MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

SEGURANÇA DA INFORMAÇÃO CONTÁBIL: procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]

MATTES, Ícaro Valente[2]
PETRI, Sérgio Murilo[3]
ROSA, Marcelo Medeiros da[4]

RESUMO

Este artigo objetiva contribuir para a elaboração de um modelo de Política de Segurança da Informação (PSI) e estruturação de um Sistema de Segurança da Informação (SGSI) para escritórios contábeis com base nas normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Trata-se de uma pesquisa aplicada, descritiva, com abordagem qualitativa e classificada como *survey*. Os instrumentos de pesquisa foram: a análise documental; pesquisas e a aplicação de questionário semiestruturado com gestores de escritórios contábeis da Grande Florianópolis. A fonte de dados secundários indica crescimento mundial do tema Segurança da Informação e principais problemas encontrados em escritórios contábeis. Como resposta, foram levantados os itens mínimos do padrão ISO 27002 relacionados com os riscos pertinentes à contabilidade e a formulação de um exemplo de PSI aplicável às organizações contábeis.

Palavras-chave: Segurança da Informação. Tecnologia da Informação. Contabilidade. ISO 27001. ISO 27002.

ABSTRACT

This article aims to contribute to the development of a model of Information Security Policy (ISP) and structuring of a Security System Information (ISMS) for accounting offices based on the standards ISO / IEC 27001 and ISO / IEC 27002. This is an applied descriptive study, with qualitative approach and classified as survey. The research instruments were: document analysis ; research and the application of semi-structured questionnaire with accounting office managers in Florianópolis . The source of secondary data indicates growth in worldwide

[1] Artigo apresentado no 10º CONTECSI – Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação. São Paulo, 2013.

[2] Bacharel em Ciências Contábeis pela Universidade Federal de Santa Catarina. E-mail: icaromattes@hotmail.com

[3] Doutor em Engenharia de Produção pela Universidade Federal de Santa Catarina. Professor Adjunto da Universidade Federal de Santa Catarina – Programa de Pós-graduação em Contabilidade. E-mail: smpetri@gmail.com

[4] Especialista em Controle da Gestão Pública Municipal pela Universidade Federal de Santa Catarina. Discente do Programa de Pós-Graduação em Contabilidade da Universidade Federal de Santa Catarina. E-mail: mmr2801@yahoo.com.br

information security theme and main problems encountered in accounting offices. In response, were raised the minimum ISO 27002 standard items related to the risks of the accounting and the formulation of an applicable example of PSI to the financial organizations

Keywords: Information Security. Information Technology. Accounting. ISO 27001. ISO 27002.

1 INTRODUÇÃO

A constante evolução das ferramentas de tecnologia da informação permite o compartilhamento e processamento de dados em tempo real e contribui para a tomada de decisão mais rápida. Este fenômeno não se limitou simplesmente à automação e produção: passou a subsidiar a reflexão sobre o processo empresarial como um todo.

Entretanto, concomitantemente com os benefícios provenientes de tal cenário, as ferramentas de TI permitiram que a informação, ativo intangível que desempenha papel estratégico no mundo contemporâneo, pudesse ser acessada, compartilhada e até mesmo violada por usuários não autorizados, que danificam ou extraem conteúdos sigilosos de banco de dados corporativos.

Logo, foi-se o tempo em que o essencial era apenas resguardar documentos em meio físico e em um lugar com restrição ao acesso de pessoal não autorizado. De acordo com Silva (2012), a utilização da tecnologia de informação na contabilidade tem importância vital para a sobrevivência da organização, pois sem computadores, redes, banco de dados e um sistema seguro, a prestação de serviços se torna inviável.

A informação armazenada no banco de dados de uma organização é um ativo com alto valor, com extrema importância e indispensável para o seu funcionamento. Portanto, necessita de políticas claras e seguras para sua preservação. O trabalho de segurança da informação abarca o local físico, *hardware*, *software*, colaboradores, processos e, principalmente, a política aplicada.

O intuito da Segurança da Informação não se restringe apenas em manter a disponibilidade da informação, mas também suas características essenciais: consistência, integridade, autenticidade e confidencialidade. Segundo a ISO 27002: “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a

continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio." (ABNT NBR ISO/IEC 27002:2005).

Uma informação só possuirá importância se gerar conhecimento e, assim, subsidiar a tomada de decisão, agregando valor e sendo reconhecida como um ativo, como especifica a NBR ISO/IEC 27002:2005:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é essencialmente importante no ambiente dos negócios, cada vez mais interconectado.

Neste contexto, corroborando com Alves (2006), a aplicação de mecanismos de proteção é fundamental para a maximização dos resultados e perpetuidade do negócio e a redação da Política de Segurança da Informação (PSI) é o primeiro passo para aplicação de um Sistema de Gestão da Segurança da Informação.

Segundo a NBR ISO/IEC 27002, trata-se a PSI de uma aglutinação de diversos aspectos: "A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware".

O sucesso na implantação da Política de Segurança da Informação está condicionado, segundo Fontes (2012), no respaldo da alta direção. Este respaldo deve ocorrer não só por meio de investimentos financeiros, mas por meio do apoio à equipe que elaborou as normas de disseminação do seu conteúdo à força de trabalho.

Baseado no que foi citado acima, levantou-se o seguinte problema de pesquisa: **Quais procedimentos e padrões mínimos devem ser adotados para a elaboração prática de uma Política de Segurança da Informação em escritórios contábeis?**

Para responder tal questionamento, objetivou-se reunir e compilar as informações sobre a elaboração de políticas de Segurança da Informação a fim de indicar o padrão mínimo para normas de segurança em escritórios contábeis.

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

Na busca de resposta e respaldo técnico do problema de pesquisa, os objetivos específicos traçados foram: (i) Sumarizar os problemas e as ameaças relativas à segurança da informação nos escritórios contábeis e as barreiras na aplicação de políticas de segurança da informação.; (ii) Identificar e relacionar os padrões e normas mínimas, selecionando os principais pontos das ISO 27001 e ISO 27002 relacionáveis com escritórios contábeis; (iii) Elaborar um exemplo de gestão da segurança da informação voltado à contabilidade, baseando-se em exemplos de casos reais.

A justificativa, quanto à relevância social, reside na importância do assunto para uma classe profissional, conseqüência da grande valorização da matéria pelos gestores, tanto no Brasil quanto no exterior; Quanto à relevância científica, por se tratar de uma pesquisa bibliográfica voltada a acrescentar informações sobre o assunto, a fim de trazer informações oportunas e com caráter cumulativo, permitindo uma cobertura mais ampla da temática. (GONÇALVES, 2012).

Como delimitação da pesquisa, foi contemplado o estudo da ISO 27001 que trata dos requisitos para adaptação e implantação do SGSI e da ISO 27002 - que se refere aos códigos de prática de um SGSI. Além destes, foi utilizada a Pesquisa Global de Segurança da Informação, considerada a maior pesquisa do gênero no mundo, realizada pela PwC, CIO Magazine e CSO Magazine.

2 METODOLOGIA DA PESQUISA

2.1 ENQUADRAMENTO METODOLÓGICO

A presente pesquisa, em relação aos objetivos, caracteriza-se como descritiva, pois, segundo Triviños (1987), procura conhecer a realidade, características e problemas, indicando as peculiaridades atuais dos sistemas de gestão de segurança e possíveis dificuldades em sua aplicação. Quanto à abordagem do problema, este estudo é caracterizado como uma pesquisa qualitativa, por oportunizar o acesso um campo mais amplo de possibilidades ao levantar as ideias do público pesquisado e, ao mesmo tempo, quantificar as opiniões, com intuito de interpretar e analisar os dados coletados utilizando ou não recursos e técnicas estatísticas (GIL, 2007; ALMEIDA, 2011).

Ademais, realizou-se uma pesquisa bibliográfica em livros, artigos científicos e materiais disponibilizados na internet, com os quais foi possível selecionar e interpretar as contribuições teóricas já existentes sobre o assunto investigado. No que diz respeito à busca na internet foram utilizadas, como critério de seleção, as seguintes terminologias: Tecnologia da Informação, Segurança da Informação, Sistema de Gestão da Segurança da Informação Digital e NBR ISO/IEC 27001 e 27002.

Sob o aspecto dos procedimentos técnicos utilizados, a pesquisa se classifica como do tipo levantamento *survey*. A opção pelo método se deu pela sua aplicabilidade em estudos descritivos e sua utilização ocorre quando se objetiva responder questões sobre a incidência, a distribuição e a relação entre determinadas características da população (PALHARES, 2011).

De acordo com Malhotra (2006), este método visa à obtenção de informações sobre as percepções dos respondentes. Neste sentido, Palhares (2011) complementa apresentando que neste método os dados são coletados em um intervalo de tempo pré-determinado, com base em uma amostra para descrever a população em determinado momento. Complementa o mesmo autor: "o fato dos informantes responderem às mesmas questões permite que a incidência e a distribuição de determinadas características populacionais sejam estruturadas e que as relações entre elas sejam exploradas" (PALHARES, 2011, p. 54).

2.2 POPULAÇÃO E AMOSTRA

A população alvo, segundo Barbetta (2004, p. 18), é "conjunto de elementos que queremos abranger em nosso estudo". Desta forma, para atender o objetivo desta pesquisa, definiu-se como público alvo os escritórios de contabilidade usuários de um software de gestão para organizações contábeis situados em qualquer um dos 22 municípios da região da Grande Florianópolis. A amostra representa cerca de 10% da população de empresas da região.

O método de amostragem utilizado foi o da amostragem não probabilística, por acessibilidade e intencional, a qual é conceituada por Cooper e Schindler (2003, p. 169) como "uma amostragem não probabilística que atenda a certos critérios". Na amostragem por

acessibilidade, a seleção dos elementos se dá pela acessibilidade aos respondentes, admitindo-se que estes podem, de alguma forma, representar o universo.

O questionário, instrumento utilizado para coleta de dados primários, conteve questões dos tipos fechadas, fechadas/aberta e abertas. Os dados coletados na pesquisa foram tratados descritivamente e apresentados em forma de quadro e gráficos.

Como fonte de dados secundários, utilizaram-se a Pesquisa Global de Segurança da Informação feita em conjunto pela PwC, CIO Magazine e CSO Magazine em 2012, em que foram entrevistados mais de 9.600 CEOs, CFOs, CISOs, CIOs, CSOs, vice-presidentes e diretores de TI e de Segurança da Informação de 138 países (10% dos respondentes são do Brasil), e 10ª Pesquisa Nacional de Segurança da Informação, de iniciativa da empresa Módulo Segurity Solitions S.A, que entrevistou aproximadamente 600 profissionais das áreas de Tecnologia e Segurança da Informação de mais da metade das mil maiores empresas brasileiras de diversos setores da economia entre os anos de 2005 e 2006.

2.3 PESQUISAS SIMILARES

Por meio de pesquisas, foi possível criar uma relação do assunto com os seguintes estudos: Fontes (2011), Palhares, Lorens (2007), Benz (2008), Cavalcante (2003), Menezes (2005), Roza (2010), Venturini (2006) e Ribas (2010).

Destacam-se os estudos de Benz (2008), que faz estudo de caso em instituições financeiras, Cavalcante (2003) e Palhares, que utilizam como estudo de caso instituições de ensino superior, e Roza (2010) e Ribas (2010), que aplicam seus estudos em hospitais e na área da saúde.

Sem dúvidas, o estudo que mais se aproxima ao objetivo desta pesquisa é o de Fontes (2011), por se tratar do único a criar um estudo a fim de indicar um padrão mínimo na aplicação da ISO 27002 em instituições de diversas áreas. Por este motivo, este artigo baseia-se em alguns procedimentos aplicados pelo autor, demonstrados em suas obras publicadas, com o objetivo de validar os resultados encontrados.

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

3 FUNDAMENTAÇÃO TEÓRICA

3.1 A INFORMAÇÃO

A importância da informação é inegável, tanto para indivíduos, como para organizações. Ela move relações, negócios e representa, segundo Fontes (2006) muito mais que um conjunto de dados: transformar esses dados em informação é transformar algo pouco significativo em um recurso de valor.

De acordo com Padoveze (2000), informação é o dado que foi processado e armazenado de tal forma que seja compreensível, acessível e que tenha valor (real ou percebido) para seu receptor. A informação é, portanto, um produto dos dados organizados para análise e suporte à tomada de decisão. Na mesma linha, Oliveira (1998) indica que a informação é o produto dos dados, devidamente registrados, classificados, organizados e interpretados. Este contexto abarca não só a qualidade da informação, mas também os aspectos relacionados com aspectos relativos à integridade, confiabilidade e veracidade da mesma.

Por sua essência e relevância, a informação deve ser suficientemente resguardada e protegida. Entretanto, graças à evolução da tecnologia e consequente aumento da interconectividade, a informação tende a se tornar vulnerável e suscetível à alterações de conteúdo não autorizadas e apropriação indevida por terceiros, denominadas de fraudes eletrônicas (ANDRADE et al., 2007).

3.2 SEGURANÇA DA INFORMAÇÃO

Como forma de prevenção a eventuais fraudes em sistemas de gestão que danifiquem e/ou alterem a integridade da informação, criaram-se políticas e instrumentos para aumentar a segurança da informação. Por definição, segundo a ABNT NBR ISO/IEC 17799:2005, segurança da informação corresponde ao desenvolvimento de ações que visam proteger o conteúdo das informações quanto a sua veracidade, confidencialidade, disponibilidade e integridade, minimizando riscos e maximizando as oportunidades de negócio das organizações (ABNT, 2005).

Desta forma, percebe-se que a segurança da informação tende a interferir diretamente no cotidiano de indivíduos e nos resultados das organizações.

A segurança da informação é formada por um contexto de variáveis necessárias para se chegar a um Sistema de Gestão da Segurança da Informação confiável, como citado por Fontes (2006). Para o autor, a segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que têm por objetivo proteger o recurso informação, indicando os pontos básicos necessários para aplicação de um SGSI.

Uma política implica em definir diretrizes, limites e o direcionamento que a organização deseja para os controles que serão implantados na proteção da informação (VIANEZ et al, 2008)

3.3 *FRAMEWORK* ABNT NBR ISO/IEC 27001/ 27002

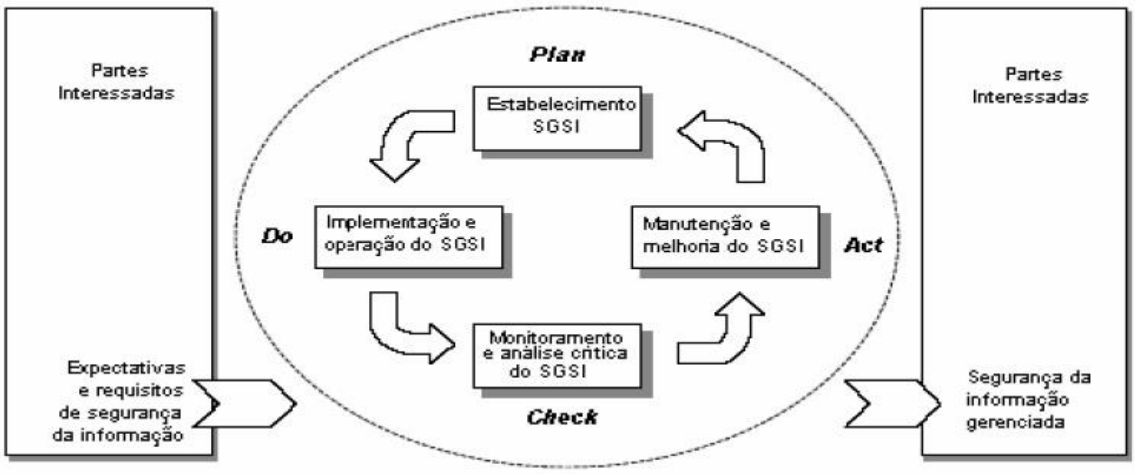
A história das normas ISO 27001 e ISO 27002 teve seu nascimento no Padrão Britânico - criação da Norma BS7799, sendo republicada pela *British Standard International*, devido ao grande crescimento das organizações (SÊMOLA, 2003). Em 2000, a norma britânica foi publicada por um órgão de caráter mundial - *International Organization for Standardization* (ISO) com o nome de ISO 17799.

A mesma organização, após revisões e atualizações, publicou, em 2005, nova versão a ISO 27001. No Brasil, o referido instrumento foi adotado pela Associação Brasileira de Normas Técnicas (ABNT) com o nome de ABNT NBR ISO/IEC (FONTES, 2012).

A aplicação de um Sistema de Gestão da Segurança da Informação (SGSI) segundo a NBR ISO/IEC 27001 adota ,como abordagem de processo, o modelo PDCA *(Plan-Do-Check-Act*). Abaixo segue esquema utilizado, segundo a ABNT (2005):

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

Figura 1 – Modelo do PDCA aplicado aos processos do SGSI



Fonte: NBR ISO/ IEC 27001 (2005)

A primeira etapa - Planejamento (P – *Plan*), é essencial para implantação de um sistema de segurança da informação. Trata-se da criação de políticas e objetivos de segurança (ABNT, 2006), que indicam a necessidade da elaboração de uma política de segurança que oriente a direção para a segurança da informação, de acordo com os requisitos de negócio e com as leis e regulamentações pertinentes.

Segundo Sêmola (2003), uma política de segurança tem um papel similar à Constituição Federal, pois explicita as regras primordiais de direção do SGSI. O mesmo autor apresenta ainda, que esta Política deve estar focada nas camadas estratégica, tática e operacional da organização.

Neste contexto, o papel do gestor da segurança da informação é essencial, sendo necessário, para o bom desempenho de suas funções, o máximo de autonomia e autoridade possível para desenvolver, implantar e manter processos, a fim de aumentar as chances de sucesso na proteção das informações. Entretanto, apesar da liberdade, o gestor da informação deve ser submetido a regulamentos e controles indicados na política (FONTES, 2012).

Seguindo as etapas do PDCA, após a elaboração de políticas e objetivos, são demonstrados os passos seguintes no quadro 01:

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

Quadro 01 – Atividades do PDCA de um SGSI

Plan (planejar) – Programar e Estabelecer o SGSI	Estabelecer a política, objetivos, processos e procedimentos dos SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) – Implementar e Operar o SGSI	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (checar) – Monitorar e Analisar Criticamente o SGSI	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
Act (Agir) – Manter o Melhorar o SGSI	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna e relativas à análise crítica pela melhoria contínua do SGSI.

Fonte: Adaptado NBR ISO/ IEC 27001.

A norma NBR ISO/IEC 27001 incorpora um processo que visa escalonar o risco e valorizar os ativos, orientando quanto à analise e identificação de riscos e implantação de controles sua mitigação. A forma como o sistema é organizado e a estruturação de seus processos facilitará a replicação do sistema em outros locais (PALHARES, 2011).

Para melhor compreensão dessa norma, que provê e apresenta requisitos para a organização que possa estruturar um Sistema de Gestão da Segurança da Informação, elaborou-se o quadro 02, que apresenta os requisitos para sua implantação:

Quadro 02: Requisitos da NBR ISO/IEC 27001

Requisito	**Descrição**
Escopo	Abrangência da Norma.
Referência Normativa	Normas e Padrões relacionados à Norma 27001.
Termos e Definições	Termos e Definições relacionados à Segurança da Informação.
Sistema de Gestão de Segurança da Informação	Referente à criação, implementação, monitoramento e melhoria do SGSI; Trata também de documentos e registros de informações.
Responsabilidade da Direção	Definição de Responsabilidades, Treinamento e Provisão de Recursos relativos ao SGSI.
Auditorias Internas	Auditorias Internas realizadas por pessoal

	treinado e comprometido com o SGSI
Análise Crítica do SGSI	Análise realizada pelo corpo diretivo da organização das ações efetuadas pelo SGSI
Melhoria do SGSI	Trata das ações corretivas e preventivas efetuadas pelo SGSI

Fonte: Adaptado de Palhares (2011, p. 50-51).

Cabe ressalta que um Sistema de Gestão de Segurança da Informação pode ser definido como um comitê multidisciplinar, cuja principal responsabilidade seja estabelecer as políticas de segurança, disseminar o conhecimento e as práticas aos envolvidos, determinar quem são os responsáveis pelo mesmo e quais atribuições dentro de seus limites de atuação (ABNT, 2006).

Quanto à NBR ISO/IEC 27002, pode-se afirmar que se trata de um conjunto de boas práticas que podem ser aplicadas por um Sistema de Gestão de Segurança da Informação. Este instrumento é utilizado como referência e apresenta inúmeros controles para garantir a segurança da informação.

Como forma de expor as principais características dessa norma, elaborou-se o quadro 03, utilizando-se como referência a dissertação de Carlos Palhares (2011):

Quadro 03: Requisitos da NBR ISO/IEC 27002

Requisito	**Descrição**
Política de Segurança	São as normas desenvolvidas que consideram as responsabilidades, punições e as autoridades.
Segurança Organizacional	Estrutura da Gerência de Segurança.
Classificação e Controle de Ativos da Informação	Classificação, Registro e Controle dos Ativos.
Segurança Relacionada às Pessoas	Foco do Risco decorrente de atos praticados por pessoas.
Segurança Ambiental e Física	Levantamento da necessidade de definição das áreas de circulação restrita e de proteger equipamentos e a infraestrutura de TI.
Gerenciamento das Operações e Comunicações	Aborda temas relacionados a: procedimentos operacionais, homologação e implantação de sistemas, entre outros.
Controle de Acesso	Controle do Acesso a Sistemas, definição de competências e responsabilidades.
Desenvolvimento e Manutenção de Sistemas	Requisitos para Sistemas, Criptografia, Armazenamento de Arquivos e desenvolvimento e suporte para os Sistemas.
Gestão de Incidentes de Segurança	Notificação de vulnerabilidades, ocorrência de segurança e gestão de incidentes.
Gestão da Continuidade do Negócio	Reforço na necessidade de ter um plano de

	continuidade e contingência.
Conformidade	Referente à necessidade de observar os requisitos legais, como a propriedade intelectual.

Fonte: Adaptado de Palhares (2011, p. 51).

Em síntese, a norma NBR ISO/IEC 27001 apresenta os procedimentos para geração de um Sistema de Gestão de Segurança da Informação (SGSI), indo ao encontro da norma NBR ISO/IEC 27002, que indica os elementos essenciais para aplicar a proteção da informação. Na primeira página da referida instrução (ABNT, 2005), a norma indica seus objetivos:

> Esta norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos desta Norma proveem diretrizes gerais sobre metas geralmente aceitas para a gestão da segurança da informação.

De acordo com Palhares (2011), o conjunto das duas normas pode ser descrito como um método estruturado, reconhecido internacionalmente, para a segurança da informação. Ademais, tendo em vista suas características e requisitos de implantação, formam um processo definido para avaliar, implantar, manter e gerenciar a segurança da informação, proporcionando um arcabouço de práticas a serem adotadas pelas organizações que se preocupam com o tema.

Segundo Albertin (2006), a adoção de padrões conhecidos no mercado, como as ISO 27001 e 27002, possuem diversas vantagens. A principal é a conformidade (compliance) dos processos corporativos com a norma, indicando aos parceiros de negócio sua preocupação com a Confidencialidade, Integridade e Disponibilidade da informação manipulada.

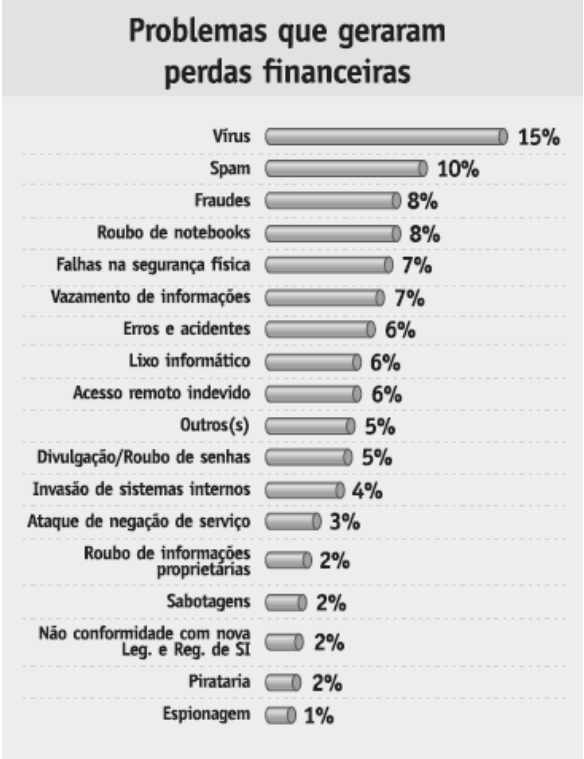
4 APRESENTAÇÃO E DISCUSÃO DOS RESULTADOS

4.1 PROBLEMAS, AMEAÇAS E AS BARREIRAS COM SEGURANÇA DA INFORMAÇÃO

Um dos pontos de um planejamento é a análise e reconhecimento dos reais riscos que podemos encontrar pelo caminho. Neste sentido são demonstrados, segundo a pesquisa da

empresa Módulo (2007), os problemas que mais estiveram presentes nas organizações e contribuíram para despender dinheiro sem retorno.

Figura 02 – Problemas que geraram perdas financeiras.

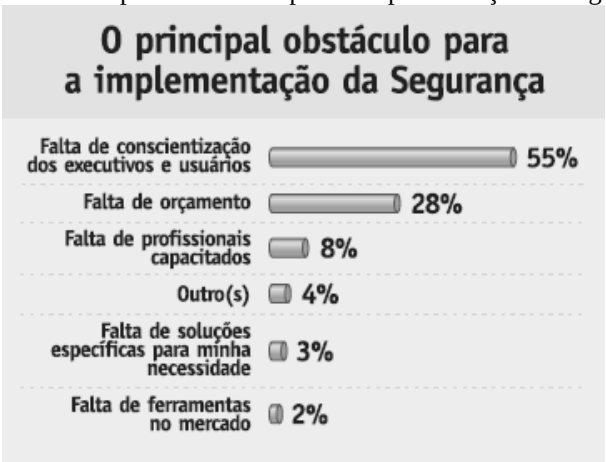


Fonte: Módulo Security Solutions (2007).

Conhecendo os problemas, o próximo passo é a criação da política de segurança para tentar minimizar os riscos. No entanto, as empresas esbarram em diversas barreiras, como relaciona a pesquisa da empresa Módulo (2007), que indica como sendo o principal obstáculo a falta de consciência dos gerentes e dos usuários, que muitas vezes não são favoráveis à mudanças na sua rotina.

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

Figura 03 – Principais obstáculos para a implementação da Segurança.



Fonte: Módulo Security Solutions (2007)

Segundo dados coletados, os problemas existentes nos escritórios respondentes não divergem dos que foram apontados pela 10ª Pesquisa Nacional de Segurança da Informação (2007), a saber: Inexistência de planejamento formal de segurança; falta de treinamento e capacitação de usuários; falta de previsão orçamentária para investimentos em segurança; impacto sobre as rotinas operacionais; e problemas nos sistemas operacionais e banco de dados existentes e utilizados.

Cabe ressaltar que escritórios com até três funcionários apontaram como principal dificuldade a falta de recursos para investir em sistemas de segurança da informação, enquanto escritórios com mais estrutura, embora executem rotinas alicerçadas em procedimentos de segurança, não possuem formalização ou padronização efetiva destes procedimentos. Percebeu-se também que as perdas de informação e o retrabalho ocorrem, em mais da metade dos escritórios pesquisados, devido à falha no sistema de gestão e/ou no banco de dados corporativo.

4.2 PADRÕES E NORMAS MÍNIMAS PARA ESCRITÓRIOS CONTÁBEIS

Com base na pesquisa realizada e com os dados apresentados por Fontes (2011), é possível vincular aos erros e problemas encontrados neste estudo alguns itens da ISO 27002 (2005), cabíveis à situação destes escritórios, a saber:

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

Quadro 04 – Itens Mínimos da NBR ISO/IEC 27002 Indicado a Escritórios Contábeis.

Item 5.1 Política de Segurança da Informação	Formalizar orientações sobre segurança da informação, como: definições, declarações de comprometimento, estrutura da segurança e meta. É delineada também a periodicidade de uma análise crítica sobre a própria política.
Item 8.2 Segurança em Recursos Humanos: Durante a Contratação	Certificar que os colaboradores estão cientes dos riscos ligados à informação e que estes estejam devidamente prontos à colaborar com a política de segurança da informação
Item 8.3 Segurança em Recursos Humanos: Encerramento ou Mudança da Contratação	Definir responsabilidades claras no momento do término do contrato seja ele funcionário, fornecedor ou terceiro, formalizando a devolução de ativos da organização e retirando os direitos de acesso às informações, recursos e sistemas.
Item 9.1 Segurança Física e do Ambiente: Áreas Seguras	Impedir o acesso físico de não autorizados, aplicando controles de entrada ao local a fim de evitar riscos internos e externos, como, por exemplo, incêndio ou inundação.
Item 9.2 Segurança de Equipamentos	Assegurar o funcionamento dos equipamentos como computadores, energia elétrica e cabeamento de rede. Aplicar frequentemente a manutenção assegurando a disponibilidade e integridade.
Item 10.3 Gerenciamento das Operações e Comunicações: Planejamento e Aceitação dos Sistemas	Analisar se o sistema terá capacidade para suprir necessidades futuras que virão com o crescimento da organização e certificar que o sistema possui atualizações frequentes e devidamente testadas.
Item 10.5 Cópias de Segurança	Criar cópias de segurança das informações com o objetivo de manter a integridade e disponibilidade, definindo arquivos necessários, frequência, localidade remota, testes sobre *backup* e encriptação.
Item 10.6 Gerenciamento da Segurança em Redes	Coordenar e controlar as redes com o propósito de prevenir o dano e a perda da informação e o funcionamento da infraestrutura.
Item 10.10 Monitoramento do Uso do Sistema	Submeter o uso das informações a controles de monitoramento para que possam ser analisadas futuramente – criação de um LOG de uso.
Item 11 Controle de Acesso	Neste item são indicados os controles ligados aos sistemas de informação, como registros de usuários, privilégios e controle de senhas.

Fonte: Os Autores, 2012.

4.3 EXEMPLO DE POLÍTICA E NORMAS DA SEGURANÇA DA INFORMAÇÃO VOLTADO À CONTABILIDADE

Uma política ou norma de SGSI visa estabelecer procedimentos sobre o funcionamento e a sistemática da empresa, quais os cuidados e detalhes de funcionamento. A linguagem deve ser clara, objetiva e interessante ao leitor, com o intuito de se fazer entender facilmente (FONTES, 2012).

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

Com o auxílio de diversos modelos apresentados por Fontes (2012) e os itens levantados como específicos para a amostra pesquisada, segue abaixo um exemplo de Política de Segurança da Informação formalizada.

Cabe ressaltar que a elaboração se deu a partir dos dados levantados junto aos escritórios de contabilidade respondente e não são aplicáveis a qualquer negócio ou escritório em outra região do Estado de Santa Catarina ou do Brasil.

EXEMPLO

POLÍTICA DE SEGURANÇA E PROTEÇÃO DA INFORMAÇÃO

OBJETIVO *- Definir normas e procedimentos para tratamento e precauções sobre informações geradas, armazenadas e manipuladas nos meios lógicos e físicos no ambiente do escritório.*

ABRANGÊNCIA *- Esta política é aplicável a todos os usuários (gerentes, contadores, colaboradores, estagiários, clientes e fornecedores) da informação que estejam vinculados de alguma forma ao escritório.*

IMPLEMENTAÇÃO *- Serão escolhidos representantes responsáveis pela Gestão da Segurança da Informação, estes farão a implementação e manutenção para continuidade da política de segurança. Terão o rotulo de Gerente de Segurança da Informação (GSI), este pode indicar subgerentes a fim de auxiliar na aplicação e controle da política.*

PROCEDIMENTOS E RESPONSABILIDADES

Declaração de Responsabilidade: Todos os usuários devem preencher a Declaração de Responsabilidades, com o intuito de se declararem cientes de seus direitos e obrigações sobre o uso de equipamentos, acessos físicos e lógicos e disseminação de informações em caráter interno do escritório, tanto durante o período de contrato com o escritório como após o término.

Término de Contrato: O GSI tem a responsabilidade de aplicar os procedimentos a seguir no momento da saída de algum colaborador ou término de contrato com algum cliente ou fornecedor:
- Devolução de equipamentos e documentos do escritório;
- Devolução de chaves e cartões da empresa;
- Exclusão de login e senha dos usuários nos sistemas; e
- Aplicação da Declaração de Confidência.
Obs. A Declaração de Confidência especifica pontos sobre a divulgação de informações internas da empresa a concorrentes diretos e/ou clientes e fornecedores.

Acessos Físicos: Fica o GSI responsável por rotular documentos e informações, bem como o banco de dados da empresa, pela importância e aplicar a segurança física sobre estes, as chaves de acesso ficarão exclusivamente com o GSI.

Segurança dos Equipamentos: Com a frequência trimensal o Gerente de Segurança deverá contratar um Técnico em Computadores e Redes com a finalidade de analisar o funcionamento da estrutura de cabeamento e os equipamentos, fica também responsável pela contratação quando de ocorrência de sinistros sem previsão.

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

Planejamento e Aceitação do Sistema: Juntamente com a alta gerência e supervisores dos colaboradores o GSI fará análises com frequência semestral nos sistemas utilizados e na estrutura de banco de dados, com o intuito de aplicar uma estrutura condizente com as necessidades futuras do escritório.

Cópias de Segurança: Serão realizadas cópias de segurança duas vezes ao dia,uma no período de almoço dos usuários e outra ao final do expediente. Estas cópias ficarão em três locais:
- Servidor local;
- Discos Rígidos (HD) externos; e
- Servidor em nuvem (Internet).
O Gerente de Segurança será responsável pela contratação do servidor em nuvem e terá posse exclusiva do HD externo. O GSI terá que uma vez por semana testar as cópias de segurança.

Acessos Lógicos: Fica o Gerente de Segurança responsável por indicar subgerente pelo cadastro de usuário no sistema utilizado pelo escritório, bem como aplicar controle geral de senhas, privilégios de uso e restrição a informações.

Monitoramento e Controle: O Gerente é exclusivo responsável pelo controle permanente desta política e poderá fazer uso de processo de registro de eventos (LOG) a todos os usuários com o objetivo de analisar futuros problemas e ocorrências.

***CUMPRIMENTO** - O não cumprimento dos procedimentos e responsabilidades apontados nesta política acarretará penas administrativas, contratuais e até legais. Cabendo demissão de colaboradores e/ou rescisão de contrato com clientes e fornecedores.*
Em caso de situações não previstas, os usuários poderão preencher a Ficha de Sugestões e encaminhar para análise do GSI e gerência.

Todos os usuários devem preencher a Declaração de Responsabilidades, com o intuito de se declararem cientes de seus direitos e obrigações sobre uso de equipamentos, acessos físicos e lógicos e disseminação de informações de caráter interno, durante o período de contrato com o escritório como após o termino.

Assim, tem-se um exemplo que inclui os itens relevantes indicados pela pesquisa para aplicação de uma Política de Segurança da Informação em escritórios contábeis. Apesar de sucinta, sua aplicação em escritórios depende de ajustes de acordo com a peculiaridade de cada estrutura.

4.4 ANÁLISE DOS RESULTADOS

Os problemas previstos antes da ocorrência são riscos que podem ser evitados com a implantação de uma política de segurança. Em muito dos casos, os escritórios respondentes

possuem ferramentas para evitar alguns dos gastos não orçados no planejamento mensal. Porém, estes escritórios não possuem formalização ou profissional responsável para manter a política de segurança em execução.

Pelo fato de não ser possível indicar uma política padrão que seja capaz de ser aplicada a qualquer escritório, a presente pesquisa conseguiu apontar alguns dos problemas mais comuns na área de contabilidade e levantar quais itens seriam aplicáveis a uma política de segurança mais efetiva. No entanto, é salutar que exista investimento suficiente para a continuidade da ideia, gerando assim a melhora contínua do processo. Embora acarrete no dispêndio de tempo e de dinheiro, o processo é um esforço necessário não só aos escritórios contábeis, mas a todas as empresas que tenham grandes perspectivas de crescimento.

A partir do artigo, pode-se observar que com uma Política de Segurança bem aplicada e relacionada com os objetivos de negócio, tem-se a melhoria de processos e de controle sobre os dados e as informações que concernem à empresa.

5 CONSIDERAÇÕES FINAIS

Este artigo teve como principal foco levantar os pontos mais importantes no quesito segurança da informação em escritórios contábeis. Foi desenvolvido a partir de um estudo em escritórios da Grande Florianópolis com o objetivo de levantar principais problemas com segurança da informação e as barreiras na aplicação de uma política de segurança da informação.

O questionamento principal, acerca de quais procedimentos e padrões mínimos deve ser adotado para a elaboração prática de uma Política de Segurança da Informação em escritórios contábeis foi respondido pela apresentação dos pontos comuns entre os dados levantados junto à amostra selecionada e as pesquisas utilizadas como fonte secundárias da informação.

Os objetivos específicos foram atendidos pela sumarização dos problemas, ameaças e barreiras na aplicação da segurança da informação em escritórios de contabilidade, mediante a aplicação de questionário semiestruturado e cruzamento de informações regionais e de outras pesquisas; identificação dos problemas levantados sob o prisma dos padrões mínimos da ISO

27002; e a elaboração de um exemplo de Política de Segurança da Informação com base nos itens selecionados.

Como mencionado, foram constatadas similaridades dos escritórios locais entrevistados com os resultados das pesquisas utilizadas como fonte de dados secundários demonstrando que os problemas e as barreiras de implantação de políticas e práticas de segurança da informação independem do continente.

Ademais, os resultados obtidos indicam que há conscientização por parte dos empresários sobre a necessidade de priorização de ações para a segurança da informação. Isto requer o dispêndio de um volume de recursos para aumentar a integridade, autenticidade, confiabilidade e disponibilidade das informações a fim de subsidiar a tomada de decisão.

A pesquisa teve como principais limitações a falta de recursos para maior seleção amostral e de pessoal com capacidade técnica sobre segurança da informação, bem como o acesso amplo e irrestrito às informações das organizações estudadas, motivos pelos quais se justificou o método de seleção dos entrevistados.

Por se tratar de um tema de cunho prático, a maioria do referencial teórico utilizado se baseia em estudos de caso e em suas conclusões e indicações. Porém, por se tratar de um assunto relativamente atual, indica-se, a futuros pesquisadores, a investigação utilizando a técnica de pesquisa *ex-post-facto*, com o objetivo de avaliar quais foram os impactos causados pela implantação das ABNT NBR ISO/IEC 27001 e 27002 nas organizações contábeis da região estudada.

REFERÊNCIAS

ABNT, **NBR ISO/ IEC 27001 Tecnologia da informação – Técnicas de segurança – Sistema de Gestão da segurança da informação – Requisitos**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2006.

ABNT, **NBR ISO/ IEC 27002 Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

ANDRADE, A. D; SOUSA, F. C. A.; COLAUTO, R. D; PINHEIRO, L. E. T. Políticas de Segurança em Sistemas de Informação Contábil: um estudo em cooperativas de crédito do

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

estado de Minas Gerais. **Revista Contemporânea de Contabilidade**, v. 04, nº. 7, jan/jul., Florianópolis; UFSC, 2007.

ALBERTIN, Alberto Luiz; PINOCHET, Luis Hernan Contreras**. Política de Segurança de Informações**. Rio de Janeiro: Elsevier, 2010.

ALMEIDA, Mário de Souza. **Elaboração de Projeto, TCC, Dissertação e Tese:** Uma Abordagem Simples, Prática e Objetiva. São Paulo: Edito Atlas, 2011.

ALVES, Gustavo Alberto. **Segurança da Informação** – Uma Visão Inovadora da Gestão. 1. Ed. Rio de Janeiro: Editora Ciência Moderna, 2006.

BARBETTA, Pedro Alberto. **Estatística Aplicada às Ciências Sociais**. Florianópolis: Editora da UFSC, 1994.

BENZ, Karl Heinz. **Alinhamento estratégico entre políticas de segurança da informação e as estratégias e práticas adotadas na TI: estudo de casos em instituições financeiras**. Porto Alegre: Universidade Federal do Rio Grande do Sul, Dissertação de Mestrado, Programa de Pós Graduação em Administração, 2008.

CAVALCANTE, Sayonara de Medeiros. **Segurança da informação no correio eletrônico baseada na ISO/IEC 17799: um estudo de caso em uma instituição de ensino superior, foco no treinamento**. Natal: Universidade Federal do Rio Grande do Norte, Dissertação de Mestrado, Programa de Engenharia de produção, 2003.

COOPER, Donald. R.; SCHINDLER, Pamela. S. **Métodos de Pesquisa em Administração**. 7ª. Ed. Porto Alegre: Bookman, 2003.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação**: o usuário faz a diferença. 1. Ed. São Paulo: Saraiva, 2006.

FONTES, Edison. **Política de segurança da informação**: uma contribuição para o estabelecimento de um padrão mínimo. São Paulo: Centro Estadual de Educação Tecnológica Paula Souza, Dissertação de Mestrado, Programa de Pós-Graduação em Tecnologia, 2011.

FONTES, Edison Luiz Gonçalves. **Políticas e normas para segurança da informação**. 1. Ed. Rio de Janeiro: Brasport, 2012.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social**. 5ª ed. São Paulo: Atlas, 2007.

GONÇALVES, José Artur Teixeira. **Metodologia da pesquisa**. Blog do professor. Disponível em: http://metodologiadapesquisa.blogspot.com/2009/04/conhecimento-cientifico-e-conhecimento.html. Acesso em: 22 nov. 2012.

ISACA/ **Information System Audit and Control Association.** Disponível em: < http://www.isaca.org/>. Acesso em: 11 de dez. de 2012.

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

LORENS, Evandro. **Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação**. Brasília: Universidade de Brasília, Dissertação de Mestrado, Departamento de Ciência da Informação e Documentação, 2007.

MALHOTRA, Naresh K. **Pesquisa de Marketing**: uma orientação aplicada. 4ª. Ed. Porto Alegre: Bookman, 2006.

MENEZES, Josué das Chagas. **Gestão da segurança da informação: análise em três organizações brasileiras**. Salvador: Universidade Federal da Bahia, Dissertação de Mestrado, Núcleo de Pós Graduação em Administração, 2005.

MENEZES, Josué das Chagas. **Gestão da segurança da informação**. 1. Ed. Leme: Mizuno, 2006.

MODULO SECURITY SOLUTIONS. **10º Pesquisa Nacional de Segurança da Informação.** 2006. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. Acesso em: 11 de ago. de 2012.

OLIVEIRA, Djalma de Pinho Rebouças. **Sistemas, organização e métodos – uma abordagem gerencial.** 10. ed. São Paulo: Atlas, 1998.

PADOVEZE, Clovis Luiz. **Sistemas de informações contábeis** – fundamentos e análise**.** 2. ed. São Paulo: Atlas, 2000.

PALHARES, Carlos Alberto de Magalhães Cordeiro. **Governança de TI: Cenário atual das Instituições de Ensino Superior Brasileiras**. São Paulo: Centro Estadual de Educação Tecnológica Paula Souza, Dissertação de Mestrado em Tecnologia, 2011.

PELTIER, Thomas**. Information Security Policies and Procedures**. USA: Auerbach, 2005.

PRICEWATERHOUSECOOPERS. **Pesquisa Global de Segurança da Informação.** São Paulo: PricewaterhouseCoopers, 2012.

RIBAS, Carlos Eduardo. **Sistema de gestão da segurança da informação em organizações na área da saúde**. São Paulo: Universidade de São Paulo - USP, Dissertação de Mestrado, Faculdade de Medicina, 2010.

ROZA, Fabiana Freitas Furtado. **Política de segurança da informação em ambientes hospitalares**. São Caetano do Sul: Faculdade de Tecnologia, Trabalho de Conclusão de Curso de Graduação em Tecnologia em Segurança da Informação, 2010.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 1. Ed. São Paulo: Campus, 2002.

SILVA, Terezinha Elizabeth; TOMÁEL, Maria Inês. Gestão da Informação nas Organizações. **Revista Informação&Informação,** n. 12. Londrina: Universidade Estadual de Londrina, 2007.

MATTES, Ícaro Valente; PETRI, Sérgio Murilo; ROSA, Marcelo Medeiros da. **SEGURANÇA DA INFORMAÇÃO CONTÁBIL:** Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002[1]. Revista Interdisciplinar Científica Aplicada, Blumenau, v.9, n.4, p.39-60, TRIV 2015. ISSN 1980-7031.

SILVA, Antônio Everardo Nunes Da. **Segurança da Informação** – Vazamento de Informações – As informação estão realmente seguras em sua empresa. 1. Ed. Rio de Janeiro: Editora Ciência Moderna Ltda., 2012.

TRIVIÑOS, Augusto N. S. **Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação.** São Paulo: Atlas, 1987.

VENTURINI, Yeda Regina. **Modelo Ontológico de segurança para negociação de política de controle de acesso em multidomínios**. São Paulo: Universidade de São Paulo - USP, 2006.

VIEIRA, Marcelo Milano Falcão. **A Comparative study on quality management in the Brazilian and the Scottish prison service. Scotland: University of Edinburg.** Tese (Doutorado, PhD on Business Studies). Edimburgo. 1996.

VIANEZ, Marcos S.; SEGOBIA, Roberta H.; CAMARGO, Vander. Segurança de Informação: Aderência à Norma ABNT NBR ISO/IEC N. 17.799:2005. **Revista de Informática Aplicada**, v. IV n.1- Jan./Jun., São Caetano do Sul; USCS, 2008.