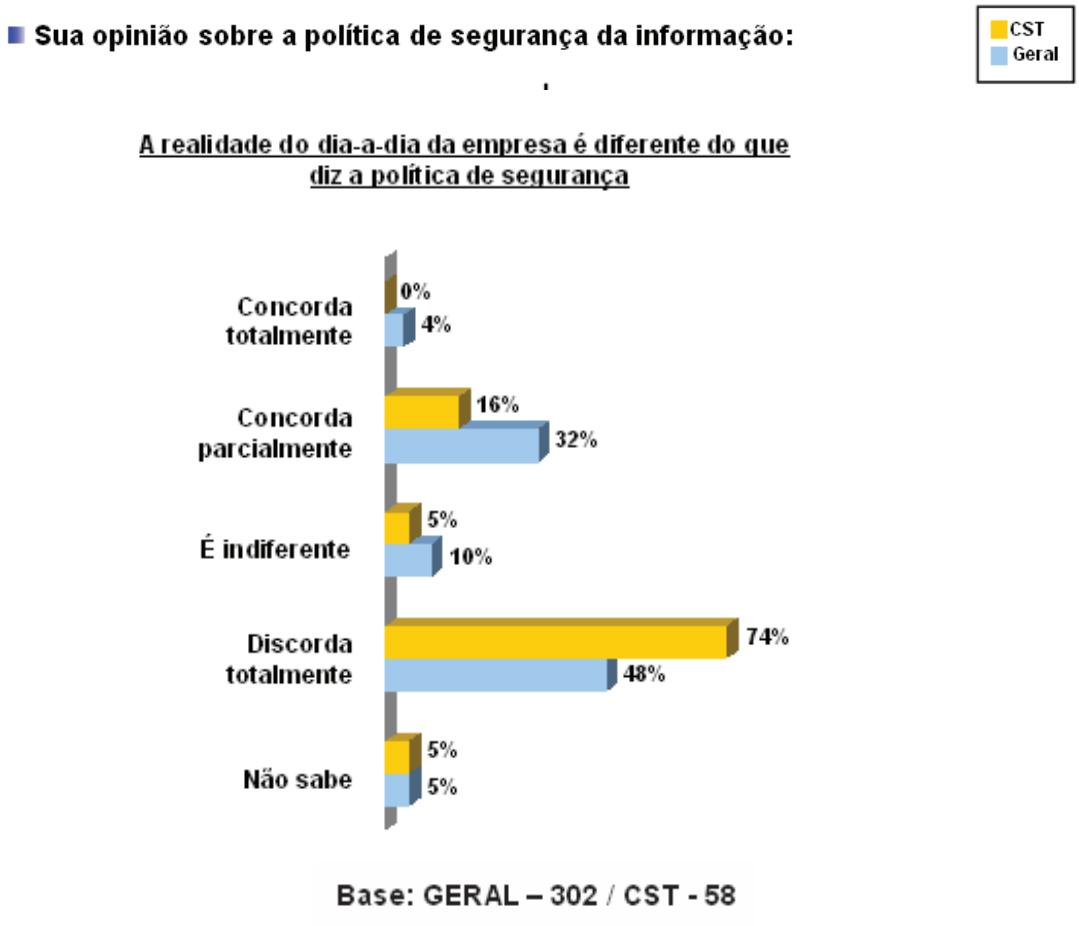


Figura 21 – Circulação da informação.

3. A SAMARCO distingue-se da média geral no que se refere à continuidade da política de segurança (Ponto Fraco), ao entendimento da informação como ativo organizacional e aos recursos utilizados para o controle da informação (Pontos Fortes).

Na figura abaixo, 23% dos entrevistados concordam que as movimentações em torno da segurança da informação são modismos. Este é um percentual alto, para o atual estágio de conformidade da empresa com a BS-7799, abrangidos pelo entendimento da não continuidade dos padrões estabelecidos pela Norma, o que amplia as preocupações dos gestores, haja vista estar se referenciando um site certificado. Observa-se que apenas 56% dos entrevistados discordam que a segurança da informação é um modismo (Ponto Fraco)

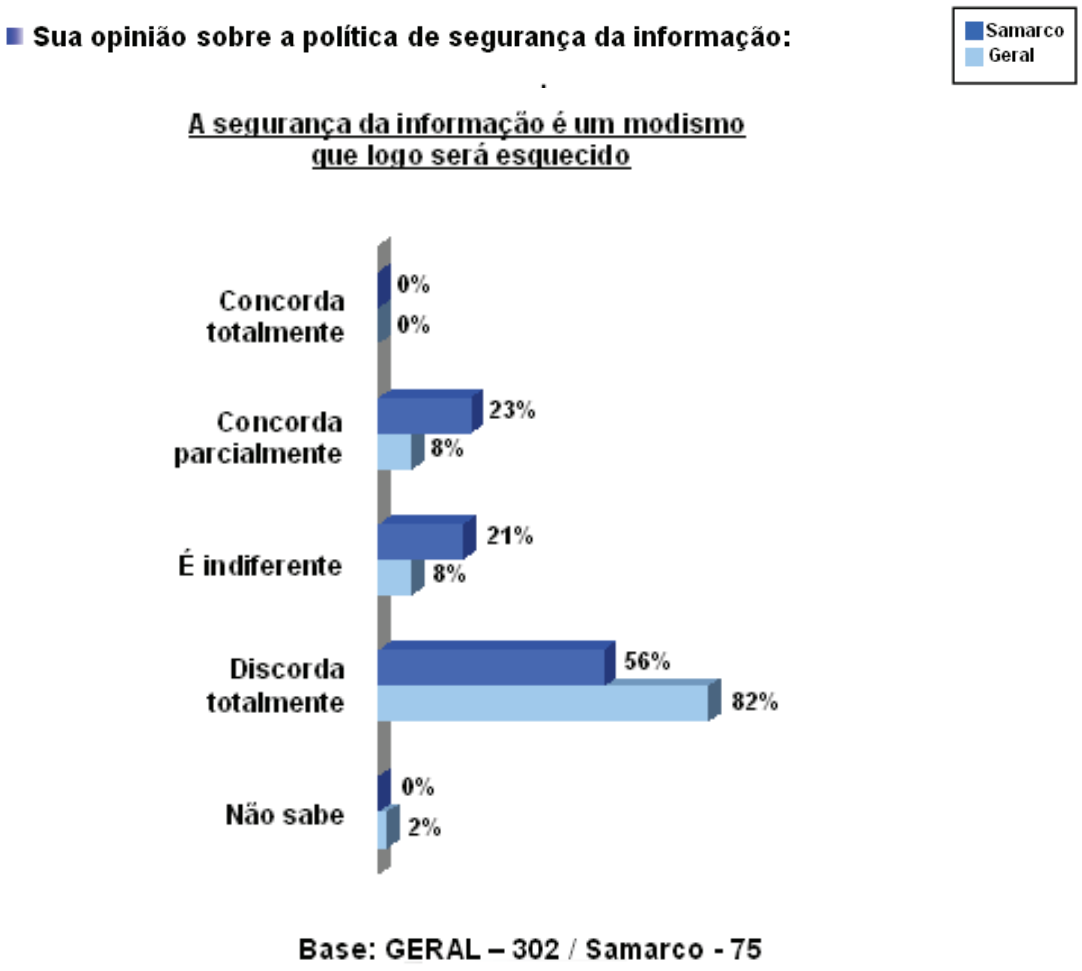


Figura 22 – Segurança da informação.

A análise da Figura 23 fornece um dado com perfil de empresa certificada pela Norma BS-7799, destacando-se das demais pelo quase absoluto entendimento do conceito de ativo (99%). O seu valor é ampliado pela importância estratégica que

representa para a alta administração o perfeito entendimento deste conceito. Este, portanto é um ponto forte observado.

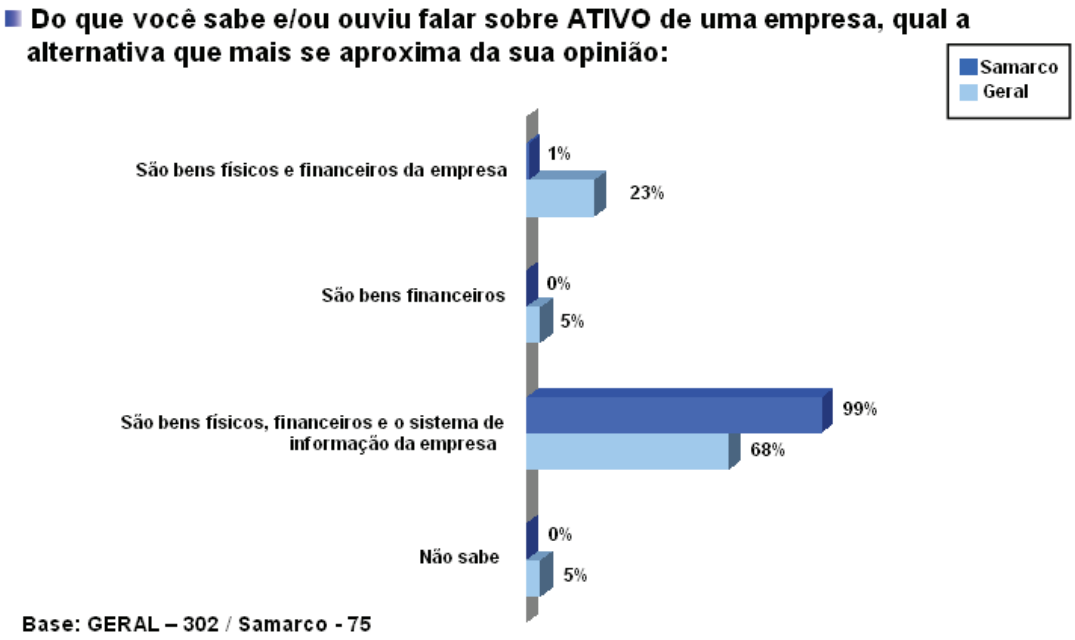


Figura 23 – Ativo. Conceito.

Na Figura 24, destacam-se os percentuais elevados de aceitabilidade dos recursos utilizados para o controle da segurança da informação, constituindo-se em Pontos Fortes da organização. Entende-se que a aceitabilidade poderá estar indicando que a cultura de segurança da informação já é uma realidade incorporada na rotina operacional.

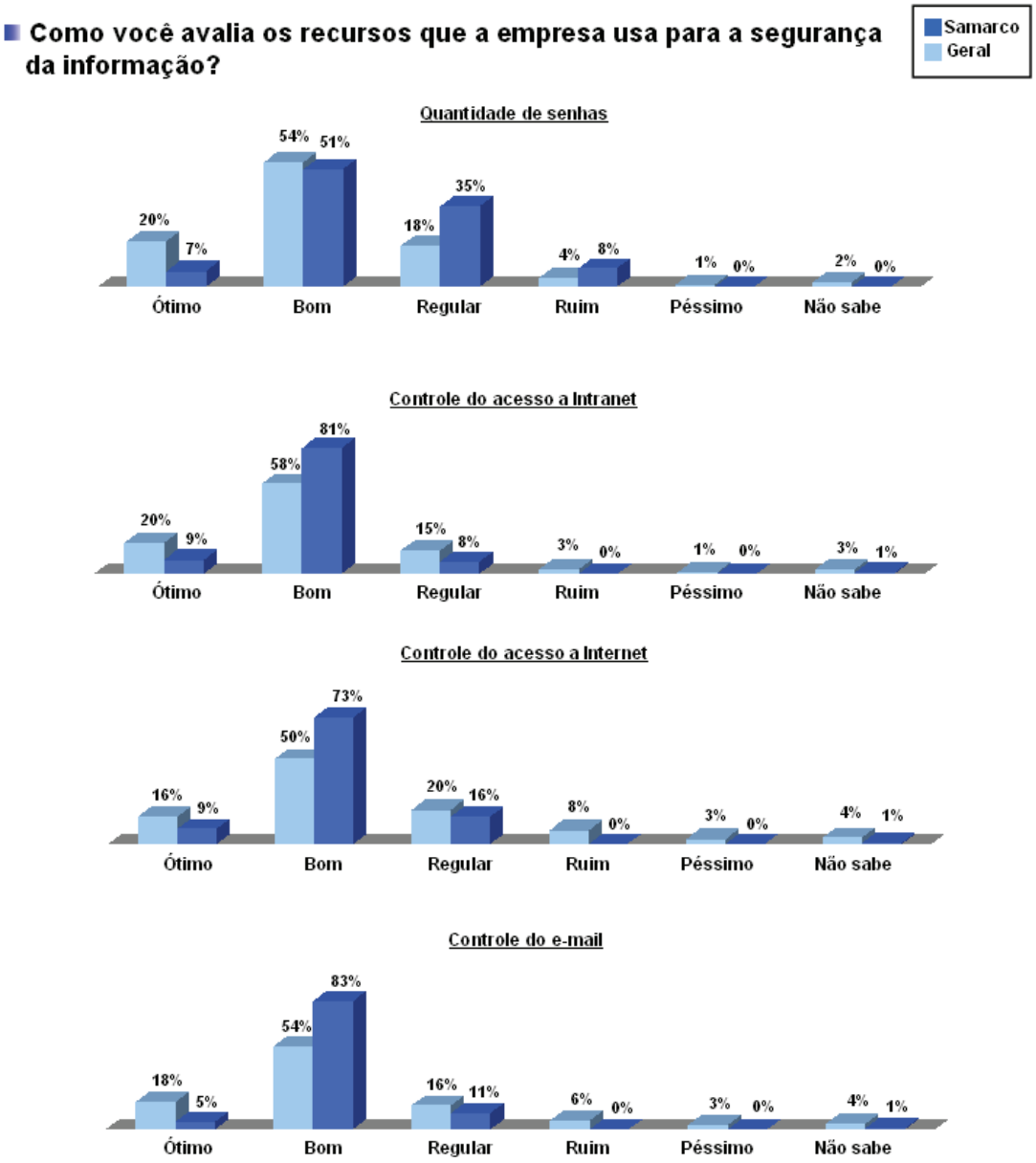


Figura 24 – Recursos utilizados

11. CONCLUSÃO

Este trabalho teve por objetivo identificar a percepção dos empregados de três organizações no Brasil a respeito do tema segurança da informação.

Para alcançar este objetivo, buscou-se conhecer as reações aos novos procedimentos de segurança e controle, as opiniões dos empregados sobre a relação entre o princípio da livre circulação da informação e a restrição pelos procedimentos de segurança, a existência de coerência entre momento de crise e aprendizado, as evidências de inserção do sistema de segurança da informação no Planejamento estratégico, a compreensão da informação como bem econômico e a compreensão da informação como ativo organizacional.

Os resultados gerais obtidos por intermédio da pesquisa indicam que:

- O conceito de segurança da informação já é adotado nas organizações estudadas;
- A política de segurança da informação é conhecida pelos empregados das organizações que a adotam;
- As campanhas promocionais são os veículos mais eficazes na disseminação de conceitos;
- A segurança da informação é compreendida como fator importante para a realização do Planejamento estratégico;
- A informação é compreendida como Ativo Organizacional e Bem Econômico;
- Os recursos utilizados pelas empresas para o controle da segurança da informação são bem aceitos pelos empregados;
- Os controles de segurança da informação são percebidos pelos empregados como fundamentais para a segurança da informação.

Entretanto, na comparação dos dados gerais com os dados específicos, tornam identificados alguns Pontos Fortes e Pontos Fracos que merecem a atenção dos gestores.

Um percentual pouco expressivo de entrevistados da Petrobras que vêem compatibilidade entre o dia-a-dia e novos procedimentos, e isto nos leva a recomendar a necessidade de se empreender esforços para adequação da rotina

aos procedimentos de segurança. Por exemplo, a promoção de campanhas educativas e a implementação de auditorias comportamentais.

O conceito de segurança da informação na CST não está bem claro para a maioria dos entrevistados, recomendando-se também a promoção de campanhas educativas com ênfase no conceito.

Observa-se que a continuidade da política de segurança ainda não é uma crença na Samarco, recomendando-se trabalho promocional por diferentes mídias e o envolvimento dos gestores em todas as fases das mobilizações, ainda mais por estar se referenciando a um *site* certificado.

A prática das rotinas baseadas nos procedimentos de segurança da informação, já pertence aos costumes corporativos da CST, recomendando-se periódicas análises críticas para reforço dessa posição.

O entendimento da informação como ativo da organização na Samarco é um dado com perfil de empresa certificada, tendo o seu valor ampliado pela importância estratégica que representa para a alta administração.

Os percentuais observados de aceitabilidade dos recursos utilizados para o controle da segurança da informação na Samarco, destacam-se em relação à média das empresas estudadas, recomendando-se, contudo, que alternativas tecnológicas sejam utilizadas para a redução da quantidade de senhas.

Finalmente, espera-se que este trabalho contribua para que:

- Os cursos de graduação em Administração de Empresas adotem as disciplinas Inteligência Competitiva e Segurança da Informação, a primeira abordando técnicas para a coleta de informação no mercado e desenvolvimento de barreiras contra a concorrência e a segunda voltada para o desenvolvimento nas Organizações de uma cultura de proteção do conhecimento, preocupada com a garantia da informação - nos seus aspectos de confidencialidade, integridade, disponibilidade - e com a construção de redes de relacionamentos, em processo conhecido como engenharia social que tem implicações na mudança da atitude, da postura e dos hábitos das pessoas e da empresa, a fim de que a nova geração de administradores esteja mais bem preparada para perceber o dinamismo avassalador da Nova Economia.
- As organizações, que são grandes compradoras no mercado interno, difundam o conceito de Segurança da Informação junto aos fornecedores

de bens e serviços, no sentido de contribuir para que estes internalizem os postulados dessa nova era. Esta será uma condição imperativa, pois de nada significará o fortalecimento da corrente de proteção intramuros, quando seus fornecedores, na maioria das vezes, por desconhecimento, enfraquecem esta corrente. A extensão desses cuidados à família é também pressuposto básico para a responsabilidade social, uma vez que o adolescente de hoje será o executivo de amanhã. O usuário da tecnologia da informação doméstico de hoje, será o usuário corporativo de amanhã.

GLOSSÁRIO

1. Browser. Programa usado para visualizar página na Internet.
2. Business-to-business. Transações eletrônicas entre empresas.
3. Business-to-consumer. Transações eletrônicas entre empresas e consumidor.
4. Business-to-government. Transações eletrônicas envolvendo o mercado e área governamental.
5. Cracker. Invasor de sistemas com o objetivo de roubar, destruir ou se beneficiar das informações subtraídas.
6. Cookies. Arquivo que grava no HD o endereço das conexões feitas pela Internet.
7. E-comerce. Comércio eletrônico.
8. Engenharia social. Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.
9. E-procurement. Transação eletrônica destinada à obtenção ou venda de bens e serviços.
10. ERP – Enterprise Resource Planning. Sistema integrado de gestão que organiza todos os processos da empresa, possibilitando velocidade na tomada de decisão nos negócios. Fornece em tempo real a fotografia da organização permitindo bases mais consistentes em simulações para fins de Planejamento estratégico
11. Firewall. Sistema ou grupo de sistemas através do qual flui o tráfego de dados entre duas redes distintas de computadores, permitindo que se implemente uma política de segurança que determine o que pode ou não pode passar de uma rede para outra.
12. Hacker. Invasor de sistemas com objetivo de testar a própria capacidade. Não se apropriam das informações.
13. Hosts. Local onde se hospeda o banco de dados. Servidor.
14. HTML – Hypertext Markup Language.
15. HTTP – Hypertext Transfer Protocol.

16. MarketPlace. Mercado eletrônico, onde elementos da cadeia produtiva, como fornecedores, parceiros, clientes e governo passam a interagir também eletronicamente, integrando e compartilhando suas bases de conhecimento.
17. NCP - Network Control Protocol. Sistema de comutação de pacotes onde os dados a serem comunicados são divididos em pequenas partes e estas são identificadas de modo a mostrar de onde vieram e para onde devem ir. Analogamente como o endereçamento postal
18. Phreaker. Piratas eletrônicos que utilizam o telefone para ataques a provedores fora do País de origem para que não sejam identificados.
19. Scanner. Programa que verifica portas abertas em determinadas máquinas com o intuito de direcionar ataques.
20. Sniffer. Ação de capturar informações destinadas à outra máquina.
21. Spam. Termo usado para se referir a e-mails são solicitados, que geralmente são enviados para um grande número de pessoas.
22. Trojan Horse. Programa que além de executar funções para as quais foi aparentemente projetado. Também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.
23. Vírus. Programa de computador que pode infectar outro programa de computador através da modificação dele, de forma a incluir uma cópia de si mesmo. A denominação vem de uma analogia com o vírus biológico, que transforma a célula numa fábrica de cópias dele.
24. Wireless. Tecnologia que permite a conexão entre computadores e redes através da transmissão e recepção de sinais de rádio.
25. WWW - World Wide Web.

REFERÊNCIAS

ABIN – Agência Brasileira de Inteligência. **Programa Nacional de Proteção ao Conhecimento.** Disponível em www.abin.gov.br. Acesso em 2004

ABRAIC – Associação Brasileira dos Analistas de Inteligência Competitiva. **Workshop Brasileiro de Inteligência Competitiva e Gestão do Conhecimento**. Brasília. 10/2004.

BRASIL. **Lei nº 7.647,** de 18 de dezembro de 1987, que dispõe sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no País e dá outras providências. Diário Oficial [da República Federal do Brasil]

_____. **Projeto Lei 1.713/1996,** de 27 de março de 1996, que dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores e dá outras providências. Proposições. Câmara dos Deputados.

_____. **Projeto Lei 84/1999,** de 24 de fevereiro de 1999, que dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Proposições. Câmara dos Deputados.

_____. **Projeto Lei 3.016/2000,** de 16 de maio de 2000, que dispõe sobre o registro de transações de acesso a redes de computadores destinados ao uso público, inclusive a Internet. Proposições. Câmara dos Deputados.

_____. **Projeto lei 2.000,** de 27 de março de 2000, que tipifica os delitos informáticos. Subsecretaria de informações. Senado Federal.

_____. **Lei nº 9.296,** Art. 10, de 24 de julho de 1996. Constitui crime realizar interceptação de comunicações telefônicas, de informática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa. Diário Oficial [da República Federal do Brasil]

_____. **Lei nº 9.983,** Art. 313-A, de 14 de julho de 2000. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano. Pena: reclusão, de dois a doze anos, e multa. Diário Oficial [da República Federal do Brasil]

_____. **Lei nº 10.764,** Art. 241, de 12 de novembro de 2003. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo exPlícito envolvendo criança ou adolescente. Pena: reclusão de dois a seis anos, e multa. Diário Oficial. [da República Federal do Brasil]

CARVALHEIRA, Jorge R. **Os princípios essenciais da Basiléia**. A versão original em inglês encontra-se disponível em http://www.bis.org. Acesso em 2004.

CBCE – Câmara Brasileira de Comércio Eletrônico. **Institucional.** Disponível em www.camara.e-net.com.br. Acesso em 2004.

COHEN, David. **Pequenos, mas sabidos**. Revista Exame, ano 38, n.23, p.119, nov.2004.

FINEP. **Automação e conforto, segurança e economia**. Disponível em www.finep.gov.br. Acesso em 2004.

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

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. São Paulo: Atlas, 1987.

GIL, Antonio de Loureiro. **Segurança em Informática**. São Paulo: Atlas, 1994.

GOMES, Elizabeth. **Capitais do conhecimento**. Disponível na Universidade Petrobras. Acesso em 2004.

GOMES, Ricardo Reis. **Monografia**. Curso de Direito. Universidade de Brasília. 2001.

KELLY, Kevin. **Entrevista**. Disponível em www.janelaweb.com. Acesso em 2004.

LATERI, Ana Celina. **Pesquisa.** Gerenciamento de Risco. Brasiliano & Associados. 2003.

MARINHO, Zilda Penna. **Pesquisa.** A segurança da informação e o cidadão. Disponível em www.modulo.com.br. Acesso em 2003.

MELO, Renata Homem de, SIMON, Renata Cruz, **SARBANES-OXLEY ACT: Aspectos da nova lei contra fraude corporativa norte-americana.** Disponível em www.societario.com.br. Acesso em 2004

MODULO SECURITY. **9ª Pesquisa Nacional de Segurança da Informação**. 2003.

NBR ISO/IEC 17799 – **Código de Prática para a Gestão da Segurança da Informação.** Associação Brasileira de Normas Técnicas – ABNT disponibiliza para aquisição, através do seu site www.abnt.gov.br. Acesso em 2005.

ORWELL, George. **1984.** 29 ed. Editora Nacional. 2003

PECK, Patrícia. **O seguro para a proteção de ativos intangíveis**. Disponível em www.modulo.com.br/comum. Acesso em 08/2004.

PLATT, Washington. **A produção de informações estratégicas**; tradução de Álvaro Galvão Pereira e Heitor Aquino Ferreira. Rio de Janeiro: Biblioteca do Exército, 1974.

POOLE, Patrick S. **ECHELON: America's Secret Global Surveillance Network.** Copyright 1999/2000. Disponível em http://fly.hiwaay.net/~pspoole/echelon.html . Acesso em 2004.

PORTER, Michael E. **Estratégia competitiva**: Técnicas para análise de indústrias e da concorrência; tradução de Elizabeth Maria de Pinho Braga. 7 ed. Rio de Janeiro: Campus, 1986.

PURPURA, Philip P., **Security and loss prevention:** an introduction. Butterworth-Heinemann. 3d ed. Woburn,MA. 1998.

REBITTE, L. Manual ComPleto do Hacker. Rio de Janeiro. Book Expresse. 2000

REIS, Ruth. **Opinião**. Jornal A GAZETA. Espírito Santo. Tiragem 08/08/2004.

SANTOS, Neri dos. **Inteligência Competitiva**. Núcleo de Pós-graduação em Engenharia da Produção. Universidade Federal de Santa Catarina. 2000.

TOFFLER, Alvin. **Powershift**: as mudanças do poder. 6 ed. Rio de Janeiro: Record, 2003.

www.petrobras.com.br

www.cst.com.br

www.samarco.com.br

BIBLIOGRAFIA

ALAVATE, William. **2004 - O ano da recuperação de desastres.** Disponível em www.modulo.com.br/comum. Acesso em 01/2004.

ANCHIESCHI, Olavo José Gomes. **Segurança Total**. São Paulo: Makron Books, 2000.

BAZERMAN, Max H. **Processo decisório**: para cursos de administração e economia; tradução de Arlete Simille Marques. Rio de Janeiro: Elsevier, 2004.

BEAL, Adriana. **Gestão da segurança da informação**. Disponível em www.modulo.com.br/comum. Acesso em 06/2004.

BIZZOCCHI, Aldo. **Anatomia da cultura**: uma nova visão sobre ciência, arte, religião, esporte e técnica. São Paulo: Palas Athena, 2003.

BLUM, Renato Opice. Disponível em www.opiceblum.com.br. Acesso em 2004.

BOGO, Kellen Cristina. **A História da Internet** – Como Tudo Começou. Disponível em www.kPlus.cosmo.com.br/matéria. Acesso em 2004.

BORGES, André. Segurança com qualidade total. Disponível em www.csoline.com.br. Acesso em 2004.

CONTI, Fátima. **História da Internet**. Disponível em www.cultura.ufpa.br. Acesso em 2004.

DELGADO, Silvia. **Biometria:** os olhos são mesmo o espelho da alma. Disponível em www.e-security.blogspot.com. Acesso em 2004.

DRUCKER, Peter F. Foundation. **A organização do futuro**: como preparar hoje as empresas de amanhã; tradução Nota Assessoria. São Paulo: Futura, 1997.

ECO, Humberto. **Como se faz uma tese**. 14 ed. São Paulo: Editora Perspectiva, 1998.

FLEURY, Maria Teresa Leme. **Cultura e Poder nas Organizações**. 2 ed. São Paulo: Atlas, 1996.

FONTES, Edison Luiz Gonçalves. **Vivendo a segurança da informação**: orientações práticas para as organizações. São Paulo: Sicurezza: Brasiliano & Associados, 2000.

HAICAL, Cristiane. **Entrevista:** as mudanças no cotidiano das empresas e dos gestores. Disponível em www.modulo.com.br/comum. Acesso em 01/2004.

HANDY, Charles B. **Como compreender as organizações**. Tradução de Helena Maria Camacho Martins Pereira. Rio de Janeiro: Zahar Editores S.A., 1978.

KUMAR, Krishan. **Da sociedade pós-industrial à pós-moderna**: novas teorias sobre o mundo contemporâneo; tradução Ruy Jungmann. Rio de Janeiro: Jorge Zahar Ed., 1997.

KEY, Wilson Bryan. **A Era da Manipulação**. São Paulo: Ed. Página Aberta, 1993.

LEVIN, Jack. **Estatística aPlicada a ciências humanas**; tradução e adaptação de Sergio Francisco Costa. 2 ed. São Paulo: editora Harbra ltda, 1987.

LOES, Cláudio. **Segurança e os conceitos da nova economia**. Disponível em www.scua.com.br. Acesso em 2003.

LOPES JUNIOR, Rubens. **Segurança eletrônica**: proteção ativa / Rubens Lopes Junior, Marcelo B. de Souza. São Paulo: Sicurezza:Brasiliano&Associados, 2000.

LUCKESI, Cipriano Carlos. **Introdução à filosofia**: aprendendo a pensar / Cipriano Carlos Luckesi, Elisete Silva Passos. 2 ed. São Paulo: Cortez, 1996.

MOURA, Maria Teresa e MALINCONICO. **Considerações para a elaboração de uma política de segurança.** Disponível em www.modulo.com.br/comum. Acesso em 12/2003.

NERO, Rubens Del. **Fundamentos da segurança patrimonial**. São Paulo: Planaudis, 1980.

NERY, Fernando. **Por que proteger as informações?** Disponível em www.modulo.com.br/comum. Acesso em 06/2004.

NETO, Cláudio de Lucena. **Segurança da informação corporativa**: aspectos e imPlicações jurídicas. Disponível em www.jus.com.br. Acesso em 2004.

NÓBREGA, Clemente. **O glorioso acidente**. São Paulo: Editora Objetiva, 1998.

OLIVEIRA, Salomão de. **Agentes digitais do crime.** Disponível em www.modulo.com.br/comum. Acesso em 07/2004.

PITASSI, Cláudio. **Tecnologia de informação e mudança**: uma abordagem crítica / Cláudio Pitassi e Sergio Proença Leitão. Revista de administração de empresas. Abr/Jun 2002.

RAMOS, F.F.**BS 7799-2: Certificar ou não certificar? Eis a questão**. Disponível em www.hackernews.com.br . Acesso em 05/2004

RIFKIN, Jeremy. **A economia do hidrogênio**. São Paulo: M. Books do Brasil Editora Ltda, 2003

ROCHA, Luís Fernando. **As conseqüências da ação dos spyware no ambiente corporativo.** Disponível em www.modulo.com.br/comum. Acesso em 05/2004.

_____. **Como os hábitos no ambiente de trabalho afetam a segurança corporativa**. Disponível em www.modulo.com.br/comum. Acesso em 05/2004.

_____. **CSO 2004:** O que o security officer precisa saber sobre as leis. Disponível em www.modulo.com.br/comum. Acesso em 01/2004.

_____. **CSO 2004:** certificando a segurança de sua empresa – parte 1. Disponível em www.modulo.com.br/comum. Acesso em 07/2004.

_____. **Leis e normas**: o aumento da responsabilidade legal na gestão dos riscos. Disponível em www.modulo.com.br/comum. Acesso em 06/2004

_____. **Perspectiva 2004** – part 1 e part 2. Disponível em www.modulo.com.br/comum. Acesso em 01/2004.

_____. **PL 84/89**. Disponível em www.modulo.com.br/comum. Acesso em 03/2004.

ROCHA, Pedro Paulo. **A eletrônica na sua segurança**. Rio de Janeiro: Antenna Edições, 1987.

RUDIO, Franz Vitor. **Introdução ao projeto de pesquisa científica**. Petrópolis: Vozes, 1992.

SÊMOLA, Marcos. **Gestão da segurança da informação**: visão executiva da segurança da informação. Rio de Janeiro: Campus, 2003.

SODRÉ, Nelson Werneck. **Síntese de história da cultura brasileira**. 20 ed. Rio de Janeiro: Bertrand Brasil, 2003.

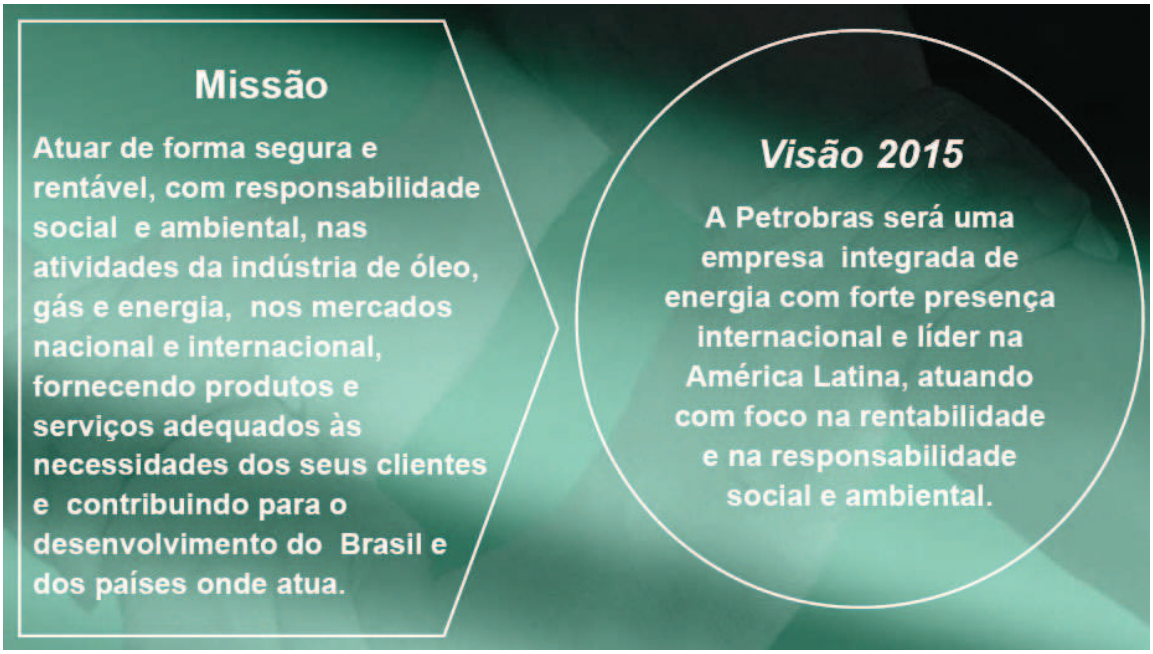
STARLIN, Gorki. **Manual ComPleto do Hacker**. Copyright 2000 Book Express Publisher.

VIEIRA, Marcelo Milano Falcão e ZOUAIN, Deborah Moraes. **Organizadores. Pesquisa Qualitativa em Administração**. Rio de Janeiro: Editora FGV, 2004

VIVEIROS, Ricardo. **As TI e a nova economia**. Disponível em www.bit.pt/revista. Acesso em 2004.

ANEXO A

PERFIL DAS EMPRESAS



A PETROBRAS apurou um lucro líquido consolidado de R$ 4.566 milhões no quarto trimestre de 2004 (4T-2004). No exercício de 2004, a PETROBRAS obteve um lucro líquido consolidado de R$ 17.861 milhões. A receita operacional líquida consolidada, no 4T-2004, atingiu o montante de R$ 28.692 milhões e no exercício de 2004 correspondeu a R$ 108.202 milhões. O valor de mercado da Companhia alcançou R$ 112.458 milhões, em 31 de dezembro de 2004, sendo 29% maior do que o alcançado no exercício anterior.

Demonstração Consolidada do Resultado por Área de Negócio

RESULTADO POR ÁREA DE NEGÓCIO R$ milhões [1]

4º TRIMESTRE					JAN-DEZ		
3T-2004 [4]	2004	2003 [3] [4]	Δ %		2004	2003 [3] [4]	Δ %
5.728	4.506	2.727	65	EXPLORAÇÃO & PRODUÇÃO	18.083	14.826	22
274	838	947	(12)	ABASTECIMENTO	2.553	5.199	(51)
270	252	(710)	135	GÁS & ENERGIA	460	(1.259)	137
109	267	72	271	DISTRIBUIÇÃO	623	353	76
(34)	119	(50)	338	INTERNACIONAL [2]	347	746	(53)
(404)	(1.313)	(158)	731	CORPORATIVO	(3.677)	(1.657)	(122)
(455)	(103)	193	(153)	ELIMINAÇÕES E AJUSTES	(528)	(413)	(28)
5.488	4.566	3.021		LUCRO LÍQUIDO CONSOLIDADO	17.861	17.795	

>> Perfil



» Perfil

A história da Petrobras se confunde com a própria história do petróleo brasileiro. Uma empresa que inicia o século XXI enfrentando todos os desafios com muita eficiência.

A Petróleo Brasileiro S/A é:

- Uma companhia integrada que atua na exploração, produção, refino, comercialização e transporte de petróleo e seus derivados no Brasil e no exterior.
- Uma empresa de energia com enorme responsabilidade social e profundamente preocupada com a preservação do meio ambiente.
- Uma companhia que tem a sua trajetória de conquistas premiada por inúmeros recordes e pelo reconhecimento internacional.

Noventa e três plataformas de produção, mais de dez refinarias, quase dezesseis mil quilômetros em dutos e mais de sete mil postos de combustíveis. Por onde você passa há uma forte presença da Petrobras contribuindo para o desenvolvimento do Brasil.

Com sede na cidade do Rio de Janeiro, a Petrobras possui escritórios e gerências de administração em importantes cidades brasileiras como Salvador, Brasília e São Paulo. Devido a alta competitividade do novo cenário da indústria de energia, a Petrobras reposicionou-se em relação ao futuro, utilizando os mais modernos instrumentos de gestão.

Uma nova estrutura, forte e bem posicionada, está fazendo com que a empresa alcance suas metas estratégicas de expansão, internacionalização, rentabilidade e produtividade.

De acordo com o modelo de estrutura organizacional, a Companhia passa a funcionar com quatro áreas de negócio - E&P (Exploração e Produção), Abastecimento, Gás & Energia e Internacional -, duas de apoio - Financeira e Serviços - e as unidades corporativas ligadas diretamente ao presidente. Além de melhorar todo aspecto operacional e os resultados da empresa, a nova estrutura abre espaço para que os empregados desenvolvam seu potencial e se beneficiem do valor agregado ao negócio.

Além das atividades da holding, o Sistema Petrobras inclui subsidiárias - empresas independentes com diretorias próprias, interligadas à Sede.

A Petrobras desenvolve diversas atividades no exterior e mantém uma consistente atividade internacional, tal como: compra e venda de petróleo, tecnologias, equipamentos, materiais e serviços; acompanhamento do desenvolvimento da economia americana e européia; operação financeira com bancos e bolsa de valores; recrutamento de pessoal especializado; afretamento de navios; apoio em eventos internacionais, entre outros.

Além de estar presente em diversos países como Angola, Argentina, Bolívia, Colômbia, Estados Unidos, Nigéria, a Petrobras conta ainda com o apoio de seus escritórios no exterior como em Nova Iorque (ESNOR), e no Japão (ESJAP).

A presença nos principais eventos e fóruns internacionais torna-se muito importante na medida em que permite a Petrobras viabilizar ótimas oportunidades de negócios. O conhecimento do mercado e dos agentes que nele integram fazem com que as vantagens competitivas sejam transmitidas aos clientes de uma forma direta e objetiva.

Além disso, há o CENPES , o centro de pesquisas da Petrobras, que possui uma das mais avançadas tecnologias do mundo e é reconhecido internacionalmente pela sua grande competência.

>> Petrobras em Números



» Petrobras em Números

A Petrobras apresenta dados nas áreas de exploração, produção, abastecimento entre outras que dão orgulho ao nosso país. Abaixo você encontra alguns desses números. Na área Relações com o Investidor há outras informações relativas a Companhia.

Dados referentes ao ano de 2003

RECEITAS LÍQUIDAS (em bilhões de R$)
R$ 95,743

LUCRO LÍQUIDO (em bilhões de R$)
R$ 17,795

INVESTIMENTOS (em bilhões de R$)
R$ 18,485

INVESTIMENTOS (em bilhões de R$)
R$ 18,485

ACIONISTAS
131.577

EXPLORAÇÃO
35 sondas de perfuração (22 marítimas)

RESERVAS (CRITÉRIO SEC)
11,6 bilhões de barris de óleo e gás equivalente (boe)

POÇOS PRODUTORES
15.834 (838 marítimos)

PLATAFORMAS DE PRODUÇÃO
98 (68 fixas; 30 flutuantes)

PRODUÇÃO DIÁRIA
1,701 milhão bpd de óleo e LGN
53 milhões de m3 de gás natural

REFINARIAS
16

RENDIMENTO DAS REFINARIAS
1,709 milhão barris por dia - bpd

DUTOS
27.120 km

FROTA DE NAVIOS
97 (54 de propriedade da Petrobras)

POSTOS
5.074 Ativos (612 próprios)

FERTILIZANTES
5 Fábricas: 2.141 toneladas métricas de amônia e 2.437 toneladas métricas de uréia

>> Empresas do Grupo

» Empresas do Grupo

Além das atividades da holding, o Sistema Petrobras inclui subsidiárias - empresas independentes com diretorias próprias, interligadas à Sede. São elas:

- Petrobras Gás S.A - Gaspetro, subsidiária responsável pela comercialização do gás natural nacional e importado.
- Petrobras Química S.A - Petroquisa, que atua na indústria petroquímica;
- Petrobras Distribuidora S.A. - BR, na distribuição de derivados de petróleo;
- Petrobras Transporte S.A. - Transpetro, criada para executar as atividades de transporte marítimo e dutoviário da Companhia.
- Braspetro Oil Services Company - BRASOIL, que atua, principalmente, na prestação de serviços em todas as áreas da indústria do petróleo, bem como no comércio de petróleo e de seus derivados.
- Braspetro Oil Company - BOC, que atua na pesquisa, lavra, industrialização, comércio, transporte, armazenamento, importação e exportação de petróleo e de seus derivados.
- Petrobras International Braspetro B.V. - PIB, participa em sociedades que atuam em pesquisa, lavra, industrialização, comércio, transporte armazenamento, importação e exportação de petróleo e de seus derivados.
- Petrobras Comercializadora de Energia Ltda, que permite a atuação da Companhia nas novas atividades da indústria de energia elétrica no Brasil.
- Petrobras Negócios Eletrônicos S.A., participa no capital social de outras sociedades que tenham por objetivo atividades realizadas pela Internet ou meios eletrônicos.
- Petrobras International Finance Company – PIFCO, criada com o objetivo de facilitar a importação de óleo e produtos derivados de petróleo.
- Downstream Participações S.A, que facilita a permuta de ativos entre a Petrobras e a Repsol-YPF.

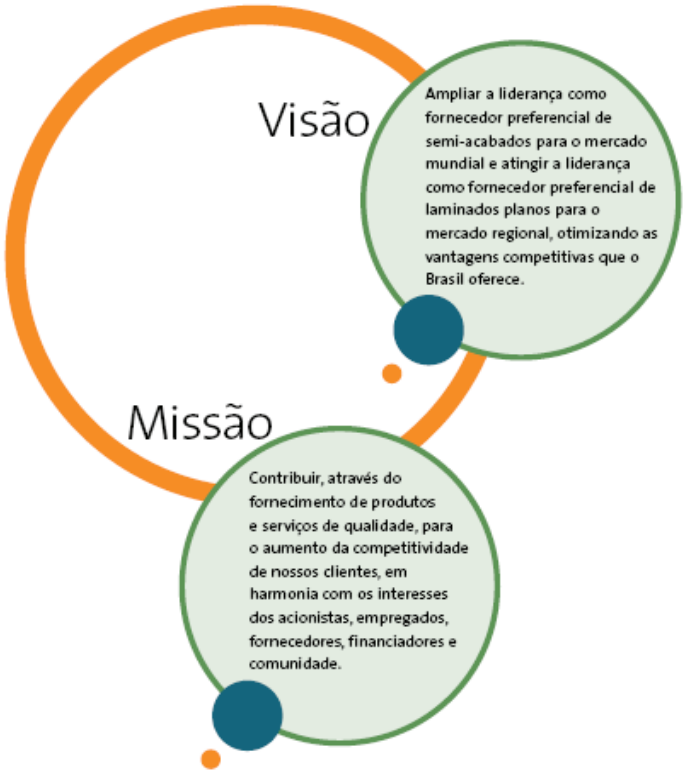
Estrategicamente localizada na região da Grande Vitória, Estado do Espírito Santo, no sudeste brasileiro, a **CST** possui uma área total de 13,5 milhões de m^2, sendo que a usina ocupa 7 milhões de m^2.

A **Companhia** é servida por uma bem aparelhada malha rodo-ferroviária: Estrada de Ferro Vitória-Minas e Ferrovia Centro - Atlântica (antiga Rede Ferroviária Federal) e Rodovias BRs - 101 / 262.

Também é ligada a um excelente complexo portuário dentre os mais eficientes do mundo, em que se destaca o porto de Praia Mole.

Essa infra-estrutura favorece o recebimento das principais matérias-primas e insumos - principalmente minério de ferro e carvão mineral - e facilita o escoamento dos produtos, sendo fornecida por um terminal para exportação de produtos siderúrgicos, com **capacidade para 5,8 Mt/ano**.

Brasil - Espírito Santo



Perfil da CST

A CST, inaugurada em 1983, é uma siderúrgica de renome internacional, especializada na produção de aço de alta qualidade, utilizado na fabricação de produtos presentes no dia-a-dia de milhões de pessoas.

Estrategicamente localizada na região metropolitana da Grande Vitória, no Estado do Espírito Santo, ocupa uma área, junto ao mar, de 7 milhões m2, parte de um terreno de 13,5 milhões m2. A completa infra-estrutura de que dispõe lhe proporciona condições privilegiadas, tato para a produção como para o abastecimento dos mercados interno e externo.

Desde sua privatização, em 1992, acumula investimentos superiores a US$ 2,1 milhões em atualização tecnológica, aumento da produção e enobrecimento do *mix* de produtos. Nesse período registrou algumas alterações na sua composição acionária, passando por fim a integrar o Grupo Arcelor – um dos maiores conglomerados siderúrgicos do mundo.

Em contínua evolução, atualmente produz placas e laminados a quente (bobinas) – produtos semi-acabados de aço – para o atendimento, mediante relações estruturadas de longo prazo, de uma carteira de clientes estrategicamente selecionados por segmentos industriais e regiões, no Brasil e no exterior.

Sua capacidade instalada de produção, por conta de uma nova expansão em andamento, passará de 7,5 milhões de toneladas/ano a partir de meados de 2006.

A sustentabilidade do negócio é assegurada na CST por um modelo de gestão que busca manter o equilíbrio entre as dimensões econômica, social e ambiental, em sintonia com os princípios do desenvolvimento sustentável.

SAMARCO

Perfil da Organização

A Samarco Mineração S.A, empresa de lavra, beneficiamento, transporte e pelotização de minério de ferro, é a segunda maior exportadora transoceânica de pelotas de minério de ferro destinadas aos processos siderúrgicos de alto-forno e de redução direta. Em 2003, a Samarco deteve 17% de participação no mercado mundial. Seu controle acionário é dividido entre a brasileira Companhia Vale do Rio Doce (50%) e a anglo-australiana BHP Billiton (50%), que figuram entre os três maiores grupos mineradores do mundo.

As operações de extração e beneficiamento do minério são realizadas na unidade de Germano, onde está a mina de Alegria (com reservas de 4 bilhões de toneladas), localizada nos municípios de Mariana e de Ouro Preto (MG). A planta de pelotização e o porto ficam na unidade de Ubu, situada em Anchieta (ES). Um mineroduto de 396km liga as duas unidades, transportando a polpa do minério concentrado para a pelotização.

A Samarco possui escritórios de vendas próprios em Amsterdã (Holanda), Hong Kong (China) e Belo Horizonte (Brasil). É por meio deles que a empresa comercializa sua produção que, em 2003, atingiu o número recorde de 15,2 milhões de toneladas de minério de ferro (pelotas e finos).

A totalidade da produção da Samarco é destinada ao mercado siderúrgico internacional. Em 2003, no entanto, uma pequena parcela da produção (1,3%) foi vendida no mercado interno.

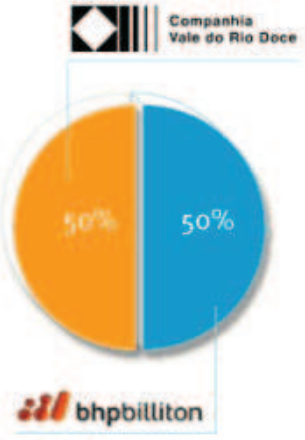
Desde o final da década de 1990, a Samarco vem ampliando a sua participação no mercado chinês, atualmente o maior mercado consumidor da empresa. Em 2003, a China respondeu por cerca de 37% do total de vendas da Samarco.

Estrutura global

A SAMARCO MINERAÇÃO S.A. é uma empresa de lavra, beneficiamento, pelotização e exportação de minério de ferro. Em 2002, foi a segunda maior exportadora de pelotas de minério de ferro no mercado transoceânico, comercializando 100% de seus produtos para mais de 15 países na Europa, Ásia, África/Oriente Médio e Américas.

Com sede e escritório central em Belo Horizonte (MG), a Samarco mantém unidades industriais em dois estados brasileiros: Minas Gerais, nos municípios de Mariana e Ouro Preto, onde se localiza a Unidade de Germano, de mineração e beneficiamento; e Espírito Santo, no município de Anchieta, onde está a Unidade de Ponta Ubu, que compreende a pelotização e o porto. O transporte do concentrado de minério de ferro entre Germano e Ponta Ubu é feito por um mineroduto de 396 km de extensão. A empresa também possui escritório na cidade de Vitória (ES) para operações de comércio exterior e câmbio, além de escritórios de vendas em Amsterdã e Hong Kong.

O controle acionário da Samarco pertence à Companhia Vale do Rio Doce (maior exportadora de minério de ferro do mundo) e à BHPBilliton (terceira maior produtora mundial de minério de ferro), cada uma detendo 50% das ações.



A SAMARCO é a primeira mineradora no mundo e a primeira empresa do setor industrial das Américas a ser certificada na norma inglesa de segurança da informação, BS 7799-2:2002.

NOTÍCIAS
SAMARCO

:: 29/11/2004

Informações Seguras: Samarco é certificada na norma de Segurança da Informação

A Samarco, segunda maior exportadora mundial de pelotas de minério de ferro, é a primeira mineradora no mundo e a primeira empresa do setor industrial das Américas a ser certificada na norma inglesa de segurança da informação, a BS 7799-2. Essa norma define um modelo de gestão para garantir a confidencialidade, a integridade e a disponibilidade das informações. No Brasil só existiam três empresas certificadas por essa norma, duas do setor financeiro e uma especializada em gestão de segurança da informação. A norma utiliza a ISO/IEC 17799:2000, um padrão internacional que consiste em um código das melhores práticas (best – practices) de segurança da informação nas organizações e onde também são sugeridos os controles a serem implementados para atingir este objetivo. Outro aspecto bastante positivo está relacionado à participação e envolvimento de todos os empregados na implementação da política de segurança da informação. Estatísticas mostram que falhas em segurança são em sua maioria devido ao comportamento das pessoas. Com isso, todos aqueles que têm acesso a informações se preocupam em agir de acordo com as normas implementadas e reportar os fatos que possam comprometer a segurança das informações da empresa. A Samarco está convicta que com a implementação desse modelo de gestão, a transparência e o alinhamento dos conceitos e práticas de segurança da informação pelos empregados e demais partes interessadas, contribuam para a sustentação do seu processo de geração de valor. A auditoria de certificação foi realizada no final do mês de outubro pelo órgão certificador norueguês Det Norske Veritas (DNV), o mesmo que conferiu as certificações ISO 9001, 14001 e OHSAS 18001 para a empresa.

APÊNDICE A

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PETROBRAS [1]

A Política de Segurança da Informação do Sistema Petrobras, está preconizada no padrão PB-PL-01-00002-0, aprovado pela Diretoria Executiva em 23/12/2002. Segmentada em oito títulos (Objetivo – Documentos Complementares – Definições – Compromisso da Administração Superior – Princípios de Segurança da Informação – Comitê de Segurança da Informação – Responsabilidades – Disposições Gerais), é complementada pelos seguintes documentos:

PB-PL-01-00001 – Política de Segurança Empresarial do Sistema Petrobras

Código de Ética da Petrobras

PG-20-06-01 – Regime Disciplinar da Petrobras

PB-PG-04-00002 – Norma Classificação da Informação do Sistema Petrobras

NBR ISO / IEC 17799:2001. Tecnologia da Informação – Código de prática para a gestão da segurança da informação.

A Política de Segurança da Informação abrange os aspectos físico, lógico e comportamental, preservando sua confidencialidade, integridade e disponibilidade.

O Comitê de Segurança da Informação – Comseg é representado pelas áreas de Exploração e Produção, Abastecimento, Internacional, Gás e Energia, Desenvolvimento de Sistemas de Gestão, Estratégia Corporativa, Gestão do Desempenho Empresarial, Comunicação Institucional, Recursos Humanos, Jurídico, Tecnologia da Informação, Telecomunicações, Cenpes, Relacionamento com Investidores, BR Distribuidora S/A e Segurança Empresarial que o coordena.

> O vazamento de informações prejudica a nossa empresa e nós não podemos ficar indiferentes a esse risco. Ë necessário que tomemos consciência de que proteger o sigilo, tanto de práticas comerciais quanto de assuntos técnicos é

[1] Para maiores informações sobre o perfil corporativo da Petrobras, ver Apêndice B

> um fator primordial, neste ambiente competitivo em que a Petrobras se encontra. Envolve a necessidade de uma verdadeira mudança cultural, onde cada empregado e contratado do Sistema Petrobras precisa adquirir novos valores, assumir novas premissas, adotar novas condutas no trabalho. (Trecho de texto publicado no Editorial – HSM Management, Segurança Empresarial do Sistema Petrobras).

Dentre as responsabilidades atribuídas à Segurança Empresarial, consta promover programas educacionais e de comunicação relacionados à segurança da informação e a promoção de ações de melhoria da segurança da informação no Sistema Petrobras.

CST [2]

A Política de Segurança da Informação da Companhia Siderúrgica de Tubarão, está preconizada no Padrão Empresarial PE-INF-0001, aprovado em 13/10/1999. Segmentada em seis títulos (Objetivo – Documentos Complementares – Definições – Condições Normativas – Responsabilidade - Autoridade), é complementada pelo PE-INF-0005 – Segurança da Informação no Ambiente da Rede Corporativa e por padrões específicos com as seguintes diretrizes: a) segurança de pessoal; b) segurança física; c) gerenciamento de rede e de equipamentos; d) controle de acesso a sistemas; e) desenvolvimento e manutenção de sistemas; e f) plano de continuidade do negócio.

Abrange todos os usuários que utilizam ou acessam quaisquer recursos de informação oferecidos pelo ambiente da rede corporativa da CST.

O Comitê de Segurança da Informação – CSI é composto por representantes das áreas de Informática, Recursos Humanos, Auditoria Interna e Automação de Processos. Entre as responsabilidades definidas pela política consta colaborar com o Departamento de Informática / Divisão de Suporte Técnico na disseminação da cultura da segurança da informação na Companhia. Por sua vez, o Departamento de

[2] Para maiores informações sobre o perfil corporativo da CST, ver Apêndice B

Informática, dentre as responsabilidades atribuídas, consta promover a divulgação da Política de Segurança da Informação, bem como treinamento e cultura da informação; e implementar e administrar padrões e procedimentos de segurança.

O padrão PE-INF-0005 que dá suporte ao PE-INF-0001, estabelece os critérios e procedimentos que devem garantir a segurança dos recursos da informação no ambiente da rede corporativa e de dados. Os documentos a seguir relacionados, o complementa:

PE-ABA-0002 – Serviços de Terceiros – Condições Normativas, Responsabilidades e Níveis de Autoridade

PE-ADM-0003 – Entrada e Saída de Materiais

PE-ADM-0007 – Serviços de Terceiros – Condições Relativas à Segurança Patrimonial

PE-GRH-0002 – Deveres e Proibições

PE-GRH-0003 – Penalidades Disciplinares

SAMARCO [3]

A Política de Segurança da Informação da Samarco está alinhada com a BS 7799-2:2002 e com a NBR ISO IEC 17799:2001. Implementada em 2003, tem o patrocínio da alta direção, está em conformidade com a legislação pertinente, leva em consideração a gestão da continuidade dos negócios e estabelece qual as conseqüências quando da violação da política de segurança da informação.

Por ser uma empresa certificada pela BS 7799-2:2002, o seu escopo abrange a área de tecnologia da informação (Operação de Data Center; Operação de Help Desk, Controle de LAN / WAN e Desenvolvimento e Manutenção de Sistemas Aplicativos) e marketing (CRM – Inside Samarco), esta por ser uma área que possui um relacionamento direto com os clientes e por este relacionamento também ser on-line (CRM).

[3] Para maiores informações sobre o perfil corporativo da SAMARCO, ver Apêndice B

O Sistema de Gestão de Segurança da Informação (SGSI) tem por objetivo estabelecer um modelo de gestão para atender às diretrizes da Política de Segurança da Informação da Samarco, definida e aprovada pela diretoria, por meio da implementação e aplicação de normas, procedimentos, recursos tecnológicos, treinamento e conscientização de todas as partes envolvidas sobre a importância da informação, considerada um ativo da empresa. Compõe a sua estrutura o Fórum de Segurança da Informação, composto pelo Comitê de Tecnologia da Informação e Subcomitê de Segurança da Informação. A sua coordenação é exercida por um empregado da empresa, indicado pela Diretoria.

A documentação que suporta a Política de Segurança da Informação da Samarco, a seguir relacionada, está segmentada em normas e procedimentos da Segurança da Informação - SI e normas e procedimentos da Tecnologia da Informação – TI.

Segurança da Informação

S-SI-I01 Norma para Avaliação de Riscos de SI
S-SI-I02 Norma para Análise Critica SGSI
S-SI-I03 Norma para Auditoria Interna SGSI
S-SI-I04 Norma para Ação Corretiva Preventiva
S-SI-I05 Norma para Controle Salvaguarda Registros SGSI
S-SI-I06 Norma para Classificação Tratamento Informação
S-SI-I07 Norma para Processo Disciplinar
S-SI-I08 Norma para Notificação Incidentes de SI
S-SI-I09 Norma para Controle de Documentos

Tecnologia da Informação

S-TI-I01 Norma para Aquisição, Disponibilização, Uso, Remoção e Alienação de Softwares
S-TI-I02 Norma para Aquisição, Disponibilização, Uso, Remoção e Alienação de Hardware
S-TI-I02-A1 Termo de Responsabilidade - Anexo 1

S-TI-I02-A2 Comprovante de Utilização e Circulação de Equipamento nas Unidades da Samarco - Anexo 2

S-TI-I03 Esta norma foi incorporada na norma S-TI-I02

S-TI-I04 Norma para Controle de Acesso Físico

S-TI-I05 Norma para Supervisão de Visitantes e ou Prestadores de Serviços

S-TI-I06 Esta norma foi incorporada na norma S-TI-I01

S-TI-I07 Norma para Controle de Mudanças e Implementação de Sistemas de Informação

S-TI-I08 Norma para Segurança e Tratamento de Mídias

S-TI-I09 Norma para Uso Correio Eletrônico

S-TI-I10 Norma para Uso Intranet e Internet

S-TI-I11 Norma para Utilização de Recursos de TI

AVALIAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

Este questionário de pesquisa, autorizado pelo Gerente Executivo, tem como objetivo levantar informações a respeito da **cultura de segurança da informação nas empresas**, visando:

Auxiliar uma dissertação de Mestrado Profissional em Administração na Universidade Federal da Bahia;

Identificar o nível de conhecimento dos empregados sobre o tema segurança da informação.

INSTRUÇÕES

Em cada questão está descrita a maneira como ela deverá ser respondida

Esta pesquisa é confidencial, não havendo necessidade de informar o seu nome.

Após responder o questionário, colocá-lo no envelope e enviá-lo pelo malote.

PERFIL DO ENTREVISTADO

Por favor, **circule** o número correspondente às suas características.

TEMPO DE TRABALHO	ÁREA EM QUE TRABALHA	REGIME QUE TRABALHA
1 Até 3 anos	**1** Operacional	**1** Turno
2 De 3 a 10 anos	**2** Administrativa	**2** Horário Adm
3 + 10 anos		

POLÍTICA DE SEGURANÇA

1 - Na sua opinião, segurança da informação é:
(CIRCULE a alternativa que esteja mais próxima do que você entende sobre o assunto**)**

a) Procedimentos que a empresa adota para controle do sistema de informática (TI).
b) Procedimentos que a empresa adota para classificar, armazenar, transportar e divulgar toda a informação que circula na empresa.
c) Não tem conhecimento sobre o assunto que permita uma opinião segura.
d) Não sabe o que é segurança da informação.

Após ler cada frase a seguir, expresse sua opinião de acordo com a legenda:

1 – CONCORDA TOTALMENTE (CT)
2 – CONCORDA, SÓ EM PARTE (CP)
3 – É INDIFERENTE (NEM CONCORDA / NEM DISCORDA**) – IND**
4 – DISCORDA TOTALMENTE (DT)
5 – NÃO SABE (NS)

2 – Sua opinião sobre a política de segurança da informação.
(CIRCULE o número correspondente à sua opinião)

FRASE	CT	CP	IND	DT	NS
Tenho conhecimento sobre a política de segurança da informação da minha empresa	1	2	3	4	5
A minha empresa tem uma boa política de segurança da informação	1	2	3	4	5
O controle da segurança da informação da minha empresa é muito rígido e dificulta o trabalho dos empregados	1	2	3	4	5
A segurança da informação é um modismo que logo será esquecido	1	2	3	4	5
A realidade do dia-a-dia da empresa é diferente do que diz a política de segurança	1	2	3	4	5
A informação deve circular livremente, sem controles.	1	2	3	4	5

3 - Seu entendimento quanto aos cuidados com a segurança da informação:

FRASE	CT	CP	IND	DT	NS
Aumenta a lucratividade da empresa	1	2	3	4	5
Preserva a imagem da empresa	1	2	3	4	5
Garante a continuidade do negócio	1	2	3	4	5
Aumenta o valor de mercado da empresa	1	2	3	4	5
Segurança da Informação não tem nada a ver com o lucro	1	2	3	4	5
Informação sobre conhecimento tecnológico não deve chegar ao conhecimento de todos os empregados	1	2	3	4	5
Informações sobre uma licitação não precisam ser confidenciais	1	2	3	4	5

4 – Como você avalia os recursos que a empresa usa para a segurança da informação?

SERVIÇO	ÓTIMO	BOM	REGULAR	RUIM	PÉSSIMO	NÃO SABE
Quantidade de senhas	1	2	3	4	5	6
Controle do acesso a Intranet	1	2	3	4	5	6
Controle do acesso a Internet	1	2	3	4	5	6
Controle do e-mail	1	2	3	4	5	6

5 – Os controles de segurança da informação são melhores entendidos pelos empregados: (apenas 1 alternativa – a mais importante)

a) Quando acontece algo que compromete a imagem da empresa (aprende-se com o erro)
b) Promoção de campanhas educativas, esclarecendo o assunto.
c) Ocorrências em outras empresas (aprende-se com o erro de outros)
d) Não sabe

6 – Na sua opinião, analisando a estrutura da empresa como um todo, os controles de segurança da informação são: (Circule apenas 1 alternativa – a mais importante).

a) Fundamentais
b) Importantes, mas não fundamentais.
c) Desnecessários
d) Não sabe

INFORMAÇÃO COMO ATIVO E BEM ECONÔMICO

7 - Do que você sabe e/ou ouviu falar sobre ATIVO de uma empresa, qual a alternativa que mais se aproxima da sua opinião:

1. São bens físicos e financeiros da empresa
2. São bens financeiros da empresa
3. São bens físicos, financeiros e o sistema de informação da empresa
4. Não sabe

8 - Do que você sabe e/ou ouviu falar sobre BEM ECONÔMICO de uma empresa, qual a alternativa que mais se aproxima da sua opinião:

1. São objetos que se compram e se vendem
2. São objetos e/ou informações que se compram e se vendem
3. Não sabe

PLANEJAMENTO ESTRATÉGICO

9 - Do que você sabe sobre PLANEJAMENTO ESTRATÉGICO de uma empresa, qual a alternativa que mais se aproxima da sua opinião:

a) O Planejamento Estratégico manifesta preocupação com a Segurança da Informação
b) A Segurança da Informação é importante para o cumprimento das metas estabelecidas no Planejamento Estratégico da Empresa
c) Segurança da informação não é tema para ser abordado em planos estratégicos
d) Não conhece o Planejamento Estratégico
e) Não sabe

AGRADECEMOS A SUA PARTICIPAÇÃO

APÊNDICE C

QUADROS

APÊNDICE D

FIGURAS