Universidade Presbiteriana Mackenzie

Centro de Ciências Sociais e Aplicadas

Programa de Pós-Graduação em Ciências Contábeis

Segurança da Informação: Um Estudo Sobre a Percepção do Usuário da Informação Contábil

Wagner Lima da Silva

São Paulo

2011

Wagner Lima da Silva

Segurança da Informação: Um Estudo Sobre a Percepção do Usuário da Informação Contábil

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Contábeis da Universidade Presbiteriana Mackenzie para a obtenção do título de Mestre em Controladoria Empresarial.

Orientador: Prof. Dr. Gilberto Perez

São Paulo

2011

Reitor da Universidade Presbiteriana Mackenzie

Prof. Dr. Benedito Guimarães Aguiar Neto

Decano de Pesquisa e Pós-Graduação

Prof. Dr. Moisés Ari Zilber

Diretor do Centro de Ciências Sociais e Aplicadas

Prof. Dr. Sérgio Lex

Coordenadora do Programa de Pós-Graduação em Ciências Contábeis

Profa. Dra. Maria Thereza Pompa Antunes

FICHA CATALOGRÁFICA

S586s Silva, Wagner Lima da.
Segurança da informação: um estudo sobre a percepção do usuário da informação contábil / Wagner Lima da Silva – 2011.
92 f. : il. ; 30 cm

Dissertação (Mestrado em Controladoria Empresarial) – Universidade Presbiteriana Mackenzie, São Paulo, 2011.
Orientação: Prof. Gilberto Perez
Bibliografia: f. 82-86.

1. Segurança da informação. 2. Informação contábil. 3. Percepção do usuário. I. Título.

CDD 658.151

A nova fonte de poder não é o dinheiro nas mãos de poucos, mas a informação nas mãos de muitos.

John Naisbitt

AGRADECIMENTOS

Agradeço a Deus e a Nossa Senhora Aparecida, a quem sempre elevo meus pensamentos nos momentos de alegria, tristeza e dificuldade.

Aos meus pais, Deracy e Maria, meus exemplos de vida, a quem devo tudo que sou.

As minhas irmãs, Claudia e Rose, pelo apoio e atenção que sempre tiveram comigo.

À minha namorada Adriana, pelo apoio, incentivo e compreensão durante este período de dedicação ao mestrado.

Aos amigos e professores do Programa de Pós-Graduação em Ciências Contábeis da Universidade Presbiteriana Mackenzie, pelos valiosos ensinamentos e experiências compartilhadas.

Ao meu orientador Prof. Dr. Gilberto Perez, pelo apoio e ensinamentos prestados durante o desenvolvimento deste trabalho.

Gostaria também de agradecer aos professores Marco Antonio Figueiredo Milani Filho e Fernando Carvalho de Almeida, pela disponibilidade e importantes contribuições dadas no exame de qualificação.

RESUMO

A segurança da informação se tornou um problema que atinge as organizações, uma vez que coloca em risco a continuidade dos negócios. Sendo a contabilidade a área responsável por consolidar todas as informações da organização, torna-se relevante avaliar a percepção dos usuários da informação contábil a respeito do tema. Esta pesquisa, com base na revisão da literatura, identificou seis construtos de segurança da informação (Integridade, Disponibilidade, Confidencialidade, Equipamentos, Políticas e Procedimentos e Pessoas). Estes construtos foram utilizados em um questionário eletrônico do tipo *survey*, em que uma amostra composta por 129 usuários da informação contábil de diversas organizações brasileiras forneceram a sua percepção a respeito da segurança da informação. Estes dados possibilitaram a realização de uma análise de *gap* que consistiu na comparação das médias de avaliação (como o respondente avalia a segurança da informação na sua organização) e importância (o quanto o respondente considera a segurança da informação importante) atribuída a cada construto de segurança da informação. Como resultado, constatou-se a existência de *gaps* estatisticamente significativos para todos os seis construtos de segurança da informação estudados, evidenciando que as organizações estão atribuindo menor importância ao tema do que o esperado pelos respondentes. Os usuários da informação contábil estão conscientes da importância da segurança da informação e demonstraram estarem insatisfeitos com os equipamentos, políticas e procedimentos utilizados para garantir a segurança da informação nas organizações. O construto Pessoas apresentou o maior *gap* desta pesquisa, sugerindo que as organizações enfrentam dificuldades para controlar o componente humano na segurança da informação, e as pessoas não estão conscientes da importância do seu papel para a eficácia da segurança da informação nas organizações. Os resultados desta pesquisa sugerem que os gestores devem direcionar seus esforços na conscientização dos funcionários e na implantação de políticas e procedimentos de segurança, objetivando a instituição da cultura de segurança da informação na organização.

Palavras-chave: Segurança da informação, informação contábil, análise de *gap*, percepção do usuário.

ABSTRACT

Information security has become an issue that reaches the organizations, once it puts at risk the continuity of the businesses. As the accounting is the responsible area for consolidating all the information of the organization, it becomes relevant evaluate the perception of users of accounting information regarding the subject. This research, on the basis of literature review identified six constructs of information security (Integrity, Availability, Confidentiality, Equipment, Policies and Procedures and People). These constructs had been used in a survey electronic questionnaire, where one sample composed by 129 users of accounting information from various Brazilian organizations provided their perceptions regarding information security. These data allowed the realization of a gap analysis which consisted in comparing the means of assessment (how the respondent evaluates information security in your organization) and importance (how much the respondent considers information security important) attributed to each construct of information security. As a result, it was evidenced the existence of statistically significant gaps for all the six constructs of information security checked, showing that the organizations are giving less importance to the matter than expected by respondents. The users of accounting information are aware of the importance of information security and had shown to be unsatisfied with the equipment, policies and procedures used to guarantee the information security in the organizations. People construct presented the largest gap of this research, suggesting that the organizations face difficulties to control the human component in information security, and people are not aware of the importance of their role in the effectiveness of information security in the organizations. The research findings suggest that managers should focus their efforts on employee awareness and implementation of security policies and procedures, aiming at the establishment of information security culture in the organization.

Keywords: Information security, accounting information, gap analysis, user's perception.

SUMÁRIO

1. INTRODUÇÃO 14
1.1. Contextualização do Tema 15
1.2. Questão de Pesquisa 18
1.3. Hipóteses de Pesquisa 19
1.4. Objetivo Geral 20
1.5. Objetivos Específicos 20
1.6. Justificativas e Contribuições 21
2. REFERENCIAL TEÓRICO 22
2.1. Informação 22
2.2. Informação Contábil 22
2.3. Sistemas de Informação 25
2.4. Sistemas de Informação Contábil 26
2.5. Segurança da Informação 27
2.6. Abordagens não Tecnológicas da Segurança da Informação 34
2.7. Fatores Críticos de Sucesso da Segurança da Informação 39
2.8. Melhores Práticas em Segurança da Informação 41
2.9. Segurança da Informação Contábil 46
2.10. Teoria da Percepção 49
3. PROCEDIMENTOS METODOLÓGICOS 52
3.1. Tipo de Pesquisa 52
3.2. Método de Pesquisa 53
3.3. População e Amostra 53
3.4. Procedimentos de Coleta de Dados 54
3.4.1. Elaboração do Instrumento de Coleta de Dados 55
3.4.2. Coleta de Dados 58
3.5. Procedimentos de Tratamento de Dados 58
3.5.1. Análise de *Gap* 59
3.5.2. Técnicas Estatísticas 59
3.5.3. Coeficiente Alfa de Cronbach 60
3.5.4. Teste de Wilcoxon para Amostras Pareadas 61

4. APRESENTAÇÃO E ANÁLISE DOS RESULTADOS 62
4.1. Caracterização da Amostra 62
4.2. Validação dos Construtos de Segurança da Informação 66
4.3. Análise de *Gap* 70
4.3.1. Construto Integridade 70
4.3.2. Construto Disponibilidade 71
4.3.3. Construto Confidencialidade 72
4.3.4. Construto Equipamentos 72
4.3.5. Construto Políticas e Procedimentos 73
4.3.6. Construto Pessoas 74
4.3.7. Resumo da Análise de *Gap* 74
4.3.8. Análise das Diferenças de Percepção 77
5. CONCLUSÃO 79
REFERÊNCIAS 82
APÊNDICES 87

LISTA DE FIGURAS

Figura 1 – Evolução dos Incidentes de Segurança da Informação 16
Figura 2 – Obstáculos para Implantação da Segurança da Informação 17
Figura 3 – Motivação dos Gastos com Segurança da Informação 17
Figura 4 – Modelo Adotado na Pesquisa 19
Figura 5 – Componentes dos Sistemas de Informação 25
Figura 6 – Objetivos da Segurança da Informação 30
Figura 7 – Construtos de Segurança da Informação 32
Figura 8 – Ameaças à Segurança da Informação Contábil 46
Figura 9 – Fatores que Influenciam a Percepção 50
Figura 10 – Avaliação e Importância por Construto 76

LISTA DE QUADROS

Quadro 1 – Construtos de Segurança da Informação 55
Quadro 2 – Variáveis Utilizadas na Pesquisa 56
Quadro 3 – Resultado do Teste das Hipóteses 77

LISTA DE TABELAS

Tabela 1 – Distribuição dos Respondentes por Nível de Escolaridade e Formação 63
Tabela 2 – Distribuição dos Respondentes por Área de Atuação e Cargo 63
Tabela 3 – Distribuição dos Respondentes por Tempo de Empresa 64
Tabela 4 – Distribuição das Empresas por Segmento e Tempo de Atuação 64
Tabela 5 – Distribuição das Empresas por Número de Funcionários 65
Tabela 6 – Distribuição das Empresas por Sistema Corporativo Utilizado 65
Tabela 7 – Teste de Confiabilidade - Construto Integridade 66
Tabela 8 – Teste de Confiabilidade - Construto Disponibilidade 67
Tabela 9 – Teste de Confiabilidade - Construto Confidencialidade 67
Tabela 10 – Teste de Confiabilidade - Construto Equipamentos 68
Tabela 11 – Teste de Confiabilidade - Construto Políticas e Procedimentos 68
Tabela 12 – Teste de Confiabilidade - Construto Pessoas 69
Tabela 13 – Alfa de Cronbach dos Construtos de Segurança da Informação 69
Tabela 14 – Teste Pareado de Amostras - Construto Integridade 71
Tabela 15 – Teste Pareado de Amostras - Construto Disponibilidade 71
Tabela 16 – Teste Pareado de Amostras - Construto Confidencialidade 72
Tabela 17 – Teste Pareado de Amostras - Construto Equipamentos 73
Tabela 18 – Teste Pareado de Amostras - Construto Políticas e Procedimentos 73
Tabela 19 – Teste Pareado de Amostras - Construto Pessoas 74
Tabela 20 – Resumo do *Gap* por Construto 75
Tabela 21 – *Gap* por Cargo do Respondente 78
Tabela 22 – *Gap* por Tamanho da Empresa 78

1. INTRODUÇÃO

O uso dos sistemas de informação e da internet para a realização das mais diversas atividades se tornou um recurso indispensável para sociedade e para a economia mundial. Os recursos tecnológicos proporcionam inúmeros benefícios, contudo, é importante lembrar que esse universo digital está sujeito a várias formas de ameaças, físicas ou virtuais, que podem comprometer a segurança da informação nas organizações.

Segundo Kayworth e Whitten (2010), nenhuma solução ou mecanismo tecnológico é suficiente para garantir a eficácia da segurança da informação nas organizações, pois esta eficácia só pode ser atingida através da aplicação de uma estratégia corporativa de segurança que envolva aspectos técnicos e sociais.

Neste contexto, os problemas relacionados à segurança da informação estão cada vez mais evidentes no cenário mundial. O ataque às torres gêmeas no dia 11 de setembro de 2001 comprometeu a atividade de diversas empresas que mantinham suas cópias de segurança na torre vizinha (que também desmoronou), evidenciando a necessidade de práticas de segurança da informação para garantir a continuidade dos negócios (EXAME, 2001). Alguns casos no Brasil, como o vazamento de informações de candidatos nas Eleições 2010 (ESTADO, 2010) e a fraude contábil do Banco Panamericano em 2011 (FOLHA, 2011), trazem indícios de que o tema ainda não é tratado com a devida relevância pelas organizações brasileiras.

Na contabilidade o cenário não é diferente, uma vez que na maioria das organizações as informações contábeis são captadas, processadas e armazenadas através de sistemas computadorizados (HERATH, 2011). Segundo Moscove, Simkin e Bagranoff (2002), a contabilidade é o principal produtor e distribuidor de informações da organização. Desta forma, as vulnerabilidades e ameaças nas quais os sistemas de informação estão expostos se apresentam como uma limitação à integridade das informações contábeis que são apresentadas e utilizadas pelos usuários.

De acordo com Abu-Musa (2006), muitas organizações não se preocupam com a segurança dos sistemas contábeis até que aconteça algum acesso não autorizado, modificação, alteração ou destruição de informações críticas. Desta forma, torna-se relevante avaliar a percepção dos usuários da informação contábil a respeito da segurança da informação nas organizações.

1.1. Contextualização do Tema

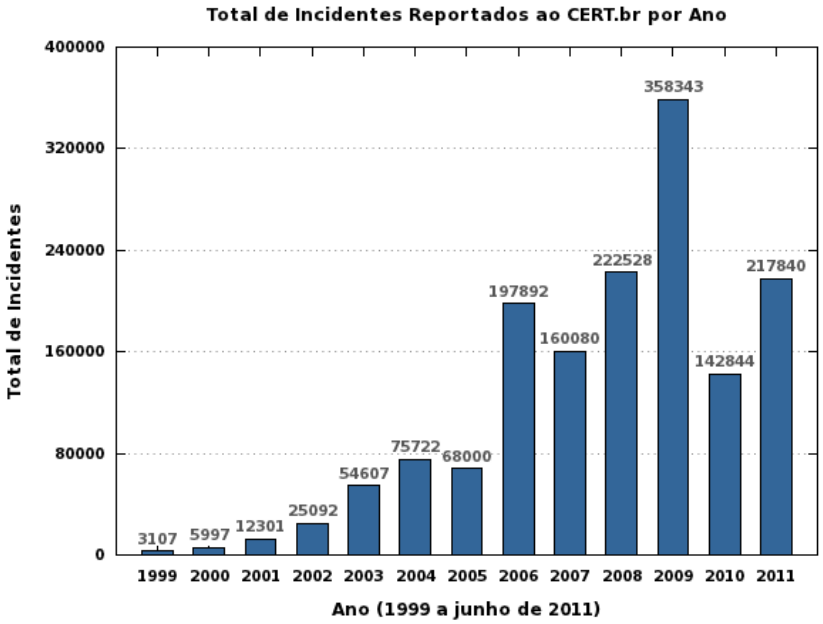
Atualmente, os sistemas de informação são considerados uma ferramenta essencial e estão presentes em quase todas as atividades de uma organização (PEREZ, 2006). Os recursos computacionais são utilizados para a realização das mais variadas tarefas, com o objetivo de proporcionar maior velocidade e controle nos processos das empresas. Adicionalmente, com a popularização da internet, as transações eletrônicas que são realizadas entre empresas, clientes e órgãos governamentais, se tornaram um recurso indispensável para a realização de negócios.

De acordo com Knapp et al. (2007), as organizações perceberam que a tecnologia da informação é essencial não somente para as operações diárias, mas também para obter vantagem competitiva no mercado. Desta forma, a importância da tecnologia da informação fez com que a segurança da informação também se tornasse importante, uma vez que, incidentes envolvendo segurança da informação podem resultar em processos judiciais, prejuízos financeiros, danos à marca, perda de confiança dos clientes e parceiros de negócios, entre outros riscos.

Neste contexto, a informação se apresenta como um ativo importante e valioso para as organizações, devendo ser protegida adequadamente. Para Marciano (2006), o grau de valor e de relevância conferido à segurança da informação pela organização deve estar diretamente relacionado ao grau dos mesmos conceitos quanto aplicados à informação. Segundo Jourdan et al. (2010), apesar do crescente número e variedade de ameaças à segurança da informação, muitas organizações continuam a negligenciar a implementação de políticas e procedimentos de segurança da informação.

Nos últimos anos, tem-se observado uma tendência crescente em incidentes de segurança da informação, tanto na esfera pessoal como corporativa. É comum o recebimento e envio de *e-mails* maliciosos, que tem por objetivo capturar senhas de contas bancárias, números de cartão de crédito, entre outras informações relevantes e passíveis de fraude. A Figura 1 apresenta a evolução dos incidentes de segurança da informação reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2011).

Figura 1 – Evolução dos Incidentes de Segurança da Informação



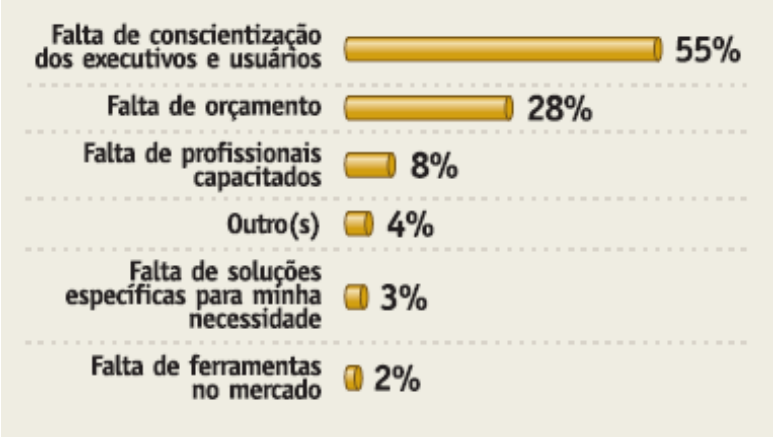
Fonte: CERT, 2011

No ambiente corporativo, as conseqüências dos problemas envolvendo segurança da informação são ainda maiores. Em 11 de setembro de 2001, quando as torres gêmeas do World Trade Center em New York foram alvo de ataques terroristas, muitas das 430 empresas sediadas no local adotavam como estratégia de contingência a manutenção de cópias de segurança na torre vizinha. Como as duas torres foram atacadas quase que simultaneamente, o plano de contingência não pode ser acionado, comprometendo a continuidade de negócio destas empresas (EXAME, 2001).

Em 2011 presenciou-se no Brasil um caso de fraude contábil envolvendo valores superiores a R$ 4 bilhões, o caso do Banco Panamericano. Segundo Celso Antunes da Costa, diretor superintendente da instituição, os sistemas contábeis e de controle do Banco Panamericano eram corrompidos, de modo que a maior parte dos processos fraudulentos funcionava de forma automatizada pelos sistemas de informação (FOLHA, 2011).

De acordo com Carvalho (2003), os executivos consideram a segurança da informação como um fator crítico para a garantia de continuidade do negócio, porém não conseguem defender perante a alta direção das empresas o orçamento necessário para implantação de um sistema de gestão de segurança da informação compatível com o nível de risco com o qual as empresas estão sujeitas. Tal fato também pode ser observado na 10ª Pesquisa Nacional de Segurança da Informação (MÓDULO, 2006), a qual evidenciou os principais obstáculos para implantação da segurança da informação nas organizações, conforme apresentado na Figura 2.

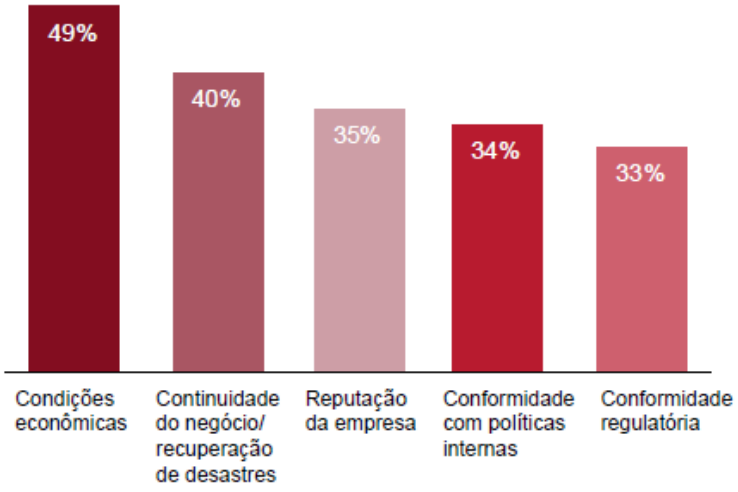
Figura 2 – Obstáculos para Implantação da Segurança da Informação



Fonte: Módulo, 2006

Os resultados da 8ª Pesquisa Global de Segurança da Informação (PWC, 2011) demonstraram os fatores que direcionam os gastos com segurança da informação nas empresas. Conforme apresentado na Figura 3, pode-se observar que condições econômicas foram indicadas por 49% dos respondentes, seguida da necessidade de continuidade de negócios e recuperação de desastres que foi citada por 40% dos pesquisados. Os executivos da área de segurança da informação informaram que suas empresas também sofrem com a contenção de investimentos e despesas operacionais, o que em muitos casos, resulta na perda ou degradação de algumas competências fundamentais da segurança da informação. Neste contexto, pode-se deduzir que os investimentos em segurança da informação são influenciados pela situação econômica da empresa, podendo muitas vezes ser negligenciado em detrimento a investimentos julgados mais importantes ou prioritários aos negócios.

Figura 3 – Motivação dos Gastos com Segurança da Informação



Fonte: PWC, 2011

Desta forma, fica evidente que a segurança da informação se tornou um problema que atinge todas as organizações, colocando em risco a continuidade dos negócios. Adicionalmente, a segurança da informação não pode ser considerada um problema meramente técnico, pois os recursos tecnológicos não são suficientes para proteger as organizações das diversas ameaças existentes no ambiente virtual.

1.2. Questão de Pesquisa

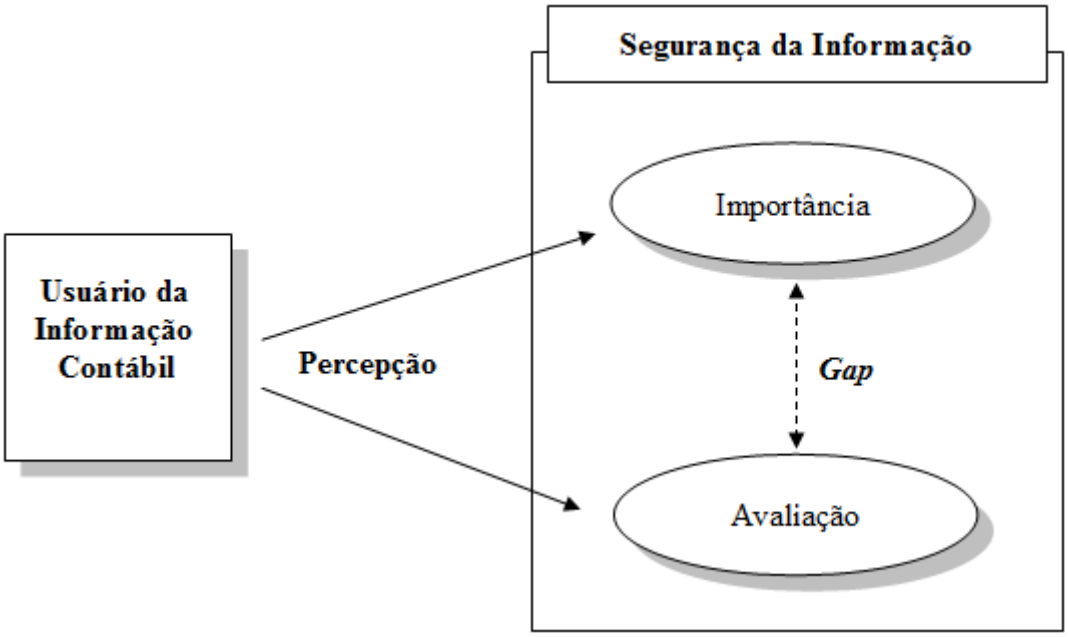
De acordo com Beuren (2009), o raciocínio de um trabalho científico não se desencadeia enquanto não se estabelece devidamente o problema, isto é, o tema precisa ser problematizado. Köche (2000) afirma que um problema de pesquisa deve ser enunciado na forma interrogativa e questionar sobre uma possível relação entre pelo menos duas variáveis que estejam ligadas ao objeto de estudo investigado, adicionalmente, o problema de pesquisa deve ser passível de teste ou observação empírica.

Motivado pelo fato de que a segurança da informação é um problema que atinge todas as organizações, e que a informação contábil é sensível aos diversos riscos de segurança da informação nas quais as organizações estão expostas, torna-se relevante analisar qual é a percepção dos usuários da informação contábil acerca do tema segurança da informação. Neste contexto, a seguinte questão de pesquisa é apresentada para esse estudo:

- **Existe um *gap* na percepção dos usuários da informação contábil com relação à segurança da informação nas organizações?**

Para esta pesquisa, entende-se como *gap* a diferença entre a **Avaliação** (como o usuário da informação contábil avalia a segurança da informação na sua organização) e a **Importância** (o quanto o usuário da informação contábil considera a segurança da informação importante). Com o objetivo de facilitar o entendimento deste trabalho, criou-se um modelo que ilustra os objetivos da pesquisa, que pode ser observado na Figura 4:

Figura 4 – Modelo Adotado na Pesquisa



1.3. Hipóteses de Pesquisa

Segundo Pádua (1996), uma hipótese indica uma possível solução para o problema que esta sendo pesquisado, e constitui uma interpretação provisória ou antecipada, que a pesquisa pretende confirmar. Lakatos e Marconi (2000) ressaltam também que a hipótese deve ser compatível com uma fundamentação teórica preliminar.

Uma pesquisa realizada por Madnick et al. (2007) identificou a existência de um significativo *gap* entre a avaliação e a importância percebida pelos membros das organizações acerca dos construtos de segurança da informação, de modo que, a avaliação das boas práticas de segurança nas organizações está muito abaixo do que é considerado importante para os respondentes. Neste contexto, as seguintes hipóteses foram consideradas neste estudo:

- **H1:** Existe um *gap* entre a avaliação e a importância da **Integridade** da informação percebida pelo usuário da informação contábil nas organizações.
- **H2:** Existe um *gap* entre a avaliação e a importância da **Disponibilidade** da informação percebida pelo usuário da informação contábil nas organizações.
- **H3:** Existe um *gap* entre a avaliação e a importância da **Confidencialidade** da informação percebida pelo usuário da informação contábil nas organizações.
- **H4:** Existe um *gap* entre a avaliação e a importância dos **Equipamentos** de segurança da informação percebida pelo usuário da informação contábil nas organizações.

- **H5:** Existe um *gap* entre a avaliação e a importância das **Políticas e Procedimentos** de segurança da informação percebida pelo usuário da informação contábil nas organizações.
- **H6:** Existe um *gap* entre a avaliação e a importância da conscientização das **Pessoas** percebida pelo usuário da informação contábil nas organizações.

1.4. Objetivo Geral

De acordo com Beuren (2009), o objetivo geral de uma pesquisa deve indicar uma ação ampla do problema, devendo ser elaborado com base na questão de pesquisa.

O objetivo proposto para este trabalho é estudar a percepção dos usuários da informação contábil com relação à segurança da informação. Pretende-se identificar como os usuários da informação contábil avaliam a segurança da informação em suas organizações, bem como, o quanto os usuários da informação contábil consideram a segurança da informação importante, permitindo desta forma, avaliar a eventual existência de *gap* entre as percepções.

1.5. Objetivos Específicos

Ainda segundo Beuren (2009), os objetivos específicos devem descrever ações específicas para alcançar o objetivo geral da pesquisa. Os objetivos específicos propostos para este trabalho estão indicados a seguir:

- Identificar como os usuários da informação contábil avaliam a segurança da informação em suas organizações e o quanto estes usuários consideram a segurança da informação importante.
- Avaliar a existência de *gap* entre a avaliação e a importância da segurança da informação nas organizações.
- Avaliar as eventuais diferenças de percepção de segurança da informação de acordo com as características do usuário da informação contábil.
- Evidenciar as oportunidades de melhoria na segurança da informação das organizações, de acordo com a percepção dos usuários da informação contábil.

1.6. Justificativas e Contribuições

As práticas de segurança da informação em uma organização são comparadas a uma corrente com diversos elos que representam os componentes envolvidos, tais como, equipamentos, *software*, protocolos de comunicação, usuários, entre outros. Na literatura sobre segurança da informação, o usuário é freqüentemente referenciado como o elo mais fraco, uma vez que os recursos computacionais estão protegidos por um considerável acervo tecnológico (MARCIANO, 2006).

Segundo Albrechtsen (2007), entre as diversas atividades atribuídas aos funcionários das organizações, os cuidados com a segurança da informação normalmente são tratadas com menor prioridade do que as demais. Adicionalmente, Abu-Musa (2003) afirma que a informação contábil pode ser alvo de uma série de ameaças, incluindo fraude, espionagem, sabotagem, vandalismo, vírus e ataques *hacker*.

Neste contexto, esta pesquisa torna-se relevante, uma vez que, a contabilidade e os sistemas de informação contábil possuem forte dependência da ação dos usuários, e as informações geradas pela contabilidade são muitas vezes utilizadas como base para tomada de decisão e definição de estratégias das organizações. Desta forma, é importante avaliar e evidenciar a percepção dos usuários da informação contábil com relação à segurança da informação nas organizações.

É importante citar que Herath (2011) criticou a ausência de trabalhos sobre segurança da informação no âmbito da pesquisa contábil, enfatizando que se trata de uma importante área onde a pesquisa poderia auxiliar na resolução dos problemas existentes na prática. A necessidade de pesquisas em segurança da informação com o objetivo de fornecer soluções para aplicação prática também foi apresentada por Doherty e Fulford (2005). Desta forma, espera-se que o resultado desta pesquisa gere contribuições práticas e recomendações que possam ser utilizadas com o objetivo de melhorar a gestão de segurança da informação das organizações.

2. REFERENCIAL TEÓRICO

De acordo com Collis e Hussey (2005), a busca na literatura é o processo de explorar a literatura existente para averiguar o que já foi escrito ou publicado sobre o tópico de pesquisa escolhido. Neste capítulo estão apresentados alguns conceitos teóricos sobre informação e sistemas de informação, os quais são discutidos de um modo geral e especificamente na contabilidade. Estão apresentados também os conceitos relacionados à segurança da informação, segurança da informação contábil e a teoria da percepção.

2.1. Informação

A informação é um recurso vital para as organizações, capaz de assumir um papel importante no apoio às estratégias e processos de tomada de decisão e também no controle das operações empresariais (BEUREN, 2000).

Stair (1998) alerta para a distinção entre os conceitos de dado e informação. Para Moscove, Simkin e Bagranoff (2002) dados são fatos brutos sobre eventos que não tem nenhuma organização ou significado, contudo, os dados podem ser organizados de maneira que sejam úteis e tenham significado, transformando-se desta forma em informações.

Padoveze (2000) define informação como um dado que foi processado e armazenado de forma compreensível para seu receptor e que apresenta valor real ou percebido para suas decisões correntes ou prospectivas. Para Beal (2004), informação é o resultado da transformação ocorrida quando os registros ou fatos que caracterizam os dados são organizados ou combinados de forma lógica e significativa.

O valor da informação reside no fato de que ela deve reduzir a incerteza na tomada de decisão, ao mesmo tempo em que procura aumentar a qualidade da decisão. Neste contexto, uma informação passa a ser válida quando a sua utilização aumenta a qualidade decisória, diminuindo a incerteza do gestor no ato da decisão (PADOVEZE, 2000).

2.2. Informação Contábil

Segundo Padoveze (2000), o objetivo da informação contábil é a mensuração econômica das transações através do processo contábil de atribuir um ou mais valores a todos

os eventos que acontecem na organização e possuem significado patrimonial. O autor define algumas características que devem ser observadas na informação contábil:

a) Deve trazer mais benefícios do que custo para sua obtenção.
b) Deve ser compreensível.
c) Deve ter utilidade para o decisor.
d) Deve possuir relevância e confiabilidade.
e) Deve ter consistência e possibilitar comparabilidade.

De acordo com Ribeiro Filho, Lopes e Pederneiras (2009), a informação contábil é o resultado do processamento dos dados relacionados ao empreendimento, decorrentes das atividades desenvolvidas na organização. Os autores comentam que a principal forma de a contabilidade evidenciar informações aos seus diversos usuários é por meio de demonstrações contábeis padronizadas.

Neste contexto, o Comitê de Pronunciamentos Contábeis (CPC) através do Pronunciamento Conceitual Básico (CPC, 2008) estabelece que as demonstrações contábeis sejam elaboradas com o objetivo de fornecer informações sobre a posição patrimonial, financeira e o desempenho da entidade, de modo que sejam úteis a um grande número de usuários em suas avaliações e tomadas de decisões econômicas, entre as quais se destacam:

a) Decidir quando comprar, manter ou vender um investimento em ações.
b) Avaliar a administração quanto à responsabilidade que lhe tenha sido conferida, qualidade de seu desempenho e prestação de contas.
c) Avaliar a capacidade da entidade de pagar seus empregados e proporcionar outros benefícios.
d) Avaliar a segurança quanto à recuperação dos recursos financeiros emprestados à entidade.
e) Determinar políticas tributárias.
f) Determinar a distribuição de lucros e dividendos.
g) Preparar e usar estatísticas da renda nacional.
h) Regulamentar as atividades das entidades.

Adicionalmente, o Pronunciamento Conceitual Básico (CPC, 2008) define as quatro principais características qualitativas que devem obrigatoriamente estar presentes nas demonstrações contábeis, conforme resumido a seguir:

1. **Compreensibilidade:** se fundamenta no objetivo do pronto entendimento por parte do usuário, mas a complexidade de qualquer matéria não deve levar à falta de registro, de registro adequado ou de evidenciação sob o argumento de eventual dificuldade de entendimento por parte desse usuário (CPC, 2008).

2. **Relevância:** diz respeito à influência de uma informação contábil na tomada de decisões. As informações são relevantes quando podem influenciar as decisões econômicas dos usuários, ajudando-os a avaliar o impacto de eventos passados, presentes ou futuros ou confirmando ou corrigindo as suas avaliações anteriores. A relevância depende da natureza e também da materialidade do item em discussão (CPC, 2008).

3. **Confiabilidade:** exige que a informação seja apresentada da forma mais apropriada possível, retratando adequadamente o que se pretende evidenciar. Para a confiabilidade estar presente é fundamental que seja sempre respeitada a primazia da essência sobre a forma, ou seja, que, no que se espera sejam raros os casos de não conformidade dos documentos formais com a realidade econômica, que esta última prevaleça nas demonstrações contábeis. É necessário também que se observem a neutralidade, a prudência e a integridade nas informações contábeis (CPC, 2008).

4. **Comparabilidade:** trata-se de característica que permite a melhor visão da evolução da entidade medida sob os mesmos critérios e princípios ao longo do tempo, mas sem que isso leve a não evolução das práticas contábeis. A comparabilidade também se aplica à adoção das mesmas práticas por empresas semelhantes (CPC, 2008).

Estas características qualitativas são necessárias para que a informação contábil seja útil para os seus diversos usuários. Segundo Ribeiro Filho, Lopes e Pederneiras (2009), os usuários da informação contábil podem ser internos ou externos, possuem interesses diversificados e buscam nas informações contábeis a satisfação de suas necessidades. Entre os

usuários da informação contábil destacam-se os clientes, empregados, governo, fornecedores, credores, acionistas e a comunidade.

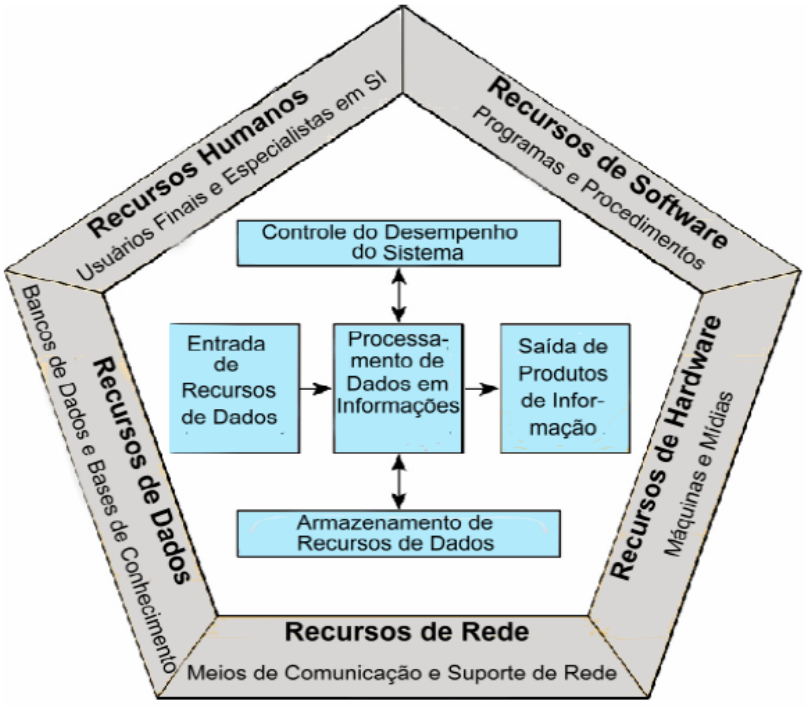
2.3. Sistemas de Informação

Segundo Boockholdt (1999), um sistema consiste de seus componentes (*hardware* e *software*), o processo que coordena essas partes para um determinado fim e os objetivos para os quais ambos são coordenados e se destinam.

De acordo com Imoniana (2008), um sistema é um conjunto de elementos inter-relacionados com o objetivo de produzir relatórios que nortearão as tomadas de decisões gerenciais. O autor classifica os sistemas como abertos (recebem influência do ambiente interno e externo onde operam) e fechados (recebem apenas dados controlados).

O'Brien e Marakas (2008) apresentam um modelo (Figura 5) que expressa uma estrutura conceitual básica com os principais componentes e atividades de um sistema de informação. Os autores assumem que o sistema de informação tem como finalidade executar atividades de entrada, processamento, produção, armazenamento e controle, para converter os dados em produtos de informação.

Figura 5 – Componentes dos Sistemas de Informação



Fonte: O'Brien e Marakas, 2008

Padoveze (2000) define sistema de informação como um conjunto de recursos humanos, materiais, tecnológicos e financeiros agregados segundo uma seqüência lógica para o processamento dos dados e tradução em informações, para com seu produto, permitir as organizações o cumprimento de seus objetivos principais.

Para Moscove, Simkin e Bagranoff (2002) um sistema de informação é um conjunto de subsistemas inter-relacionados que funcionam para coletar, processar, armazenar, transformar e distribuir informações para fins de planejamento, tomada de decisões e controle.

Segundo Turban et al. (2006), um sistema de informação é um sistema capaz de coletar, armazenar, analisar e disseminar informações para atender um propósito específico.

Perez (2006) destaca que embora um sistema de informação não tenha seu funcionamento necessariamente baseado em computadores, a maior parte dos sistemas de informação encontrados nas organizações modernas são computadorizados.

Por fim, cabe ressaltar que segundo a norma NBR ISO/IEC 17799 (ABNT, 2005), muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados.

2.4. Sistemas de Informação Contábil

De acordo com Riccio (2001), a contabilidade é um sistema de controle largamente utilizado pela sociedade, que por sua natureza, é uma área controladora e consolidadora dos sistemas de informações da empresa.

Segundo Padoveze (2000), as ações da empresa que são realizadas nas áreas de produção, comercialização e finanças, devem conduzir a resultados econômicos positivos. Neste contexto, sendo a contabilidade a entidade especializada em avaliar economicamente a empresa e seus resultados, todas as ações terminam por convergir para o sistema de informação contábil, que é essencialmente um sistema de avaliação de gestão econômica.

Um sistema de informação contábil é uma estrutura unificada dentro de uma entidade, que emprega recursos físicos e outros componentes para transformar dados econômicos em informação contábil, com o propósito de satisfazer as necessidades de informação de uma variedade de usuários (WILKINSON et al., 2000).

Para Riccio (2001) o sistema de informação contábil é o conjunto de atividades que realiza as operações de coleta, processamento dos dados e emissão das informações ou

relatórios contábeis, financeiros, gerenciais e estratégicos, destinados à administração, ao fisco e aos demais órgãos externos à empresa. Segundo o autor, o sistema de informação contábil é o principal instrumento do contador, sendo por meio dele que o contador exerce sua função e estabelece os padrões de controle contábil da empresa.

Boockholdt (1999) define sistema de informação contábil como um sistema que registra, processa e reporta transações passadas de acordo com os padrões contábeis geralmente aceitos. O autor comenta que a estrutura de um sistema de informação contábil é semelhante em qualquer organização, principalmente nos seguintes aspectos:

- **Estrutura similar:** recursos humanos e computacionais.
- **Processos similares:** utilizam padrões contábeis.
- **Propósitos similares:** prover informações.

Por fim, Moscove, Simkin e Bagranoff (2002) definem o sistema de informação contábil como um sistema de informação que capta, registra e comunica todas as informações financeiras e não financeiras relativas às atividades empresariais. A definição de sistema de informação contábil como um sistema de âmbito corporativo elege a contabilidade como o principal produtor e distribuidor de informações da organização.

2.5. Segurança da Informação

A informação é um ativo que, como qualquer outro ativo, é importante para os negócios de uma organização, desta forma, necessita ser adequadamente protegida. É importante lembrar que a informação pode existir de diversas formas, entre elas, impressa em papel, armazenada eletronicamente, transmitida por meios físicos ou eletrônicos, falada, entre outros. Independente da forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela esteja sempre protegida (ABNT, 2005).

Neste contexto, a norma NBR ISO/IEC 17799 (ABNT, 2005) define segurança da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida a partir da implantação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e recursos de *software* e *hardware*. Estes controles

precisam ser estabelecidos, implantados, monitorados, analisados criticamente e melhorados quando necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Ainda segundo a NBR ISO/IEC 17799 (ABNT, 2005), a segurança da informação pode ser caracterizada pela preservação dos princípios de confidencialidade, integridade e disponibilidade. Abaixo estão apresentadas as definições destes princípios:

- **Confidencialidade:** Princípio que trata sobre a disponibilidade de informações apenas às pessoas autorizadas. Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento (TCU, 2008).

- **Integridade:** Princípio que trata sobre a proteção da informação contra a criação ou modificação não autorizada. Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital (TCU, 2008).

- **Disponibilidade:** Princípio que trata sobre garantir que a informação ou o recurso de informação esteja disponível sempre que necessário. Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito (TCU, 2008).

De acordo com Doherty e Fulford (2005) a preservação da integridade, confidencialidade e disponibilidade da informação só pode ser alcançada através da implantação de procedimentos e controles que protejam a informação contra as diversas

vulnerabilidades e ameaças nas quais ela está exposta. Para um melhor entendimento deste conceito, se faz necessário definir alguns termos que são comumente utilizados na literatura sobre segurança da informação, os quais estão apresentados a seguir:

- **Vulnerabilidades**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (ABNT, 2005).
- **Ameaças:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização (ABNT, 2005).
- **Eventos de segurança da informação:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação, falha de controles ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação (ABNT, 2005).
- **Incidentes de segurança da informação:** um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação (ABNT, 2005).

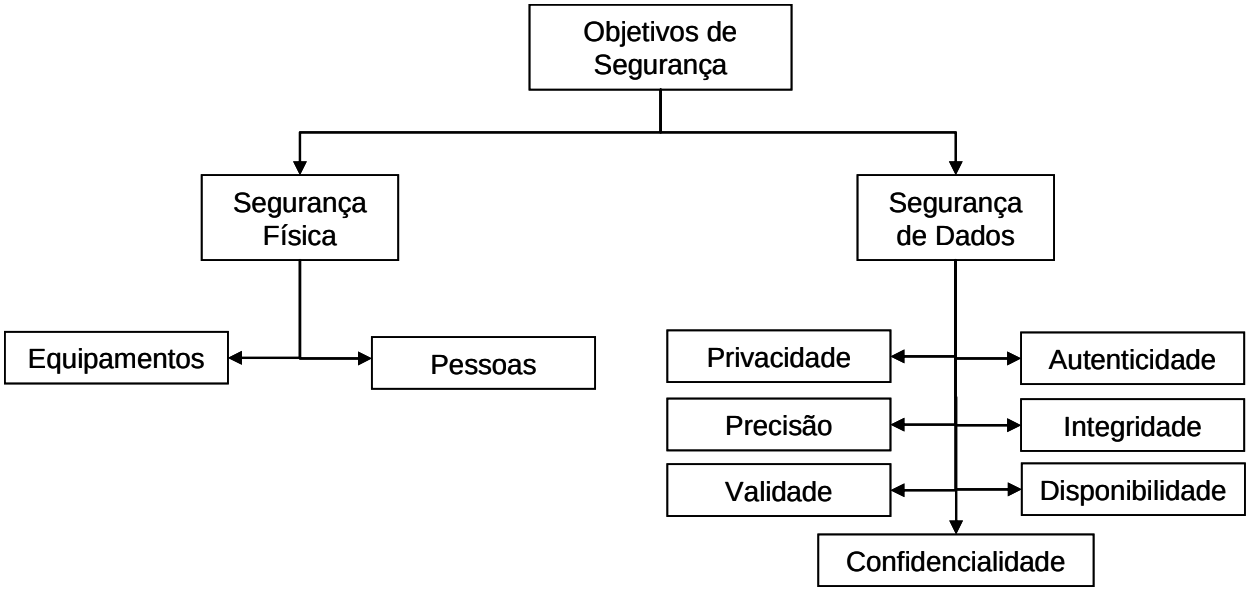
Ainda segundo Doherty e Fulford (2005) os incidentes de segurança da informação podem ocorrer em virtude de vulnerabilidades e ameaças internas ou externas a organização. Os autores apresentaram os oito principais tipos de incidentes de segurança da informação, os quais estão demonstrados a seguir:

1. **Vírus de computador:** são programas maliciosos de computador que possuem a capacidade de se replicar automaticamente entre os sistemas e redes.
2. **Ataque *Hacker*:** refere-se à invasão aos sistemas e redes da organização com o objetivo de se obter ou manipular informações de forma ilícita. Normalmente o ataque é realizado por indivíduos externos a organização.
3. **Acesso não autorizado:** ocorre quando um usuário obtém acesso aos sistemas e dados sem a devida autorização, por exemplo, quando um usuário empresta sua senha a outro usuário.
4. **Roubo de recursos:** refere-se ao roubo de *hardware*, *software* e demais ativos relacionados à informação.

5. **Fraude baseada em computador:** ocorre quando os sistemas de informação, normalmente os sistemas financeiros, são adulterados por indivíduos que buscam fraudar a organização.
6. **Erro humano:** refere-se à destruição acidental de recursos ou informações, bem como, erros não intencionais na entrada de dados pelos usuários dos sistemas.
7. **Desastres naturais:** ocorre quando os recursos computacionais e as informações são danificados por eventos naturais como terremotos ou inundações.
8. **Danos causados por empregados:** ocorre quando funcionários descontentes ou mal intencionados danificam os sistemas e informações da organização.

Abu-Musa (2002) propôs um modelo que demonstra os objetivos e os componentes da segurança da informação, especificamente em sistemas de informação contábil, conforme apresentado na Figura 6.

Figura 6 – Objetivos da Segurança da Informação



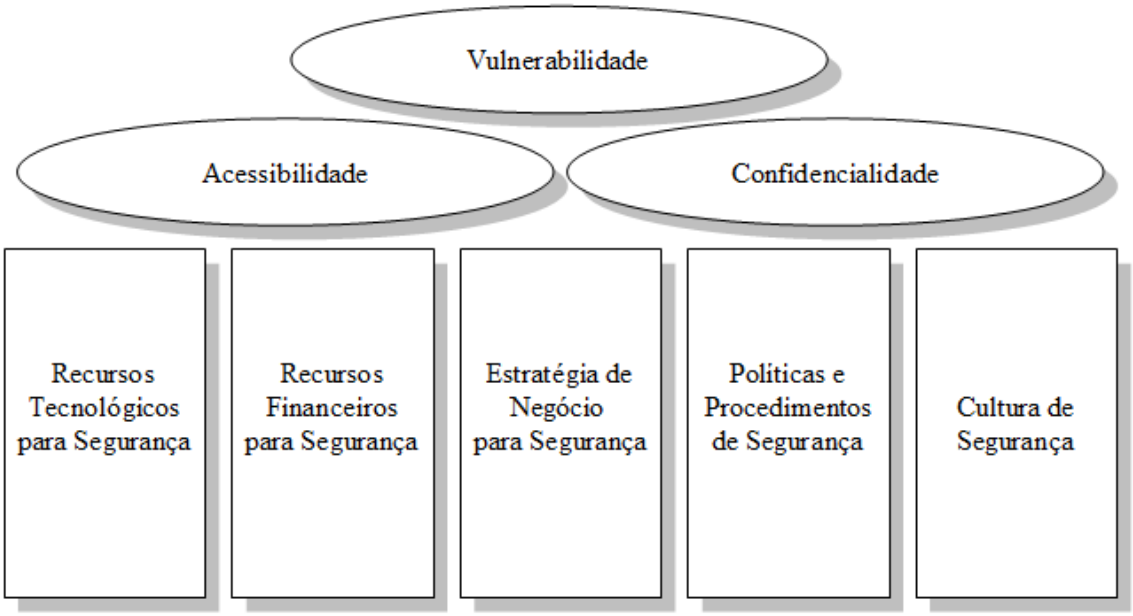
Fonte: Abu-Musa, 2002

O modelo proposto pelo autor assume que os principais objetivos da segurança da informação estão relacionados à preservação da segurança física e a segurança dos dados. Estes objetivos são alcançados através da integração de diversos componentes, os quais estão apresentados a seguir:

- **Equipamentos:** refere-se à proteção contra danos e roubo dos recursos físicos e instalações utilizados para armazenar e processar as informações.
- **Pessoas:** trata da conscientização e treinamento de todas as pessoas envolvidas na manipulação das informações.
- **Privacidade:** diz respeito à proteção de informações consideradas privadas e secretas, de modo que a privacidade é garantida pela imposição de regras de confidencialidade para o uso de dados pessoais.
- **Precisão:** refere-se à manutenção da legitimidade da informação de modo que ela represente exatamente o que deve representar.
- **Validade:** pode ser definida como a total precisão e integridade das informações de modo que seja útil ao usuário final.
- **Autenticidade:** refere-se à manutenção da integridade e precisão das informações através do controle das alterações que são realizadas.
- **Integridade:** refere-se à prevenção de criação e modificação de informações por pessoas não autorizadas.
- **Disponibilidade:** pode ser definida como a prevenção da indisponibilidade, temporária ou permanente, no acesso as informações por usuários autorizados.
- **Confidencialidade:** diz respeito à garantia de que as informações são divulgadas apenas às pessoas, entidades e processos autorizados.

Segundo Madnick et al. (2006), a segurança da informação deve oferecer acessibilidade aos dados e as redes aos usuários apropriados, ao mesmo tempo em que protege a confidencialidade dos dados e minimiza as vulnerabilidades a ataques e ameaças. Segundo os autores, as boas práticas de segurança da informação vão além de soluções de tecnologia da informação. A segurança da informação deve ser direcionada por uma estratégia de negócio associada com políticas e procedimentos que instituam a cultura de segurança na organização. Essas práticas são apoiadas por recursos tecnológicos e recursos financeiros dedicados à segurança. Os autores desenvolveram um modelo denominado *House of Security*, o qual sugere que a segurança da informação pode ser compreendida através de oito construtos, conforme demonstrado na Figura 7.

Figura 7 – Construtos de Segurança da Informação



Fonte: Madnick et al., 2006

Para Peltier (2001), o sistema de proteção da informação deve considerar aspectos ligados a segurança física da informação, segurança lógica, segurança das relações financeiras, garantia da reputação e imagem da organização, aspectos legais, comportamento dos funcionários, e para com os funcionários, e todos os ativos tangíveis e intangíveis. O autor descreve os oito principais elementos necessários para implantação do sistema de proteção da informação nas organizações, conforme descrito a seguir:

1. O sistema de proteção da informação deve estar alinhado com as estratégias e objetivos de negócios da organização.
2. A proteção da informação requer comprometimento da alta direção em manter alinhados os objetivos de segurança com os níveis de segurança desejados para o negócio.
3. Os investimentos em segurança da informação devem ser compatíveis com o nível de segurança e proteção da informação esperado pela organização, ou seja, necessário para suportar os negócios.
4. As responsabilidades com a segurança e a proteção da informação devem estar explícitas para todos os funcionários, clientes e fornecedores e as conseqüências advindas do não cumprimento das políticas, normas e procedimentos devem ser claramente divulgadas e conhecidas por todos.

5. Os responsáveis pela guarda, monitoramento e administração das informações possuem responsabilidades sobre a manutenção da integridade, confidencialidade e disponibilidade, podendo dar permissões de acesso ou retirá-las de acordo com as necessidades do negócio.
6. A proteção da informação deve fazer parte de um sistema com análise, revisões e correções permanentes que devem incluir a análise de risco e de impacto no negócio, e a classificação da informação, visando garantir a manutenção do nível esperado de segurança pela organização.
7. O sistema de segurança da informação deve ser periodicamente auditado e testado, considerando as disposições ou ações corretivas para desvios ou falhas de funcionamento encontradas, e realimentando assim todo o sistema com a verificação de novas vulnerabilidades que possam ter surgido ao longo de seu funcionamento.
8. A segurança da informação deve ser construída com base na cultura da organização e nas necessidades de proteção identificadas, preservando as devidas características inerentes aos países onde as mesmas existem ou suas filiais estão instaladas.

Ainda segundo Peltier (2001), a implantação das práticas de segurança da informação deve transpor as fronteiras da utilização de dispositivos de *hardware* e *software*, os quais muitas vezes não oferecem a segurança necessária ou esperada devido a falhas de funcionamento ou de parametrização e instalação. A segurança da informação deve considerar o grau de dependência da organização na utilização da informática como ferramenta de trabalho, as necessidades de manutenção dos sistemas ativos em caso de desastre e o comprometimento de áreas críticas do negócio em virtude de problemas de vazamento de informações.

De acordo com Pemble (2004), a segurança da informação pode ser compreendida com base nas responsabilidades atribuídas aos profissionais de segurança. O autor entende que o profissional de segurança desempenha um papel estratégico e preventivo, avaliando riscos e fornecendo as informações necessárias para que os executivos possam tomar decisões sobre questões de segurança da informação nas organizações. Os três principais segmentos de atuação dos profissionais de segurança da informação estão apresentados a seguir.

1. **Segmento operacional:** atividades voltadas ao impacto que os incidentes de segurança da informação podem gerar na continuidade dos processos do negócio.

2. **Segmento da reputação:** atividades voltadas ao impacto que os incidentes de segurança da informação podem gerar sobre a marca e o valor das ações da empresa, considerando aspectos legais e regulatórios.
3. **Segmento financeiro:** atividades voltadas aos custos em que se incorre na eventualidade de algum incidente de segurança da informação na organização.

Por fim, Anderson (2003) critica a ausência de um conceito abrangente sobre segurança da informação, evidenciado o viés tecnológico nas definições existentes. Segundo o autor, a segurança da informação pode ser definida como um sentimento bem fundamentado da garantia de que os controles e riscos da informação estão bem equilibrados.

2.6. Abordagens não Tecnológicas da Segurança da Informação

Segundo Kayworth e Whitten (2010), nenhuma solução ou mecanismo tecnológico é suficiente para garantir a eficácia da segurança da informação nas organizações. Os autores comentam que esta eficácia só pode ser alcançada através da aplicação de uma estratégia corporativa de segurança da informação que envolva aspectos técnicos e sociais. Adicionalmente, os executivos devem considerar a segurança da informação como uma questão de negócio e não um problema técnico.

Para Marciano (2006) não se conhece nenhuma solução meramente tecnológica para problemas sociais, desta forma, a segurança da informação necessita de uma visão embasada em conceitos sociais para sua correta cobertura. O autor propôs a integração de disciplinas oriundas das ciências sociais para a construção de um modelo destinado a elaboração, implantação e acompanhamento de políticas de segurança da informação que contemplem com o adequado equilíbrio os aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos atuais, notadamente voltados às questões tecnológicas. Neste estudo, o autor apresenta alguns conceitos sociais para a compreensão de segurança da informação, os quais estão apresentados a seguir.

- **Sistema de informação:** é composto pela somatória do sistema social no qual ele se apresenta, ou seja, dos usuários e suas interações entre si e com o próprio sistema, e do complexo tecnológico sobre o qual estas interações se sustentam.

- **Segurança da informação:** é um fenômeno social no qual os usuários dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como, sobre os papéis que devem desempenhar no exercício deste uso.
- **Política de segurança da informação:** é um conjunto de regras, normas e procedimentos que regulam como deve ser gerenciada e protegida a informação sensível, assim classificada pela organização ou pelo estado, além dos recursos e usuários que com ela interagem. Todo o ciclo de vida da informação deve ser objeto da política.

Segundo Jourdan et al. (2010) a segurança da informação é formada pelo conjunto de processos, procedimentos, pessoas e tecnologia. Os autores enfatizam a importância da adoção de políticas de segurança da informação nas organizações, uma vez que a política contém as normas e procedimentos detalhados que devem direcionar as atividades da gestão da segurança da informação na organização. Os autores destacam as principais atividades que devem ser definidas na política de segurança da informação, as quais estão apresentadas a seguir:

- **Treinamento do usuário final:** é realizado pela área de segurança da informação com o objetivo de reduzir o número de incidentes de segurança que ocorrem por falta de consciência dos usuários.
- **Operações:** refere-se à operação e manutenção das atividades e procedimentos de segurança da informação na organização.
- **Gestão de projetos:** diz respeito à criação e implementação de novos recursos de segurança da informação.
- **Gestão de riscos:** trata-se do processo de identificação de vulnerabilidades em segurança da informação, bem como, a recomendação de medidas para controlar essas fraquezas.
- **Avaliação da política:** devido ao constante surgimento de novas ameaças e vulnerabilidades, a política de segurança da informação deve ser revisada periodicamente de modo a garantir a sua eficácia.

Um estudo realizado por Da Veiga e Eloff (2007) demonstrou que segurança da informação engloba tecnologia, processos e pessoas, e que o comportamento do usuário exerce influência importante nestes itens. Esta influência pode ser explicada se comparado com a proteção de uma residência, onde o proprietário pode instalar travas em todas as portas e janelas, contudo, ao sair se esquece de trancar a porta da frente, anulando desta forma a eficácia de todos os recursos de segurança. Nas organizações, situação semelhante pode ser observada quando os usuários compartilham senhas de acesso. Neste contexto, os autores afirmam que o comportamento dos funcionários no ambiente empresarial deve ser monitorado para certificar o cumprimento das normas de segurança da informação da organização.

Eloff e Eloff (2005) desenvolveram um modelo multidisciplinar para gestão da segurança da informação denominado PROTECT (um acrônimo para Políticas, Riscos, Objetivos, Tecnologia, Execução, Conformidade e Time). O modelo propõe uma abordagem integrada entre aspectos humanos e tecnológicos, com o objetivo de minimizar os riscos e garantir a eficácia da gestão de segurança da informação nas organizações. Os sete componentes do modelo PROTECT estão apresentados abaixo:

1. **Políticas:** este componente inclui a política e os procedimentos de segurança da informação, bem como, as diretrizes para manutenção dos mesmos.
2. **Riscos:** este componente aborda as metodologias de avaliação de risco, bem como as ferramentas automatizadas para identificar as vulnerabilidades do ambiente.
3. **Objetivos:** refere-se ao objetivo principal do PROTECT, ou seja, minimizar a exposição ao risco e maximizar a segurança da informação através da implantação e monitoramento de um conjunto abrangente de controles.
4. **Tecnologia:** refere-se ao *hardware*, *software*, sistemas e demais componentes de infra-estrutura de tecnologia da informação.
5. **Execução:** os controles de segurança da informação precisam ser estabelecidos, mantidos e gerenciados, desta forma, a execução refere-se à operacionalização do sistema de gestão de segurança da informação na organização.
6. **Conformidade:** refere-se tanto a conformidade interna (políticas da organização), como conformidade externa (exigências governamentais, entre outras). Este componente também inclui os códigos de prática, requisitos legais e normas internacionais em segurança da informação.

7. **Time:** refere-se ao componente humano, ou seja, todos os funcionários da organização, os quais possuem responsabilidades definidas, contribuindo para a disseminação da cultura da segurança da informação na organização.

Segundo Gordon e Loeb (2006) os custos associados à segurança da informação geralmente estão relacionados a *hardware*, *software* e pessoas. A maioria destes gastos são tratados como investimentos de capital, embora algumas empresas prefiram tratar como despesas operacionais. Contudo, independente da forma de contabilização, os gastos com segurança da informação não podem ser negligenciados quando da elaboração do orçamento das organizações. Os autores alertam que estes gastos não devem ser avaliados pela perspectiva econômica, mais sim, em ternos de custo-benefício.

Com relação aos investimentos em segurança da informação, Gordon e Loeb (2002) e Wood e Parker (2004) lembram que estes investimentos não podem ser tratados como outros tipos de investimentos. Os autores comentam que os métodos usualmente utilizados para avaliação de investimentos de caráter geral como ROI (*Return on Investments*), NPV (*Net Present Value*) e *Payback* não se aplicam aos investimentos em segurança da informação, pois estes não necessariamente se associam a bens tangíveis ou de retorno mensurável por medidas convencionais.

Um estudo realizado por Gordon et al. (2008) evidenciou que o desenho e uso dos sistemas de controle gerencial (SCG) exercem um papel fundamental nas questões relacionadas à segurança da informação, reduzindo significativamente as perdas com os incidentes de segurança. Os autores afirmam que, devido a problemas de assimetria informacional, o gestor da segurança da informação tende a exagerar nos investimentos, não considerando uma ponderação entre custos e benefícios. Como resultado, o estudo demonstrou que a auditoria de segurança da informação (componente do SCG) é um recurso importante para avaliação da eficácia dos investimentos em segurança da informação. Adicionalmente, os autores sugerem ajustes no sistema de compensação do gestor de segurança da informação para auxiliar na redução de assimetria e melhor uso dos recursos.

De acordo com Von Solms e Von Solms (2004), o objetivo da segurança da informação é fornecer medidas para mitigar os riscos associados aos recursos de informação da organização. Os autores esclarecem que se a organização não conhece de forma clara quais são as ameaças nas quais ela está exposta, bem como, quais são os bens que deverão ser protegidos, os investimentos em segurança da informação podem ser mal direcionados,

protegendo-se contra as ameaças que possuem baixa probabilidade de ocorrência, e ignorando outras que podem gerar um impacto muito maior caso venham a ocorrer.

Stewart (2004) e Marciano (2006) comentam sobre a importância e dificuldades da avaliação de riscos em segurança da informação. Os autores alertam para a característica cíclica do processo de ataques que afetam a segurança da informação nas organizações. Na prática, as empresas melhoram os seus controles em resposta aos ataques, e os *hackers*, por sua vez, melhoram os seus ataques em resposta aos controles implantados, e assim sucessivamente. Esta característica torna qualquer cálculo de risco extremamente difícil, porque os parâmetros da equação se alteram rapidamente ao longo do tempo.

A necessidade do alinhamento da segurança da informação com a estratégia dos negócios foi uma preocupação enfatizada por Peltier (2001) e Kayworth e Whitten (2010). A falta de integração entre estes dois aspectos pode resultar em políticas e investimentos em segurança da informação que não refletem a real necessidade do negócio. Os autores alertam que a segurança da informação não é o principal produto das organizações, desta forma, as práticas de segurança da informação devem estar alinhadas com os objetivos do negócio. Segundo Keyworth e Whitten (2010) existem três objetivos principais que devem ser considerados no desenvolvimento da estratégia de segurança da informação, os quais estão apresentados a seguir:

1. **Equilíbrio com as necessidades do negócio:** a estratégia de segurança da informação deve ser direcionada pelas necessidades do negócio, evitando que as práticas de segurança sejam barreiras para a realização das atividades principais da organização.
2. **Conformidade:** o desenvolvimento e implantação da segurança da informação devem estar em conformidade com os requisitos exigidos por órgãos externos.
3. **Adequação cultural:** as políticas e procedimentos da segurança da informação devem ser elaborados levando em consideração os aspectos culturais da organização, facilitando desta forma o seu cumprimento pelos membros da organização.

Seguindo o mesmo raciocínio, Knapp et al. (2007) comentam que os profissionais de segurança da informação devem trabalhar em conjunto com gestores de negócios e com todos os usuários durante o processo de avaliação de risco e planejamento de continuidade dos negócios da organização. Os autores enfatizam a necessidade do desenvolvimento de habilidades gerenciais por parte dos profissionais de segurança da informação, uma vez que

estes normalmente possuem formação e perfil técnico. Desta maneira, os profissionais de segurança da informação serão capazes de compreender os aspectos de segurança da informação no contexto organizacional, além de discutir com maior propriedade as necessidades da segurança da informação, o retorno sobre os investimentos e as métricas utilizadas para mensurar o sucesso dos trabalhos em segurança da informação.

Segundo Knapp et al. (2007) e Albrechtsen (2007), a implantação de medidas rigorosas de segurança da informação pode reduzir a produtividade dos funcionários nas organizações. Os autores afirmam que exigir que os funcionários memorizem senhas complexas em diversos sistemas, pode causar irritação e conseqüente perda de produtividade. Adicionalmente, tal medida pode fazer com que o funcionário registre as suas senhas em locais de fácil visualização, o que acaba anulando as medidas de segurança implantadas.

A segurança da informação também é considerada relevante no mercado de capitais. Gordon, Loeb e Sohail (2010) realizaram uma pesquisa com o objetivo de avaliar empiricamente o valor adicionado para os acionistas em virtude de divulgações voluntárias sobre segurança da informação. A pesquisa considerou o pressuposto de que o objetivo da divulgação voluntária é fornecer evidências para o mercado de que a empresa está ativamente engajada na prevenção e detecção de falhas relacionadas à segurança da informação. O estudo utilizou como base os relatórios anuais de todas as empresas listadas na SEC entre 2000 e 2004. Como resultado, a pesquisa obteve significativas evidências de que a divulgação voluntária de informações relativas à segurança da informação esta associada positivamente com o valor de mercado das companhias, principalmente em negócios que dependem fortemente de comércio eletrônico.

Segundo Herath (2011) a pesquisa em segurança da informação deve se realizada de forma colaborativa, envolvendo pesquisadores de diversas disciplinas para resolução de problemas que são de interesse mútuo. Neste contexto, podemos observar que diversos aspectos não tecnológicos, entre eles a psicologia, sociologia e economia estão sendo utilizados para auxiliar na compreensão e solução de problemas relacionados à segurança da informação nas organizações.

2.7. Fatores Críticos de Sucesso da Segurança da Informação

Existem diversos fatores críticos de sucesso que devem ser considerados no desenvolvimento e implantação de políticas e procedimentos em segurança da informação nas

organizações. Em um estudo denominado *The 10 deadly sins of information security management*, Von Solms e Von Solms (2004) apresentaram uma lista que descreve os dez principais erros cometidos no planejamento e execução da segurança da informação nas organizações, os quais estão descritos a seguir:

1. Não perceber que a segurança da informação é responsabilidade da governança corporativa.
2. Não perceber que a segurança da informação é um assunto do negócio e não um assunto técnico.
3. Não perceber que a governança da segurança da informação é um tema multidisciplinar e um assunto complexo, onde não existe solução única ou já pronta, disponível na prateleira.
4. Não perceber que o planejamento da segurança da informação deve ser baseado na identificação de riscos.
5. Não perceber o importante papel das melhores práticas internacionais para o gerenciamento de segurança da informação.
6. Não perceber que uma política corporativa de segurança da informação é absolutamente essencial.
7. Não perceber que a execução da conformidade em segurança da informação e seu monitoramento são absolutamente essenciais.
8. Não perceber que uma estrutura organizacional adequada para a governança da segurança da informação é absolutamente essencial.
9. Não perceber a fundamental importância da conscientização da segurança da informação entre todos os usuários da organização.
10. Não proporcionar aos gestores de segurança da informação a estrutura, ferramentas e mecanismos de suporte para que eles cumpram adequadamente suas responsabilidades.

Estes aspectos evidenciam a necessidade do comprometimento da alta administração nos projetos de segurança da informação, e que estes projetos devem ser parte integrante das práticas de governança corporativa da organização. Alguns outros fatores críticos de sucesso são apresentados pela norma NBR ISO/IEC 17799 (ABNT, 2005):

a) Política de segurança, objetivos e atividades que reflitam os objetivos do negócio.
b) Um enfoque para a implementação da segurança que seja consistente com a cultura organizacional.
c) Comprometimento e apoio visível da administração.
d) Um bom entendimento dos requisitos de segurança, análise de risco e gerenciamento de risco.
e) Divulgação eficiente da segurança para todos os gerentes e funcionários.
f) Distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e fornecedores.
g) Provisão de recursos financeiros para as atividades de gestão da segurança.
h) Proporcionar educação e treinamentos adequados.
i) Implantação de um sistema de medição, que seja usado para avaliar o desempenho da gestão de segurança da informação e obtenção de sugestões para a melhoria.

Por fim, cabe ressaltar que a gestão da segurança da informação necessita da participação de todos os membros da organização, uma vez que o conhecimento do usuário sobre segurança da informação é essencial para que a empresa esteja protegida contra os diversos tipos de ameaças. A disseminação da cultura de segurança da informação é fundamental para o sucesso do projeto de segurança, e somente um esforço no sentido de convencer o usuário da importância de sua atuação, pode fazer com que essa cultura seja espalhada por toda a organização (LIMA, 2006).

2.8. Melhores Práticas em Segurança da Informação

Von Solms e Von Solms (2004) sugerem a utilização de melhores práticas internacionais para gestão da segurança da informação, uma vez que uma grande parte das ameaças, vulnerabilidades, riscos e controles relacionados à segurança da informação são comuns para todas as empresas. As melhores práticas em segurança da informação descrevem as práticas e experiências seguidas por pessoas e empresas relevantes na área de gestão da segurança da informação. Desta forma, seguindo as melhores práticas, a empresa estará compartilhando experiências adotadas com sucesso em outras organizações.

A NBR ISO/IEC 17799 (ABNT, 2005), norma da Associação Brasileira de Normas Técnicas, trata de técnicas de segurança em tecnologia da informação, e funciona como um

código de prática para a gestão da segurança da informação. Essa norma foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados, pela Comissão de Estudo de Segurança Física em Instalações de Informática, e é equivalente à norma ISO/IEC 17799.

Além do reconhecimento da ABNT como instituição normalizadora brasileira, as instituições internacionais ISO (*International Organization for Standardization*) e IEC (*International Eletrotechnical Commission*), autoras da norma, são mundialmente reconhecidas por sua capacitação técnica. A norma ISO/IEC 17799, equivalente à norma brasileira, é amplamente reconhecida e utilizada por entidades fiscalizadoras, órgãos de governo, empresas públicas e privadas nacionais e internacionais atentas ao tema segurança da informação.

Os objetivos definidos nessa norma provêem diretrizes gerais sobre as práticas geralmente aceitas para a gestão da segurança da informação. A norma NBR ISO/IEC 17799 (ABNT, 2005) está dividida em 11 seções de controles de segurança da informação, conforme descrita de forma resumida a seguir:

a) Política de segurança da informação

Essa seção orienta a direção no estabelecimento de uma política clara de segurança da informação, alinhada com os objetivos do negócio, com demonstração de seu apoio e comprometimento com a segurança da informação por meio da publicação, manutenção e divulgação da política para toda a organização. São fornecidas diretrizes para elaboração do documento e sua análise crítica (TCU, 2008).

b) Organizando a segurança da informação

Essa seção da norma orienta a direção de como gerenciar a segurança da informação dentro da organização e, ainda, de como manter a segurança de seus recursos de processamento da informação, que são acessados, processados, comunicados ou gerenciados por partes externas. São fornecidas diretrizes para definição de infra-estrutura de segurança da informação, detalhando os itens: comprometimento da gerência, coordenação, atribuição de responsabilidades, processo de autorização para recursos de processamento da informação, acordos de confidencialidade, análise crítica independente, contato com autoridades e grupos de interesses especiais. São fornecidas ainda diretrizes para o relacionamento com partes externas, na identificação dos riscos relacionados e dos

requisitos de segurança da informação necessários ao tratar com clientes e terceiros (TCU, 2008).

c) Gestão de ativos

Essa seção da norma orienta a direção a alcançar e manter a proteção adequada dos ativos da organização, além de assegurar que a informação seja classificada de acordo com seu nível adequado de proteção. São fornecidas diretrizes para realização de inventário dos ativos, definição de seus proprietários e regras para seu uso. Em relação à classificação da informação, a norma faz algumas recomendações e sugere a definição de procedimentos para rotulação e tratamento da informação (TCU, 2008).

d) Segurança em recursos humanos

Essa seção da norma orienta a direção a assegurar que funcionários, fornecedores e terceiros compreendam suas responsabilidades, estejam conscientes das ameaças relativas à segurança da informação e prontos para apoiar a política de segurança da informação da organização. São fornecidas diretrizes para definição de papéis e responsabilidades, inclusive da direção, seleção de pessoal, termos e condições de contratação, conscientização, educação e treinamento em segurança da informação, e processo disciplinar. Para os casos de encerramento ou mudança da contratação, são fornecidas diretrizes para encerramento de atividades, devolução de ativos e retirada de direitos de acesso. Essa seção abrange contratação temporária ou de longa duração de pessoas, nomeação e mudança de funções, atribuição de contratos e encerramento de qualquer uma dessas situações (TCU, 2008).

e) Segurança física e do ambiente

Essa seção da norma orienta a direção a prevenir acesso físico não autorizado, danos e interferências nas instalações e informações, assim como a impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização. São fornecidas as diretrizes para áreas seguras, incluindo perímetro de segurança física, controles de entrada física, segurança em escritórios, salas e instalações, proteção contra ameaças externas e do meio ambiente e acesso do público, áreas de entrega e carregamento. Para a segurança de equipamentos, são dadas recomendações para instalação e proteção de equipamento, inclusive contra falta de energia elétrica e outras interrupções provocadas

por falhas das utilidades, segurança do cabeamento, manutenção de equipamentos, segurança de equipamentos fora das dependências da organização, reutilização e alienação segura de equipamentos, e, por fim, remoção de propriedade (TCU, 2008).

f) Gestão das operações e comunicações

Essa seção da norma orienta a direção quanto aos procedimentos e responsabilidades operacionais, incluindo gestão de mudanças, segregação de funções e separação dos ambientes de produção, desenvolvimento e teste. São fornecidas diretrizes também para gerenciamento de serviços terceirizados, planejamento e aceitação de sistemas, proteção contra códigos maliciosos e móveis, cópias de segurança, gerenciamento da segurança em redes, manuseio de mídias, troca de informações, serviços de correio eletrônico e, por fim, monitoramento (TCU, 2008).

g) Controle de acessos

Essa seção da norma orienta a direção quanto aos controles de acesso à informação e aos recursos de processamento das informações. São fornecidas diretrizes para definição de requisitos de negócio para controle de acesso, gerenciamento de acesso e responsabilidades do usuário, controle de acesso à rede, sistema operacional, aplicação e informação, e, por fim, aspectos sobre computação móvel e trabalho remoto. Tais diretrizes englobam desde a definição de uma política de controle de acesso e o gerenciamento de privilégios até o isolamento de sistemas sensíveis (TCU, 2008).

h) Aquisição, desenvolvimento e manutenção de sistemas de informação

Essa seção da norma orienta a direção quanto à definição dos requisitos necessários de segurança de sistemas de informação, medidas preventivas contra processamento incorreto das aplicações, uso de controles criptográficos, além de fornecer diretrizes para a segurança dos arquivos de sistema, segurança em processos de desenvolvimento e suporte, e gestão de vulnerabilidades técnicas (TCU, 2008).

i) Gestão de incidentes de segurança da informação

Essa seção da norma orienta a direção para que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados e gerenciados de forma consistente e efetiva, permitindo a tomada de ação corretiva em tempo hábil. São

fornecidas diretrizes para notificação de eventos e fragilidades de segurança da informação, definição de responsabilidades e procedimentos de gestão desses eventos e fragilidades, além da coleta de evidências e do estabelecimento de mecanismos para análise dos incidentes recorrentes ou de alto impacto com vistas à sua quantificação e monitoramento (TCU, 2008).

j) Gestão da continuidade do negócio

Essa seção da norma orienta a direção quanto às medidas a serem tomadas para prevenir a interrupção das atividades do negócio e proteger os processos críticos contra defeitos, falhas ou desastres significativos, assegurando sua retomada em tempo hábil, se for o caso. São fornecidas diretrizes para incluir a segurança da informação no processo de gestão da continuidade de negócio e para realizar análise e avaliação de riscos, além de desenvolver, implementar, testar e reavaliar planos de continuidade relativos à segurança da informação (TCU, 2008).

k) Conformidade

Essa seção da norma orienta a direção a evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação, além de garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação. São fornecidas diretrizes para identificação da legislação vigente, proteção dos direitos de propriedade intelectual, proteção dos registros organizacionais, proteção de dados e privacidade de informações pessoais, prevenção de mau uso de recursos de processamento da informação e regulamentação de controles de criptografia. Além disso, são feitas algumas considerações quanto à auditoria de sistemas de informação (TCU, 2008).

Por fim, Von Solms e Von Solms (2004) enfatizam que ninguém precisa reinventar a roda da segurança da informação. Muitas empresas gastam tempo e dinheiro desnecessariamente para se chegar a uma solução que, muito provavelmente, já foi documentada. Cumpre observar que o fato de uma organização seguir estritamente as melhores práticas em segurança da informação não significa estar totalmente imune aos incidentes de segurança. Contudo, a utilização das melhores práticas demonstra que a gestão

se preocupa e está tomando os devidos cuidados com os riscos relacionados à segurança da informação.

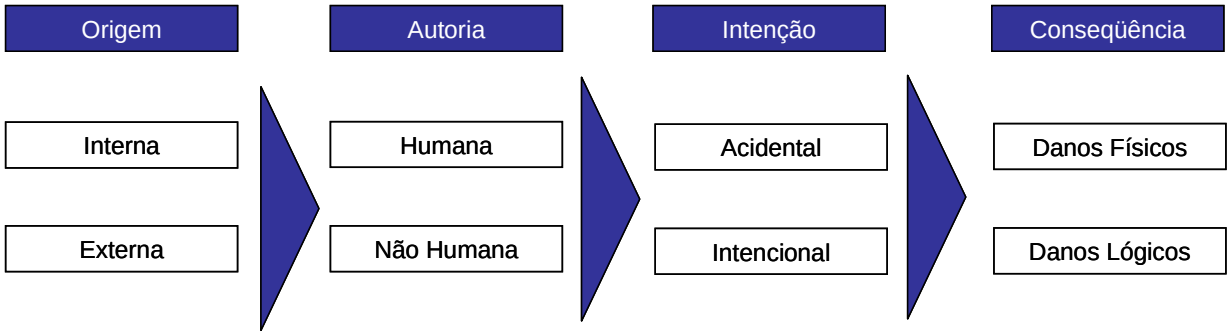
2.9. Segurança da Informação Contábil

Segundo Boockholdt (1999) informações contábeis imprecisas podem prejudicar a eficiência das organizações, uma vez que produzem relatórios financeiros não confiáveis e informações incorretas que podem violar a legislação. O autor descreve que os dois principais riscos relacionados à informação contábil são os erros e as irregularidades. Os erros são acidentais enquanto as irregularidades são intencionais. Desta maneira, as organizações precisam adotar políticas e procedimentos de controle para detectar e prevenir erros e irregularidades nas informações contábeis.

Para Abusa-Musa (2003) o sistema de informação contábil pode ser alvo de uma série de ameaças graves, incluindo fraude, espionagem, sabotagem, vandalismo, vírus e ataques *hacker*. Segundo o autor, estas ameaças podem ser classificadas como ameaças ativas e ameaças passivas. As ameaças ativas são os ataques deliberados e maliciosos ao sistema de informação contábil, enquanto as ameaças passivas são imprevisíveis, e podem ser oriundas de desastres naturais, acidentes, erros humanos, entre outras causas.

Ainda segundo Abu-Musa (2003) as ameaças à segurança da informação contábil podem ser compreendidas através de quatro dimensões (origem, autoria, intenção e conseqüência), conforme apresentado na Figura 8. O conceito de cada dimensão esta apresentado a seguir.

Figura 8 – Ameaças à Segurança da Informação Contábil



Fonte: Adaptado de Abu-Musa, 2003

- **Origem:** as ameaças à segurança da informação contábil podem ser de origem interna ou externa. Os funcionários da organização são considerados a principal fonte de ameaças internas, enquanto os *hackers* e os desastres naturais são considerados as principais fontes de ameaças externas (ABU-MUSA, 2003).

- **Autoria:** as ameaças à segurança da informação contábil podem ser de autoria humana ou não humana. As ameaças de autoria humana são aquelas que se originam a partir das ações de um ser humano, enquanto as ameaças de origem não-humanas estão normalmente relacionadas com problemas técnicos (falha técnica do sistema, falha do disco rígido, entre outros) e desastres naturais (enchentes, terremotos, entre outros) (ABU-MUSA, 2003).

- **Intenção:** as ameaças à segurança da informação contábil podem ser acidentais ou intencionais. As ameaças acidentais são ameaças de segurança que cuja origem não envolve qualquer intenção maliciosa como erro humano e desastres naturais, por outro lado, as ameaças intencionais envolvem intenções maliciosas, como sabotagem, fraude, roubo, entre outras intenções (ABU-MUSA, 2003).

- **Conseqüência:** as conseqüências provenientes das ameaças à segurança da informação contábil podem gerar danos físicos e danos lógicos. Os danos físicos estão relacionados a danos causados nos equipamentos, instalações e toda a infra-estrutura utilizada para armazenagem e processamento da informação contábil, enquanto os danos lógicos ocorrem quando informação contábil é modificada, destruída ou divulgada de maneira não autorizada, ferindo os princípios de integridade, disponibilidade e confidencialidade da informação contábil (ABU-MUSA, 2003).

De acordo com Abu-Musa (2006) os sistemas de informação contábil devem contemplar controles com o objetivo de impedir, prevenir, detectar e corrigir as ameaças à segurança da informação. Segundo o autor, os controles de segurança da informação podem ser classificados de acordo com sua associação com o estágio de processamento de dados, conforme apresentado a seguir:

- **Controles de entrada:** são utilizados para garantir que cada transação é autorizada, tratada corretamente e processada somente uma vez.
- **Controles de processamento:** são utilizados para garantir que as operações realizadas no sistema contábil são válidas e precisas, que dados externos não foram perdidos ou alterados e que as transações inválidas sejam reprocessadas corretamente.
- **Controles de saída:** são utilizados para impedir que cópias não autorizadas das informações sejam feitas, e que as impressões sejam direcionadas somente para pessoas autorizadas.
- **Controles armazenamento:** são utilizados para garantir que todos os dados e programas armazenados sejam protegidos contra acesso não autorizado, alteração, manipulação e divulgação.

Para Wilkinson et al. (2000), o controle interno é um estado no qual a administração se esforça para alcançar, de forma a fornecer uma garantia razoável de que os objetivos da organização serão atingidos. Estes controles abrangem uma série de práticas que são utilizadas com o objetivo de tentar neutralizar as exposições aos riscos. Os autores afirmam que os sistemas de informação contábil estão expostos a uma variedade de riscos os quais podem ser de origem interna ou externa, destacando:

a) Funcionários que processam dados e possuem acesso aos ativos da organização.
b) Os programadores e analistas de sistemas, que possuem conhecimentos sobre o processamento das transações.
c) Gerentes e contadores, que têm acesso aos registros e relatórios financeiros, e muitas vezes possuem autoridade para aprovar transações.
d) Os funcionários desligados que conhecem a estrutura de controle e podem praticar ações contra a organização.
e) Clientes e fornecedores que geram muitas das transações processadas pela organização.
f) Concorrentes que desejam obter informações confidenciais sobre os negócios.
g) Pessoas externas, tais como *hackers* e criminosos, que tentar acessar os dados e ativos da organização, com o objetivo de cometer atos destrutivos ou fraudulentos.
h) Eventos da natureza ou acidentes, tais como inundações, incêndios e quebra de equipamentos.

Ainda segundo Wilkinson et al. (2000), os riscos relacionados à informação contábil podem ser classificados conforme segue:

- **Erros não intencionais:** os erros não intencionais podem ocorrer em virtude de erro na digitação no processo de entrada de dados no sistema contábil ou erros nas instruções de processamento do sistema.
- **Erros intencionais:** os erros intencionais constituem fraude, uma vez que são realizados para proporcionar ganhos ilegais. As fraudes podem ocorrer em qualquer fase do ciclo do sistema de informação contábil (entrada, processamento ou saída).
- **Perdas não intencionais de ativos:** perdas não intencionais de ativos normalmente ocorrem por acidentes, por exemplo, o extravio de um documento ou um disco rígido danificado em virtude de queda de energia elétrica.
- **Roubo de ativos:** os ativos da organização podem ser roubados por pessoas internas ou externas a organização.
- **Violações de segurança:** pessoas não autorizadas podem ter acesso às informações da organização. As violações de segurança podem ser cometidas por pessoas internas ou externas a organização.
- **Atos de violência e desastres naturais:** situações inesperadas que podem gerar perda de ativos e comprometer a continuidade dos negócios, como por exemplo, atos de terrorismo, inundações, terremotos, entre outros.

Segundo Beard e Wen (2007), o contador deve ser conhecedor das ameaças de segurança da informação e dos controles adequados a fim de proteger o sistema de informação contábil e aconselhar a organização sobre os riscos relacionados à segurança da informação.

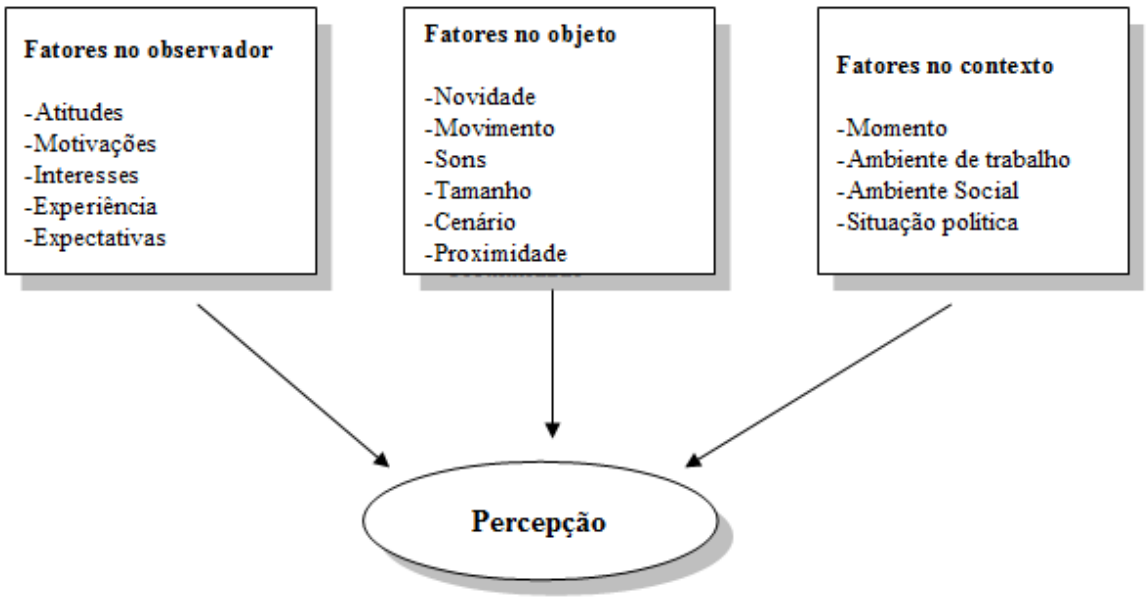
2.10. Teoria da Percepção

Este estudo tem como objetivo avaliar a percepção dos usuários da informação contábil a respeito da segurança da informação nas organizações, desta forma, se faz necessário entender os conceitos da percepção, bem como, os fatores que exercem influencia sobre a percepção.

Segundo Karsaklian (2000) cada indivíduo possui sua própria imagem do mundo, pois essa imagem é derivada da somatória de variáveis próprias e exclusivas do mesmo, entre elas a sua história passada, meio ambiente físico e social, além da personalidade e sua estrutura fisiológica e psicológica. Neste contexto, a autora define a percepção como um processo dinâmico pelo qual aquele que percebe atribui um significado as matérias brutas oriundas do meio ambiente, no qual o indivíduo não é o objeto, mais um ator confrontado a primeira etapa do processamento de informação.

Para Robbins (2002), o estudo da percepção pode ser definido como um processo pelo qual os indivíduos organizam e interpretam suas impressões sensoriais a fim de dar sentido ao seu ambiente. Segundo o autor, o comportamento do indivíduo baseia-se em sua percepção da realidade e não na realidade em si. Adicionalmente, o autor comenta que existe uma série de fatores que podem moldar e às vezes distorcer a percepção. Estes fatores podem estar no observador, no objeto alvo da percepção ou no contexto ou situação em que a percepção ocorre. A Figura 9 apresenta os fatores que influenciam a percepção, e em seguida, estão apresentados os conceitos de cada fator.

Figura 9 – Fatores que Influenciam a Percepção



Fonte: Adaptado de Robbins, 2002

- **Observador:** quando se observa um alvo e se tenta interpretar o que se está percebendo, esta interpretação é fortemente influenciada pelas características pessoais do observador. Necessidades insatisfeitas ou motivações estimulam os indivíduos e

podem exercer uma forte influência sobre a sua percepção. Do mesmo modo, interesses e experiências passadas também direcionam o enfoque do indivíduo, podendo, ainda, em contrapartida, anular o interesse por algum objeto.

- **Objeto:** as características do objeto, ou alvo, que está sendo observado também podem afetar a percepção. Objetos e eventos que nunca foram antes experimentados são mais perceptíveis que aqueles já conhecidos. Como os alvos não são observados isoladamente e deslocados de todo o contexto, a sua relação com o cenário influencia a percepção, indicando a tendência de se agrupar coisas próximas ou parecidas. O que se percebe irá depender, então, de como se separa o objeto de seu cenário geral.

- **Contexto:** o contexto, ou situação, dentro do qual se percebe o objeto é igualmente importante, uma vez que os elementos que fazem parte do ambiente influenciam a percepção. Pode-se não se reparar numa determinada jovem de biquíni numa praia, num final de semana. Contudo, se ela usar os mesmos trajes numa cerimônia religiosa, com certeza chamará muito mais a atenção dos presentes. Mantidos o observador e o alvo, a mudança do contexto operou uma modificação radical na percepção. Além disso, fatores situacionais e ambientais, como a localização, a temperatura e a iluminação também influenciam na atenção que se dedica ao objeto.

Neste contexto, fica evidente que a percepção de segurança da informação que foi obtida dos usuários da informação contábil pode sofrer influência de fatores como o observador (cargo, formação, etc.) e contexto (segmento da empresa, tamanho, etc.). Desta forma, o instrumento de coleta de dados utilizado nesta pesquisa contemplou perguntas para caracterização do respondente e da empresa, de modo que seja possível aferir as eventuais diferenças de percepção entre os usuários da informação contábil.

3. PROCEDIMENTOS METODOLÓGICOS

Para o desenvolvimento deste trabalho, optou-se por realizar uma pesquisa descritiva de caráter quantitativo, utilizando um questionário eletrônico tipo *survey* para coleta dos dados (Apêndice I). Os tópicos a seguir descrevem os detalhes e a justificativa dos procedimentos metodológicos que foram utilizados neste estudo.

3.1. Tipo de Pesquisa

Segundo Beuren (2009), as tipologias de delineamentos de pesquisa aplicadas na contabilidade podem ser agrupadas em três categorias: pesquisa quanto aos objetivos, pesquisa quanto aos procedimentos e pesquisa quanto à abordagem do problema, conforme apresentado a seguir.

a) Tipologia de pesquisa quanto aos objetivos:

Conforme Gil (1999), uma pesquisa descritiva tem como principal objetivo descrever características de determinada população ou fenômeno ou o estabelecimento de relação entre as variáveis. Uma de suas características mais significativas esta na utilização de técnicas padronizadas de coleta de dados.

Para Collis e Hussey (2005) a pesquisa descritiva descreve o comportamento dos fenômenos e busca identificar informações sobre as características de um determinado problema ou questão.

Deste modo, esta pesquisa que tem por objetivo, identificar e descrever a percepção dos usuários da informação contábil acerca do tema segurança da informação se enquadra como uma pesquisa descritiva.

b) Tipologia de pesquisa quanto aos procedimentos:

De acordo com Gil (1999), as pesquisas de levantamento ou *survey* se caracterizam pela interrogação direta das pessoas com o objetivo de conhecer o seu comportamento. Neste tipo de pesquisa, procede-se a solicitação de informações a um grupo significativo de pessoas

acerca do problema estudado para em seguida, mediante análise quantitativa, obter as conclusões correspondentes aos dados coletados.

Neste contexto, esta pesquisa utilizou como instrumento de coleta de dados um questionário eletrônico, com o objetivo de identificar a percepção de segurança da informação dos usuários da informação contábil, podendo se classificada como levantamento ou *survey*.

c) Tipologia de pesquisa quanto à abordagem do problema:

Richardson (2007) afirma que a abordagem quantitativa caracteriza-se pelo emprego de quantificação tanto nas modalidades de coleta de informações, quanto no tratamento delas por meio de técnicas estatísticas. O método quantitativo é normalmente aplicado em estudos descritivos que procuram descobrir e classificar a relação entre variáveis, bem como, estudos que investigam a relação de causalidade entre fenômenos. Segundo o autor, este tipo de pesquisa é utilizado para garantir a precisão e evitar distorções das análises e interpretações, atribuindo aos resultados obtidos uma maior margem de confiança.

Esta pesquisa teve como objetivo identificar a percepção dos usuários da informação contábil com relação à segurança da informação nas organizações, além de analisar a eventual existência de *gap* entre a avaliação da segurança da informação na organização e a importância da segurança da informação para os respondentes. Os dados coletados e utilizados nesta pesquisa são de origem quantitativa e foram analisados através de técnicas estatísticas, deste modo, esta pesquisa se caracteriza como uma pesquisa quantitativa.

3.2. Método de Pesquisa

Conforme mencionado no tópico anterior, o método a ser adotado é o quantitativo descritivo, sendo, que a coleta de dados foi realizada através da aplicação de um questionário eletrônico do tipo *survey* (Apêndice I).

3.3. População e Amostra

De acordo com Collis e Hussey (2005), o estágio mais crítico da *survey* é a seleção da amostra, uma vez que é importante garantir que a mesma não tenha vieses, e seja representativa da população da qual é retirada.

Para Richardson (2007) a amostra deve essencialmente constituir uma porção de uma determinada população e deve contemplar um número suficiente de casos, escolhidos aleatoriamente, para oferecer segurança estatística em relação à representatividade dos dados.

Esta pesquisa utilizou como população os usuários da informação contábil que atuam em organizações brasileiras de diversos segmentos. Entende-se como usuário da informação contábil, qualquer membro da organização que utilize a informação contábil para realização das suas atividades.

Com o objetivo de segmentar o usuário da informação contábil e permitir a análise da percepção da segurança da informação nos diferentes níveis organizacionais, foi estabelecida uma classificação conforme apresentado a seguir:

- **Cargos:** diretores, gerentes, coordenadores, auditores, analistas e outros.
- **Áreas:** contabilidade, controladoria, financeiro, auditoria e outros.

Segundo Hair et al. (2007) o tamanho da amostra deve representar, no mínimo, cinco vezes mais observações do que o número de variáveis utilizadas no estudo. Os autores recomendam que as análises multivariadas sejam realizadas com pelo menos 100 observações.

A amostra utilizada nesta pesquisa foi composta por 129 usuários da informação contábil que atuam em organizações brasileiras de diversos segmentos. O tamanho da amostra foi determinado visando atender aos pré-requisitos mínimos para realização das análises multivariadas, os quais foram plenamente atendidos. A amostra utilizada neste estudo foi escolhida de forma aleatória, sem levar em consideração a sua probabilidade de ocorrência, o que caracteriza uma amostra não probabilística por conveniência, devido às dificuldades e limitações para se garantir a aplicação de uma técnica de amostragem probabilística.

3.4. Procedimentos de Coleta de Dados

Segundo Richardson (2007) o instrumento de coleta de dados mais comum para obter informações acerca de grupos sociais é o questionário. Gil (1999) define o questionário como uma técnica de investigação composta por um número mais ou menos elevado de questões apresentadas por escrito às pessoas, tendo como objetivo o conhecimento de suas opiniões, crenças, sentimentos, interesses, expectativas e situações vivenciadas.

Esta pesquisa utilizou como instrumento de coleta de dados um questionário eletrônico, composto de questões predominantemente fechadas, com o objetivo de identificar a percepção de segurança da informação dos usuários da informação contábil (Apêndice I). Os detalhes referentes à elaboração do instrumento e coleta dos dados estão apresentados nos tópicos seguintes.

3.4.1. Elaboração do Instrumento de Coleta de Dados

Para elaboração do instrumento de coleta de dados utilizado nesta pesquisa, foi efetuada uma revisão na literatura, visando identificar estudos que utilizaram instrumentos confiáveis para mensurar os construtos relacionados à segurança da informação. Como resultado, foram identificados e considerados adequados os modelos propostos por Abu-Musa (2002) e Madnick et al. (2006), conforme apresentado de forma comparativa no Quadro 1. Observa-se que embora utilizem nomenclaturas diferentes, os construtos utilizados pelos autores seguem uma abordagem semelhante. Deste modo, foram selecionados 6 construtos que foram utilizados neste estudo, os quais contemplam os principais componentes da segurança da informação, conforme foi observado na revisão da literatura realizada sobre o tema (PELTIER, 2001; ELOFF e ELLOF, 2005; DA VEIGA e ELOFF, 2007; JOURDAN et al. 2010).

Quadro 1 – Construtos de Segurança da Informação

Construtos	**Abu-Musa (2002)**	**Madnick et al. (2006)**	**Utilizados neste estudo**
Vulnerabilidade		X	
Acessibilidade		X	
Confidencialidade	X	X	X
Integridade	X		X
Disponibilidade	X		X
Privacidade	X		
Precisão	X		
Validade	X		
Autenticidade	X		
Recursos Tecnológicos (Equipamentos)	X	X	X
Recursos Financeiros		X	
Políticas e Procedimentos		X	X
Cultura de Segurança (Pessoas)	X	X	X

Após a definição dos construtos, as assertivas utilizadas pelos autores foram traduzidas e adaptadas para uma melhor adequação ao usuário da informação contábil. Neste estudo,

foram selecionadas 4 assertivas para mensurar cada construto da segurança da informação. Hair et al. (2007) recomenda a utilização de no mínimo 3 indicadores para cada construto. As variáveis utilizadas para mensurar cada construto estão apresentadas no Quadro 2.

Quadro 2 – Variáveis utilizadas na pesquisa

Construto	Variável	Assertiva
Integridade	V4	O sistema de informação contábil raramente é violado por acesso não autorizado.
	V10	A organização possui recursos de segurança da informação adequados contra ameaças internas e externas ao sistema de informação contábil.
	V16	A organização verifica a identidade dos usuários antes de permitir acesso ao sistema de informação contábil.
	V17	As informações contábeis da organização raramente apresentam distorções ou erros.
Disponibilidade	V5	O sistema de informação contábil da organização está disponível apenas para usuários autorizados.
	V11	A organização mantém cópias de segurança dos sistemas e informações contábeis as quais estão sempre disponíveis quando necessário.
	V22	A organização possui um plano de contingência adequado para manutenção do funcionamento do sistema de informação contábil.
	V24	O sistema de informação contábil da organização está sempre disponível quando necessário.
Confidencialidade	V6	A organização possui políticas adequadas que definem como e quando a informação contábil pode ser compartilhada.
	V12	A organização possui políticas adequadas sobre a identificação de usuários, senhas e privilégios de acesso ao sistema de informação contábil.
	V18	A organização protege a privacidade dos dados confidenciais de clientes, fornecedores e funcionários.
	V23	A organização se preocupa com a proteção das informações corporativas confidenciais.
Equipamentos	V1	A organização possui especialistas em segurança da informação suficientes para cobrir as suas necessidades.
	V7	A organização realiza investimentos em segurança da informação sempre que necessário.
	V13	A organização possui recursos tecnológicos adequados para apoiar a segurança da informação.
	V19	A organização utiliza os seus recursos tecnológicos de forma eficaz para melhorar a segurança da informação.
Políticas e Procedimentos	V2	A organização realiza auditorias de segurança da informação periodicamente.
	V8	A organização possui uma estratégia de segurança da informação bem definida a qual é divulgada de forma adequada.
	V14	A organização tem políticas e procedimentos bem definidos para a segurança dos seus dados e da rede.
	V20	A organização dispõe de procedimentos para detectar e punir violações de segurança da informação.
Pessoas	V3	As pessoas da organização possuem conhecimento sobre as ferramentas e práticas de segurança da informação.
	V9	As pessoas da organização seguem cuidadosamente as boas práticas de segurança da informação.
	V15	As pessoas da organização sempre exercem conduta ética com os dados e redes.
	V21	As pessoas da organização estão conscientes das práticas de segurança da informação.

Fonte: Adaptado de Madnick et al. (2006) e Abu-Musa (2002)

Com o objetivo de transparecer uma maior organização e facilitar o preenchimento por parte dos respondentes, o questionário utilizado nesta pesquisa foi divido em cinco seções.

Na primeira seção foi apresentada uma breve introdução com os objetivos do estudo e as instruções para o preenchimento do questionário.

A segunda e a terceira seção contemplaram questões demográficas para delinear o perfil do respondente e da organização.

Na quarta seção, foram incluídas as 24 assertivas relacionadas aos construtos de segurança da informação, onde os respondentes foram convidados a atribuir notas de 1 a 10 (sendo 1 o mínimo e 10 o máximo) para cada assertiva, de modo que refletisse a sua percepção da segurança da informação em duas escalas, sendo:

- **Avaliação:** em sua opinião, o quanto a sua organização considera importante esta assertiva de segurança da informação.
- **Importância:** em sua opinião, o quanto você considera importante esta assertiva de segurança da informação.

A quinta e última seção do questionário foi utilizada para agradecer a participação e solicitar de forma voluntária, o endereço de *e-mail* do respondente, para posterior envio dos resultados obtidos na pesquisa.

Vale destacar que Hair et al. (2007) recomendam a utilização de escalas com muitos itens para se obter uma maior confiabilidade nos testes estatísticos, deste modo, optou-se por utilizar neste instrumento de coleta de dados uma escala do tipo *Likert* de 10 pontos. Em adição, Finney e Di Stefano (2006) citados por Silva (2009) comentam que no campo de estudos das ciências sociais é comum o tratamento dos dados categóricos como se fossem contínuos, quando esses dados são provenientes de escalas ordinais com cinco ou mais categorias e, com distribuições aproximadamente normais. Neste caso, os dados são tratados como se fossem contínuos sem grandes distorções nos índices de ajuste, pois quanto maior o aumento das categorias mais os dados se aproximarão de um nível de mensuração contínuo.

Segundo Richardson (2007) depois de definido o instrumento de coleta de dados, o pesquisador deve realizar um pré-teste aplicando o instrumento a um número reduzido de elementos que possuam as mesmas características da amostra que esta sendo estudada. Seguindo esta recomendação, a primeira versão do questionário foi submetida a uma amostra pré-teste contendo 6 usuários da informação contábil, os quais foram convidados a realizar

uma análise de aplicabilidade de cada assertiva em seu ambiente de atuação, bem como, reportar sugestões e comentários quanto às instruções ou questões que não estivessem claras no questionário. Tais sugestões foram analisadas e, na medida do necessário, incorporadas ao questionário final que esta disponível no Apêndice I deste trabalho.

3.4.2. Coleta de Dados

Com o objetivo de facilitar a coleta e posterior análise dos dados da pesquisa, optou-se por desenvolver um questionário eletrônico, o qual ficou disponível na internet através do *link* http://fs4.formsite.com/wagnerlimas/form1/index.html.

O convite para participação na pesquisa (Apêndice II) foi enviado via *e-mail* para cerca de 300 potenciais respondentes. Passadas duas semanas do envio do convite inicial, outro *e-mail* foi enviado aos potenciais respondentes, agradecendo aos que já participaram e relembrando os demais da importância da sua participação.

A coleta de dados foi realizada entre outubro e novembro de 2011, e obteve 131 questionários respondidos por usuários da informação contábil. Deste total de questionários, 2 exemplares foram excluídos por apresentarem dados extremos (*outliers*). Desta forma, a amostra final foi composta por 129 questionários válidos, o que representa uma taxa de resposta de 43%. Vale lembrar que o convite enviado aos potenciais respondentes contemplava uma solicitação para que a pesquisa fosse encaminhada a outros colegas de trabalho, deste modo, a disseminação do questionário entre os próprios respondentes pode ter auxiliado na obtenção das respostas.

3.5. Procedimentos de Tratamento de Dados

Segundo Collis e Hussey (2005) a escolha da técnica de análise de dados depende da natureza da pesquisa, podendo ser quantitativa ou qualitativa. Para Hair et al (2007) as técnicas multivariadas são recomendadas quando se tem um número grande de variáveis com relação de dependência ou inter-relações entre elas. Para os autores, a análise multivariada contempla todos os métodos estatísticos que simultaneamente analisam múltiplas medidas sobre cada indivíduo ou objeto de investigação.

O modelo de análise de *gap* e as técnicas estatísticas que foram utilizadas neste estudo estão apresentados de forma detalhada nos tópicos seguintes.

3.5.1. Análise de *Gap*

Neste trabalho foi utilizado o modelo de análise de *gap* proposto por Parasuraman, Zeithaml e Berry (1985) que consiste em analisar o *gap* existente entre a expectativa do serviço que os usuários esperam receber, e a percepção do que realmente recebem.

O modelo sugere que sob o ponto de vista dos usuários, a qualidade dos serviços é a diferença entre a sua expectativa do que é esperado e a sua percepção daquilo que é recebido. Se a expectativa se iguala a percepção, o usuário está tecnicamente satisfeito. Quando a percepção excede a expectativa, o usuário está mais do que satisfeito. Quando a expectativa excede a percepção, o usuário está insatisfeito, evidenciando um problema de qualidade nos serviços.

A análise de *gap* foi realizada de acordo com a percepção do usuário da informação contábil acerca do tema segurança da informação. O *gap* foi obtido através da diferença entre as médias da avaliação (como o respondente avalia a segurança da informação na sua organização) e da importância (o quanto o respondente considera a segurança da informação importante) atribuída a cada construto mensurado no instrumento de coleta de dados. Quando a avaliação se iguala a importância, pode-se deduzir que o usuário da informação contábil está satisfeito com a segurança da informação na organização. No caso da avaliação superar a importância, haverá evidencias de que o usuário da informação contábil atribui menor importância ao tema do que o esperado pela organização. Por fim, quando a importância superar a avaliação, haverá indícios de que as organizações atribuem menor importância ao tema do que o esperado pelo usuário da informação contábil.

3.5.2. Técnicas Estatísticas

Os dados obtidos através do instrumento de coleta de dados foram inicialmente codificados e tabulados para receberem tratamento estatístico no *software* IBM SPSS (*Statistical Package for Social Sciences*) em sua versão 17.0. As análises necessárias para elaboração da estatística descritiva foram realizadas com auxílio do *software* Microsoft Excel, em sua versão 2003.

Para análise dos resultados desta pesquisa foram utilizadas duas técnicas estatísticas. A primeira técnica refere-se ao coeficiente Alfa de Cronbach, que foi utilizado com o objetivo

de validar a confiabilidade dos construtos de segurança da informação. O teste não-paramétrico de Wilcoxon para comparação de amostras pareadas foi a segunda técnica utilizada neste trabalho, e teve como objetivo comprovar estatisticamente a diferença entre as médias de avaliação e importância da segurança da informação. Nos tópicos seguintes estão detalhadas as técnicas estatísticas que foram utilizadas nesta pesquisa.

3.5.3. Coeficiente Alfa de Cronbach

De acordo com Corrar et al. (2007) o pesquisador deve certificar-se de que as medidas escolhidas para mensurar os resultados da pesquisa estão corretas. Os autores recomendam a utilização de análises de confiabilidade com o objetivo de certificar que uma escala produz resultados consistentes entre medidas repetidas ou equivalentes de um mesmo objeto ou pessoa, revelando a ausência de erro aleatório.

Segundo Pestana e Gageiro (2000), o Alfa de Cronbach é uma das medidas mais utilizadas para verificação da consistência interna de um grupo de variáveis. O Alfa de Cronbach pode ser definido como a correlação que se espera obter entre a escala usada e outras escalas hipotéticas do mesmo universo, com igual número de itens, que meçam a mesma característica.

Para Hair et al. (2007) os testes de consistência interna são utilizados para certificar que os itens ou indicadores individuais da escala estão medindo o mesmo construto, de modo que sejam inter-correlacionados. Segundo os autores, o Alfa de Cronbach é um coeficiente de confiabilidade que avalia a consistência da escala inteira, desta forma, quanto maior o número de itens na escala, maior a confiabilidade do coeficiente Alfa de Cronbach.

O Alfa de Crombach é analisado observando-se uma variação de 0 até 1, de modo que, quanto mais próximo de 1 estiver o seu valor, maior a fidedignidade das dimensões do construto. Para Hair et al. (2007) o limite inferior de consistência geralmente aceito no Alfa de Cronbach é 0,70, podendo ser reduzido ao patamar de 0,60 em pesquisas exploratórias. As situações em que o Alfa de Cronbach apresenta valores inferiores a 0,60 indicam a falta de consistência do construto, bem como, a existência de algum indicador não apropriado para mensurar o conceito subjacente.

3.5.4. Teste de Wilcoxon para Amostras Pareadas

Um dos objetivos propostos para este estudo foi verificar a existência de diferenças significativas (*gap*) entre as médias das variáveis relacionadas à avaliação e a importância da segurança da informação, de acordo com a percepção do usuário da informação contábil. Para tanto, recorreu-se ao teste não-paramétrico de Wilcoxon para comparação de amostras pareadas.

Segundo Fávero et al (2009), os testes não-paramétricos não exigem suposições numerosas ou restringentes em relação a distribuição dos dados, sendo uma alternativa aos testes paramétricos quando as condições de aplicação destes testes não se verificam. Desta forma, optou-se por utilizar um teste não-paramétrico devido aos dados utilizados nesta pesquisa não apresentarem uma distribuição normal.

De acordo com Maroco (2010), o teste de Wilcoxon para amostras pareadas é uma alternativa não-paramétrica ao teste *t*-Student quando o pressuposto de distribuição normal da variável nas duas medições não se verifica. O teste de Wilcoxon, ou de sinais postos, é utilizado para determinar se os valores de uma amostra são inferiores, iguais ou superiores aos valores de outra amostra. Além da informação sobre a direção das diferenças para cada par, o teste de Wilcoxon leva em consideração a magnitude da diferença dentro dos pares. As hipóteses testadas pelo teste de Wilcoxon para amostras pareadas estão apresentadas a seguir:

- H0: $\mu 1 = \mu 2$ (indica que não há diferença entre os dados amostrais)
- H1: $\mu 1 \neq \mu 2$ (indica que há diferença entre os dados amostrais)

Para realização do teste de Wilcoxon para amostras pareadas são calculadas as diferenças entre os pares de variáveis e ordenados por postos de diferenças absolutas. Em seguida, são somados os postos positivos e negativos, o que permite o cálculo da estatística Z. Para analisar o resultado fornecido pelo teste deve-se verificar a significância obtida, de modo que, se a significância for superior a 0,05, não há evidências suficientes contra a hipótese nula, ou seja, não se deve rejeitar a hipótese nula ao nível de significância de 5%. Caso contrário há evidencias suficientes contra a hipótese nula e a mesma deve ser rejeitada (MAROCO, 2010).

4. APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Os resultados desta pesquisa estão apresentados em três grupos. No primeiro grupo está demonstrada a análise descritiva da amostra utilizada na pesquisa, em seguida estão apresentados os testes que foram realizados para obter a confiabilidade dos construtos de segurança da informação, e por fim, estão apresentados os testes estatísticos e discussões referentes à análise de *gap*.

4.1. Caracterização da Amostra

A pesquisa de campo ocorreu entre os meses de outubro e novembro de 2011, e foi realizada através de um questionário eletrônico que ficou disponível na internet durante o período de coleta de dados (Apêndice I). Os potenciais respondentes foram convidados a participar da pesquisa através de um convite enviado via *e-mail*, contendo o *link* para a pesquisa (Apêndice II). No total, foram enviados cerca de 300 *e-mails* aos potenciais respondentes. Ao final da coleta de dados, foram obtidos 131 questionários que foram respondidos por usuários da informação contábil, contudo, 2 exemplares foram excluídos da amostra por apresentarem dados extremos (*outliers*). Deste modo, a amostra final foi composta de 129 questionários válidos, o que representa uma taxa de resposta de 43%.

A distribuição dos respondentes por nível de escolaridade e formação está sumarizada na Tabela 1. Com relação ao nível de escolaridade, pode-se observar que 30% dos respondentes possuem nível superior, 40% pós-graduação e 26% possuem mestrado. Observa-se que apenas 3% dos respondentes não possuem nível superior. A maioria dos respondentes possui formação em contabilidade, e representam 48% da amostra. Os administradores e economistas participantes da pesquisa representam 34% da amostra.

Tabela 1 – Distribuição dos Respondentes por Nível de Escolaridade e Formação

Escolaridade	Formação					Total	%
	Contabilidade	Economia	Administração	Engenharia	Outro		
Segundo Grau	-	-	1	-	-	**1**	**1%**
Técnico	2	-	-	-	-	**2**	**2%**
Superior	20	3	7	3	6	**39**	**30%**
Pós-Graduação	22	4	14	4	7	**51**	**40%**
Mestrado	18	8	5	1	2	**34**	**26%**
Doutorado	-	-	1	-	-	**1**	**1%**
Outro	-	-	1	-	-	**1**	**1%**
Total	**62**	**15**	**29**	**8**	**15**	**129**	**100%**
%	**48%**	**12%**	**22%**	**6%**	**12%**	**100%**	

Esta pesquisa estabeleceu como população os usuários da informação contábil que atuam em organizações brasileiras, deste modo, uma característica importante a ser observada é a área de atuação e cargo dos respondentes. A Tabela 2 apresenta a distribuição dos respondentes por área de atuação e cargo. Pode-se observar que a maior parte da amostra é constituída por usuários da informação contábil que atuam nas áreas de controladoria (36%), contabilidade (16%) e financeiro (20%). Com relação ao cargo dos respondentes, os gerentes representam 31% da amostra, diretores 15% e coordenadores 13%. Desta forma, é possível deduzir que 59% da amostra é composta por usuários da informação contábil que possuem cargo de liderança nas organizações. Esta característica se faz importante para este estudo, pois possibilitará a comparação da percepção entre os diversos níveis funcionais dos usuários da informação contábil com relação à segurança da informação.

Tabela 2 – Distribuição dos Respondentes por Área de Atuação e Cargo

Área de Atuação	Cargo						Total	%
	Diretor	Gerente	Coordenador	Analista	Auditor	Outro		
Administração Geral	3	3	-	4	-	-	**10**	**8%**
Contabilidade	3	4	5	3	-	6	**21**	**16%**
Controladoria	4	20	4	17	-	2	**47**	**36%**
Financeiro	5	8	3	8	-	2	**26**	**20%**
Auditoria	1	1	3	-	6	1	**12**	**9%**
Outro	3	4	2	3	-	1	**13**	**10%**
Total	**19**	**40**	**17**	**35**	**6**	**12**	**129**	**100%**
%	**15%**	**31%**	**13%**	**27%**	**5%**	**9%**	**100%**	

O tempo de empresa dos respondentes pode ser observado na Tabela 3. Percebe-se que apenas 12% da amostra é representada por usuários da informação contábil que possuem

menos de 1 ano de empresa. A maior parte dos respondentes possui entre 1 e 5 anos de empresa (42%), seguido dos que possuem entre 5 e 10 anos (22%).

Tabela 3 – Distribuição dos Respondentes por Tempo de Empresa

Tempo de Empresa	**Total**	**%**
Menos de 1 ano	**16**	**12%**
Entre 1 e 5 anos	**54**	**42%**
Entre 5 e 10 anos	**29**	**22%**
Entre 10 e 20 anos	**20**	**16%**
Acima de 20 anos	**10**	**8%**
Total	**129**	**100%**

O instrumento de coleta de dados contemplou questões com o objetivo de obter as características das empresas nas quais os respondentes atuam. A distribuição das empresas por segmento e tempo de atuação está apresentada na Tabela 4. Observa-se que 39% das empresas atuam no segmento de indústria, 30% no segmento de serviço e 12% são instituições financeiras. Dentre as empresas que compõe a amostra, a maior parte possui mais de 10 anos de atuação no mercado, sendo que 18% possuem entre 10 e 20 anos, 12% possuem entre 20 e 30 anos e 40% estão no mercado a mais de 30 anos.

Tabela 4 – Distribuição das Empresas por Segmento e Tempo de Atuação

Segmento de Atuação	**Tempo de Atuação**					**Total**	**%**
	Até 5 anos	**Entre 5 e 10 anos**	**Entre 10 e 20 anos**	**Entre 20 e 30 anos**	**Acima de 30 anos**		
Agronegócio	-	-	-	1	-	**1**	**1%**
Indústria	7	2	11	2	28	**50**	**39%**
Comércio	2	2	-	-	5	**9**	**7%**
Serviço	8	9	7	6	9	**39**	**30%**
Instituição Financeira	3	3	2	4	3	**15**	**12%**
Outro	2	2	3	2	6	**15**	**12%**
Total	**22**	**18**	**23**	**15**	**51**	**129**	**100%**
%	**17%**	**14%**	**18%**	**12%**	**40%**	**100%**	

Nesta pesquisa, utilizou-se o número de funcionários para classificação do tamanho da empresa, entre pequena, média e grande. Na Tabela 5 está apresentada a distribuição das empresas por número de funcionários. Considerando que as empresas de pequeno porte possuem até 500 funcionários, a amostra analisada é composta por 32% de empresas com esta característica. As empresas consideradas médias (de 501 a 5.000 funcionários) representam

28% da amostra. Por fim, empresas que possuem mais de 5.000 funcionários, consideradas grandes, representam 41%, caracterizando, desta forma, a maior parte da amostra.

Tabela 5 – Distribuição das Empresas por Número de Funcionários

Número de Funcionários	Total	%
De 1 a 100	**21**	**16%**
De 101 a 500	**20**	**16%**
De 501 a 1.000	**8**	**6%**
De 1.001 a 5.000	**28**	**22%**
De 5.001 a 10.000	**32**	**25%**
Acima de 10.000	**20**	**16%**
Total	**129**	**100%**

Com o objetivo de avaliar eventuais relações entre a segurança da informação contábil e o sistema corporativo utilizado pelas empresas, os usuários da informação contábil participantes da pesquisa foram convidados a fornecer o nome do sistema corporativo que suas respectivas organizações utilizam. Conforme pode ser observado na Tabela 6, o sistema SAP é utilizado por 26% das empresas que compõem a amostra, enquanto o sistema Tovs - Datasul representa 19% da amostra. No instrumento de coleta dados, foram incluídos os sistemas corporativos mais comumente utilizados nas empresas, contudo, 35% dos respondentes indicaram que o sistema utilizado na sua organização não constava na lista de opções utilizada nesta pesquisa.

Tabela 6 – Distribuição das Empresas por Sistema Corporativo Utilizado

Sistema Corporativo Utilizado	Total	%
Totvs - Microsiga	**10**	**8%**
Totvs - RM Sistemas	**2**	**2%**
Totvs - Data Sul	**25**	**19%**
Oracle - Applications	**9**	**7%**
Oracle - Peoplesoft	**2**	**2%**
Microsoft - Dynamics	**2**	**2%**
SAP	**34**	**26%**
Outro	**45**	**35%**
Total	**129**	**100%**

De acordo com os dados que foram utilizados na análise descritiva, pode-se deduzir que a amostra obtida neste trabalho representa de forma satisfatória a população alvo desta pesquisa, ou seja, os usuários da informação contábil que atuam em organizações brasileiras.

O tamanho da amostra baseou-se na recomendação de Hair et al. (2007) que sugere um número mínimo de 5 observações por variável, premissa que foi cumprida satisfatoriamente neste estudo.

4.2. Validação dos Construtos de Segurança da Informação

Com o objetivo de avaliar a consistência interna entre as variáveis utilizadas para mensurar os construtos de segurança da informação, foi utilizado o coeficiente Alfa de Cronbach. Segundo Pestana e Gageiro (2000), o Alfa de Cronbach é uma das medidas mais utilizadas para verificação da consistência interna de um grupo de variáveis, o que justifica o emprego dessa técnica para averiguar a confiabilidade do instrumento de pesquisa utilizado.

A análise de confiabilidade foi realizada através do procedimento *Reliability Analysis* disponível no *software* SPSS. O teste foi aplicado duas vezes para cada construto, uma vez que as variáveis utilizadas neste trabalho foram mensuradas em duas escalas de respostas (avaliação e importância), sendo necessário, desta forma, validar a confiabilidade do construto nas duas dimensões.

O resultado do teste de confiabilidade realizado para o construto Integridade esta apresentado na Tabela 7. Observa-se que o Alfa de Cronbach foi de 0,804 para a escala de avaliação e de 0,892 para a escala de importância. Segundo Hair et al. (2007), o valor mínimo para o Alfa de Cronbach deve ser 0,700, desta forma, não houve necessidade de retirar qualquer variável da análise. Os resultados apresentados indicam que as assertivas propostas são confiáveis para mensurar o construto Integridade, desta forma, este construto é considerado consistente.

Tabela 7 – Teste de Confiabilidade - Construto Integridade

Escala	Variável	Escala de Médias se o Item é Retirado	Variância se o Item é Retirado	Correlação Total do Item	Alfa se o Item é Retirado	Alfa de Cronbach
Avaliação	V4_A	23,233	28,133	0,533	0,797	0,804
	V10_A	23,798	25,803	0,716	0,706	
	V16_A	22,845	30,351	0,594	0,770	
	V17_A	23,961	24,928	0,653	0,739	
Importância	V4_I	27,271	14,777	0,737	0,871	0,892
	V10_I	27,442	13,889	0,842	0,830	
	V16_I	27,326	14,753	0,828	0,838	
	V17_I	27,357	16,200	0,651	0,901	

Para o construto Disponibilidade, o Alfa de Cronbach foi de 0,771 para a escala de avaliação e de 0,878 para a escala de importância (Tabela 8). Segundo Hair et al. (2007), o valor mínimo para o Alfa de Cronbach deve ser 0,700, desta forma, não houve necessidade de retirar qualquer variável da análise. Os resultados apresentados indicam que as assertivas propostas são confiáveis para mensurar o construto Disponibilidade, desta forma, este construto é considerado consistente.

Tabela 8 – Teste de Confiabilidade - Construto Disponibilidade

Escala	Variável	Escala de Médias se o Item é Retirado	Variância se o Item é Retirado	Correlação Total do Item	Alfa se o Item é Retirado	Alfa de Cronbach
Avaliação	V5_A	23,248	26,875	0,457	0,773	0,771
	V11_A	23,891	22,488	0,645	0,674	
	V22_A	24,829	21,314	0,664	0,663	
	V24_A	23,636	27,733	0,544	0,734	
Importância	V5_I	27,163	16,887	0,623	0,884	0,878
	V11_I	27,310	14,122	0,787	0,823	
	V22_I	27,550	13,453	0,794	0,821	
	V24_I	27,326	15,065	0,752	0,838	

A Tabela 9 apresenta o resultado do teste de confiabilidade para o construto Confidencialidade. Para este construto o Alfa de Cronbach foi de 0,838 na escala de avaliação e de 0,901 na escala de importância. Segundo Hair et al. (2007), o valor mínimo para o Alfa de Cronbach deve ser 0,700, desta forma, não houve necessidade de retirar qualquer variável da análise. Os resultados apresentados indicam que as assertivas propostas são confiáveis para mensurar o construto Confidencialidade, desta forma, este construto é considerado consistente.

Tabela 9 – Teste de Confiabilidade - Construto Confidencialidade

Escala	Variável	Escala de Médias se o Item é Retirado	Variância se o Item é Retirado	Correlação Total do Item	Alfa se o Item é Retirado	Alfa de Cronbach
Avaliação	V6_A	24,264	30,055	0,600	0,831	0,838
	V12_A	23,364	31,780	0,673	0,794	
	V18_A	23,240	31,106	0,691	0,786	
	V23_A	23,271	29,949	0,728	0,769	
Importância	V6_I	27,636	11,437	0,780	0,874	0,901
	V12_I	27,411	12,400	0,730	0,890	
	V18_I	27,256	12,192	0,805	0,864	
	V23_I	27,326	12,049	0,810	0,862	

Com relação ao construto Equipamentos, observa-se na Tabela 10 que o Alfa de Cronbach foi de 0,896 para a escala de avaliação e de 0,893 para a escala de importância. Segundo Hair et al. (2007), o valor mínimo para o Alfa de Cronbach deve ser 0,700, desta forma, não houve necessidade de retirar qualquer variável da análise. Os resultados apresentados indicam que as assertivas propostas são confiáveis para mensurar o construto Equipamentos, desta forma, este construto é considerado consistente.

Tabela 10 – Teste de Confiabilidade - Construto Equipamentos

Escala	Variável	Escala de Médias se o Item é Retirado	Variância se o Item é Retirado	Correlação Total do Item	Alfa se o Item é Retirado	Alfa de Cronbach
Avaliação	V1_A	22,163	35,606	0,736	0,880	0,896
	V7_A	22,008	33,445	0,829	0,844	
	V13_A	21,543	38,516	0,761	0,870	
	V19_A	21,589	38,760	0,767	0,869	
Importância	V1_I	26,651	16,245	0,755	0,869	0,893
	V7_I	26,628	16,720	0,753	0,868	
	V13_I	26,442	18,670	0,775	0,863	
	V19_I	26,442	17,514	0,796	0,852	

No caso do construto Políticas e Procedimentos, o Alfa de Cronbach apresentado (Tabela 11) foi de 0,865 para a escala de avaliação e de 0,888 para a escala de importância. Segundo Hair et al. (2007), o valor mínimo para o Alfa de Cronbach deve ser 0,700, desta forma, não houve necessidade de retirar qualquer variável da análise. Os resultados apresentados indicam que as assertivas propostas são confiáveis para mensurar o construto Políticas e Procedimentos, desta forma, este construto é considerado consistente.

Tabela 11 – Teste de Confiabilidade - Construto Políticas e Procedimentos

Escala	Variável	Escala de Médias se o Item é Retirado	Variância se o Item é Retirado	Correlação Total do Item	Alfa se o Item é Retirado	Alfa de Cronbach
Avaliação	V2_A	21,008	38,648	0,662	0,857	0,865
	V8_A	20,752	39,829	0,777	0,802	
	V14_A	20,062	44,371	0,753	0,819	
	V20_A	20,481	41,845	0,698	0,834	
Importância	V2_I	26,349	17,370	0,705	0,875	0,888
	V8_I	26,581	16,105	0,771	0,851	
	V14_I	26,271	17,512	0,765	0,853	
	V20_I	26,171	16,877	0,784	0,845	

Por fim, foi realizado o teste de confiabilidade para o construto Pessoas, conforme apresentado na Tabela 12. O Alfa de Cronbach obtido foi de 0,839 para a escala de avaliação e de 0,906 para a escala de importância. Segundo Hair et al. (2007), o valor mínimo para o Alfa de Cronbach deve ser 0,700, desta forma, não houve necessidade de retirar qualquer variável da análise. Os resultados apresentados indicam que as assertivas propostas são confiáveis para mensurar o construto Pessoas, desta forma, este construto é considerado consistente.

Tabela 12 – Teste de Confiabilidade - Construto Pessoas

Escala	Variável	Escala de Médias se o Item é Retirado	Variância se o Item é Retirado	Correlação Total do Item	Alfa se o Item é Retirado	Alfa de Cronbach
Avaliação	V3_A	20,822	28,070	0,623	0,819	0,839
	V9_A	20,721	26,937	0,689	0,789	
	V15_A	20,016	29,797	0,623	0,817	
	V21_A	20,372	27,423	0,760	0,759	
Importância	V3_I	26,535	18,579	0,706	0,918	0,906
	V9_I	26,287	19,566	0,864	0,852	
	V15_I	26,101	20,623	0,794	0,877	
	V21_I	26,217	19,953	0,822	0,867	

Um resumo dos coeficientes Alfa de Cronbach obtidos para cada construto nas escalas de avaliação e importância pode ser verificado na Tabela 13.

Tabela 13 – Alfa de Cronbach dos Construtos de Segurança da Informação

	Alfa de Cronbach	
Construto	**Avaliação**	**Importância**
Integridade	0,804	0,892
Disponibilidade	0,771	0,878
Confidencialidade	0,838	0,901
Equipamentos	0,896	0,893
Políticas e Procedimentos	0,865	0,888
Pessoas	0,839	0,906

Como resultado do teste de confiabilidade dos construtos, constatou-se que todos os seis construtos utilizados para mensurar a percepção de segurança da informação apresentaram valores satisfatórios (acima de 0,700), e podem ser considerados consistentes conforme as premissas recomendadas por Hair et al. (2007).

4.3. Análise de *Gap*

A análise de *gap* deste estudo foi realizada de acordo com a percepção do usuário da informação contábil acerca do tema segurança da informação. O *gap* foi obtido através da diferença entre as médias da avaliação (como o respondente avalia a segurança da informação na sua organização) e da importância (o quanto o respondente considera a segurança da informação importante) atribuída para cada construto mensurado no instrumento de coleta de dados.

Para realização da análise de *gap*, optou-se por criar duas novas variáveis para cada construto, as quais representaram as escalas de avaliação e importância. A criação destas variáveis foi realizada através do método das escalas somadas, de modo que as novas variáveis foram compostas pela média aritmética das variáveis que compõe cada construto. Segundo Hair et al. (2007), esse método permite reduzir os erros de medida das variáveis individuais, e permite o uso de uma nova variável mais rica, que capta as múltiplas faces de uma dimensão mais complexa.

Com o objetivo de identificar diferenças estaticamente significativas entre as médias apresentadas para os construtos de segurança da informação nas escalas de avaliação e importância, recorreu-se ao teste não-paramétrico de Wilcoxon para amostras pareadas, através do procedimento *Two Related Samples Test* disponível no *software* SPSS.

Para a realização deste teste, foi avaliada a seguinte hipótese: H0: $\mu 1 = \mu 2$, onde $\mu 1$ e $\mu 2$ representam as médias das variáveis da avaliação e da importância da segurança da informação atribuídas pelo usuário da informação contábil em cada construto. Os resultados obtidos para cada construto estão apresentados nos tópicos seguintes.

4.3.1. Construto Integridade

A integridade é o princípio que garante a conformidade dos dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados, bem como a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário (TCU, 2008). Segundo Abu-Musa (2002) a integridade refere-se à prevenção de criação e modificação de informações por pessoas não autorizadas.

As médias das variáveis de avaliação e importância atribuídas pelo usuário da informação contábil ao construto Integridade foram submetidas ao teste pareado de amostras,

conforme apresentado na Tabela 14. Como resultado, obteve-se os valores (*gap*=1,297; Z=-7,606; Sig=0,000); o que indica a rejeição da hipótese nula e a não igualdade das médias das variáveis, devido ao nível de significância inferior a 0,05 (MAROCO, 2010).

Tabela 14 – Teste Pareado de Amostras – Construto Integridade

Variáveis Comparadas	Média das Variáveis	*Gap*	Ranks			Z	Significância
			Negativo	Positivo	Igual		
INTE_I	9,116						
INTE_A	7,820	1,297	100	15	14	-7,606	0,000

Observa-se que o *gap* entre a avaliação e a importância para o construto Integridade foi de 1,297, desta forma, os usuários da informação contábil demonstraram que as organizações atribuem menor importância ao tema do que o esperado (Confirma-se H1).

4.3.2. Construto Disponibilidade

O princípio da disponibilidade consiste em garantir que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido (TCU, 2008). Abu-Musa (2002) define a disponibilidade como a prevenção da indisponibilidade, temporária ou permanente, no acesso as informações por usuários autorizados.

As médias das variáveis de avaliação e importância atribuídas pelo usuário da informação contábil ao construto Disponibilidade foram submetidas ao teste pareado de amostras, conforme apresentado na Tabela 15. Como resultado, obteve-se os valores (*gap*=1,145; Z=-7,438; Sig=0,000), o que indica a rejeição da hipótese nula e a não igualdade das médias das variáveis, devido ao nível de significância inferior a 0,05 (MAROCO, 2010).

Tabela 15 – Teste Pareado de Amostras – Construto Disponibilidade

Variáveis Comparadas	Média das Variáveis	*Gap*	Ranks			Z	Significância
			Negativo	Positivo	Igual		
DISP_I	9,112						
DISP_A	7,967	1,145	100	16	13	-7,438	0,000

Observa-se que o *gap* entre a avaliação e a importância para o construto Disponibilidade foi de 1,145, desta forma, os usuários da informação contábil demonstraram que as organizações atribuem menor importância ao tema do que o esperado (Confirma-se H2).

4.3.3. Construto Confidencialidade

A confidencialidade é princípio que tem por objetivo garantir que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação (TCU, 2008). Segundo Abu-Musa (2002), a confidencialidade diz respeito à garantia de que as informações são divulgadas apenas a pessoas, entidades e processos autorizados.

As médias das variáveis de avaliação e importância atribuídas pelo usuário da informação contábil ao construto Confidencialidade foram submetidas ao teste pareado de amostras, conforme apresentado na Tabela 16. Como resultado, obteve-se os valores (*gap*=1,291; Z=-7,590; Sig=0,000), o que indica a rejeição da hipótese nula e a não igualdade das médias das variáveis, devido ao nível de significância inferior a 0,05 (MAROCO, 2010).

Tabela 16 – Teste Pareado de Amostras – Construto Confidencialidade

Variáveis Comparadas	Média das Variáveis	*Gap*	Ranks			Z	Significância
			Negativo	Positivo	Igual		
CONF_I	9,136						
CONF_A	7,845	1,291	86	18	25	-7,590	0,000

Observa-se que o *gap* entre a avaliação e importância do construto Confidencialidade foi de 1,291, desta forma, os usuários da informação contábil demonstraram que as organizações atribuem menor importância ao tema do que o esperado (Confirma-se H3).

4.3.4. Construto Equipamentos

Segundo Madnick et al. (2006) as práticas de segurança da informação devem ser apoiadas por recursos tecnológicos e financeiros. Os equipamentos utilizados para armazenar e processar as informações devem ser protegidos contra acesso físico não autorizado, roubo e eventuais danos (ABU-MUSA, 2002). É importante lembrar que, segundo Kayworth e Whitten (2010), nenhuma solução ou mecanismo tecnológico é suficiente para garantir a eficácia da segurança da informação nas organizações.

As médias das variáveis de avaliação e importância atribuídas pelo usuário da informação contábil ao construto Equipamentos foram submetidas ao teste pareado de amostras, conforme apresentado na Tabela 17. Como resultado, obteve-se os valores

(*gap*=1,572; Z=-8,189; Sig= 0,000), o que indica a rejeição da hipótese nula e a não igualdade das médias das variáveis, devido ao nível de significância inferior a 0,05 (MAROCO, 2010).

Tabela 17 – Teste Pareado de Amostras – Construto Equipamentos

Variáveis Comparadas	Média das Variáveis	*Gap*	Ranks			Z	Significância
			Negativo	Positivo	Igual		
EQUI_I	8,847						
EQUI_A	7,275	1,572	100	15	14	-8,189	0,000

Observa-se que o *gap* entre a avaliação e a importância para o construto Equipamentos foi de 1,572, desta forma, os usuários da informação contábil demonstraram que as organizações atribuem menor importância ao tema do que o esperado (Confirma-se H4).

4.3.5. Construto Políticas e Procedimentos

Segundo Marciano (2006) a política de segurança da informação é um conjunto de regras, normas e procedimentos que regulam como as informações devem ser gerenciadas e protegidas. Jourdan et al. (2010) afirmam que a política de segurança da informação contém as normas e procedimentos detalhados que devem direcionar as atividades da gestão da segurança da informação na organização.

As médias das variáveis de avaliação e importância atribuídas pelo usuário da informação contábil ao construto Políticas e Procedimentos foram submetidas ao teste pareado de amostras, conforme apresentado na Tabela 18. Como resultado, obteve-se os valores (*gap*=1,922; Z=-8,498; Sig=0,000), o que indica a rejeição da hipótese nula e a não igualdade das médias das variáveis, devido ao nível de significância inferior a 0,05 (MAROCO, 2010).

Tabela 18 – Teste Pareado de Amostras – Construto Políticas e Procedimentos

Variáveis Comparadas	Média das Variáveis	*Gap*	Ranks			Z	Significância
			Negativo	Positivo	Igual		
POLI_I	8,781						
POLI_A	6,859	1,922	108	11	10	-8,498	0,000

Observa-se que o *gap* entre a avaliação e a importância para o construto Políticas e Procedimentos foi de 1,922, desta forma, os usuários da informação contábil demonstraram

que as organizações atribuem menor importância ao tema do que o esperado (Confirma-se H5).

4.3.6. Construto Pessoas

As organizações devem assegurar que funcionários, fornecedores e terceiros compreendam suas responsabilidades e estejam conscientes das ameaças relativas à segurança da informação (ABNT, 2005). Segundo Abu-Musa (2002) este construto trata da conscientização e treinamento de todas as pessoas envolvidas na manipulação das informações nas organizações.

As médias das variáveis de avaliação e importância atribuídas pelo usuário da informação contábil ao construto Pessoas foram submetidas ao teste pareado de amostras, conforme apresentado na Tabela 19. Como resultado, obteve-se os valores (*gap*=1,934; Z=-8,518; Sig=0,000), o que indica a rejeição da hipótese nula e a não igualdade das médias das variáveis, devido ao nível de significância inferior a 0,05 (MAROCO, 2010).

Tabela 19 – Teste Pareado de Amostras – Construto Pessoas

Variáveis Comparadas	Média das Variáveis	*Gap*	Ranks			Z	Significância
			Negativo	Positivo	Igual		
PESS_I	8,762						
PESS_A	6,828	1,934	107	16	6	-8,518	0,000

Observa-se que o *gap* entre a avaliação e a importância do construto Pessoas foi de 1,934, desta forma, os usuários da informação contábil demonstraram que as organizações atribuem menor importância ao tema do que o esperado (Confirma-se H6).

4.3.7. Resumo da Análise de *Gap*

De acordo com os resultados apresentados, foi possível identificar que para os seis construtos estudados, existem *gaps* estatisticamente significativos entre a avaliação (como o respondente avalia a segurança da informação na sua organização) e a importância (o quanto o respondente considera a segurança da informação importante) da segurança da informação atribuída pelo usuário da informação contábil nas organizações, conforme apresentado de forma resumida na Tabela 20.

Tabela 20 – Resumo do *Gap* por Construto

Construto	**Avaliação**	**Importância**	***Gap***
Integridade	7,820	9,116	1,297
Disponibilidade	7,967	9,112	1,145
Confidencialidade	7,845	9,136	1,291
Equipamentos	7,275	8,847	1,572
Políticas e Procedimentos	6,859	8,781	1,922
Pessoas	6,828	8,762	1,934
Média Geral	**7,432**	**8,959**	**1,527**

Os maiores índices de importância atribuídos pelos usuários da informação contábil foram obtidos nos construtos relacionados à integridade (9,116), disponibilidade (9,112) e confidencialidade (9,136) das informações. As organizações também receberam os maiores índices de avaliação nestes construtos. Estes dados sugerem que os usuários da informação contábil e as organizações estão conscientes de que informações contábeis imprecisas podem prejudicar a eficiência das organizações, uma vez que produzem relatórios financeiros não confiáveis (BOOCKHOLDT, 1999).

Com relação ao construto Equipamentos, os usuários da informação contábil evidenciaram que existe um *gap* de 1,572, o qual pode estar relacionado com a insuficiência de investimentos em segurança da informação nas organizações. Diversos estudos demonstraram que as organizações enfrentam limitações orçamentárias para implantação das práticas de segurança da informação (CARVALHO, 2003; MÓDULO, 2006; PWC, 2011). Segundo Gordon e Loeb (2006) os custos associados à segurança da informação não devem ser avaliados pela perspectiva econômica, mais sim, em ternos de custo-benefício.

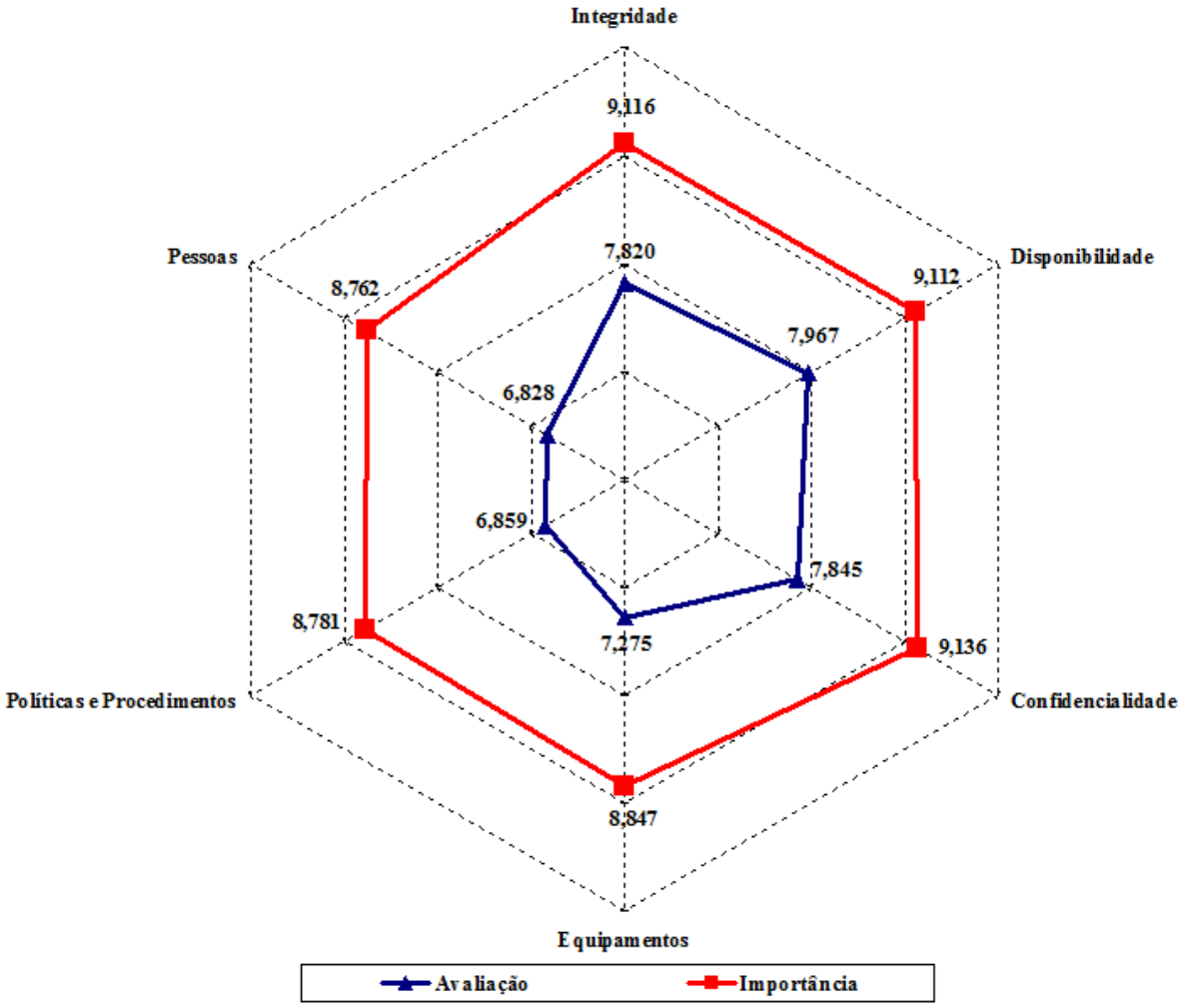
Para o construto Políticas e Procedimentos, obteve-se um *gap* de 1,922, sendo este o segundo maior *gap* apurado nesta pesquisa. Carvalho (2003) realizou um estudo com o objetivo de avaliar a segurança da informação nas empresas do segmento de telecomunicações e identificou que 53% das empresas analisadas não possuíam ou utilizavam políticas desatualizadas. A importância das políticas, procedimentos e adoção de melhores práticas para segurança da informação foi evidenciada em diversos estudos (PELTIER, 2001; MARCIANO, 2006; JOURDAN et al., 2010), sendo consideradas, em alguns casos, como fatores críticos de sucesso para a eficácia da segurança da informação nas organizações (VON SOLMS e VON SOLMS, 2004; ABNT, 2005).

O maior *gap* obtido neste estudo foi apurado no construto Pessoas (1,934). Uma característica interessante a ser observada é que embora os usuários da informação contábil tenham demonstrado que este é o construto mais negligenciado pelas organizações (6,828),

eles também atribuíram a este construto o menor índice de importância (8,762). Desta forma, pode-se deduzir que o usuário é o elo mais fraco da segurança da informação, e que os cuidados com a segurança da informação não são tratados com prioridade pelos funcionários das organizações (MARCIANO, 2006; ALBRECHTSEN, 2007).

De um modo geral, os usuários da informação contábil demonstraram que as organizações atribuem menor importância ao tema segurança da informação do que o esperado, dado que a média geral atribuída à avaliação das organizações foi de 7,432, enquanto a média da importância que os usuários da informação contábil atribuem à segurança da informação foi de 8,959, resultando em um *gap* de 1,527. A Figura 10 ilustra os índices de avaliação e importância atribuídos para cada construto.

Figura 10 – Avaliação e Importância por Construto



Por fim, cumpre registrar que todas as hipóteses propostas para este estudo foram confirmadas, conforme pode ser verificado no Quadro 3.

Quadro 3 – Resultado do Teste das Hipóteses

Hipótese	**Resultado**
H1: Existe um *gap* entre a avaliação e a importância da Integridade da informação percebida pelo usuário da informação contábil nas organizações.	Confirmada
H2: Existe um *gap* entre a avaliação e a importância da Disponibilidade da informação percebida pelo usuário da informação contábil nas organizações.	Confirmada
H3: Existe um *gap* entre a avaliação e a importância da Confidencialidade da informação percebida pelo usuário da informação contábil nas organizações.	Confirmada
H4: Existe um *gap* entre a avaliação e a importância dos Equipamentos de segurança da informação percebida pelo usuário da informação contábil nas organizações.	Confirmada
H5: Existe um *gap* entre a avaliação e a importância das Políticas e Procedimentos de segurança da informação percebida pelo usuário da informação contábil nas organizações.	Confirmada
H6: Existe um *gap* entre a avaliação e a importância da conscientização das Pessoas percebida pelo usuário da informação contábil nas organizações.	Confirmada

4.3.8. Análise das Diferenças de Percepção

Um dos objetivos específicos propostos para esta pesquisa foi avaliar as eventuais diferenças de percepção entre os usuários da informação contábil. Segundo Robbins (2002) a percepção pode ser influenciada por diversos fatores, entre eles o observador e o contexto, deste modo, optou-se por avaliar a percepção dos usuários da informação contábil de acordo com o cargo que ocupam e o tamanho da empresa em que atuam.

A Tabela 21 apresenta o *gap* obtido para cada construto de acordo com a percepção dos respondentes que possuem cargo de liderança (diretores, gerentes e coordenadores) e outros respondentes (analistas, auditores e outros). Observa-se que o *gap* percebido pelos usuários da informação contábil que possuem cargo de liderança (1,661) é maior do que o *gap* percebido pelos demais cargos (1,335). Ambos os cargos atribuem índices de importância semelhantes à segurança da informação, contudo, os respondentes que possuem cargo de liderança avaliam a segurança da informação nas organizações com maior insatisfação do que os demais, sobretudo, para os construtos Políticas e Procedimentos e Pessoas. Esta característica também foi observada por Madnick et al. (2007), onde os autores identificaram que os altos executivos demonstram uma maior insatisfação quanto às práticas de segurança da informação do que os demais membros da organização. Segundo os autores, este achado pode ser justificado pelo fato de que os executivos possuem uma visão mais abrangente dos problemas se comparado com os demais membros da organização.

Tabela 21 – *Gap* por Cargo do Respondente

	Cargos de Liderança			Outros		
Construto	**Avaliação**	**Importância**	***Gap***	**Avaliação**	**Importância**	***Gap***
Integridade	7,783	9,158	1,375	7,873	9,057	1,184
Disponibilidade	7,908	9,197	1,289	8,052	8,991	0,939
Confidencialidade	7,730	9,243	1,513	8,009	8,981	0,972
Equipamentos	7,207	8,809	1,602	7,373	8,901	1,528
Políticas e Procedimentos	6,681	8,793	2,112	7,113	8,764	1,651
Pessoas	6,688	8,760	2,072	7,028	8,764	1,736
Média total	**7,333**	**8,993**	**1,661**	**7,575**	**8,910**	**1,335**

O *gap* obtido para cada construto de acordo com o tamanho da empresa em que o usuário da informação contábil atua pode ser verificado na Tabela 22. Utilizou-se como premissa, que as grandes empresas possuem mais do que 1.000 funcionários, sendo as demais classificadas como pequenas e médias empresas. Observa-se que o índice de avaliação da segurança da informação obtido nas grandes empresas (7,701) é maior do que o apresentando para as pequenas e médias empresas (6,994). Os usuários da informação contábil que atuam em grandes empresas também atribuem maior importância ao tema (9,107) do que os que atuam em pequenas e médias empresas (8,717). Um dos principais fatores que influenciam a adoção de práticas de segurança da informação nas organizações está relacionado às necessidades de conformidades regulatórias (BEARD e WEN, 2007; PWC; 2011). Neste contexto, é possível deduzir que as grandes empresas, por estarem mais expostas às exigências regulatórias, adotam práticas de segurança da informação com maior freqüência do que as empresas de pequeno e médio porte.

Tabela 22 – *Gap* por Tamanho da Empresa

	Grandes			Pequenas e Médias		
Construto	**Avaliação**	**Importância**	***Gap***	**Avaliação**	**Importância**	***Gap***
Integridade	8,009	9,250	1,241	7,510	8,898	1,388
Disponibilidade	8,103	9,203	1,100	7,745	8,964	1,219
Confidencialidade	8,159	9,278	1,119	7,332	8,903	1,571
Equipamentos	7,688	8,997	1,309	6,602	8,602	2,000
Políticas e Procedimentos	7,331	8,981	1,650	6,087	8,454	2,367
Pessoas	6,913	8,934	2,022	6,689	8,480	1,791
Média total	**7,701**	**9,107**	**1,407**	**6,994**	**8,717**	**1,723**

Constatou-se que existem diferenças de percepção em função do cargo do respondente e tamanho da organização, contudo, o *gap* entre a avaliação e a importância permaneceu em ambas as situações. Desta forma, é possível deduzir que as eventuais diferenças de percepção podem afetar, sobretudo, a magnitude do *gap*.

5. CONCLUSÃO

A segurança da informação se tornou um problema que atinge as organizações, uma vez que coloca em risco a continuidade dos negócios. Sendo a contabilidade a área responsável por consolidar todas as informações da organização, torna-se relevante avaliar a percepção dos usuários da informação contábil a respeito da segurança da informação.

Neste contexto, este estudo foi desenvolvido com o objetivo de responder ao seguinte problema de pesquisa: **Existe um *gap* na percepção dos usuários da informação contábil com relação à segurança da informação nas organizações?** Para obtenção da resposta, foi realizada uma pesquisa quantitativa descritiva, que utilizou como instrumento de coleta de dados um questionário eletrônico do tipo *survey*, em que uma amostra composta por 129 usuários da informação contábil de diversas organizações brasileiras forneceram as suas percepções a respeito da segurança da informação.

Com base na revisão da literatura, foram selecionados seis construtos de segurança da informação (Integridade, Disponibilidade, Confidencialidade, Equipamentos, Políticas e Procedimentos e Pessoas) os quais foram utilizados na pesquisa de campo. Todos os construtos foram validados estatisticamente através do coeficiente Alfa de Cronbach. Procedeu-se então a análise de *gap*, que consistiu na comparação das médias de avaliação (como o respondente avalia a segurança da informação na sua organização) e importância (o quanto o respondente considera a segurança da informação importante) atribuída pelos usuários da informação contábil a cada construto de segurança da informação considerado na pesquisa. Como resultado, constatou-se a existência de *gaps* estatisticamente significativos para todos os seis construtos de segurança da informação estudados, o que caracterizou a confirmação das seis hipóteses sugeridas para este estudo.

Os resultados obtidos pela pesquisa indicaram que os usuários da informação contábil estão conscientes da importância da segurança da informação nas organizações, uma vez que atribuíram altos índices de importância aos construtos Integridade, Disponibilidade e Confidencialidade. Observou-se também, que na percepção dos participantes da pesquisa, as organizações atribuem menor importância a estes construtos do que o esperado pelos usuários da informação contábil, de tal sorte que foram identificados *gaps* estatisticamente significativos para os três construtos.

Os usuários da informação contábil demonstraram insatisfação com relação aos recursos e equipamentos utilizados para garantir a segurança da informação nas organizações.

Este achado pode estar relacionado à insuficiência de investimentos em segurança da informação nas organizações, dado que a literatura evidencia as limitações orçamentárias para este fim (CARVALHO, 2003; MÓDULO, 2006; PWC, 2011).

As políticas e procedimentos em segurança da informação adotados pelas organizações também foram avaliadas de forma insatisfatória pelos usuários da informação contábil, uma vez que o segundo maior *gap* mensurado neste estudo diz respeito a este construto. Estes resultados sugerem que as organizações não estão utilizando ou divulgando de forma adequada as políticas e procedimentos de segurança da informação.

A segurança da informação é considerada um problema social por diversos autores, sobretudo, devido ao importante papel exercido pelo componente humano. Nesta pesquisa, o maior *gap* foi identificado no construto Pessoas. Adicionalmente, observou-se que este foi o construto que recebeu os menores índices de avaliação e importância. Estes resultados trouxeram indícios de que as organizações enfrentam dificuldades para controlar o componente humano da segurança da informação, sobretudo devido aos funcionários não estarem conscientes da importância do seu papel para a eficácia da segurança da informação nas organizações.

Neste contexto, entende-se que o primeiro e o segundo objetivo específico proposto para este trabalho foi atingido, uma vez que foi possível identificar como os usuários da informação contábil avaliam a segurança da informação em suas organizações, o quanto estes usuários consideram a segurança da informação importante, bem como, avaliar a existência de *gap* entre a avaliação e importância da segurança da informação nas organizações.

Com relação ao terceiro objetivo específico, que propôs analisar as eventuais diferenças de percepção entre os usuários da informação contábil, constatou-se que os respondentes que possuem cargo de liderança atribuem menores índices de avaliação à segurança da informação nas organizações se comparado com os demais cargos. Este achado corroborou com o identificado em estudos prévios (MADNICK et al., 2007). Adicionalmente, as empresas consideradas grandes apresentaram *gap*s inferiores aos observados em empresas pequenas e médias, fato que pode estar relacionado a uma maior exposição a conformidades regulatórias vivenciadas pelas grandes empresas. Cumpre observar que as diferenças de percepção não anularam a existência de *gap*, apenas diferenciam a sua magnitude.

A contribuição prática deste estudo reside no quarto objetivo específico que propôs evidenciar as eventuais oportunidades de melhoria da segurança da informação nas organizações. Com base nos resultados da pesquisa, constatou-se que os menores índices de

avaliação da segurança da informação nas organizações foram atribuídos aos construtos Pessoas e Políticas e Procedimentos. Os achados da pesquisa sugerem que as organizações devem direcionar seus esforços na conscientização dos funcionários e na implantação de políticas e procedimentos de segurança da informação, objetivando a instituição da cultura de segurança da informação na organização.

Desta forma, considera-se que esta pesquisa foi concluída de forma satisfatória, uma vez que o problema de pesquisa sugerido foi respondido adequadamente, o objetivo geral e os objetivos específicos propostos foram atingidos e todas as hipóteses foram testadas.

Cumpre ressaltar que uma limitação deste estudo esta relacionada à utilização de uma amostra intencional e não probabilística. Os resultados e fatos aqui relacionados dizem respeito ao conjunto de usuários da informação contábil que aceitaram participar da pesquisa, não permitindo nenhum tipo de generalização. Contudo, esses resultados podem e devem ser considerados pelos gestores responsáveis pela informação contábil e pelos responsáveis pela área de segurança da informação nas organizações.

Ao final deste estudo, recomenda-se que ele seja continuado, por meio de novas pesquisas que tenham como objetivo avaliar a percepção de segurança da informação em diferentes áreas, níveis organizacionais, segmentos de mercado, países, entre outras características que possibilitem a comparação dos resultados e novas descobertas a respeito do assunto.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO / IEC 17799 : 2005 Tecnologia da informação - Código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2005.

ABU-MUSA, Ahmad A. Security of Computerized Accounting Information Systems: A Theoretical Framework. **Journal of American Academy of Business**. Cambridge, v.2, n.1, p. 150-155, 2002.

ABU-MUSA, Ahmad A. The Perceived Threats to the Security of Computadorized Accounting Information Systems. **Journal of American Academy of Business**. Cambridge, v.3, p.9-20, 2003.

ABU-MUSA, Ahmad A. Evaluating the Security Controls of CAIS in Developing Countries: The Case of Saudi Arabia. **The International Journal of Digital Accounting Research**. v.6, n.11, p.25-64, 2006.

ALBRECHTSEN, Eirik. A qualitative study of user's view on information security. **Computers and Security**. v. 26, p. 276-289, 2007.

ANDERSON, J. M. Why we need a new definition of information security. **Computers & Security**. v. 22, n. 4, p. 308–313, 2003.

BEAL, Adriana. **Gestão Estratégica da Informação: Como transformar a informação e a TI em fatores de crescimento e de alto desempenho nas organizações**. São Paulo : Atlas, 2004.

BEARD, Deborah; WEN, H. Joseph. Reducing the Threat Levels for Accounting Information Systems. **The CPA Journal**. v. 77, n. 5, p. 34-42, 2007.

BEUREN, Ilse Maria. **Gerenciamento da Informação: Um recurso estratégico no processo de gestão empresarial.** 2.ed. São Paulo : Atlas, 2000.

BEUREN, Ilse Maria. **Como elaborar trabalhos monográficos em contabilidade.** 3.ed. São Paulo : Atlas, 2009.

BOOCKHOLDT, James. L. **Accounting Information Systems: Transaction Processing and Controls.** 5.ed. New York : McGraw-Hill, 1999.

CARVALHO, Rosangela Caubit de. **A aplicação de um modelo de gestão de segurança da informação e a sua influência na percepção de competitividade no setor de telecomunicações e informática.** 2003. 208p. Dissertação (Mestrado) - Universidade Federal Fluminense, Niterói, 2003.

CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas dos Incidentes Reportados**. Disponível em: http://www.cert.br/stats/incidentes/. Acesso em: outubro de 2011.

COLLIS, Hill; HUSSEY, Roger. **Pesquisa em administração.** 2.ed. Porto Alegre : Bookman, 2005.

CORRAR, L. J.; PAULO, E.; DIAS FILHO, J. M. (Coordenadores) **Análise Multivariada: para os cursos de Administração, Ciências Contábeis e Economia.** São Paulo : Atlas, 2007.

CPC - COMITÊ DE PRONUNCIAMENTOS CONTÁBEIS. **Pronunciamento Conceitual Básico**. 2008. Disponível em: http://www.cpc.org.br/pronunciamentosIndex.php. Acesso em: setembro de 2011.

DA VEIGA, A.; ELOFF, J.H.P. An Information Security Governance Framework. **Information Systems Management,** v. 24, p.361-372, 2007.

DOHERTY, Neil F.; FULFORD, Heather. Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. **Information Resources Management Journal**. v. 18, n. 4, p. 21-39, 2005.

ELOFF, J. H. P.; ELOFF, M. M. Information Security Architecture. **Computer Fraud and Security**, v. 11, p. 10–16, 2005.

ESTADO – JORNAL O ESTADO DE SÃO PAULO. 02 de setembro de 2010. Disponível em: http://www.estadao.com.br/noticias/nacional,serra-na-tv-vazamento-de-dados-da-receita-e-sujeira,604471,0.htm. Acesso em: Outubro de 2011.

EXAME – REVISTA EXAME. Edição 0751, Outubro de 2001. Disponível em: http://exame.abril.com.br/revista-exame/edicoes/0751/noticias/o-plano-b-m0050962. Acesso em: Outubro de 2011.

FÁVERO, L. P.; BELFIORE, P. B.; SILVA, F. L.; CHAN, B. L. **Análise de dados: modelagem multivariada para tomada de decisões.** Rio de Janeiro : Elsevier, 2009.

FOLHA – JORNAL FOLHA DE SÃO PAULO. 16 de fevereiro de 2011. Disponível em: http://www1.folha.uol.com.br/mercado/876511-sistemas-do-panamericano-eram-corrompidos-diz-diretor.shtml. Acesso em: fevereiro de 2011.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social.** 5. ed. São Paulo : Atlas, 1999.

GORDON, L. A.; LOEB, M. P. Return on Information Security Investments: Myths vs. Realities. **Strategic finance**, v. 84, n. 5, p. 26–31, 2002.

GORDON, L. A.; LOEB, M. P. Budgeting Process for Information Security Expenditures. **Communications of the ACM**. v. 49, n. 1, p. 121-125, 2006.

GORDON, L.A.; LOEB, M.P.; SOHAIL, T.; TSENG, C.H.; ZHOU, L. Cybersecurity, Capital Allocations and Management Control Systems. **European Accounting Review**, v. 17, n. 2, p. 215-241, 2008.

GORDON, L. A.; LOEB, M. P.; SOHAIL, T. Market Value of Voluntary Disclosures Concerning Information Security. **MIS Quarterly**, v. 34, n. 3, p. 567-594, 2010.

HAIR, Joseph F.; Anderson, R. E.; Tathan, R. L.; Black, W. C. **Análise Multivariada de Dados.** 5.ed. Porto Alegre : Bookman, 2007.

HERATH, Hemantha S. B. Cybersecurity: An Emerging Area for Collaborative Post-Modern Management Accounting Research. **Journal of Cost Management**. v. 25, n. 1, 2011.

IMONIANA, Joshua Onome. **Auditoria de sistemas de informação.** 2. ed. São Paulo : Atlas, 2008.

JOURDAN, Zack; RAINER , R. Kelly, Jr.;MARSHALL, Thomas E.; FORD, F. Nelson. An Investigation of Organizational Information Security Risk Analysis. **Journal of Service Science.** v. 3, n. 2, p. 33-42, 2010.

KARSAKLIAN, Eliane. **Comportamento do Consumidor**. São Paulo : Atlas, 2000.

KAYWORTH, T.; WHITTEN D. Effective Information Security Requires a Balance of Social and Technology Factors. **MIS Quarterly Executive,** v. 9, n. 3, p. 163-175, 2010.

KNAPP, Kenneth J., MARSHALL, Thomas E., MONTGOMERY, Gina H., RAINER, R. Kelly, Jr. Do Information Security Professionals and Business Managers View Information Security Issues Differently? **Information Security Journal**, v. 16, n. 2, p.100-108, 2007.

KÖCHE, J. C. **Fundamentos de Metodologia Científica**. Teoria da Ciência e prática da pesquisa. 17.ed. Petrópolis : Editora Vozes, 2000.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Metodologia científica.** 3.ed. São Paulo : Atlas, 2000.

LIMA, Luiz Fernando F. M. **Percepção de segurança em sistemas de informação e sua relação com a qualidade percebida de serviços, perfil de liderança e perfil dos seguidores, entre as diretorias do Inmetro.** 2006. 292p. Dissertação (Mestrado), Universidade Federal Fluminense, Niterói, 2006.

MADNICK, S. E.; ANG, W. H.; LEE, Y. W.; MISTREE, D.; SIEGEL, M.; STRONG, D. M.; WANG, R. Y.; YAO, C. **House of Security: Locale, Roles and Resources for Ensuring Information Security**. Massachusetts Institute of Technology, Cambridge, 2006.

MADNICK, S. E.; ANG, W. H; DENG, V.; LEE, Y.; MISTREE, D.; SIEGEL, M.; STRONG, D.; WANG, R. **The House of Security: Stakeholder Perceptions of Security Assessment and Importance**. Massachusetts Institute of Technology, Cambridge, 2007.

MARCIANO, João Luiz Pereira. **Segurança da informação - uma abordagem social.** 2006. 211p. Tese (Doutorado).Universidade de Brasília, Brasília, 2006.

MAROCO, João. **Análise Estatística - Com Utilização do SPSS**. 3.ed. Lisboa : Silabo, 2010.

MÓDULO. **10ª Pesquisa Nacional de Segurança da Informação**. 2006. Disponível em: http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf. Acesso em fevereiro de 2011.

MOSCOVE, Stephen A.; SIMKIN, Mark G.; BAGRANOFF, Nacy A. **Sistemas de informações contábeis.** São Paulo : Atlas, 2002.

O'BRIEN, J. A.; MARAKAS, G. M. **Administração de Sistemas de Informação. Uma introdução.** 13.ed., São Paulo : McGrawHill, 2008.

PADOVEZE, Clovis Luís. **Sistemas de Informações Contábeis – Fundamentos e Análise**. 2.ed., São Paulo : Atlas, 2000.

PÁDUA, E. M. M. **Metodologia da Pesquisa: abordagem teórico-prática.** São Paulo : Papirus, 1996.

PARASURAMAN, A.; ZEITHAML, Valarie A.; BERRY, Leonard L. A conceptual Model of Service Quality and Its Implications for Future Research. **Journal of Marketing**, v. 49, p. 41-50, 1985.

PELTIER, T. **Information Security Policies, Procedures, and Standards – Guideline for effective Information Security Management**. Florida : Auerbach, 2001.

PEMBLE, M. What do we mean by "information security"?. **Computer fraud & security**, v. 2004, n. 5, p. 17–19, 2004.

PEREZ, Gilberto. **Adoção de inovações tecnológicas: um estudo sobre o uso de sistemas de informação na área da saúde.** 2006. 227p. Tese (Doutorado) – Universidade de São Paulo, 2006.

PESTANA, Maria Helena; GAGEIRO, João Nunes. **Análise de dados para ciências sociais: a complementaridade do SPSS.** 2.ed. Lisboa : Edições Silabo, 2000.

PWC - PRICEWATERHOUSECOOPERS. **8º Pesquisa Global de Segurança da Informação.** 2011. Disponível em: http://www.pwc.com.br/pt/estudos-pesquisas/index.jhtml. Acesso em fevereiro de 2011.

RIBEIRO FILHO, J. F. R.; LOPES, J.; PEDERNEIRAS, M. **Estudando a Teoria da Contabilidade**, São Paulo : Atlas, 2009.

RICCIO, Edson Luiz. **Efeitos da tecnologia de informação na contabilidade: estudo de casos de implementação de sistemas empresariais integrados - ERP.** 2001. 154p. Tese (Livre-Docência) Universidade de São Paulo, São Paulo, 2001.

RICHARDSON, Roberto Jarry. **Pesquisa Social: Métodos e Técnicas.** 3.ed. São Paulo : Atlas, 2007.

ROBBINS, S. P. **Comportamento Organizacional**. 9.ed. São Paulo : Prentice Hall, 2002.

SILVA, Adilson A. **Integração vertical em cadeias de suprimentos e os pressupostos da teoria dos custos de transação: um teste empírico.** 2009. 144p. Tese (Doutorado). Universidade Presbiteriana Mackenzie, São Paulo, 2009.

STAIR, R. M. **Princípios de sistemas de informação: uma abordagem Gerencial**. 2.ed. Rio de Janeiro : Livros Técnicos e Científicos, 1998.

STEWART, Andrew. On risk: perception and direction. **Computers & Security**, v. 23, p. 362-370, 2004.

TCU – TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em segurança da informação**. – 3.ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008.

TURBAN, E.; LEIDNER, D.; MCLEAN, E.; WETHERBE, J. **Information Technology for management - transforming organizations in the digital economy.** J. Wiley & Sons, 2006.

VON SOLMS, B.; VON SOLMS, R. The 10 deadly sins of information security management. **Computers & Security**, v. 23, p. 371-376, 2004.

WILKINSON, J. W.; CERULLO, M. J.; RAVAL, V.; WONG-ON-WING, B. **Accounting information systems: essential concepts and applications.** 4.ed. New York : John Wiley & Sons, 2000.

WOOD, C. C.; PARKER, D. B. Why ROI and similar financial tools are not advisable for evaluating the merits of security projects. **Computer Fraud & Security**, v. 2004, n. 5, p. 8–10, 2004.

APÊNDICES

APÊNDICE I – INSTRUMENTO DE COLETA DE DADOS

SEÇÃO 1: Introdução

Segurança da Informação: Um Estudo sobre a Percepção do Usuário da Informação Contábil

Este questionário é parte integrante da pesquisa Segurança da Informação: Um Estudo sobre a Percepção do Usuário da Informação Contábil.

Se você é usuário da informação contábil, sua participação será de extrema importância para a conclusão deste estudo.

Instruções Gerais

1. Apesar de ser um questionário para respostas anônimas, precisamos de algumas informações para definir o perfil da organização e do respondente. No final você poderá optar em receber ou não um relatório com os resultados e, somente nesse caso, vamos precisar conhecer o seu endereço e-mail.

2. A pesquisa solicitará que você forneça a sua percepção sobre diversas assertivas relacionadas à segurança da informação. Você deverá avaliar as assertivas em duas escalas, sendo:

Avaliação: em sua opinião, o quanto a sua organização considera importante estas assertivas de segurança da informação.

Importância: em sua opinião, o quanto você considera importante estas assertivas de segurança da informação.

3. Caso você não tenha conhecimento dos detalhes exatos sobre a segurança da informação na sua organização, por favor, forneça a sua melhor estimativa.

4. O tempo estimado para preenchimento do questionário é de 5 minutos.

Agradecemos a sua participação.

Aluno: Wagner Lima da Silva (wagnerlimas@gmail.com)
Orientador: Prof. Dr. Gilberto Perez

Mestrado Profissional em Controladoria Empresarial da Universidade Presbiteriana Mackenzie.

SEÇÃO 2: Caracterização do Respondente

Escolaridade:

	Fundamental
	Segundo Grau
	Técnico
	Superior
	Pós Graduação
	Mestrado
	Doutorado
	Outro

Formação:

	Administração
	Contabilidade
	Economia
	Engenharia
	Outro

Área de Atuação:

	Administração Geral
	Contabilidade
	Controladoria
	Financeiro
	Auditoria
	Outro

Cargo / Função:

	Diretor
	Gerente
	Coordenador
	Analista
	Auditor
	Outro

Tempo de Empresa:

	Menos de 1 ano
	Entre 1 e 5 anos
	Entre 5 e 10 anos
	Entre 10 e 20 anos
	Acima de 20 anos

SEÇÃO 3: Caracterização da Empresa

Segmento de Atuação:

	Agronegócio
	Indústria
	Comércio
	Serviço
	Instituição Financeira
	Outro

Tempo de Atuação da Empresa:

	Até 5 anos
	Entre 5 e 10 anos
	Entre 10 e 20 anos
	Entre 20 e 30 anos
	Acima de 30 anos

Número Aproximado de Funcionários:

	De 1 a 100
	De 101 a 500
	De 501 a 1.000
	De 1.001 a 5.000
	De 5.001 a 10.000
	Acima de 10.000

Sistema Corporativo Utilizado:

	Totvs – Microsiga
	Totvs – Logix
	Totvs – RM Sistemas
	Totvs – Data Sul
	Oracle – Applications
	Oracle – Peoplesoft
	Oracle – JDEdwards
	Microsoft Dynamics
	SAP
	Outro

SEÇÃO 4 – Questões Relacionadas à Segurança da Informação

Atribua notas de 1 a 10 (sendo 1 mínimo e 10 máximo) para cada assertiva abaixo, de modo que reflita a sua percepção sobre a segurança da informação.

Observe que para cada assertiva existem 2 escalas de respostas, sendo:

Avaliação: em sua opinião, o quanto a sua organização considera importante esta assertiva de segurança da informação.

Importância: em sua opinião, o quanto você considera importante esta assertiva de segurança da informação.

Caso você não tenha conhecimento de algum detalhe específico sobre a segurança da informação na sua organização, por favor, forneça a sua melhor estimativa.

Por gentileza, não deixe questões em branco.

	Avaliação											Importância									
	1	2	3	4	5	6	7	8	9	10		1	2	3	4	5	6	7	8	9	10
1. A organização possui especialistas em segurança da informação suficientes para cobrir as suas necessidades.																					
2. A organização realiza auditorias de segurança da informação periodicamente.																					
3. As pessoas da organização possuem conhecimento sobre as ferramentas e práticas de segurança da informação.																					
4. O sistema de informação contábil raramente é violado por acesso não autorizado.																					
5. O sistema de informação contábil da organização está disponível apenas para usuários autorizados.																					
6. A organização possui políticas adequadas que definem como e quando a informação contábil pode ser compartilhada.																					
7. A organização realiza investimentos em segurança da informação sempre que necessário.																					
8. A organização possui uma estratégia de segurança da informação bem definida a qual é divulgada de forma adequada.																					
9. As pessoas da organização seguem cuidadosamente as boas práticas de segurança da informação.																					
10. A organização possui recursos de segurança da informação adequados contra ameaças internas e externas ao sistema de informação contábil.																					
11. A organização mantém cópias de segurança dos sistemas e informações contábeis as quais estão sempre disponíveis quando necessário.																					
12. A organização possui políticas adequadas sobre a identificação de usuários, senhas e privilégios de acesso ao sistema de informação contábil.																					
13. A organização possui recursos tecnológicos adequados para apoiar a segurança da informação.																					
14. A organização tem políticas e procedimentos bem definidos para a segurança dos seus dados e da rede.																					

15. As pessoas da organização sempre exercem conduta ética com os dados e redes.																					
16. A organização verifica a identidade dos usuários antes de permitir acesso ao sistema de informação contábil.																					
17. As informações contábeis da organização raramente apresentam distorções ou erros.																					
18. A organização protege a privacidade dos dados confidenciais de clientes, fornecedores e funcionários.																					
19. A organização utiliza os seus recursos tecnológicos de forma eficaz para melhorar a segurança da informação.																					
20. A organização dispõe de procedimentos para detectar e punir violações de segurança da informação.																					
21. As pessoas da organização estão conscientes das práticas de segurança da informação.																					
22. A organização possui um plano de contingência adequado para manutenção do funcionamento do sistema de informação contábil.																					
23. A organização se preocupa com a proteção das informações corporativas confidenciais.																					
24. O sistema de informação contábil da organização está sempre disponível quando necessário.																					

SEÇÃO 5 – Finalização

Por fim, informe o seu endereço de e-mail caso deseje receber um relatório com os resultados desta pesquisa.

O preenchimento deste campo é opcional.

Muito obrigado, a sua participação foi muito importante para conclusão desta pesquisa.

APÊNDICE II – CONVITE PARA PARTICIPAÇÃO NA PESQUISA

Prezado XXXXXXX,

Sou aluno do Mestrado em Controladoria Empresarial da Universidade Presbiteriana Mackenzie, e gostaria de convidá-lo a participar da minha pesquisa denominada **"Segurança da Informação: Um Estudo sobre a Percepção do Usuário da Informação Contábil".**

Esta pesquisa é direcionada aos usuários da informação contábil nas organizações. Caso possa encaminhar este email a alguns outros colegas de trabalho, será de grande valia.

O tempo estimado para preenchimento do questionário é de 3 a 5 minutos. Todas as questões são de múltipla escolha. Segue o link abaixo:

http://fs4.formsite.com/wagnerlimas/form1/index.html

Agradeço antecipadamente.

Atenciosamente,
Wagner Lima da Silva