Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Carlos Alberto Zani

O ESTADO BRASILEIRO E A CULTURA DE SEGURANÇA DA INFORMAÇÃO:
Estudo de Caso Sobre a Implantação de Um Projeto de Segurança da Informação em Um Órgão da Administração Pública Federal.

Rio de Janeiro

2009

Carlos Alberto Zani

O ESTADO BRASILEIRO E A CULTURA DE SEGURANÇA DA INFORMAÇÃO:

Estudo de Caso Sobre a Implantação de Um Projeto de Segurança da Informação em Um Órgão da Administração Pública Federal.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computadores Eletrônica da Universidade Federal do Rio de Janeiro – NCE / UFRJ.

Orientador:

Mônica Ferreira da Silva, D.Sc., UFRJ. Brasil

Rio de Janeiro

2009

Carlos Alberto Zani

O ESTADO BRASILEIRO E A CULTURA DE SEGURANÇA DA INFORMAÇÃO:

Estudo de Caso Sobre a Implantação de Um Projeto de Segurança da Informação em Um Órgão da Administração Pública Federal.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computadores Eletrônica da Universidade Federal do Rio de Janeiro – NCE / UFRJ.

Aprovada em dezembro de 2009.

Mônica Ferreira da Silva, D.Sc., UFRJ. Brasil

À nobreza daqueles gigantes que nos legaram o conhecimento sobre o qual nos apoiamos para tentar enxergar mais nitidamente a realidade em que vivemos.

AGRADECIMENTOS

À minha mãe, que me ensinou com atos e palavras a valorizar a condição de ser humano e o respeito ao outro como um igual.

À Gisella: esposa, companheira, amiga, incentivadora e animadora nos momentos de desespero.

Aos companheiros de classe e professores do Programa MOT-CN do NCE/UFRJ, com quem dividi descobertas, angústias e alegrias; em especial aos professores Moacyr, por ter aceitado um sociólogo num antro de engenheiros, e Mônica, por ter aceitado orientar esse ornitorrinco acadêmico em que me transformei ao concluir esse curso.

Aos meus amigos de toda a vida, que ajudaram, também, a ser isso que chamo de eu.

RESUMO

ZANI, Carlos Alberto. **O ESTADO BRASILEIRO E A CULTURA DE SEGURANÇA DA INFORMAÇÃO: Estudo de Caso Sobre a Implantação de Um Projeto de Segurança da Informação em Um Órgão da Administração Pública Federal**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

O presente trabalho tem por objetivo demonstrar em que grau a cultura de Segurança da Informação está presente em um órgão da Administração Pública Federal Brasileira, enfatizando a diferença de percepção entre os profissionais de Tecnologia da Informação e profissionais que atuam na atividade fim da organização. Os dados em que se baseou esse estudo de caso foram levantados através de um questionário preparado com a intenção de capturar, dentro do tema da pesquisa, a situação atual da empresa, como a alta direção se posiciona, como os mecanismos utilizados impactam o trabalho dos profissionais consultados e como estes se posicionam em relação ao tema.. A tentativa inicial de compreensão dos dados e análise dos resultados, através da comparação das respostas pela leitura direta dos questionários, revelou-se árida e de difícil implementação. A compreensão dos dados só foi possível após a realização de uma consolidação dos principais argumentos levantados pelos respondentes em planilhas separadas por perfil de atuação profissional. A partir desse resultado intermediário foi possível visualizar claramente a diferença de posicionamento oriunda das expectativas inerentes aos respectivos campos de atuação, assim como analisar com maior clareza as motivações que levam às concordâncias e discordâncias observadas nas respostas. Os profissionais de Tecnologia da Informação desejam o estabelecimento de uma sólida cultura de Segurança da Informação, porque entendem que esta protege a organização e as pessoas de ameaças reais e cada vez mais presentes na sociedade contemporânea; os profissionais que são usuários dos serviços de Tecnologia da Informação da organização, apesar de compreenderem a necessidade do estabelecimento de uma forte cultura de Segurança da Informação, preocupam-se que o exagero no estabelecimento e implementação de regras e mecanismos de segurança possam prejudicar seriamente sua produtividade e sua qualidade de vida profissional. Os pontos de concordância observados revelam riscos aos planos do governo brasileiro de estabelecer a cultura de Segurança da Informação em toda a estrutura da Administração Pública Federal, porque revelam falta de compromisso da alta direção, inexistência de normativos e de um plano de conscientização e incentivo à adoção das melhores práticas de segurança nas atividades diárias das pessoas, assim como falta de interesse de toda a estrutura de gestão com relação às propostas que lhes foram apresentadas no sentido de realizar alguma atividade ou iniciar algum processo de conscientização das pessoas para os riscos a que estão sujeitas no seu dia a dia e que colocam a própria organização em risco. Diante dos resultados obtidos, faz-se necessário o acompanhamento da evolução dos acontecimentos nessa organização, especialmente após a divulgação deste trabalho, a fim de observar como será a reação dos tomadores de decisão.

ABSTRACT

ZANI, Carlos Alberto. **O ESTADO BRASILEIRO E A CULTURA DE SEGURANÇA DA INFORMAÇÃO: Estudo de Caso Sobre a Implantação de Um Projeto de Segurança da Informação em Um Órgão da Administração Pública Federal**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

This paper aims at showing to what extent the culture of Information Security is present in an organ of the Brazilian Federal Public Administration, emphasizing the difference in perception between professionals of Information Technology and professionals who work in the final activity of the organization. The data on the basis of this case study were collected through a questionnaire prepared with the intention of capturing, within the research theme, the current situation of the company as senior management positions itself as the mechanisms used impact the work of professionals consulted and how they position themselves in relation to the subject. The initial attempt to understand the data and analysis of results, by comparing the answers by reading the questionnaires, it turned out dry and difficult to implement. The data analysis was only possible after the completion of a consolidation of the main arguments raised by respondents in separate worksheets for profile professional performance. From this intermediate result could clearly see the difference in position coming from the expectations inherent in the respective fields, and consider more clearly the motivations for agreement and disagreement in the responses observed. Occupational Information Technology wishing to establish a strong culture of Information Security, because they understand that this protects the organization and people from real threats and increasingly present in contemporary society, the professionals who are customers of Technology information organization, despite understanding the need to establish a strong culture of Information Security, worries that the hype in the establishment and implementation of rules and security mechanisms can seriously damage your productivity and your quality of life. The points of agreement observed shows risks to the Brazilian government plans to establish a culture of Information Security throughout the structure of the Federal Public Administration, because they reveal a lack of commitment from top management, lack of standards and a level of awareness and encourage adoption of best safety practices in daily activities of people, as well as lack of interest of the entire management structure with the proposals presented to them in order to carry out any activity or start a process of educating the public about the risks that are subject in their daily activities and that they put their organization at risk. Considering the results obtained, it is necessary to monitor the developments in this organization, especially after the disclosure of this work in order to see how the reaction will be the decision makers.

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CD	Compact Disc
CDN	Conselho de Defesa Nacional
DVD	Digital Video Disc ou Digital Versatile Disc
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
ISO	International Standard Organization
MOT	Master of Technology
NCE	Núcleo de Computação Eletrônica
PDCA	Plan-Do-Check-Act
PSIC	Política de Segurança da Informação e Comunicação
SGSI	Sistema de Gestão de Segurança da Informação
SPAM	Mensagem eletrônica não-solicitada enviada em massa
TGA	Teoria Geral da Administração
TI	Tecnologia da Informação
TO	Teoria das Organizações
UFRJ	Universidade Federal do Rio de Janeiro

SUMÁRIO

1 **INTRODUÇÃO**

1.1 OBJETIVOS

Os pesquisadores brasileiros conquistaram respeito internacional há várias décadas e as instituições brasileiras de pesquisa mostram resultados cada vez mais promissores, alimentando a esperança de um País com presença cada vez mais destacada no cenário mundial.

Nesse contexto, seria natural esperar uma preocupação estrutural do Estado Brasileiro com a segurança das informações produzidas e mantidas sob guarda dos órgãos e entidades da Administração Pública Federal (APF). Afinal, a competitividade envolve a proteção do sigilo das informações sobre os processos e produtos que estão em gestação ou nasceram em instituições públicas e privadas que fizeram e fazem uso de preciosos recursos, originários do pagamento de tributos pela população, em projetos de pesquisa e desenvolvimento, engrandecendo nosso capital científico e tecnológico.

Formalmente, o País conta com uma Política de Segurança da Informação (PSI). A adoção de suas diretrizes pelos órgãos e entidades da APF está sob responsabilidade da Secretaria-Executiva do Conselho de Defesa Nacional (CDN), com assessoria do Comitê Gestor da Segurança da Informação. O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) responde pela Secretaria-Executiva do CDN.

Existem iniciativas do GSI/PR para levar a efeito as diretrizes da PSI nos órgãos e entidades da APF, assim como há iniciativas dos próprios órgãos e entidades da APF no sentido de estabelecer uma cultura de segurança da informação que leve em conta os requisitos e práticas internacionalmente reconhecidos

Este trabalho visa contribuir para o avanço do conhecimento sobre a forma mais adequada de estabelecimento de uma Política de Segurança da Informação no contexto do Estado Brasileiro, propondo-se responder a seguinte pergunta: **como o estabelecimento da cultura de segurança da informação num órgão ou entidade da Administração Pública Federal impacta no cumprimento da sua missão?**

Para essa tarefa, optamos pelo estudo de um caso real de implantação da PSI numa empresa pública, tendo como foco a comparação das percepções que os profissionais de Tecnologia da Informação (TI) e os profissionais de outros segmentos da empresa têm sobre o impacto desse processo na execução de suas atividades e na sua articulação com o cumprimento da missão da empresa.

1.2 RELEVÂNCIA

Acreditamos que a importância deste trabalho reside, fundamentalmente, em dois fatores: a) chegar num momento oportuno, quando o esforço de disseminação da cultura de segurança da informação está sendo intensificado por parte do atual Governo; e b) priorizar a percepção dos profissionais da empresa na qual se está buscando estabelecer essa cultura.

As pessoas são, ao mesmo tempo, o elemento mais diretamente atingido nesse processo e o elemento fundamental para a concretização da missão de qualquer organização.

Esse caráter determinante das pessoas como correia de transmissão dos esforços empregados para alcançar o sucesso em qualquer empreendimento determinou nossa escolha por focalizar o elemento humano na realização deste estudo.

A medida da importância de discutirmos esse tema pode ser percebida a partir de relatos como este, do mais famoso violador de sistemas de segurança da informação de que se tem notícia (MITINICK, 2003, p. 3):

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe.
> Mesmo assim essa empresa ainda estará vulnerável.
> Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança.
> Esses indivíduos ainda estarão completamente vulneráveis.

Não podemos perder de vista que a Internet realizou o “milagre” de conectar todos que possuem um dispositivo eletrônico dotado de um modem ou de uma interface de rede, com ou sem fios, em qualquer parte do planeta Terra, e que cada

indivíduo conectado à rede planetária é um atacante em potencial da privacidade ou dos ativos de qualquer indivíduo ou organização.

Para deixar claro a complexidade da tarefa daqueles que se dedicam à proteção desses ativos, o próprio Mitinick (2003, p. 4) declara:

> À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando cada vez mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo.

Como podemos perceber, tanto os bandidos por trás das consoles de computador quanto os bandidos por trás das armas de fogo buscam se apoderar dos valores mantidos pelos indivíduos e organizações através do elemento responsável por criar, implantar e manter todo e qualquer sistema de segurança: as pessoas.

São as pessoas que, em última instância, guardam a chave de qualquer cofre, seja ele físico ou virtual.

Não é por acaso que a segurança da informação vem se firmando como área de conhecimento específica nas universidades brasileiras, a exemplo do que já ocorre em outras partes do mundo.

2 REFERENCIAL TEÓRICO

A capacidade de criação e realização da espécie humana fez com que alcançássemos uma suposta supremacia sobre os outros organismos vivos do planeta Terra. Essa posição privilegiada não teria sido conquistada se os indivíduos humanos não tivessem feito a opção por conjugar seus esforços para se defenderem coletivamente das ameaças do ambiente e, desta forma, assegurar a sobrevivência e a evolução da espécie, desde os primórdios de nossa existência até os dias atuais. A ação organizada é determinante para a nossa existência.

Com o passar do tempo, além dos fatores objetivos como disputas por recursos materiais entre grupos dispersos geograficamente, as formas de agrupamento do Homem foram se transformando e deram origem a diferentes formas de organização social, marcadas por características particulares que, às vezes, levam ao conflito as comunidades humanas que adotam diferentes visões de mundo, seja qual for a natureza central da diferença.

Para Chiavenato (2007, p. 2), as organizações são o motor do desenvolvimento econômico e social responsável por trazer o Homem ao mundo moderno, o carro-chefe da inovação e da transformação da sociedade contemporânea.

As organizações humanas nascem a partir de uma necessidade que os indivíduos membros sentem de alcançar objetivos comuns, sejam eles econômicos, políticos, religiosos, ligados à segurança do grupo etc.. Para que esses objetivos sejam alcançados, é necessário que o(s) motivo(s) que tornam necessária a existência da organização sejam fortes o suficiente para sobrepujar as individualidades e manter o grupo coeso e propenso a seguir o mesmo caminho.

Naturalmente, a individualidade deve ceder espaço para que o convívio social seja possível. Daí a necessidade de se estabelecer regras para possibilitar esse convívio, o que deu origem aos códigos de conduta moral ou ética.

Em suma, para que uma organização exista como tal, é necessária a existência de um acordo entre os indivíduos ou grupos de indivíduos que a compõem, a fim de possibilitar seu funcionamento como um todo coerente. Esta necessidade deu origem aos estudos sobre como administrar as organizações, que, com o passar do tempo, transformaram-se num ramo específico do conhecimento, elevando a Administração ao status de ciência.

A Administração se torna mais importante na medida em que as organizações são encaradas como organismos vivos e necessitam, como tal, agir e reagir adequadamente à variação das condições do ambiente onde estão inseridas .

> Além do mais, as organizações operam em ambientes diferentes, rodeadas de um universo de fatores econômicos, políticos, tecnológicos, legais, sociais, culturais e demográficos que interagem entre si e se alternam constantemente, proporcionando um campo dinâmico de forças caracterizado por enorme mudança e instabilidade ao redor. No fundo, as organizações recebem influências de seu meio ambiente, mas, em contrapartida, nele também provocam profundas influências. Se as organizações mudam em função do impacto de forças ambientais, elas também provocam alterações nessas forças externas. Há um complicado jogo de ações e interações que provocam e recebem influências de todas as partes envolvidas. (CHIAVENATO, 2007, p. 2)

Entre as organizações, as empresas são aquelas que representam melhor o espírito do liberalismo econômico, sistema que se fundamenta na livre iniciativa de indivíduos que assumem o risco do investimento na produção e distribuição de bens e serviços, e que conquistou hegemonia global.

Como é livre a iniciativa, existem várias empresas competindo pelo mesmo conjunto de consumidores. Nessa competição, é questão de vida ou morte apresentar-se como o portador da melhor oferta e conquistar a confiança do conjunto de indivíduos e organizações que podem influenciar nas condições necessárias para a empresa alcançar seus objetivos e deixar os adversários para trás na disputa.

Com o gigantismo global das empresas da atualidade, a competição alcançou níveis também globais, ferozes e muito sofisticados. Não é raro, infelizmente, assistirmos nos noticiários cenas que revelam a ocorrência de crimes envolvendo o roubo de informações entre empresas concorrentes.

Num mundo onde a Tecnologia da Informação virou vedete global, considerando-se o uso cada vez mais intenso que dela fazem as organizações para alavancar seu desempenho, não podemos nos esquecer de que esse status foi alcançado em função da importância que as empresas e demais organizações construíram ao longo do tempo.

Nesse contexto, buscar a segurança das informações capazes de garantir vantagem competitiva em relação aos concorrentes tornou-se tão fundamental quanto criar essa vantagem. Além disso, a guarda de informações privativas de

indivíduos e organizações também constitui preocupação importante, tendo em vista que um vazamento pode comprometer ativos como a imagem do responsável pela sua segurança, que é garantida pela confiança que os proprietários das informações têm na capacidade que essas organizações possuem de manter o sigilo exigido.

2.1 HISTÓRIA DA ADMINISTRAÇÃO DAS ORGANIZAÇÕES

> Hoje vivemos em um mundo de organizações. Tudo é inventado, criado, planejado, desenvolvido, produzido, comercializado, financiado e entregue por organizações. Se a administração foi a maior invenção do século passado, as organizações constituem a invenção maior do século anterior. São elas que proporcionam produtos, serviços, crédito, financiamento, entretenimento, informação, alimentação, vestuário, saúde, educação, religião, segurança, paz e guerra – enfim, tudo de que o mundo moderno necessita. E as organizações precisam ser administradas. (CHIAVENATO, 2007, p. 38)

O caso de estudo apresentado neste trabalho não trata de uma organização cujo negócio esteja inserido diretamente no mercado de produtos e serviços de Tecnologia de Informação, mas de uma organização que os utiliza como suporte aos seus processos internos e meio de relacionamento com os seus clientes.

Nesse contexto, tratamos a Tecnologia da Informação como suporte ao negócio da organização e buscamos analisar os relacionamentos entre a estratégia de atuação desta e os requisitos necessários para que sua área de TI proporcione os níveis de serviço adequados à conquista dos objetivos definidos, garantindo, ao mesmo tempo e dentro dos parâmetros definidos pelos administradores, a segurança da informação.

Tendo este trabalho como foco a implantação de um projeto de segurança da informação num ambiente empresarial através de uma metodologia determinada, consideramos apropriado apresentar um resumo do desenvolvimento histórico da Teoria Geral da Administração, como forma de contextualizar a terminologia utilizada ao longo do texto.

Segundo Chiavenato (2007, p. 7), a história da Teoria Geral da Administração (TGA) inicia fortemente marcada pela engenharia, ou seja, a ênfase da ação do administrador recaía nas tarefas realizadas pelas pessoas incumbidas diretamente da produção dos bens ou serviços nas organizações. Estas, aliás, foram o objeto de estudo que levou às primeiras preocupações teóricas com relação à Administração,

vista como um meio para realizar o que era formulado na Teoria das Organizações (TO).

Desses primeiros passos da formulação teórica de uma TGA até os nossos dias, houve uma série de deslocamentos do paradigma teórico da Administração, resultando em fases que se superpõem e nas quais a ênfase recaiu sobre uma das seis variáveis básicas da empresa na teoria administrativa: Tarefas, Estrutura, Pessoas, Tecnologia, Ambiente, Competitividade, conforme podemos observar na tabela 1.

Tabela 1 – As fases da história das empresas e da teoria administrativa. (CHIAVENATO, 2007, p. 25)

ANOS	FASES DAS EMPRESAS	ÊNFASE	TEORIAS ADMINISTRATIVAS PREDOMINANTES
1780	• Artesanal • Início da Industrialização • Primeira Revolução Industrial		
1860	• Desenvolvimento Industrial • Segunda Revolução Industrial	• Nas tarefas	• Administração Científica
1914	• Gigantismo Industrial • As Duas Guerras Mundiais	• Na estrutura organizacional • Nas pessoas	• Teoria Clássica • Teoria Neoclássica • Teoria das Relações Humanas
1945	• Moderna • Pós-Guerra	• Na estrutura organizacional • Nas pessoas • Na tecnologia • No ambiente	• Teoria Neoclássica • Teoria da Burocracia • Teoria Estruturalista • Teoria Comportamental • Teoria da Contingência • Teoria da Contingência
1980	• Globalização • Momento Atual	• No ambiente	• Teoria Contingência

A tabela 2 nos permite uma melhor compreensão da articulação entre as teorias administrativas e seus principais enfoques sobre a atividade das empresas.

Tabela 2 – As principais teorias administrativas e suas abordagens. (CHIAVENATO, 2007, p. 24)

ÊNFASE	TEORIAS ADMINISTRATIVAS	PRINCIPAIS ENFOQUES
• Nas tarefas	• Administração Científica	• Racionalização do trabalho no nível operacional.
• Na estrutura	• Teoria Clássica • Teoria Neoclássica	• Organização formal. • Princípios gerais da Administração. • Funções do administrador.
	• Teoria da Burocracia	• Organização formal burocrática. • Racionalidade organizacional.

	• Teoria Estruturalista	• Múltipla abordagem
		  • Organização formal e informal.
		  • Análise intra-organizacional e análise interorganizacional.

• Nas pessoas	• Teoria das Relações Humanas	• Organização informal. • Motivação, liderança, comunicações e dinâmica de grupo.
	• Teoria Comportamental	• Estilos de Administração. • Teoria das decisões. • Integração dos objetivos organizacionais e individuais.
	• Teoria do Desenvolvimento Organizacional	• Mudança organizacional planejada. • Abordagem de sistema aberto.
• No ambiente	• Teoria Estruturalista	• Análise intra-organizacional e análise ambiental. • Abordagem de sistema aberto.
	• Teoria da Contingência	• Análise ambiental (imperativo ambiental). • Abordagem de sistema aberto.
• Na tecnologia	• Teoria da Contingência	• Administração da tecnologia (imperativo tecnológico).
• Na Competitividade	• Novas Abordagens na Administração	• Caos e complexidade. • Aprendizagem organizacional. • Capital intelectual.

Olhando essa história em perspectiva, percebemos que a Administração incorporou o desenvolvimento teórico resultante de cada uma dessas fases em que a lente de aumento dos estudiosos se focou numa das seis variáveis básicas da organização e ampliou seu campo de visão e de atuação, preocupando-se cada vez mais com o filme e não só com a fotografia, ou seja, enxergando a dinâmica da realidade e pensando as organizações e sua administração nesse ambiente multifacetado e em constante mutação, no qual as organizações e o meio onde atuam sofrem influências recíprocas e assim constroem a história econômica global.

A ampliação da importância de temas como liberdade, democracia, responsabilidade social e ambiental, transparência e ética para a sociedade globalizada, aliada à evolução intensa dos recursos tecnológicos, criaram um ambiente onde Aristóteles se torna insuficiente e o valor de Heráclito é redescoberto: a única coisa permanente é a mudança.

2.2 ESTRATÉGIA NAS ORGANIZAÇÕES

A análise histórica nos mostra de maneira inquestionável que a competição por recursos capazes de garantir a sobrevivência de indivíduos, povos, culturas, assim como das organizações, teve e tem um papel preponderante como motor da evolução da humanidade em todos os seus aspectos. Entretanto, em nenhuma outra dimensão da vida das sociedades humanas a sua importância foi tão sentida como no desenvolvimento científico e tecnológico.

Dos momentos da história onde a face mais aguda e terrível da competição veio à tona, as guerras, a humanidade herdou, além dos milhões de mortos e das lições sobre a necessidade de se estabelecer limites para a competição entre os povos pelos recursos disponíveis no planeta, avanços significativos em todos os ramos da Ciência e da Tecnologia.

Os períodos de guerra oferecem um ambiente onde a importância da informação pode ser percebida em escala enormemente ampliada. Ter acesso aos segredos do inimigo significa a diferença entre a vitória ou a derrota, a vida e a morte de indivíduos, organizações, povos, culturas.

Em períodos de paz formal, a importância das informações reside nos segredos industriais, patentes, autoria de obras artísticas, literárias, produtos e/ou processos comerciais ou industriais, programas de computador, proteção da privacidade dos indivíduos e organizações. A garantia da segurança dos ativos de informação pode significar a diferença entre o sucesso e o fracasso, a continuidade ou o encerramento das atividades de uma organização.

Para sobreviver e prosperar, tanto os indivíduos quanto as organizações criam, mesmo que inconscientemente, estratégias para alcançar seus objetivos e mecanismos para proteger os recursos que consideram valiosos para garantir seu sucesso, ou seja, os seus ativos.

Em função das constantes mudanças no estado das variáveis que compõem o ambiente onde está inserida uma organização, sua estratégia deve ser revista a cada mudança significativa nessas variáveis ambientais, assim como os mecanismos de proteção dos seus ativos, dos quais, como já vimos, a informação é um dos mais valiosos.

Não é tarefa simples responder às necessidades de adaptação às mudanças no ambiente, buscar vantagem competitiva sobre os concorrentes e manter seguros os seus ativos. O equilíbrio entre essas necessidades permanentes num ambiente de acirrada competição local e global desponta como a chave para o sucesso.

A estratégia de uma organização deve conjugar a solidez necessária para impulsionar a sua atuação em cada configuração do ambiente externo e a flexibilidade necessária para se adaptar às rápidas alterações das variáveis ambientais. Para que isto seja possível, é necessário que todos os seus membros estejam conscientes de alguns conceitos fundamentais sobre os quais se assentará todo e qualquer planejamento e, consequentemente, as atribuições de cada um para que os objetivos definidos sejam alcançados.

2.2.1 **Definição Do Negócio**

Nenhum vento sopra a favor de quem não sabe para onde ir.
Séneca (4 a.c.- 65 d.c.)

Assim como os indivíduos necessitam pensar sobre o que fazer com o seu tempo de vida, cuidando da sua sobrevivência e do grau de conforto que desejam conquistar como fruto da sua atividade produtiva, uma organização necessita, também, planejar como deseja que sua existência aconteça.

É preciso responder perguntas básicas e nem de longe simples, como:

- Quem sou eu?
- Onde quero chegar?
- O que estou disposto a fazer para chegar onde quero?
- Como chegar onde quero?
- Como viver confortavelmente realizando minha escolha?
- Como manter ou expandir as conquistas alcançadas?

Assim como um indivíduo mobiliza suas energias e recursos para agir em função das respostas que dá a essas perguntas, os administradores de uma

organização devem buscar reunir e mobilizar as competências, recursos e energias necessários à realização da sua razão de existir e à conquista da posição almejada no mercado em que atua e concorre com outras organizações.

Diferentemente do que ocorre no universo dos indivíduos, uma organização não nasce para atender a uma demanda desenraizada da realidade econômica vivenciada pelos seus criadores; ela é criada para atender a uma demanda real de um determinado conjunto de pessoas.

Segundo Chiavenato (2007, p. 49), todo negócio deve ter uma missão a cumprir; deve ter uma visão do futuro que o norteie e deve definir os valores que pretende consagrar. Esses são conceitos fundamentais da Administração e, consequentemente, servem de base para o estabelecimento de um SGSI, visando garantir proteção da informação produzida e armazenada em uma organização.

Ainda nos baseando em Chiavenato (2007, p. 50-55), apresentarmos a seguir uma breve apresentação do significado desses conceitos.

2.2.2 **Missão Organizacional**

Representa a razão de existir do próprio negócio, por que ele foi criado e para que ele existe. Sempre está colocada fora das fronteiras da organização e centrada na sociedade. Em síntese, define os produtos/serviços, os mercados e a tecnologia, refletindo os valores e as prioridades do negócio.

O mercado, as competências essenciais, os produtos/serviços e a tecnologia – o modo de fazer as coisas – quase sempre são considerados os quatro componentes indispensáveis na formulação da missão da empresa, porém, não se confundem com ela. São os três componentes econômicos (mercado, produtos/serviços e tecnologia) que guiam a direção estratégica de quase todos os negócios viáveis, definindo as atividades da organização no presente e o potencial futuro do negócio.

2.2.3 **Princípios E Valores Organizacionais**

São as crenças e atitudes básicas que contribuem para definir o comportamento dos indivíduos e das organizações.

Em muitas organizações, as crenças e atitudes que seus membros e parceiros desejam ver cultivadas e praticadas são escritas e reunidas num código

formal de ética, que passa a ser um documento de referência sobre os valores e padrões éticos que guiam a ação da organização como um todo em termos de cidadania, relacionamento com os clientes, respeito às leis, combate à corrupção e clareza absoluta sobre suas atividades.

Da mesma forma que ocorre em qualquer dimensão do comportamento humano, a ética dos seus membros ou das organizações em si é passível de questionamento, elogio, condenação pelas pessoas e organizações que com elas se relacionam. Como a realidade é infinita em possibilidades, não raro as pessoas e organizações se vêem na fronteira entre o que é e o que não é considerado ético e devem agir com extrema cautela para não perderem a confiança daqueles que determinam sua existência e sucesso.

2.2.4 **Visão Organizacional**

É a imagem definida pela organização a respeito do seu futuro, ou seja, do que ela pretende vir a ser; indica quais são os objetivos a serem alcançados em um tempo determinado, para orientar os seus membros quanto ao futuro que a organização pretende transformar em realidade.

O negócio de uma organização não deve ser conduzido ao sabor do vento; deve ser direcionado para a realização de um ideal almejado e compartilhado por todos os seus membros e parceiros. Essa atitude permite que sejam estabelecidos objetivos e metas, indicadores de desempenho e mensuradores de resultados futuros, para saber se a organização está ou não alcançando tais objetivos e metas.

A visão funciona como uma bússola para os parceiros envolvidos e tira a empresa da chamada zona de conforto, que é a gradativa acomodação profissional característica de certos negócios ao longo do tempo.

Assim como ocorre em relação à missão organizacional, não basta definir a visão organizacional; é preciso ir além e divulgá-la intensivamente e amplamente para toda a equipe da empresa.

2.2.5 **Objetivos Organizacionais**

Decorrentes do conceito de visão organizacional, os objetivos globais da empresa, também referidos no mercado como metas ou resultados, são estados desejáveis que pretende-se alcançar e realizar.

A formulação dos objetivos deve ser feita de forma a estimular a criatividade e oferecer uma direção clara para o negócio, simultaneamente. Deve-se tomar o cuidado de não definir objetivos mutuamente excludentes para as diversas áreas de atividade existentes na empresa, ou seja, o sucesso no alcance do objetivo de uma área não deve implicar diretamente no fracasso de outra. Por exemplo, pode-se definir a redução de custo como objetivo da área financeira e o aumento dos benefícios aos empregados como objetivo da área de recursos humanos. As vítimas serão a eficácia e a eficiência da organização.

Os objetivos podem ser definidos de acordo com os níveis hierárquicos da organização. Vejamos uma configuração normalmente adotada.

2.2.5.1 Objetivos Globais Ou Estratégicos

Considerados os mais importantes, envolvem um esforço integrado e coeso de toda a organização e se estenderem no longo prazo. Em geral, envolvem períodos de três a cinco anos e a realização de metas que mudariam o patamar da empresa frente aos seus concorrentes.

2.2.5.2 Objetivos Táticos

Sua abrangência é restrita a cada divisão da estrutura organizacional. Costumam ser dimensionados para serem alcançados no médio prazo, geralmente no período contábil de um ano. Devem ser aderentes aos objetivos estratégicos e impulsionar seu alcance.

2.2.5.3 Objetivos Operacionais

Restritos a cada tarefa ou atividade da empresa, envolvem prazos de no máximo alguns poucos meses para serem alcançados. Devem ser aderentes aos objetivos táticos e estratégicos e impulsionar seu alcance.

2.3 SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

2.3.1 **A Necessidade De Integração Dos Sistemas De Gestão**

A execução de atividades relacionadas e integradas para se chegar com sucesso à realização da razão de ser de uma organização, seja ela a prestação de serviços ou produção de um bem tangível, remete ao conceito de processo, ou seja, a obtenção de resultados a partir da entrada de matérias-primas que sofrem um determinado processamento no interior da organização. É isso que explica esse

conceito estar no centro das principais referências do arcabouço de boas práticas relacionadas com a atividade de gestão.

Neste ponto, convém destacar a fundamentação comum sobre a qual foram criadas as normas que definem boas práticas para a gestão das organizações (ABNT NBR isso 9001:2000), a gestão de segurança da informação (ABNT NBR ISO/IEC 27001:2006), a gestão ambiental (ABNT NBR ISO/IEC 14001:2004). A abordagem de processos com o uso do modelo PDCA e a análise/avaliação de riscos formam o núcleo duro dessa fundamentação.

A nota abaixo ilustra bem a estreita relação entre essas normas (ABNT, 2006, p. 1).

> Se uma organização já tiver um sistema de gestão de negócio em operação (por exemplo, em relação com a ABNT NBR isso 9001 ou ABNT NBR isso 14001), é preferível, na maioria dos casos satisfazer os requisitos desta Norma dentro deste sistema de gestão existente.

De acordo com a norma ABNT NBR ISO/IEC 27001:2006, cujo escopo engloba todos os tipos de organizações e especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Tecnologia da Informação (SGSI) documentado dentro do contexto dos riscos globais de negócio da organização, **qualquer atividade que faz uso de recursos e os gerencia para habilitar a transformação de entradas em saídas pode ser considerada um processo**. É ressaltado, na mesma norma, que a saída de um processo frequentemente forma diretamente a entrada do processo seguinte num fluxo de trabalho.

Ainda segundo a norma que trata da gestão do SGSI (ABNT, 2006, p. v e iv), “abordagem de processo” remete à aplicação e gestão de um sistema de processos dentro de uma organização, junto com a identificação e interações destes processos. Em vários itens dessa norma está consignada a subordinação dos processos do sistema de gestão do SGSI ao sistema de gestão do negócio propriamente dito, justificando-a pelo fato de que é da natureza deste último e serão definidos a missão, a visão, os valores e os objetivos da organização, que, por sua vez, serão a referência para a definição do que é valioso para ela, ou seja, para a identificação dos seus ativos, e para a atribuição do grau de valor para cada ativo identificado.

Para estruturar todos os processos do SGSI, é adotado o modelo conhecido como *"Plan-Do-Check-Act"* (PDCA), cuja aplicação considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas. A tabela abaixo demonstra a aplicação do modelo PDCA aos processos de um SGSI (ABNT, 2006, p.vi).

Tabela 3 – Descrição dos processos do modelo PDCA

***Plan* (planejar) (estabelecer o SGSI)**	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
***Do* (fazer) (implementar e operar o SGSI)**	Implementar e operar a política, controles, processos e procedimentos do SGSI.
***Check* (checar) (monitorar e analisar criticamente o SGSI)**	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
***Act* (agir) (manter e melhorar o SGSI)**	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção.

O modelo PDCA remete à melhoria contínua de um processo e reflete os princípios de governança da segurança de sistemas de informação e redes conforme definidos nas Diretrizes da OECD para esse tema (ABNT, 2006, p. v).

Identificados os ativos e atribuído a eles o respectivo grau de valor para a organização, é recomendado que sejam mapeados os riscos a que esses ativos estão expostos e estabelecidos processos para sua proteção. Entre os ativos identificados pela organização como importantes para a gestão do negócio, estão os ativos de informação e comunicação, cuja especificidade e necessidade de proteção diferenciada originou a elaboração da norma que trata especificamente do estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria de um SGSI (ABNT, 2006).

2.3.2 **Escopo Da Segurança Da Informação**

Segundo BEAL (2005, p. xi),

> A expressão *segurança da informação* é normalmente usada para referenciar a proteção de informações mantidas em componentes de tecnologia da informação (TI) contra as ameaças a que estão expostas. Entretanto, embora os sistemas informatizados se tornem cada vez mais indispensáveis para a operação de qualquer negócio, e uma parte cada vez maior do conjunto de informações importantes para as organizações esteja armazenada em computadores, é necessário considerar também a proteção dos **ativos de informação** que se encontram armazenados apenas na mente humana, num pedaço de papel ou em microfichas e microfilmes.

A própria Beal (2006, p. xi) define o termo “ativo de informação”, delimitando o escopo dos processos, requisitos e expectativas relacionados à segurança da informação.

> **Ativo de informação:** qualquer dado ou informação a que esteja associado um valor para o negócio. Representam ativos de informação as informações relevantes mantidas na mente dos tomadores de decisão, em bases de dados, arquivos de computador, documentos e planos registrados em papel etc. Neste livro, a expressão ativo de informação *será usada em sentido amplo para abranger ainda os componentes do patrimônio de TI da organização, incluindo hardware* e *software*, mídias de armazenamento e mecanismos de comunicação necessários para a execução de sistemas e processos de informação e comunicação.

Conforme ressaltamos anteriormente, a conscientização e o comprometimento das pessoas da organização com a segurança da informação é um fator primordial para o sucesso de qualquer SGSI. Assim, a importância das campanhas de informação e conscientização sobre a existência e a necessidade do SGSI e os processos que o compõem remete a uma demonstração clara e contundente da direção da organização de que está convencida da sua necessidade e comprometida com o seu sucesso. A importância dessa demonstração por parte da direção aparece explicitamente em vários itens da norma, onde ela deve, por exemplo:

- aprovar a política do SGSI, durante a fase de seu estabelecimento (ABNT, 2006, p. 4);
- autorizar a aceitação dos riscos residuais propostos no resultado do processo de análise/avaliação de riscos (ABNT, 2006, p. 6);
- autorizar a implementação e operação do SGSI (ABNT, 2006, p. 6);

- garantir o estabelecimento dos planos e objetivos do SGSI (ABNT, 2006, p. 9);
- estabelecer papéis e responsáveis pela segurança da informação (ABNT, 2006, p. 10);
- comunicar à organização da importância em atender aos objetivos de segurança da informação e a conformidade com a política de segurança da informação, suas responsabilidades perante a lei e a necessidade para melhoria contínua (ABNT, 2006, p. 10);
- provisionar recursos suficientes para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI (ABNT, 2006, p. 10);
- definir critérios para a aceitação de riscos e dos níveis de riscos aceitáveis (ABNT, 2006, p. 10);
- garantir que as auditorias internas do SGSI sejam realizadas (ABNT, 2006, p. 10);
- analisar criticamente o SGSI (ABNT, 2006, p. 10);

O processo de análise/avaliação de riscos é o núcleo de qualquer sistema de gestão de segurança. É através dele que são identificadas as ameaças aos ativos da organização, as vulnerabilidades dos ativos que podem ser exploradas pelas ameaças identificadas, o impacto que um ataque bem sucedido a uma dessas vulnerabilidades dos ativos poderia ocasionar para a organização e assim por diante.

O item 4 da norma que define as boas práticas para um SGSI descreve os passos recomendados para um processo de análise/avaliação de riscos bem sucedido (ABNT, 2006, p. 4-6):

- estabelecer, na política do SGSI, dos critérios em relação aos quais os riscos serão avaliados;
- definir a abordagem de análise/avaliação de riscos da organização, identificando a metodologia mais adequada, desenvolvendo critérios para a aceitação de riscos e identificando os níveis aceitáveis de risco;
- assegurar que a aplicação da metodologia selecionada produza resultados comparáveis e reproduzíveis;
- identificar os riscos;

- analisar e avaliar os riscos, considerando a probabilidade real da ocorrência de falhas de segurança e os impactos ao negócio associados aos ativos passíveis de serem atingidos;
- estimar os níveis de riscos;
- identificar e avaliar as opções para o tratamento dos riscos;
- selecionar objetivos de controle e controles adequados para o tratamento de riscos;
- obter aprovação da direção dos riscos residuais propostos e para a implementação e operação do SGSI;
- preparar uma Declaração de Aplicabilidade, estabelecendo:
    - os objetivos de controle e os controles selecionados, assim como as razões para sua escolha;
    - os objetivos de controle e controles atualmente implementados; e
    - a exclusão de quaisquer objetivos de controle e controles constantes do Anexo A da norma e a justificativa para a sua exclusão.

Para que seja possível implementar a melhoria contínua através do modelo PDCA, há necessidade de formalização, monitoramento e registro detalhado de todos os processos e do resultado da aplicação dos controles definidos na análise/avaliação de riscos. Também é necessário estabelecer indicadores para medir o desempenho dos controles em relação aos objetivos estabelecidos para cada um deles.

Outra necessidade importante atendida pelo registro sistemático e detalhado do resultado da aplicação dos controles e da sua comparação com os indicadores de desempenho em relação aos objetivos de controle é possibilitar a realização de auditorias, sejam elas realizadas por equipes internas ou externas.

A realização de auditorias aumenta a probabilidade de que os resultados do SGSI sejam fidedignos e cumpram o objetivo de proporcionar material importante para o processo de melhoria contínua da organização em relação á realização da sua missão e alcance da sua visão de futuro.

3 **METODOLOGIA DE PESQUISA**

3.1 TIPO DE PESQUISA

Optamos por um trabalho de pesquisa exploratória, tendo em vista que abordamos um processo que está ainda em sua infância e traz consigo um grande potencial transformador para a vida da sociedade brasileira.

Propomos este estudo de caso para analisar como a implementação da Política de Segurança da Informação do Estado está sendo absorvida pelos atores de uma instituição pública específica.

Para realizar esse trabalho, empreendemos uma pesquisa bibliográfica sobre Teoria Geral da Administração e Segurança da Informação e Comunicação, disciplinas que se entrelaçam na resposta à pergunta que pretendemos responder. Também foram consultados documentos públicos e normativos internos da organização pesquisada, com destaque para aqueles relacionados aos processos de planejamento estratégico empreendidos e aqueles que estabelecessem alguma diretriz, norma ou procedimento de segurança da informação.

Buscamos capturar a perspectiva das pessoas que atuam na organização pesquisada através de um conjunto de perguntas, que tanto poderia ser respondido por escrito, na forma de questionário, quanto verbalmente, numa entrevista presencial ou remota. A partir do registro dessas impressões, tentamos explicitar os pontos convergentes e divergentes entre o que preconiza a teoria e o que as pessoas afetadas esperam de uma Política de Segurança da Informação e Comunicação.

Adicionalmente, procuramos observar a conduta das pessoas no ambiente de trabalho, a fim de comparar, posteriormente, discurso e prática, se possível.

Como vamos tratar de informações que podem expor vulnerabilidades da organização pesquisada, serão omitidos os nomes da empresa, das pessoas e das unidades organizacionais que tenham sido citadas em qualquer parte integrante deste trabalho.

3.2 SELEÇÃO DOS SUJEITOS

Para formar um quadro que nos forneça subsídios para responder a pergunta desta pesquisa, consideramos importante mostrar a visão de pessoas que

pertençam a dois perfis básicos de profissionais que estariam envolvidos no processo de implantação de PSIC, caso o projeto viesse a ser estabelecido e implementado na organização escolhida. Assim, decidimos estabelecer o seguinte universo de respondentes:

- de dois a quatro representantes da equipe de TI da empresa que estariam diretamente envolvidos com o planejamento, implementação e manutenção da Política de Segurança da Informação e Comunicação;
- de dois a quatro representantes dos profissionais ligados à atividade fim da empresa, cuja atuação seria fortemente atingida pela implantação da PSIC.

Dentro de cada um desses perfis básicos, buscamos pessoas com tempo de atuação na organização, funções e experiência profissional e pessoal diferentes, a fim de expandir ao máximo possível a diversidade de perspectivas diante do mesmo contexto estudado.

Distribuídos os questionários, sete pessoas entregaram suas respostas, sendo quatro profissionais de TI e três profissionais ligados à atividade fim da empresa. No primeiro grupo, temos pessoas que trabalharam sempre na mesma unidade organizacional desde que chegaram à empresa. O perfil desses profissionais é descrito a seguir.

- Entrevistado 1 – Engenheiro com grande experiência em projeto, implantação e manutenção de redes de computadores; está na empresa há dezoito meses.
- Entrevistado 2 – Analista de Sistemas com experiência de vários anos em análise e desenvolvimento de sistemas e iniciando treinamentos na área de Segurança da Informação; está na empresa há vinte meses;
- Entrevistado 3 – Analista de Sistemas com mestrado na área de inteligência competitiva e atuação mais voltada para o tratamento da informação; está na empresa há seis anos.
- Entrevistado 4 – Analista de Sistemas com especialização em Ciência da Computação e histórico pregresso de atuação na área de administração de redes de computadores; atualmente integra equipe responsável pela elaboração do projeto de modernização dos sistemas de informação da empesa; está na empresa há oito anos e meio.

A seguir, as informações sobre os profissionais ligados à atividade fim que responderam o questionário:

- Entrevistado 5 – Analista com formação em Economia, atuou em diversas funções na empresa ao longo dos seus vinte e cinco anos de serviços prestados; atualmente está lotado na unidade organizacional responsável pelo planejamento corporativo.
- Entrevistado 6 – Analista com formação em Administração, atuou em várias unidades organizacionais ao longo dos seus sete anos e seis meses de serviços prestados; atualmente está trabalhando na análise e acompanhamento de operações de financiamento reembolsáveis.
- Entrevistado 7 – Analista com formação em Administração, ingressou na empresa como estagiário, passou a prestador de serviços contratado por empresa terceirizada e depois a empregado do quadro efetivo após aprovação e classificação em concurso público; na empresa há cinco anos (1,5 ano como empregado efetivo), trabalha com análise e acompanhamento de operações de capital de risco.

3.3 COLETA E ANÁLISE DE DADOS

O conjunto de perguntas utilizado para colher as impressões das pessoas diretamente envolvidas num processo de implantação de PSIC, que pode ser consultado no Anexo I, foi elaborado com o intuito de comparar duas visões marcadamente diferentes do mesmo processo, no mesmo ambiente tarefa.

Uma Política de Segurança da Informação e Comunicação abrange, além dos recursos de processamento da informação, ou seja: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem (ABNT, 2005), as pessoas que interagem com esses recursos, as quais são também consideradas ativos de informação.

Não seria surpreendente o surgimento de conflitos entre os profissionais que tem a responsabilidade de implementar os procedimentos e vigiar para que as diretrizes e normas descritas na PSIC sejam respeitadas e os profissionais que devem enquadrar seu comportamento a essas exigências.

Perguntamo-nos em quais pontos convergiriam e em quais divergiriam as opiniões desses atores; qual seria a diversidade, extensão e intensidade dessas

convergências e divergências. Acreditamos que essas informações serão de grande importância para mapear, tratar e prevenir os problemas que porventura emergirem da análise dos dados coletados.

O processo de melhoria contínua obedece a um ciclo virtuoso no qual as etapas de planejamento, implementação, monitoração e detecção de problemas e ação corretiva se sucedem num movimento infinito em busca eficácia e eficiência do sistema. Nosso desejo é que este trabalho sirva de subsídio para a melhoria dos processos de implantação de Políticas de Segurança da Informação e Comunicação, principalmente em empresas públicas brasileiras.

No decorrer da análise das entrevistas, tivemos dificuldade de formar um quadro abrangente das questões levantadas apenas pela leitura dos relatos. Dessa forma, buscamos uma forma de consolidar as opiniões sobre cada item do questionário em planilhas eletrônicas, o que se mostrou uma solução eficaz e nos possibilitou termos uma visão de conjunto de cada grupo de usuários, separados pelo perfil de atuação na empresa, bem como maior facilidade em compará-los entre si.

4 DESCRIÇÃO DO CASO

As respostas ao questionário e a consulta aos normativos a que tivemos acesso da empresa pesquisada revelaram que não existe processo formal de análise/avaliação de riscos ou documento que estabeleça um SGSI ou uma Política de Segurança da Informação e Comunicação, seja na base documental ativa ou inativa disponível.

Foi relatada uma iniciativa, originada na unidade organizacional responsável pela formulação e operacionalização dos processos de TI, situada no terceiro nível da hierarquia organizacional, no sentido de estabelecer convênio com uma instituição especializada no planejamento, projeto e execução do processo de implantação de sistemas de gestão de segurança da informação (SGSI), que culminaria no estabelecimento e implementação da PSIC dentro das especificações preconizadas nos documentos de boas práticas reconhecidos internacionalmente e na legislação que regulamenta os aspectos envolvidos no tema.

Infelizmente, a alta gestão da empresa em 2006 desistiu rapidamente da iniciativa diante do surgimento de um entrave jurídico no processo de celebração do convênio.

Outra iniciativa, também capitaneada diretamente pela unidade organizacional responsável pela TI, tentou contratar serviço de informação e sensibilização de pessoas para a necessidade do estabelecimento de controles de segurança da informação nas organizações e mesmo na vida pessoal de cada indivíduo. Esbarrou na falta de apoio da média gerência e da alta gestão da empresa em 2007.

Alguns controles existentes que pertencem à esfera de aplicação da Segurança da Informação foram citados pelos respondentes do questionário e encontrados em normativos que tratam especificamente do uso dos recursos de informática pelos usuários, empréstimo de equipamentos gerenciados pela área de TI, regulamentação do uso do correio eletrônico, guarda e descarte da documentação.

Entretanto, se comparados esses controles dispersos com o conjunto de controles identificados e descritos na norma como “Ponto de partida para a segurança da informação” (ABNT, 2005, p. xi) , podemos afirmar que a caminhada da organização rumo ao ambiente seguro que preconizam os manuais de boas

práticas, normativos e leis que tratam do tema, ainda está em seus primeiros passos.

No transcorrer da realização deste trabalho, a alta gestão da empresa apresentou o resultado do processo de planejamento estratégico, que resultou em uma nova missão, visão, perfil de atuação e valores institucionais; processo que, segundo os documentos que pudemos consultar e as pessoas envolvidas as quais tivemos acesso, contou com a participação efetiva das pessoas que se dispuseram a participar.

A análise da documentação produzida em esforços de planejamento estratégico anteriores aponta para uma fraca preocupação com requisitos de segurança fora das esferas financeira e contábil. Há referência ao tema, mas apenas como um registro e não como algo que tenha recebido realmente atenção no esforço de planejamento.

Os relatos dos respondentes demonstram indícios de que a alta gestão vem, nos últimos dois anos, sustentando iniciativas que, a continuarem sendo realizadas de forma combinada e sincronizada como ocorre até o momento em que escrevemos, levarão a uma profunda mudança nos processos da organização, na construção de sistemas de informação adequados a essa nova realidade que emergirá e, provavelmente, a um Sistema de Gestão da Segurança da Informação, no qual uma PSIC figura como um controle mandatório.

4.1 VISÃO DA TECNOLOGIA DA INFORMAÇÃO

A percepção sobre a Segurança da Informação pelos profissionais de TI da empresa foi, em geral, de insuficiência, provocada, segundo eles, principalmente pela inexistência de uma cultura de segurança na organização. Reclamam da baixa importância atribuída à segurança em geral e da informação em particular, tanto por parte da organização em si quanto das pessoas individualmente, que, por desconhecimento, expõem-se a riscos que poderiam ser reduzidos ou talvez eliminados pelo conhecimento e observação de procedimentos adequados.

Foram relatados vários fatores que concorrem para a formação dessa percepção, como:

- inexistência de qualquer processo de gerenciamento de riscos operacionais em funcionamento e nem previsão para seu estabelecimento e implementação;
- mecanismo de autenticação para uso dos sistemas corporativos não possui grau de segurança adequado;
- processos de trabalho não mapeados;
- inexistência de definição dos limites de cada nível gerencial em relação à sua legitimidade para autorizar mudanças de processos e sistemas, o que resulta em conflitos de toda ordem, inconsistências nos processos e sistemas, insegurança e instabilidade na atuação dos profissionais que operam esses processos e sistemas;
- a Segurança da Informação é tratada como assunto de responsabilidade única e exclusiva da unidade organizacional responsável pela formulação e operacionalização dos processos de TI;
- os aspectos de Segurança da Informação que não são diretamente relacionados com a Tecnologia da Informação são desprezados;
- inexistência de um Plano de Continuidade de Negócios;
- inexistência de uma unidade organizacional dedicada a propor, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Segurança da Informação (SGSI), conforme descrito na norma ABNT NBR ISO/IEC 27001:2006;
- inexistência de uma Política de Segurança da Informação abrangente e suficiente;
- inexistência de cultura de segurança, desde a alta gestão até as funções mais simples da organização;
- inexistência de um plano de comunicação e sensibilização das pessoas para a importância da Segurança da Informação em suas vidas, em qualquer ambiente onde transitem ou atuem.

Os comentários dos profissionais de TI sobre mecanismos disponíveis de Segurança da Informação chamam mais a atenção pela ausência ou pelo uso indevido do que pelo que está implementado e operando com estabilidade e confiabilidade.

As não conformidades em relação as boas práticas de Segurança da Informação relatadas pelos profissionais de TI revelam a necessidade de atuação imediata da alta gestão no sentido de solucionar os problemas mais graves que foram apontados.

- Compartilhamento de senhas – crime previsto no Artigo 325 do Código Penal;
- Ausência de uma referência corporativa para o tratamento de falhas e abusos no uso da informação corporativa, seus recipientes e/ou locais onde é armazenada;
- Exposição da unidade organizacional responsável pela formulação e operacionalização dos processos de TI a toda sorte de solicitações das demais unidades organizacionais, sem que haja uma referência normativa que delimite quem pode solicitar o quê e quem pode ter acesso ao quê e em que períodos de tempo pode ter o acesso liberado;
- Ausência de referência normativa que estabeleça delimitação de autoridade para os níveis gerenciais existentes e responsabilidades inerentes a cada função, causa sobrecarga na unidade organizacional que formula e operacionaliza os processos de TI, tendo em vista que qualquer abuso envolvendo recursos de TI, mesmo que secundariamente ou acessoriamente, são remetidos àquela unidade para providências;
- Ingresso e acesso às instalações físicas e ativos de informação da organização, seja em mídia tangível ou intangível, não recebem tratamento adequado de segurança;
- Intranet corporativa permite acesso indiscriminado ao conteúdo, expondo a organização a riscos de vazamento e/ou uso indevido de informações.

Sobre os mecanismos de segurança já implementados, os profissionais de TI alertaram para a possibilidade de prejudicarem a produtividade e a qualidade do trabalho dos usuários pelo exagero nas restrições de acesso a fontes de informações necessárias ao desempenho das atividades de alguns profissionais.

Mesmo naquilo que os profissionais de TI reconheceram como positivo, constata-se a precariedade dos controles de segurança da organização. A citação

da implementação recente de mecanismos de bloqueio de acesso ao sistema operacional ao final de quatro minutos de inatividade e a atualização automática da base de dados de antivírus e do sistema operacional nas estações de trabalho dos usuários finais também são indícios inequívocos do atraso da organização em relação aos recursos há muito disponíveis no mercado.

Com relação ao apoio da alta gestão, os profissionais de TI não falaram, em geral, dessa questão na organização em que trabalham, preferindo tratar do assunto genericamente e dentro dos requisitos descritos nas boas práticas.

A única pessoa que tratou da questão de forma específica, relatou tentativas anteriores no campo da Segurança da Informação em 2006 e 2007, mas que não foram a frente. Para essa pessoa, a atual Diretoria Executiva da empresa não demonstra qualquer interesse especial pelo tema.

Dentre aqueles que trataram da questão genericamente, todos reconheceram o apoio da alta gestão como fundamental para o sucesso do estabelecimento de uma PSIC, ressaltando que o exemplo da alta gestão no comprometimento com a PSIC é tão ou mais importante quanto a própria declaração de apoio, porque, por exemplo, é com base nele que os mecanismos de punição previstos para os transgressores das regras estabelecidas na PSIC terão sua sustentação e legitimidade.

O grande desafio que se coloca, então, é conscientizar os membros da alta gestão da importância da Segurança da Informação e conquistar seu apoio no discurso e na prática.

Da mesma forma que o apoio da alta gestão, tanto as ações de comunicação e sensibilização das pessoas para a necessidade da Segurança da Informação quanto o planejamento e execução de uma PSIC se caracterizam na organização pesquisada pela inexistência.

Como não houve até o presente momento um processo de implantação de PSIC na empresa, a avaliação sobre o impacto que esse processo poderia causar no desempenho das atividades profissionais se resumiu a um exercício de previsão dos impactos que poderiam acontecer.

Advertindo para a necessidade de coerência no processo de concepção e implantação, no geral os profissionais de TI projetaram uma fase de resistência no início do processo de implantação, motivada principalmente pela atitude natural do

ser humano de reagir defensivamente às mudanças no seu ambiente, seguida por um processo de aceitação e adaptação aos requisitos da PSIC e finalizando em um cenário em que as pessoas passariam a ser aliadas e defensoras da PSIC como consequência do reconhecimento dos benefícios que ela traria para suas vidas.

Ao responderem sobre a possível influência da implantação da PSIC no cumprimento da missão da organização, os profissionais de TI indicaram, em sua maioria, elementos positivos decorrentes de um processo de implantação de PSIC bem sucedido. Porém dividiram-se entre elencar pontos positivos na perspectiva do público externo, como aumento da credibilidade, qualidade dos resultados , melhoria da imagem, e pontos positivos na perspectiva do público interno, como maior agilidade na execução dos processos, aumento da eficiência nos processos, redução de riscos operacionais e redução do risco de incidentes de segurança e dos prejuízos decorrentes. Esses pontos citados poderiam também se encaixar como benefícios advindos do processo de implantação da PSIC.

Além de repetir alguns pontos elencados como influência da implantação da PSIC no cumprimento da missão da organização, também foram listados outros, entre os quais destacamos:

- redução do risco de interrupção dos processos de negócio;
- fortalecimento da imagem institucional;
- incremento da credibilidade, confiança e segurança;
- incremento da capacidade de identificação de falhas;
- aperfeiçoamento dos mecanismos de registros, controles e documentações;
- processos baseados em boas práticas estabelecidas;
- Agilização dos resultados.

Ainda segundo esses profissionais, o conhecimento das diretrizes, normas e procedimentos associados à PSIC servem de referência para a definição de novos processos e sistemas ou revisão dos já existentes, visando mitigar riscos, além de guiar o comportamento no uso dos recursos, ferramentas e espaços disponíveis na empresa.

Ao considerar um processo de elaboração e implantação bem sucedido, os profissionais de TI não conseguiram vislumbrar muito mais prejuízos causados pelo processo de implantação da PSIC do que um possível aumento da burocracia nos

processos, tendo em vista a inclusão de controles necessários para garantir que os requisitos de segurança sejam obedecidos. Mesmo assim, previram que o aumento da eficiência e do desempenho operacional compensariam qualquer pequeno acréscimo de tempo proveniente da inclusão dos controles necessários à PSIC.

Além desse provável aumento na burocracia, o único inconveniente citado foi a possibilidade de exagero na dose de restrições de acesso a fontes de informação e/ou ferramentas de compartilhamento e colaboração e a consequente perda de produtividade e qualidade no trabalho.

A reação das pessoas à implantação da PSIC foi, em certa medida, antevista na avaliação dos profissionais de TI sobre o impacto da implantação da PSIC na organização.

Novamente é mencionada a natural resistência do ser humano às mudanças em seu ambiente, que deve ser prevenida com as campanhas de informação e sensibilização, além da sinalização clara da alta gestão de que as regras da PSIC são universais e sua validade é garantida.

A clareza dos objetivos, aliada a campanhas contínuas de esclarecimento e sensibilização das pessoas e à constatação dos benefícios gerados transformarão, na visão desses profissionais, pessoas resistentes em aliadas e defensoras da PSIC.

Quando se pediu para dar dicas sobre como implantar uma PSIC com sucesso em uma empresa pública, o resultado foi um resumo dos requisitos descritos nos documentos de boas práticas em Segurança da Informação.

O conjunto de dicas apresentado por um dos respondentes resume bem o que foi apresentado globalmente nesse item.

- Conquistar apoio da alta gestão;
- Levantar os meios de circulação das informações na empresa;
- Definir os aspectos a serem tratados na PSIC, considerando a maior amplitude possível;
- Definir a necessidade de conhecer de cada função/pessoa relativa a cada tipo de informação;
- Categorizar as informações e seus meios de circulação;
- Definir políticas de maneira clara e simples de serem compreendidas e executadas;

- Estabelecer políticas que sejam de abrangência geral em sua aplicação;
- Capacitar pessoas envolvidas no estabelecimento da PSIC a esclarecer os motivos e objetivos do processo;
- Garantir a transparência das informações relativas ao estabelecimento da PSIC;
- Estimular e cobrar o comprometimento com a implantação da PSIC;
- Estabelecer mecanismos de monitoração e acompanhamento da implantação da PSIC;
- Estabelecer mecanismos de apresentação dos resultados do processo de implantação da PSIC;
- Reconhecer e valorizar a participação e o comprometimento das pessoas no processo de implantação da PSIC;
- Estabelecer previamente mecanismos claros de punição para os casos de descumprimento da PSIC;
- Vincular a PSIC a um Plano de Continuidade de Negócios estabelecido;
- Rever e atualizar a PSIC periodicamente.

4.2 VISÃO DO NEGÓCIO

Com relação à percepção de Segurança da Informação por profissionais cuja atuação está diretamente relacionada ao negócio da organização, consideram pontos negativos a falta de importância e a ausência de orientações relacionadas ao tema, destacando, também, que o trânsito indiscriminado de informações a bordo de dispositivos removíveis de armazenamento, como CD, DVD e *pen drives*, além de cópias impressas, apontam para a necessidade de colocar as pessoas no foco das atenções sobre Segurança da Informação, já que o rastreamento do deslocamento desse conteúdo por meio tecnológico é, até onde se conhece, impossível.

A incidência de mensagens indesejáveis (spam) é também citada como um indício de que a segurança não é suficiente e expõe a organização e as pessoas a riscos indesejáveis.

Para esses profissionais, os mecanismos existentes para garantir a Segurança da Informação não são suficientes para dar conta da necessidade da organização. Em favor dessa afirmação, argumentam que é permitido livre trânsito de pessoas estranhas a ambientes onde informações sensíveis estão depositadas

sobre as mesas de trabalho; relatam episódios de perda de dados que deveriam estar seguros nos servidores corporativos mas se perderam assim mesmo; queixam-se de que os mecanismos de Segurança da Informação consideram o usuário como adversário da sua implementação e não como parceiro, como deveria ser.

Também é relatado que os critérios de aplicação dos mecanismos de Segurança da Informação não são divulgados adequadamente, impossibilitando que as pessoas tomem conhecimento de como devem proceder e como se adaptar ou relatar mal funcionamento dos mesmos, e que o exagero na restrição de acesso às fontes de informação prejudicam a produtividade do trabalho, quebrando o ritmo constantemente pela necessidade de solicitar liberação de acesso, através de um processo demorado e precário.

As respostas desses profissionais sobre o apoio da alta gestão à implantação de uma PSIC levam a crer que, assim como mecanismos de comunicação e sensibilização e planejamento e execução da PSIC, ele não existe.

Um dos profissionais comenta que as únicas comunicações recebidas que remetem a eventos de segurança são mensagens de correio eletrônico dando conta do desaparecimento ou extravio de documentos ou pastas inteiras, ou sobre uso de senhas na rede de computadores.

O mesmo profissional lista alguns requisitos que considera importantes de serem levados em conta num processo de planejamento e execução de uma PSIC: envolvimento dos principais afetados; coordenação a cargo de consultores experientes em Segurança da Informação e gestão de mudanças. Adicionalmente, afirma que a implementação dos processos e ferramentas para certificação e assinatura digital deveriam ser estabelecidos e implementados imediatamente e declara sua crença de que o processo de implantação de uma PSIC alteraria bastante a rotina de trabalho das pessoas.

Para esses profissionais, o impacto da implantação de uma PSIC na sua produtividade e da organização será sentido na forma de uma queda inicial no primeiro momento, mas com recuperação e melhoria provocada pela migração de processos realizados através de meio físico para meio eletrônico, chegando a um ganho significativo de qualidade nesses processos.

Entretanto, chamam a atenção para o perigo de visões equivocadas transformarem potenciais benefícios em problemas a serem superados. O perigo,

segundo essa visão, é de que restrições exageradas de segurança possam comprometer o tempo de realização das atividades. Nessa perspectiva, restrição de acesso é o mesmo que restrição de produtividade, se essa restrição for arbitrária e sem transparência dos critérios de aplicação.

Sobre a influência que teria a implantação de uma PSIC no cumprimento da missão da organização, também existem visões variadas. Há o que enxerga a oportunidade de levar a empresa a um patamar mais elevado de atuação, mas também há o que projeta dois possíveis cenários; no primeiro, a perspectiva é positiva e o cumprimento da missão é facilitado pela internalização da responsabilidade sobre a informação, aumentando a precisão dos resultados das atividades; por outro lado, na perspectiva negativa, o aumento de complexidade pode comprometer a produtividade e o cumprimento da missão da organização.

A perspectiva positiva percebida na avaliação do impacto da implantação de uma PSIC na produtividade da organização se reproduz na avaliação dos benefícios da implantação de uma PSIC: aumento da produtividade pela migração de alguns processos que se utilizam meio físico e passariam a utilizar meio eletrônico. A garantia de confidencialidade da informação manipulada também é citada como benefício da PSIC.

Como prejuízos advindos de um processo de implantação de PSIC, o tempo de adaptação aos novos processos e a possibilidade de rigidez ou complexidade exagerada são apresentados como possíveis vilões.

Quanto a reação das pessoas à implantação da PSIC, acredita-se que existe uma resistência natural do ser humano a mudanças nas suas rotinas de trabalho, mas aposta-se que a PSIC é importante para a maioria das pessoas na empresa.

Chegando às dicas que esses profissionais dariam para empresas públicas que desejassem implantar uma PSIC, temos:

- buscar o equilíbrio entre garantia de segurança e produtividade do trabalho;
- foco deve recair no como implementar sem alimentar a resistência natural às mudanças em benefício da excelência técnica;
- perseverança no apoio da alta gestão ao processo;
- conquistar o usuário para o lado dos formuladores;
- combater o mito de que o usuário é o problema;

- afirmar que o problema é o mau uso da informação e que ninguém está livre de errar;
- conscientização é a chave para evitar problemas futuros;
- distribuir responsabilidade a todos;
- exercer punição aos infratores;
- implantar mecanismos que não prejudiquem os que trabalham;
- não colocar limites em quem mal utiliza os recursos de informática.

5 ANÁLISE DO CASO

Comparando o cenário desenhado pelos profissionais da empresa com as boas práticas recomendadas para a gestão da segurança da informação, conforme visto no capítulo 2, constatamos a inexistência de um SGSI e de uma PSIC. Os processos que produzirão as referências para o estabelecimento desses (planejamento estratégico, levantamento e redesenho de processos etc.) ainda estão em andamento e não foi atribuída importância estratégica, até onde pudemos acompanhar, ao tema Segurança da Informação.

A necessidade de identificação e classificação dos ativos da organização e do estabelecimento do processo de análise/avaliação de riscos não está apontada claramente nos documentos produzidos e nas ações priorizadas no âmbito do processo de planejamento estratégico. As respostas ao questionário apontam para a não existência de conscientização dos membros da organização quanto às necessidades de estruturação e ao cronograma de estabelecimento dos sistemas de gestão recomendados nos documentos de boas práticas que balizam a conquista da qualidade na gestão do negócio e da segurança da informação.

Nos diálogos travados e nas respostas ao questionário dos profissionais de TI, pudemos perceber a frustração com a falta de apoio da alta gestão ao estabelecimento de uma PSIC e com as iniciativas malogradas em 2006 e 2007, a ansiedade pela obtenção do apoio e comprometimento da alta gestão atual com o estabelecimento de uma PSIC alinhada com o resultado do novo Planejamento Estratégico, o receio de ver suas expectativas serem enterradas por mais uma troca de comando motivada pelo resultado das eleições presidenciais de 2010.

Esse cenário é preocupante, tendo em vista que o apoio da direção da organização é pré-requisito para o estabelecimento de qualquer sistema de gestão, conforme pudemos ver no item 2.3.2.

É patente o conhecimento que esses profissionais possuem sobre o tema Segurança da Informação e o baixo grau de dificuldade que teriam em contribuir decisivamente para a implantação de um Sistema de Gestão de Segurança da Informação (SGSI) e de uma Política de Segurança da Informação e Comunicação (PSIC). Contudo, também é claro que a situação dessa organização no que se refere à Segurança da Informação é preocupante e paradoxal em relação às

diretrizes do Governo Federal sobre a Segurança da Informação nos órgãos da administração direta e indireta.

A falta de persistência das gestões anteriores e a falta de apoio da alta gestão atual ao projeto de estabelecimento e implementação de um SGSI na organização pode significar ignorância ou falta de compromisso com o futuro da organização. Como são relatadas iniciativas recentes de planejamento estratégico e de modernização dos sistemas de informação, o primeiro caso parece ser o mais provável, tendo em vista que deixar de dar atenção aos apelos recorrentes da unidade organizacional responsável pela formulação e operacionalização dos processos de TI revela certo grau de desconhecimento das desastrosas consequências que podem advir dessa postura.

Não cabe aqui repetir as medidas necessárias para colocar a empresa no rumo do estabelecimento de um SGSI, seguindo as boas práticas consagradas em normativos de aplicação mundial, uma vez que já foram suficientemente levantadas e reafirmadas pelos próprios profissionais de TI da organização pesquisada.

6 **CONCLUSÃO**

A análise da situação atual da organização alvo deste estudo de caso confirma o que as boas práticas consagram: a atitude da direção de uma organização influencia decisivamente no que ela é, na construção da sua cultura, no ânimo das pessoas que nela trabalham, na imagem que dela tem a sociedade. Mais do que tudo, define se ela realizará seu potencial ou se perderá o rumo e se entregará à entropia.

No caso dessa empresa pública, a oportunidade para a correção de rumo está dada e, se a direção assim o quiser, colocará seus sistemas de gestão no caminho das boas práticas e de uma atuação cada vez mais positiva e benéfica para a sociedade.

O grande desafio, em nossa visão, é chegar a resultados o mais aproximados possível da realidade, a partir da realização da auto-análise e da análise da sua relação com o ambiente, no processo de planejamento estratégico. As conclusões e ações que daí emergirão serão a referência para a identificação e classificação dos ativos do negócio, do estabelecimento do processo de gestão de riscos etc., seguindo as recomendações consagradas para a melhoria contínua dos resultados dos seus sistemas de gestão.

6.1 PRINCIPAIS CONTRIBUIÇÕES

Consideramos que a evidenciação de que o despreparo e/ou a falta de compromisso da direção pode ser a origem da ausência de uma cultura de segurança da informação solidamente estabelecida nas instituições públicas, tendo em vista que essa condição e/ou atitude faz com que o trabalho de conscientização não aconteça, a principal contribuição deste trabalho.

Como ficou claro pela consolidação das respostas dos questionários, mesmo quando os profissionais que atuam diretamente com Tecnologia de Informação nessas instituições possuem formação e estão conscientes da necessidade do estabelecimento de um SGSI e motivados para trabalhar nesse sentido, isso não é suficiente para que isso aconteça.

Mesmo com ressalvas, os profissionais que atuam mais diretamente com o negócio da instituição também sentem falta de diretrizes claras e de referências

sobre como agir para garantir a segurança da informação no desempenho das suas funções.

Trazer à tona a diferenciação entre os pontos de vista de dois perfis de pessoas que são comuns a todas as organizações, públicas ou privadas, sobre o tema da Segurança da Informação, mostrando seus anseios, dúvidas, frustrações e esperanças, também se mostrou um caminho profícuo e portador de um potencial que merece ser mais e melhor explorado.

6.2 TRABALHOS FUTUROS

Acreditamos que o acompanhamento da evolução dos processos de planejamento estratégico, levantamento e redesenho de processos e modernização da infraestrutura de sistemas de informação serão de grande valia para formar um quadro realista sobre a disposição da direção dessa organização em estabelecer e consolidar a cultura de segurança da informação, através do estabelecimento de um SGSI como parte do sistema de gestão do negócio.

Nesse sentido, uma pesquisa longitudinal deverá ser empreendida nos próximos anos, focando não apenas os processos específicos de um SGSI, mas também os processos de gestão do negócio.

REFERÊNCIAS

CHIAVENATO, Idalberto. **Administração: teoria, processo e prática**. Rio de Janeiro: Elsevier, 2007. 4.ed.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2006.

_____. **NBR ISO/IEC 27001**: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro, 2006.

MITNICK, Kevin D.; SIMON, Willian L. **A Arte de Enganar**. São Paulo: Pearson Makron Books, 2003.

DECRETO N° 3.505, DE 13 DE JUNHO DE 2000.

LEI N° 8.183, DE 11 DE ABRIL DE 1992, com a redação dada pela MEDIDA PROVISÓRIA N° 2.216-37, DE 31 DE AGOSTO DE 2001.

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

ANEXO I

Questionário para levantamento de impressões dos colaboradores da empresa sobre o processo de implantação da Política de Segurança da Informação e Comunicação.

QUESTIONÁRIO PARA LEVANTAMENTO DE IMPRESSÕES
SOBRE A IMPLANTAÇÃO DA POLÍTICA DE
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

PERFIL DO ENTREVISTADO:
Cargo que ocupa:
Tempo na empresa:
Tempo no cargo:

PERGUNTAS:

1. Qual é a sua percepção sobre a segurança da informação no seu dia-a-dia?

2. Você considera os mecanismos de segurança da informação da empresa suficientes? Por quê?

3. Discorra sobre o apoio da alta gestão da empresa ao projeto de implantação da PSIC.

4. Como está sendo o processo de comunicação e sensibilização direcionado aos colaboradores da empresa, visando conquistar sua adesão ao projeto de implantação da PSIC?

5. Como você avalia o planejamento e a execução, se for o caso, do projeto de implantação da PSIC?

6. Após terminado o projeto de implantação da PSIC, considerando os mecanismos de segurança adotados ou a serem adotados, como você avalia o potencial impacto na produtividade do seu trabalho e a dos outros colaboradores da empresa?

7. Em sua opinião, qual será a influência da implantação da PSIC no cumprimento da missão da empresa?

8. Em sua opinião, quais foram ou serão os principais benefícios resultantes do processo de implantação da PSIC para o desempenho das suas atividades profissionais?

9. Em sua opinião, quais foram ou serão os principais prejuízos resultantes do processo de implantação da PSIC para o desempenho das suas atividades profissionais?

10. Em sua opinião, como as pessoas em geral reagiram, estão reagindo ou reagirão à implantação da PSIC na empresa?

11. Quais dicas você daria para uma empresa pública que esteja planejando implantar uma PSIC?