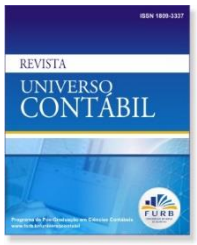


Revista Universo Contábil, ISSN 1809-3337
Blumenau, v. 10, n. 4, p. 68-85, out./dez., 2014

doi:10.4270/ruc.2014430
Disponível em www.furb.br/universocontabil

AVALIAÇÃO DE PROCESSOS DE SEGURANÇA DA INFORMAÇÃO INTEGRANDO AS ÁREAS DE CONTROLADORIA E TECNOLOGIA DA INFORMAÇÃO[1]

EVALUATION OF INFORMATION SECURITY PROCESSES INTEGRATING THE CONTROLLERSHIP AND IT AREAS

EVALUACIÓN DE PROCESOS DE SEGURIDAD DE INFORMACIÓN INTEGRANDO LAS ÁREAS DE CONTROLADORÍA Y TECNOLOGÍA DE LA INFORMACIÓN

Luiz Carlos Schneider
Mestre em Ciências Contábeis (UNISINOS)
Endereço: Rua Silveira Martins Correa, 386 – Bairro PIO X
CEP: 95180-000 – Farroupilha - RS
E-mail: schneider.luizc@gmail.com
Telefone: (55) 9903-3567

Adolfo Alberto Vanti
Doutor em Ciências Econômicas e Empresariais (Universidad de Deusto)
Professor Titular UNISINOS
Endereço: Av. Unisinos, 950 – Bairro Cristo Rei
CEP: 93.022-000 – São Leopoldo - RS
E-mail: avanti@unisinos.br
Telefone: (51) 3590-8186

Angel Cobo Ortega
Doutor em Ciências Matemáticas (Universidad de Cantabria)
Professor Titular da Universidad de Cantabria
Professor na Faculdade de Economia e Administração de Empresas
Endereço: Av. de los Castros s/n
CEP: 39005 - Santander – Espanha
E-mail: angel.cobo@unican.es
Telefone: (+34) 942 201 830

João Luis Peruchena Thomaz
Mestre em Ciências Contábeis (UNISINOS)
Endereço: Rua Rivadavia Correa, 1158/102 – Centro
CEP: 97.573-660 - Santana do Livramento - RS
E-mail: prof.peruchena@gmail.com
Telefone: (55) 3243-7309

[1] Artigo recebido em 24.03.2014. Revisado por pares em 10.09.2014. Reformulado em 29.12.2014. Recomendado para publicação em 29.12.2014 por Carlos Eduardo Facin Lavarda. Publicado em 30.12.2014. Organização responsável pelo periódico: FURB.

RESUMO

A Controladoria é responsável por informações que apoiam o processo de tomada de decisão nas organizações e devido a isso necessita participar dos processos de segurança da informação. Por isto, esta pesquisa avaliou de maneira aplicada os processos de segurança da informação integrando as áreas de Controladoria e de TI. Metodologicamente o trabalho se caracterizou como uma pesquisa descritiva em um processo quali-quanti, considerando a percepção de respondentes em 30 questões relacionadas ao problema proposto. Foi aplicado um questionário complementar com base na norma ISO/IEC 27002 inferindo explicação causal de integração de áreas, bem como definição de categorias de diferentes profissionais quando tratam a segurança da informação. Desenvolveu-se um estudo de caso aplicado com instrumentos de coleta de dados relacionados a questionários e entrevistas, identificando na análise de conteúdo os processos críticos de negócio e riscos associados ao ambiente da informação. Assim, foi possível aprimorar os processos operacionais dessas duas áreas, diminuindo riscos operacionais, através de ações conjuntas de participação de usuários, criação de equipes, maior padronização, alinhamento da comunicação, maior controle na alteração de sistemas, aprimoramento de políticas e normas de segurança da informação, uso de ferramenta de business intelligence, treinamentos, integração de informações, foco nos processos essenciais. Dessa maneira se atendeu ao objetivo de avaliar processos de segurança da informação integrando as áreas de Controladoria e de TI.

Palavras-chave: Controladoria. Tecnologia da Informação. Segurança da Informação.

ABSTRACT

The Controllership is responsible for the support decision-making process in organizations and because of that, it needs to participate in the information security processes. Therefore, this study evaluated the way of applied information security processes by integrating the areas of Controllership and IT. Methodologically the work was characterized as a descriptive research in a quali-quanti process, considering the perception of respondents in 30 questions related to the proposed problem. A supplementary questionnaire was applied based on ISO / IEC 27002 standard implying causal explanation of areas of integration and definition of different categories of professionals when they deal information security. We developed a case study applied to data collection instruments related to questionnaires and interviews, content analysis in identifying the critical business processes and risks associated with information environment. Thus, it was possible to improve the operational processes of these two areas, reducing operational risks through different actions related with participation of users, creating teams, greater standardization, communication alignment, greater control in changing systems, improvements to policies and safety standards information, use of business intelligence tools, training, information integration and focus in core process. Finally, it responded to objective of evaluating information security processes by integrating the areas of Controllership and IT.

Keywords: *Controllership. Information Technology. Information Security.*

RESUMEN

La controladoría es responsable por informaciones que suportan el proceso de toma de decisiones en las organizaciones y debido a esto necesita participar de los procesos de seguridad de información. Así, esta investigación evaluó de manera aplicada los procesos de seguridad de información, integrando las áreas de Controladoría y Tecnología de Información. Metodológicamente el trabajo se caracterizó como una investigación descriptiva en un proceso cuali-cuanti que consideró la percepción de respondientes en 30 cuestiones relacionadas al problema propuesto. Ha sido aplicado un cuestionario complementar basado en la ISO/IEC

27002 infiriendo explicación causal de integración de áreas, bien como la definición de categorías de diferentes profesionales cuando tratan la seguridad de la información. Se ha desarrollado un estudio de caso aplicado con instrumentos de coleta de datos relacionados a cuestionarios y entrevistas, identificando en un análisis de contenido los procesos críticos de negocio e riesgo al ambiente de la información. De esta manera, ha sido posible perfeccionar los procesos operacionales de estas dos áreas, disminuyendo riesgos operacionales, a través de acciones conjuntas de participación de usuarios, creación de equipos, mayor sistematización, alineación en la comunicación, mayor control en la alteración de sistemas, perfeccionamiento de políticas y normas de seguridad de información, uso de herramienta de inteligencia organizacional, entrenamientos, integración de informaciones y foco en los procesos esenciales. Así, se ha atendido al objetivo principal de evaluar los procesos de seguridad de información integrando las áreas de controladoría y tecnología de información.
Palabras clave: *Controladoría. Tecnología de la Información. Seguridad de información.*

1 INTRODUÇÃO

A evolução das tecnologias e constantes transformações no ambiente dos negócios demandam implementações nos *softwares* que refletem maior segurança nos processos de negócio, à qual segundo Kayworth e Whitten (2010), torna-se uma questão estratégica e de significativa preocupação entre os executivos das empresas. Acrescenta-se a este cenário a necessidade de informações condensadas e que estejam disponíveis no momento oportuno para tomada de decisões ágeis e precisas relacionadas a valor, controles e riscos (ITGI, 2007).

Neste sentido, faz-se necessário que a Controladoria área que responde pelas informações nas organizações, adotem procedimentos sistemáticos de avaliação dos processos relacionados aos seus sistemas de informações, com o intuito de minimizar possíveis impactos na qualidade e tempestividade das informações que possam comprometer o processo decisório.

No que se refere à qualidade e tempestividade da informação, o Comitê de Pronunciamentos Contábeis (CPC) no seu Pronunciamento Conceitual Básico 00 (2008 p.14) cita que a administração da entidade necessita ponderar os méritos relativos entre a tempestividade da divulgação e a confiabilidade da informação fornecida. Para fornecer uma informação oportuna é necessário divulgá-la antes que todos os aspectos de uma transação ou evento sejam conhecidos, do contrário prejudica sua confiabilidade e sua relevância.

Para atingir o adequado equilíbrio entre a relevância e a confiabilidade, o princípio básico consiste em identificar a melhor forma que satisfaça as necessidades do processo decisório. Essa identificação está relacionada a um sistema de informação (SI) estruturado, o qual, autores clássicos como Laudon e Laudon (2007, p.9), assim o definem: um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização. Em O'Brien e Marakas (2007, p.4) o SI pode ser qualquer combinação organizada de pessoas, *hardware*, software, redes de comunicação, recursos de dados e políticas e procedimentos que armazenam, restauram, transformam e disseminam informações em uma organização.

A extração e fluxo de dados e informações é de responsabilidade da área de Tecnologia da Informação (TI), sendo que uma de suas atribuições é adotar uma política de segurança com base em *frameworks* de governança tecnológica como a ISO 27002 (2001) que trata das recomendações de controles para a segurança da informação.

No enfoque de Controladoria, Borinelli (2006 p.136) define a função gerencial-estratégica da Controladoria como aquela compreendida às atividades relativas a prover informações de natureza contábil, patrimonial, econômica, financeira e não financeira ao

processo de gestão como um todo. Além disso, está no escopo dessa função a atividade de coordenar os esforços dos gestores para que se obtenha sinergia no processo de alcance dos objetivos empresariais.

Para Martin, Santos e Dias (2004), a Controladoria tem como uma de suas funções, as atividades de identificar, mensurar, analisar, avaliar, divulgar e controlar os diversos riscos envolvidos no negócio, bem como seus possíveis efeitos. Já para Carmen e Corina (2009), a Controladoria deve projetar e desenvolver um sistema de gestão orientado para a execução dos objetivos estratégicos da organização. Este sistema deve contemplar um conjunto de informações relevantes para a organização, conectado com seus esforços de criação de valor e visando a sustentabilidade do negócio no longo prazo.

Ampliando o conceito de Controladoria, Wilkin e Chenhall (2010) abordam a necessidade de uma sinergia entre as áreas de Controladoria e TI com o objetivo de garantir a integridade do sistema de informações dentro da exigência atual dos negócios. Isso permite a previsão de investimentos em estruturas, pessoas e mecanismos relacionados, reduzindo-se retrabalhos e decisões equivocadas e pouco tempestivas que conduzem a riscos financeiros, operacionais, tecnológicos entre outros que afetem diretamente seus ativos. Assim, torna-se necessário alinhar as percepções destas áreas (Controladoria/TI) na avaliação de processos de segurança de informações para que se minimize riscos operacionais.

A partir desta contextualização foi possível definir uma questão problema do presente estudo: Qual a avaliação dos processos de segurança da informação integrando as áreas de Controladoria e de TI? O objetivo correspondente foi o de avaliar processos de segurança da informação integrando as áreas de Controladoria e de TI.

As contribuições do estudo se relacionam ao aprimoramento dos processos operacionais entre Controladoria e TI, diminuindo riscos operacionais com a contínua avaliação de processos de segurança da informação em aspectos relacionados a uma maior participação de usuários, criação de comitês de áreas, maior padronização quanto à homologação integrada de solicitações, alinhamento da comunicação, maior controle na alteração de sistemas, aprimoramento de políticas e normas de segurança da informação, uso de ferramenta de *business intelligence* como apoio na modelagem de sistema de informações, treinamentos, melhor tratamento de riscos econômicos/financeiros, integração de informações e foco nos principais processos da empresa.

O artigo se apresenta seguindo uma estrutura de revisão da literatura contemplando a seção de controladoria, logo segurança de informações, metodologia, apresentação do caso estudado e respectiva análise de resultados para finalmente atender a considerações finais e referências bibliográficas.

2 REVISÃO DA LITERATURA

Para a revisão a literatura estão contemplados principalmente os temas de controladoria e segurança de informações, sendo os mesmos aprofundados nesta continuação.

2.1 Controladoria

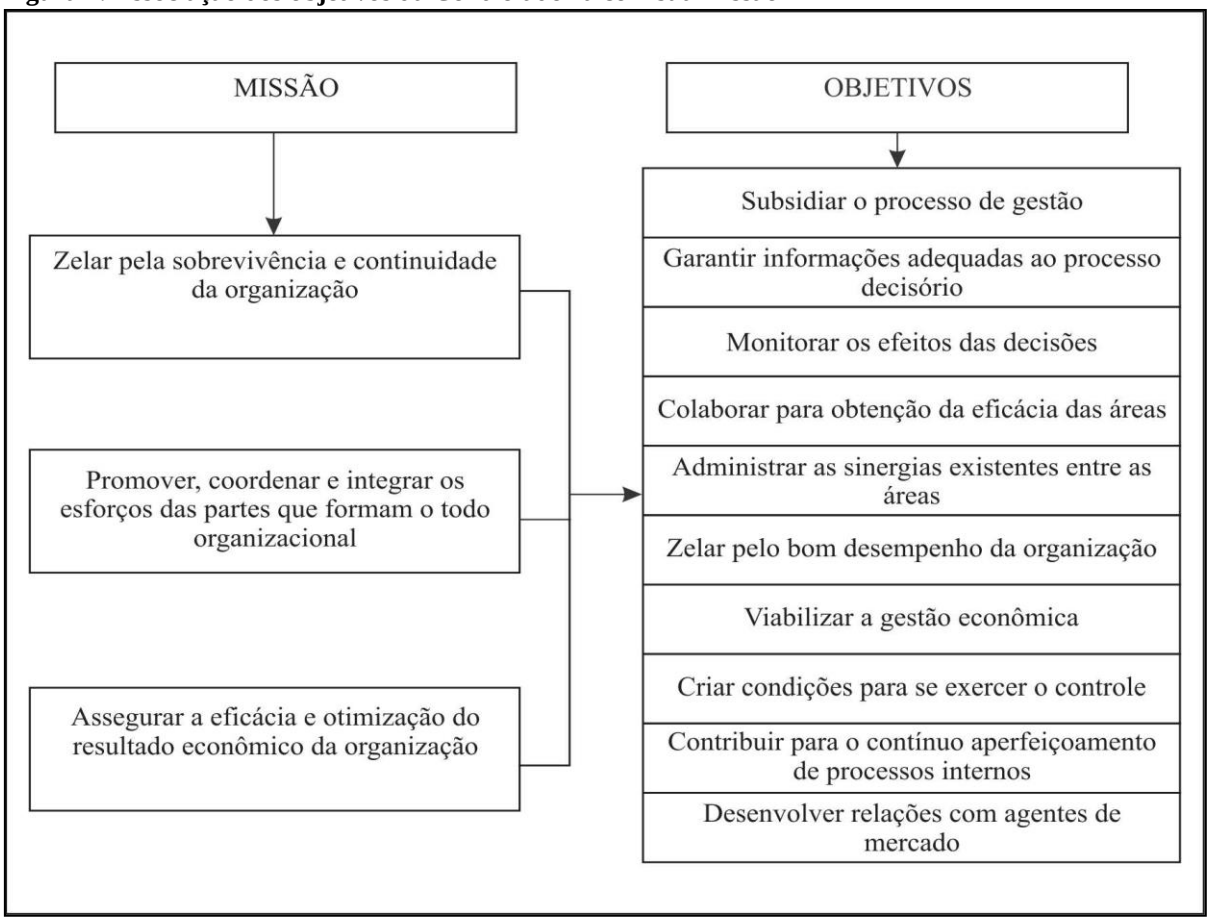
O ambiente contemporâneo dos negócios em que a globalização e a concorrência estimulam a busca constante pela eficiência da gestão nas empresas, acrescidos de órgãos reguladores intensos e o aquecimento do mercado de capitais no Brasil, desafiam a área de Controladoria a adotar uma postura mais participativa e integrada no trato da informação para poder cumprir com sua missão e objetivos perante aos órgãos diretivos das empresas.

No que se refere ao aspecto da participação da Controladoria nas organizações, Carmen; Corina (2009) consideram que esta deve estar envolvida nos processos de decisões estratégicas da organização, integrando a estratégia e as ações necessárias para alcançar os objetivos estabelecidos na estratégia. Nos processos de decisão, as informações fornecidas pela

Controladoria devem permitir a compreensão dos fenômenos medidos e ser relevantes para a tomada de decisões em níveis estratégicos, táticos e operacionais. Além disto, devem incentivar ações consistentes, apoiar e criar um conjunto de valores culturais integrados que gerem efeitos no comportamento funcional para que sejam alcançados os objetivos da organização. Estas características informacionais criam valor para a organização.

Com relação à missão e objetivos da Controladoria, Borinelli (2006, p. 208) faz uma associação entre eles conforme apresentado na figura 1.

Figura 1: **Associação dos objetivos da Controladoria com sua missão**



Fonte: Borinelli (2006, p. 208)

É possível identificar que a Controladoria diante desta associação proposta por Borinelli tem um papel estratégico nas organizações. Suas atribuições e responsabilidades requerem além dos aspectos conceituais e técnicos, a necessidade do envolvimento organizacional, com seus *stakeholders* que vislumbram na continuidade da organização, na otimização do resultado econômico e financeiro, bem como nas oportunidades de negócio.

Borinelli (2006, p.109) também cita que dentre os focos de atuação da controladoria existem as necessidades informacionais, consubstanciadas nos modelos de informação e de decisão, explicitados em referida obra. Para tal, segundo Atkinson et. al. (2008), a Controladoria atua no presente orientado para o futuro através de sistemas de informações que atendam às necessidades estratégicas e operacionais da organização. Desta forma, entende-se que a Controladoria não pode delegar ou não participar dos processos de segurança da informação, pois ela é corresponsável pelos sistemas informacionais das organizações.

Para integrar áreas e apoiar o processo de geração de informações torna-se necessário contar com profissionais que obtenham conhecimentos teóricos e práticos em diversas áreas do ambiente organizacional, sendo proativos para que efetivamente na prática possa a área de

Controladoria exercer a função atribuída pelas teorias. Na seção seguinte é abordado o tema segurança de informações por ser de fundamental importância nesse processo decisório responsabilizado pelo *Controller*.

2.2 Segurança de Informações

As informações para as empresas são um dos ativos mais relevantes e fazem parte de suas vantagens competitivas. Portanto, preservá-las e disponibilizá-las no momento adequado é requisito de uma política eficaz de segurança de informações. Esta é a proteção da informação de vários tipos de ameaças para garantir a continuidade e as oportunidades do negócio bem como maximizar o retorno sobre os investimentos (ISO/IEC 27002, 2007).

Para Araújo (2009), as organizações necessitam de uma efetiva gestão da segurança da informação diante de um ambiente de constante aumento de informações produzidas, de conectividade através de redes e do armazenamento em meios digitais. Estes fatores podem tornar o ambiente informacional mais suscetível à alteração de dados, acessos indevidos e indisponibilidade de serviços em rede, comprometendo a qualidade da informação e consequentemente afetar a tomada de decisão e a continuidade dos negócios.

Segundo Young e Windsor (2010), existe uma relação positiva relevante entre a maturidade da integração do planejamento de segurança da informação e a disponibilidade das informações. Para o autor, organizações com maior número de informações exibem mais maturidade na segurança de informação por incluir em seus processos uma gestão participativa dos usuários, o que conduz a implementações de segurança da informação mais eficaz. No entanto, a descentralização pode conduzir a problemas quando não se possui um programa de treinamento e conscientização destes usuários.

De acordo com a ISO/IEC 27002 (2007), muitos sistemas de informações 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 com essa conscientização de usuários. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes em que a segurança da informação é dependente da participação dos funcionários da organização. Pode ser necessário inclusive ampliar essa participação na política de segurança da informação aos acionistas, fornecedores e clientes, pois eles também detêm informação crítica de sucesso.

Conforme Bulgurcu, Cavusoglu, Benbasat (2010), os usuários são os principais aliados das organizações nos esforços de reduzir os riscos relacionados à segurança da informação. Neste mesmo raciocínio, Spears e Barki (2010) em estudo envolvendo executivos que atuaram em empresas financeiras norte americanas durante a Sarbanes-Oxley (SOX), afirmam que os usuários podem ser o recurso mais valioso na gestão de risco da segurança de informações.

A norma ISO/IEC 27002 (2007) estabelece critérios ao qual objetiva analisar o nível de proteção das práticas de segurança da informação nas organizações. A aplicação destes critérios contribui com uma visão sistêmica sobre o tema segurança de informações, os quais foram aplicados na parte prático deste trabalho. Na continuação são descritos os critérios utilizados no presente estudo como apoio ao processo de coleta e análise dos dados transcritos da norma 27002 (ISO/IEC 27002, 2007, p. 8-108):

- PL – Política de segurança da informação, que tem por objetivo prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes;

- OI – Organizando a segurança da informação, que tem por objetivo gerenciar a segurança da informação dentro da organização:

- GA – Gestão de ativos, que tem por objetivo alcançar e manter a proteção adequada dos ativos da organização;

- RH – Segurança em recursos humanos, que tem por objetivo assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis, e reduzir o risco de furto ou roubo, fraude ou mal uso de recursos;

- GO – Gerenciamento das operações e comunicações, que tem por objetivo garantir a operação segura e correta dos recursos de processamento da informação;

- CA – Controle de acessos, que tem por objetivo controlar acesso à informação;

- AQ – Aquisição, desenvolvimento e manutenção de sistemas de informação, que tem por objetivo garantir que segurança é parte integrante de sistemas de informação;

- GI – Gestão de incidentes de segurança da informação, que tem por objetivo assegurar que fragilidades e eventos de segurança da informação associados a sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil;

- GC – Gestão da continuidade do negócio, que tem por objetivo não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso;

- CF – Conformidade, que tem por objetivo evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

As respectivas análises relacionadas aos níveis de proteção das práticas de segurança da informação nas organizações de acordo com a norma ISO/IEC 27002 aparecem de maneira aplicada neste trabalho tendo como base as percepções dos gestores participantes do estudo para cada domínio da norma na organização estudada.

Os domínios classificados como mais frágeis quanto ao grau de proteção da informação pelos gestores podem propiciar riscos ao ambiente informacional e comprometer o processo decisório. Desta forma, a norma ISO/IEC 27002 contempla diretrizes e princípios que contribuem no aprimoramento dos controles e, por conseguinte do ambiente da informação. Na continuação, aborda-se a metodologia de pesquisa utilizada neste trabalho.

3 METODOLOGIA

O presente estudo caracteriza-se por um paradigma fenomenológico ou interpretativista (COLLINS; HUSSEY, 2005) pela utilização metodológica de abordagem qualitativa porque descreve a percepção dos respondentes ao problema proposto. Também foi aplicado um questionário complementar quantitativo tendo como base a norma ISO/IEC 27002, pois considera-se aqui que o número tem como base o próprio pensamento qualitativo e a fundamentação em palavras ou na interpretação.

Nesta conjugação de enfoque qualitativo e complementar quantitativo foi possível ao final da pesquisa inferir uma explicação causal de integração de áreas e posteriormente uma compreensão mais significativa das vivências investigadas. Consequentemente, se definiu categorias que diferentes profissionais usam no trato do mesmo tema, aqui denominado segurança da informação.

Para os instrumentos de coleta de dados utilizou-se de múltiplas fontes, tais como, questionários, entrevistas e uso de técnica de coleta de priorização de informação baseada em AHP. Na continuação são apresentados de maneira mais detalhada os instrumentos de coleta de dados. Também na referência de Schneider (2012) é possível constatar total aprofundamento de diferentes instrumentos utilizados.

A etapa inicial de coleta de dados foi verificar junto aos gestores quais os principais processos de negócio na organização ao qual a informação é primordial para a continuidade dos negócios. Identificaram os seguintes processos críticos de negócios como unidade de análises: (i) comprar; (ii) estocar; (iii) vender; (iv) distribuir; (v) pós-venda; e (vi) tributação.

Na segunda etapa, foi enviado por e-mail aos gerentes de TI, Controladoria e de Contabilidade para uma prévia análise, o primeiro instrumento de coleta de dados que se baseia

na norma ISO/IEC 27002 em que a mesma serviu de suporte para o preenchimento das respostas. Posteriormente foi agendada uma reunião conjunta com todos os gestores, onde foi realizada a apresentação do instrumento, explicações sobre sua finalidade para a pesquisa e esclarecimento de dúvidas.

Esse primeiro instrumento foi composto de seções com categorias para tratamento dos processos de segurança da informação. Foi elaborado através da seleção de seções com a adaptação das categorias ao objetivo do estudo, a fim de avaliar os controles relacionados à segurança da informação.

Questões mais técnicas estão detalhadas na dissertação desenvolvida e apresentada em Schneider (2012) em que se especifica todo o passo a passo conforme sequenciamento da continuação. Mesmo assim, de maneira mais sintética aqui é apresentado o sequenciamento e conteúdo contemplado.

a) política de segurança da informação: verificação da existência de uma política de segurança da informação;
b) organização da segurança da informação: verificação do procedimento de gerenciamento da segurança da informação dentro da organização;
c) gestão de ativos: verificação de procedimentos em como a organização mantém e protege seus ativos;
d) segurança em recursos humanos: verificação de níveis de responsabilidade de funcionários e terceiros, proteção dos ativos da empresa contra fraude, roubo ou mau uso de recursos;
e) gerenciamento das operações e comunicações: verificação da gestão dos recursos de processamento e controles da informação;
f) controle de acessos: verificação da gestão dos controles de acesso à informação;
g) aquisição, desenvolvimento e manutenção de sistemas de informação: verificação de níveis de garantia de segurança aos sistemas de informação;
h) gestão de incidentes de segurança da informação: verificação do processo de comunicação e correção quando eventualmente existir incidentes com eventos de segurança da informação;
i) gestão da continuidade do negócio: verificação de níveis de gestão que evitem interrupções das atividades de negócio;
j) conformidade: verificação do processo de gestão quanto a violações de obrigações legais, informações estatutárias, contratuais relacionadas à segurança da informação.

A aplicação desse primeiro instrumento de coleta de dados serviu de subsídios juntamente com o referencial teórico para a elaboração do roteiro da entrevista em profundidade, segundo instrumento de coleta de dados do presente estudo. Após a elaboração do roteiro de entrevista, foi contatado o Gerente de TI para agendar uma reunião com os entrevistados para validação do roteiro, estabelecer uma agenda de entrevistas e visitas à empresa. De acordo com Yin (2010), a entrevista em profundidade permite que o pesquisador elabore perguntas ao entrevistado sobre questões relacionadas ao assunto objeto do estudo, bem como possibilita emitir suas opiniões sobre esses eventos. Neste enfoque, o entrevistado participa efetivamente do estudo, atendendo às questões, propondo determinados temas para futuras investigações, sugerindo pessoas para serem entrevistadas ou fontes de evidências.

Antes da etapa de aplicação da entrevista, efetuou-se uma rodada de perguntas e respostas de forma individualizada com os gerentes das áreas de Controladoria, Contabilidade e de TI, participantes dessa etapa de coleta, onde foram tiradas dúvidas e efetuadas anotações de detalhes para serem tratados no momento da entrevista. Posteriormente foram realizadas as entrevistas, primeiramente com o Gerente de TI, após com o Gerente de Controladoria e, por fim, com o Gerente de Contabilidade, que foram gravadas e posteriormente transcritas. Ainda como complemento às entrevistas, após a transcrição das perguntas e respostas, os gerentes

receberam por e-mail suas respostas, que foram validadas, possibilitando, assim, a correção dos erros decorrentes do processo de transcrição.

Para aumentar a confiabilidade da pesquisa, as entrevistas realizadas foram gravadas em arquivo digital e transcritas para um editor de textos, que facilitaram o manuseio e a criação de um banco de dados, para posterior consulta caso fosse necessário. Na última etapa, desenvolveu-se o terceiro instrumento de coleta de dados AHP (SAATY, 1980) ao qual é direcionado aos processos de TI, mais especificamente aos níveis de maturidade do Cobit 4.1. Esse instrumento foi enviado por e-mail aos Gerentes e Supervisor de TI participantes dessa etapa para uma prévia análise. Posteriormente foi agendada uma reunião conjunta com os dois gestores, onde foram realizadas a apresentação do instrumento, explicações sobre sua finalidade para a pesquisa e esclarecimento de dúvidas.

Esse instrumento foi desenvolvido a partir do trabalho de Vanti, Cobo e Rocha (2011) e complementarmente ao questionário de níveis de maturidade do Cobit 4.1 foi usado para tratar a importância e o processamento da análise dos dados via software Expert Choice. O sistema Expert Choice é uma ferramenta que implementa a metodologia AHP e que permite aos gestores priorizar objetivos e avaliar alternativas de uma maneira intuitiva. Esse tipo de ferramenta pode combinar a experiência e a intuição dos gestores também com informação quantitativa, pois o software permite a integração dos dados desde outras aplicações como planilhas de cálculo ou gerenciadores de bancos de dados.

Esse instrumento complementar pode ser verificado no quadro a seguir, na parte direita do instrumento clássico de avaliação dos processos do Cobit 4.1 (3a coluna) em que seu Nível de Importância é uma inovação nesse tipo de processo, contemplando assim a análise multicritério posterior.

Quadro 1 - Avaliação nível maturidade e importância Cobit 4.1 - AHP

Processos Cobit 4.1	Nível de maturidade							Nível de Importância		
	0 - Inexistente	1 - Inicial	2 - Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado		Baixa	Média	Alta

Dessa forma, para cada processo do Cobit, foi atribuído um nível de maturidade e acrescido um Nível de Importância (Baixa, Média ou Alta) que o processo representa dentro da organização na percepção dos gestores participantes do estudo.

As evidências coletadas baseiam-se nas respostas obtidas na aplicação dos instrumentos (questionários) de avaliação do grau de proteção e de maturidade na gestão de segurança da informação, bem como, das entrevistas e observações de trabalho de campo. Foram abordados os seguintes profissionais: Gerente de TI, Gerente de Contabilidade e Gerente de Controladoria. Na seção seguinte apresenta-se o caso estudado e a análise dos resultados.

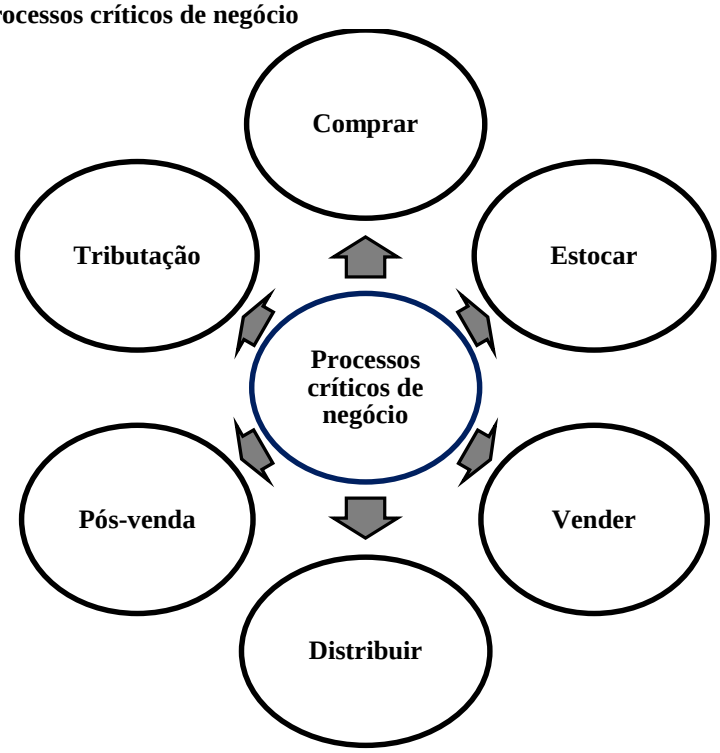
4 APRESENTAÇÃO DO CASO ESTUDADO E ANÁLISE DOS RESULTADOS

Com atividades ligadas ao ramo do varejo, as Lojas Colombo S/A foi inaugurada em 30 de novembro de 1959 na cidade de Farroupilha, onde mantém sua matriz. Atualmente possui 357 lojas distribuídas pelos estados do Rio Grande do Sul (157 lojas), Santa Catarina (44 lojas), Paraná (67 lojas), São Paulo (86 lojas), Minas Gerais (3 lojas) e centros de distribuição nas cidades de Porto Alegre (RS), Curitiba (PR) e Sumaré (SP). As Lojas Colombo S/A conta atualmente com mais de 6.000 funcionários.

Os gestores que participaram dos processos de coleta de dados foram o Gerente de Tecnologia da Informação, Gerente de Contabilidade e Gerente de Controladoria.

As organizações normalmente atuam com mais atenção sobre seus principais processos de negócio. A figura 2 apresenta os processos críticos de negócio na organização estudada de acordo com a opinião dos gestores que participaram do estudo.

Figura 2: Processos críticos de negócio

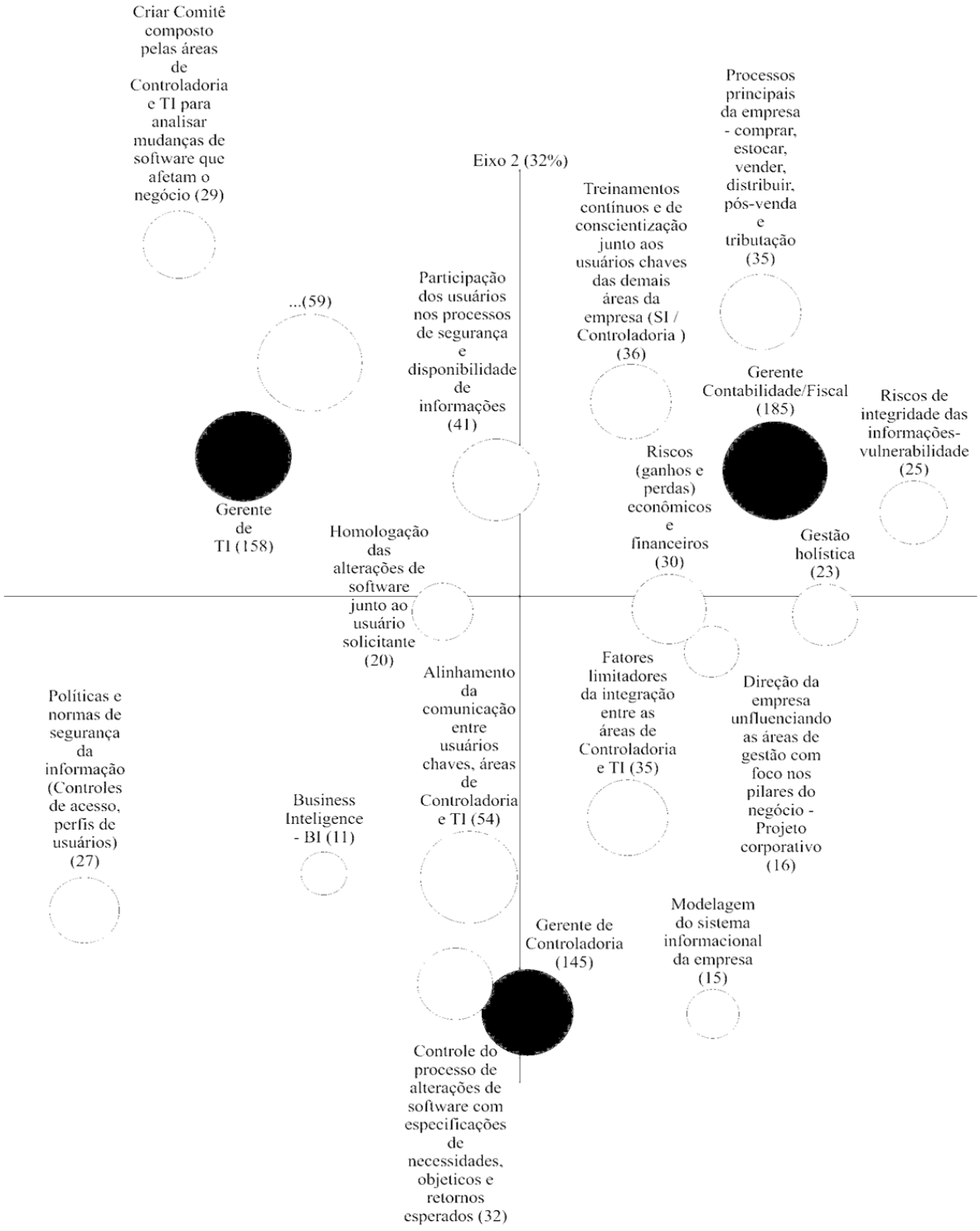


Fonte: Elaborado pelo autor com base em informações fornecidas pelos entrevistados

A avaliação de segurança da informação por parte da empresa estudada tem enfoque nos processos críticos de negócio apresentados na figura anterior, pois estes podem afetar diretamente os seus resultados.

Isto se evidencia nas entrevistas, primeiro instrumento de coleta de dados aplicado junto aos Gerentes de TI, Contabilidade e de Controladoria. Posteriormente foram realizadas as análises de Conteúdo e Léxica a partir de informações geradas com o software Sphinx, consistindo na observância de frequências de palavras e nas relações entre elementos textuais, podendo ser posteriormente visualizadas no mapa fatorial, representado na continuidade com a figura 3.

Figura 3: Visualização mapa fatorial



Fonte: Elaborado pelo autor com base nos dados fornecidos pelo *Sphinx*®

A partir da visualização do mapa fatorial anteriormente representado, evidenciam-se variáveis que permitem relacionar a percepção de cada gestor dentro da sua área de atuação relacionada à avaliação nos processos de segurança da informação integrando as áreas de Controladoria e de TI.

Na percepção do Gerente de TI, os procedimentos e ações que podem contribuir para minimizar eventos que possam afetar o sistema de informações e os principais processos de negócio na organização com a atuação conjunta das áreas de Controladoria e de TI seriam: (i) criar comitê composto pelas áreas de Controladoria e TI para analisar mudanças de software que afetam o negócio; (ii) participação usuários nos processos de segurança e disponibilidade de informações; e (iii) homologação das alterações de software junto ao usuário solicitante.

Para o Gerente de Controladoria, o alinhamento da comunicação entre usuários-chave, áreas de Controladoria e TI é um fator que pode contribuir com a integração das áreas de Controladoria. Quanto aos processos de segurança da informação relacionados aos principais processos de negócio, relacionam-se: (i) políticas e normas de segurança da informação (Controle de acesso, perfis usuários, etc.) e (ii) controle do processo de alterações de software com especificações de necessidades, objetivos e retorno esperados, com relevante significância no mapa. A modelagem do sistema informacional da empresa e *Business Intelligence* – BI foram citados com base na forma de atuação da área na modelagem do sistema informacional, sendo o BI a ferramenta de suporte. Isso se evidencia nas respostas dos entrevistados.

[...] A Controladoria atua a partir das diretrizes estabelecidas pela direção da empresa, modelando o sistema de informações... para que esteja conectado a estas diretrizes [...] (Ao responder sobre de que forma a Controladoria atua na modelagem, construção e manutenção do sistema de informações da empresa com o objetivo de possibilitar as melhores decisões).

[...] A Controladoria atua tendo como suporte a ferramenta Business Intelligence - BI, onde foi construído um modelo de negócio, que contempla orçamento e gerações de informações, ao qual permitem agilidade ao processo decisório [...] (Ao responder sobre de que forma a Controladoria atua na modelagem, construção e manutenção do sistema de informações da empresa com o objetivo de possibilitar as melhores decisões).

O Gerente de Contabilidade relaciona os processos principais da empresa - comprar, estocar, vender, distribuir, pós-venda e tributação, como sendo processos críticos e riscos de negócio, cujos processos de segurança da informação se afetados podem gerar riscos ao negócio. Isso se verifica pela proximidade no mapa fatorial das categorias; riscos de integridade das informações – vulnerabilidade e riscos econômicos e financeiros. Dessa forma, cita que a direção da empresa influenciando as áreas de gestão com foco nos pilares do negócio e treinamentos contínuos e de conscientização junto aos usuários-chave das demais áreas pode contribuir para um ambiente corporativo de atenção a segurança da informação e de integração das áreas de Controladoria e de TI nos processos de segurança da informação. Isso se evidencia nas respostas dos entrevistados.

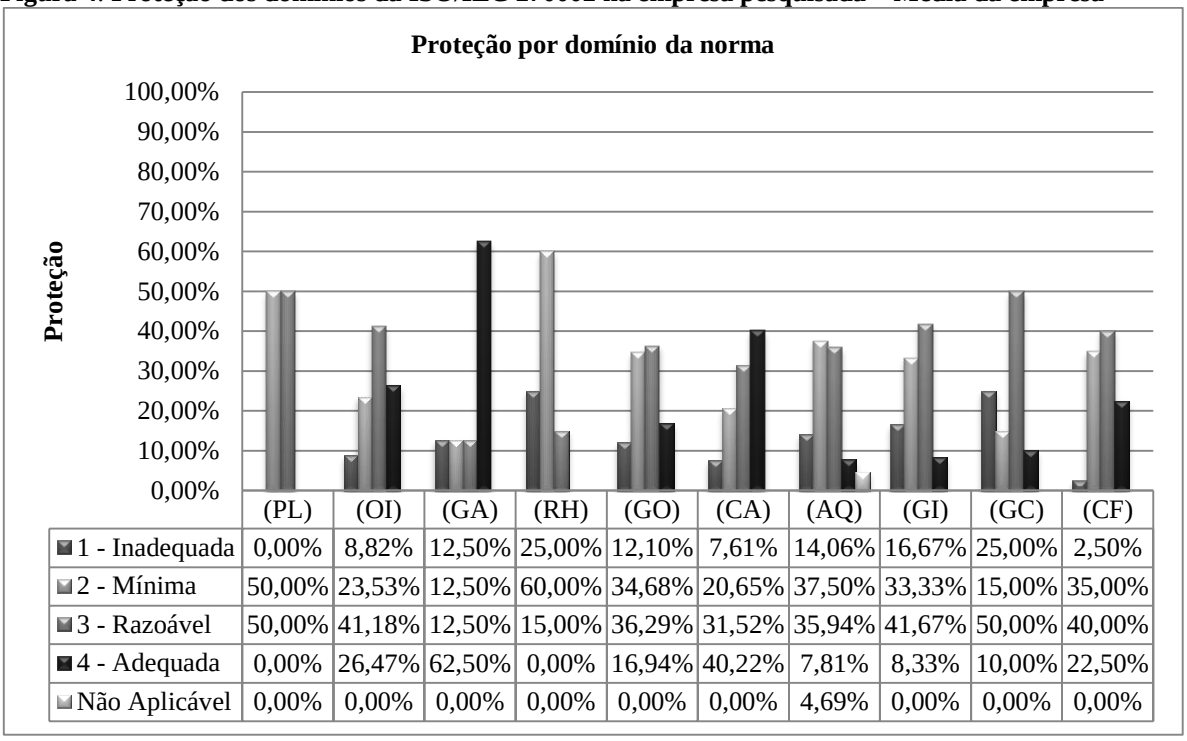
[...] Os riscos de negócio circulam nos dois principais ciclos de negócio, os ciclos de compras e de vendas. A Controladoria com estas ações e com foco nos principais pilares, quais sejam: (i) comprar; (ii) vender; (iii) estocar, (iv) entregar e (v) pós –venda, apoiando a TI, mitigaria possíveis vulnerabilidades no sistema de informações propiciando maior segurança nos processos principais da empresa, possibilitando uma melhor tomada de decisão da gestão [...] (Ao responder sobre como a Controladoria poderia atuar para evitar possíveis vulnerabilidades no sistema de informações advindos das alterações de sistemas/softwares).

[...] A implementação deveria se dar, primeiramente a partir da direção da empresa. As áreas estratégicas para o negócio da empresa como, compras, vendas e logística devem receber uma atenção especial neste processo. Entende-se que o apoio da direção da empresa, é uma credencial ao processo, gera um ambiente de atenção e de comprometimento e que é um projeto corporativo da empresa e não de determinadas áreas ou gestores. Assim, os objetivos desta implementação suportam as ações das áreas de TI e Controladoria que estão diretamente ligadas e interessadas no sucesso deste processo [...] (Ao responder sobre de que forma poderia ser implementado um processo de conscientização, educação e treinamento em segurança da informação nas áreas da empresa, e quais as áreas (ou área) deveriam liderar esse processo).

Quanto à avaliação do grau de proteção das práticas de segurança da informação na organização, foi aplicado o segundo instrumento de coleta de dados junto aos Gerentes de TI, Contábil/Fiscal e de Controladoria tendo como base um questionário elaborado a partir da norma ISO/IEC 27002.

A figura 4 apresenta a avaliação do grau de proteção da informação na média por nível dos domínios na empresa, de acordo com as práticas da norma ISO/IEC 27002, ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 4: **Proteção dos domínios da ISO/IEC 270002 na empresa pesquisada – Média da empresa**



	(PL)	(OI)	(GA)	(RH)	(GO)	(CA)	(AQ)	(GI)	(GC)	(CF)
1 - Inadequada	0,00%	8,82%	12,50%	25,00%	12,10%	7,61%	14,06%	16,67%	25,00%	2,50%
2 - Mínima	50,00%	23,53%	12,50%	60,00%	34,68%	20,65%	37,50%	33,33%	15,00%	35,00%
3 - Razoável	50,00%	41,18%	12,50%	15,00%	36,29%	31,52%	35,94%	41,67%	50,00%	40,00%
4 - Adequada	0,00%	26,47%	62,50%	0,00%	16,94%	40,22%	7,81%	8,33%	10,00%	22,50%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	4,69%	0,00%	0,00%	0,00%

Este gráfico anteriormente representado (figura 4) evidencia a avaliação do grau de proteção médio da organização referente às práticas da norma ISO/IEC 27002 na percepção integrada das áreas de Controladoria e de TI. Com ele é possível visualizar o domínio de proteção da informação mais significativo encontrado é o de GA – Gestão de Ativos que foi classificado (62,5%) como adequado na percepção dos gestores.

Os domínios de proteção da informação, OI – Organizando a Segurança da Informação e CA - Controle de acessos são classificados como razoáveis para adequados. O domínio de proteção da informação GC - Gestão da continuidade do negócio é classificado como razoável.

Os domínios de proteção da informação, PL - Política de segurança da informação, AQ - Aquisição, desenvolvimento e manutenção de sistemas de informação, GI - Gestão de incidentes de segurança da informação e CF – Conformidade, são considerados na percepção dos gestores como razoáveis quanto às práticas de segurança da informação estabelecidas pela ISO/IEC 27002. O domínio RH – Segurança em recursos humanos foi classificado (60,0%) como o mais frágil na organização.

Ao analisar as respostas no conjunto dos gestores, quanto aos processos mais frágeis nos domínios na organização, identificou-se que para o domínio PL – Política de segurança da informação a organização adota o mínimo de controles recomendados quanto a documentação da política de segurança da informação. Uma política de segurança da informação pressupõe a participação dos usuários que segundo Eloff e Eloff (2003), uma gestão em segurança da

informação deve abordar estrategicamente a perspectiva nos usuários, abordando questões como a cultura de segurança, sensibilização, formação e ética.

Para o domínio RH - Segurança em recursos humanos, os gestores citam a adoção de controles mínimos no que se refere ao estabelecimento de papeis e responsabilidades e nos processos de conscientização, educação e treinamento em segurança da informação. O domínio AQ - Aquisição, desenvolvimento e manutenção de sistemas de informação, são citados como controles inadequados ou mínimos à análise crítica técnica das aplicações após mudanças no sistema operacional, restrições sobre mudanças em pacotes de software, vazamento de informações e controle de vulnerabilidades técnicas.

O domínio GI - Gestão de incidentes de segurança da informação são citados como de controles inadequados ou mínimos, a notificação de eventos de segurança da informação e a notificando fragilidades de segurança da informação. Para o domínio CF – Conformidade são citados como de controles mínimos, a regulamentação de controles de criptografia; conformidade com as políticas e normas de segurança da informação e a proteção de ferramentas de auditoria de sistemas de informação.

Desta forma, os domínios PL, RH, AQ, GI e CF, classificados como os mais frágeis na organização, podem propiciar um ambiente em que a tempestividade, equilíbrio custo/benefício, confidencialidade, integridade, disponibilidade, relevância e confiabilidade, atributos da informação da Controladoria (CPC 00, 2008) possam ser afetados.

Conforme Schneider (2012) isto denota a percepção dos gestores ao qual consideram que a organização estabelece controles mínimos no que refere-se a: (i) documentação da política de segurança da informação (PL); (ii) papeis e responsabilidades (RH); (iii) controles inadequados ou mínimos após mudanças no sistema operacional, restrições sobre mudanças em pacotes de software, vazamento de informações e controle de vulnerabilidades técnicas (AQ); (iv) notificação de eventos ou fragilidades de segurança da informação (GI); e, (v) conformidade com as políticas e normas de segurança da informação e a proteção de ferramentas de auditoria de sistemas de informação (CF), a organização propicia um ambiente.

Assim, processos mais frágeis na adequação aos controles relacionados à segurança da informação podem gerar riscos operacionais a partir do impacto no ambiente da informação. No sentido de minimizar riscos, Borinelli (2006 p.208) cita que dentre os objetivos da Controladoria estão o de garantir informações adequadas ao processo decisório e criar condições para se exercer esse tipo de controle.

Como resultado desta integração na avaliação dos processos de segurança da informação foi possível identificar processos críticos e riscos de negócio na empresa estudada. No quadro 2 é possível verificar a avaliação quanto às práticas de segurança da informação na organização pesquisada.

A avaliação quantos as práticas de proteção da informação de acordo com a ISO 27002 a partir da visão integrada das áreas de Controladoria e de TI são as seguintes:

a) “Gestão de ativos” e “Controles de acesso”: a organização implementa todos os controles recomendados para os domínios. São os domínios com maior grau de proteção.

b) “Organizando a segurança da informação”, “Gestão de incidentes de segurança da informação”, “Gestão de continuidade do negócio” e “Conformidade”: para estes domínios a organização implementa a maioria dos controles recomendados com base em procedimentos executados em um nível razoável.

c) “Política de Segurança da Informação” e “Segurança em recursos humanos”: a organização adota o mínimo de controles recomendados. O domínio “Segurança em Recursos Humanos” tem o menor grau de proteção onde a organização adota o mínimo de controles recomendados para assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis.

Quadro 2: Processos críticos – norma ISO/IEC 27002

ISO-27002	- mínimo de controles recomendados quanto à documentação da política de segurança da informação;
	- controles mínimos no que se refere ao estabelecimento de papeis e responsabilidades e nos processos de conscientização, educação e treinamento em segurança da informação;
	- nos processos de aquisição, desenvolvimento e manutenção de sistemas de informação, são citados como controles inadequados ou mínimos à análise crítica técnica das aplicações após mudanças no sistema operacional, restrições sobre mudanças em pacotes de software, vazamento de informações e controle de vulnerabilidades técnicas;
	- no processo de gestão de incidentes de segurança da informação foram citados como inadequados ou mínimos os controles relativos à notificação de eventos de segurança da informação, e de notificando das fragilidades de segurança da informação; e
	- no que se refere à conformidade quanto à gestão da segurança da informação, são citados como de controles mínimos, a regulamentação de controles de criptografia; conformidade com as políticas e normas de segurança da informação e a proteção de ferramentas de auditoria de sistemas de informação.

Fonte: Dados da Pesquisa. Baseado em Schneider (2012)

As ações avaliadas pelas áreas de Controladoria e de TI que possibilitam aprimorar os processos e o ambiente da informação da organização estudada bem como, a integração operacional entre as áreas são apresentadas no quadro 3.

Quadro 3: Ações das áreas na avaliação dos processos de segurança da informação

Análise qualitativa das entrevistas – Integração áreas de Controladoria x Tecnologia da Informação					
Gestores Entrevistados	**Categorias Vinculadas as Respostas dos Gestores**				
Gerente de TI	Criar Comitê	Participação usuários	Homologação alterações		
Gerente de Controladoria	Alinhamento comunicação	Controles porcessos alteração software	Políticas e Normas Segurança da Informação	BI – Modelador Sisistemas Informações	
Gerente de Contabilidade	Treinamentos	Riscos econômico e financeiros	Riscos de integridade das informações	Direção Empresa influênciando Seg. Informação	Foco principais processos da empresa

Fonte: Dados da Pesquisa. Baseado em Schneider (2012)

Observa-se que na avaliação do Gerente de TI, as ações que contribuem para o processo de integração das áreas e melhoria nos processos de segurança da informação são: (i) criar comitê das áreas; (ii) participação dos usuários e; (iii) homologação integrada das solicitações de alterações. Para o Gerente de Controladoria, as ações consideradas são: (i) alinhamento da comunicação; (ii) controles sobre processos de alteração de software; (iii) políticas e normas de segurança da informação e; (iv) ferramenta BI como apoio na modelagem de sistema de informações. Para o Gerente de Contabilidade, as ações consideradas são: (i) treinamentos; (ii) riscos econômicos financeiros; (iii) riscos de integridade das informações; (iv) direção da empresa influenciando a segurança da informação e; (v) foco nos principais processos da empresa.

Foi também constatado constatou-se que estas áreas efetuam treinamentos de alinhamento técnico junto às demais áreas, contudo, os respondentes entendem que este processo pode ser aprimorado através da elaboração de um calendário formal o que

possibilitaria aprimorar os processos operacionais do trabalho conjunto das áreas. Finalmente, na seção seguinte são apresentadas as considerações finais do trabalho.

5 CONSIDERAÇÕES FINAIS

A gestão da informação no ambiente atual dos negócios é fator diferencial para as organizações manterem-se competitivas, pois tendem a propiciar uma melhor decisão. Além disso, necessita garantir transparência em suas atividades de maneira integrada entre áreas organizacionais. Desta forma, a informação é um ativo essencial para os negócios de uma organização e deve ser adequadamente protegida (ISO 27002, 2007) com a participação funcional efetiva Eloff e Eloff (2003, p. 135).

A adoção de código de práticas de segurança da informação com a identificação dos principais processos de negócio foi analisado aqui, considerando-se uma base metodológica qualitativa rigorosa com complementação quantitativa para gerar inferência de integração de áreas no tratamento do tema em questão. A participação das áreas e usuários nas políticas de segurança da informação contribui para que a informação contemple os atributos de tempestividade, equilíbrio entre custo/benefício, confiabilidade, relevância (CPC 00, 2008, p.15) que sustentam a qualidade da informação.

No que se referem à atuação das áreas responsáveis pelos sistemas de informações nas organizações de acordo com Mithas, Ramasubbu e Sambamurthy (2011), estas devem criar as condições necessárias para o desenvolvimento de infraestrutura e capacitação na gestão de informações. Borinelli (2006) direcionou a função da Controladoria com os sistemas de informações, enfatizando o enfoque de gestão dos mesmos. Wilkin e Chenhall (2010) complementaram com o ambiente crescente de conscientização sobre o papel da TI. Estes estudos proporcionaram adequado diálogo com os achados do presente estudo, tendo sido possível inferir requisitos de integração entre diferentes áreas que auxiliam no processo decisório organizacional.

A avaliação integrada das áreas de Controladoria e de TI nos processos de segurança da informação possibilitou visualizar as percepções das áreas gerando assim ações que visem aprimorar a segurança de informações da organização. Evidenciou-se ainda mais a importância da informação e da segurança da informação no ambiente atual dos negócios, bem como as responsabilidades especifica e complementares das áreas de Controladoria e de TI sobre os sistemas de informações nas organizações. Assim, instrumentos de coleta e análise de dados foram aplicados e dessa forma possibilitou avaliar os processos de segurança da informação a partir de uma visão integrada das áreas.

A que se considerar que num ambiente afetado por constantes alterações torna-se complexo para qualquer organização se cercar de conceitos, instrumentos e ferramentas que garantam um ambiente sustentável de segurança da informação. Nesse sentido, esse trabalho resultou em uma avaliação dos processos de segurança da informação como totalmente adequada e que possibilita novos trabalhos a serem desenvolvidos com visões integradas entre diferentes áreas.

Assim sendo, os resultados apresentados no estudo tanto relacionados aos níveis de proteção de segurança da informação e no alinhamento da percepção das áreas quanto aos processos de segurança da informação, possibilitou a análise de eventuais riscos associados ao ambiente da informação. Mais além, também aprimorou processos operacionais do trabalho conjunto dessas duas áreas, diminuindo assim os riscos relacionados à informação organizacional já existente no dia a dia das atividades empresariais.

Como continuidade do estudo direciona-se esforços para que a integração das áreas possa então priorizar o processo decisório. Para isso, esse tipo de pesquisa pode ser tratado através de instrumentos de decisão multicritério que estruturem o gerenciamento da informação. Assim sendo, diferentes profissionais podem avaliar prioridades como as relacionadas aos

requisitos de governança corporativa de forma que venham mitigar riscos de corporativos e tecnológicos.

REFERÊNCIAS

ARAÚJO, W.J. **A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento**. Tese (Doutorado em Ciência da Informação). UNB, Brasília, DF, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Norma brasileira ISO/IEC 27002, 2007.** Rio de Janeiro: ABNT, 2007.

ATKINSON, A. A., BANKER, R. D., KAPLAN, R. S., YOUNG, S. M. **Contabilidade gerencial**. 3. ed., São Paulo: Atlas, 2008.

BORINELLI, M.L. **Estrutura Conceitual básica de controladoria**: sistematização à luz da teoria e da práxis. Tese (Doutorado em Controladoria e Contabilidade). USP, São Paulo, SP, 2006.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly Executive**, v. 34, n. 3 Set. 2010. ISSN 1540-1960.

CARMEN, A.A.; CORINA, G. A strategic approach of management accounting. **Annals of the University of Oradea, Economic Science Series**, v. 18 n. 3, p. 736-741, 2009. ISSN: 1582-5440.

COLLINS, J.; HUSSEY, R. **Pesquisa em administração**. 2° ed. Porto Alegre: Bookman, 2005.

COMITE DE PRONUNCIAMENTOS CONTÁBEIS (CPC). **Pronunciamento conceitual básico** – Estrutura conceitual para a elaboração e apresentação das demonstrações contábeis, 2008. Disponível em: <http://www.cpc.org.br>. Acesso em: 26 nov. 2010.

ELOFF, J.; ELOFF, M. Information security management – A new paradigm. In: 2003 annual research conference of the South African. Institute of computer scientists and information technologists on enablement through technology, 2003, p.130-136. **Proceedings…**, 2003. DOI: 10.1145/180921.2180933. ISBN:1-58113-774-5.

ITGI: Information Technology Governance Institute. **CobiT 4.1 modelo, objetivos de controle, diretrizes de gerenciamento e modelos de maturidade, 2007**. Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf>. Acesso em: 28 fev. 2011.

ISO/IEC27002. Tecnologia da Informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2007.

KAYWORTH, T.; WHITTEN, D. Effective information security requires a balance of social and technology factors. **MIS Quarterly Executive,** v. 9, Set.2010. ISSN 1540-1960.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informação Gerenciais**. 7. ed. São Paulo: Pearson, 2007.

MARTIN, N.C.; SANTOS, L.R.; DIAS, J.M. Governança empresarial, riscos e controles internos: A emergência de um novo modelo de controladoria. **Revista Contabilidade e Finanças,** n. 34, p. 7, jan./abr. 2004. ISSN: 1808-057X. http://dx.doi.org/10.1590/S1519-70772004000100001

MITHAS, S.; RAMASUBBU, N.; SAMBAMURTHY, V. How information management capability influences firm performance. **MIS Quarterly Executive**, v. 35, n. 1, Mar. 2011. ISSN 1540-1960.

O'BRIEN, J. A.; MARAKAS, G. M. **Administração de Sistemas de Informação:** uma introdução. São Paulo, SP: McGraw-Hill, 2007.

SAATY, **The Analytical Hierarchy Process: Planning, Priority Setting, Resource Allocation.** Mc Graw-Hill, New York, 1980.

SCHNEIDER, L.C. **Avaliação de processos de segurança da informação na integração das áreas de controladoria e de tecnologia da informação,** 2012. Disponível em: <http://biblioteca.asav.org.br/vinculos/000000/0000006F.pdf>. CDU 005.922.1.

SPEARS, J.L.; BARKI, H. User participation information systems security risk management. **MIS Quarterly Executive**, v. 34, n. 3 Set. 2010. ISSN 1540-1960.

YIN, R. K. **Estudo de caso – Planejamento e métodos. 4ª ed.** Porto Alegre: Bookman, 2010.

YOUNG, R. F.; WINDSOR J. Empirical evaluation of information security planning and integration. **Communications of the Association for Information Systems,** v. 26, Mar. 2010. ISSN: 1529-3181.

VANTI, A. A.; COBO, A.; ROCHA, R. Avaliação de modelo de governança de TI com o uso de FAHP. In: CONTECSI, São Paulo, 2011. **Anais**…, USP, 2011.

WILKIN, C.; CHENHALL, T.; A review of IT Governance: A Taxonomy to inform Accounting Information Systems. **Journal of Information Systems**. v. 24, n. 2, p.107-146, 2010. DOI: 10.2308/isys-50922.