UNIVERSIDADE DO VALE DO RIO DOS SINOS – UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS
NÍVEL MESTRADO

LUIZ CARLOS SCHNEIDER

AVALIAÇÃO DE PROCESSOS DE SEGURANÇA DA INFORMAÇÃO NA INTEGRAÇÃO DAS ÁREAS DE CONTROLADORIA E DE TECNOLOGIA DA INFORMAÇÃO

São Leopoldo
2012

LUIZ CARLOS SCHNEIDER

AVALIAÇÃO DE PROCESSOS DE SEGURANÇA DA INFORMAÇÃO NA INTEGRAÇÃO DAS ÁREAS DE CONTROLADORIA E DE TECNOLOGIA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Contábeis da Universidade do Vale do Rio dos Sinos – Unisinos, como requisito parcial para a obtenção do título de Mestre em Ciências Contábeis.

Professor orientador: Dr. Adolfo Alberto Vanti

São Leopoldo

2012

S359a Schneider, Luiz Carlos.
Avaliação de processos de segurança da informação na integração das áreas de controladoria e de tecnologia da informação / Luiz Carlos Schneider. – 2012.
199 f. : il. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Ciências Contábeis, 2012.
"Professor orientador: Dr. Adolfo Alberto Vanti."

1. Controladoria. 2. Proteção de dados. 3. Tecnologia da informação. 4. Sistemas de informação gerencial – Medidas de segurança. I. Título.

CDU 005.922.1

Dados Internacionais de Catalogação na Publicação (CIP)
(Bibliotecário: Flávio Nunes – CRB 10/1298)

ATA MCC-D Nº. 11/2012

Aos vinte e quatro dias do mês de abril do ano de 2012, às 14h, reuniu-se na sala Conecta, a Comissão Examinadora de Defesa de Dissertação composta pelos(a) professores(a): Adolfo Alberto Vanti (Orientador e Presidente) da UNISINOS, Angel Cobo, da Universidade de Cantabria, através de vídeo conferência; Carlos Alberto Diehl, da UNISINOS e Clóvis Antônio Kronbauer, da UNISINOS, para analisar e avaliar a Dissertação intitulada **"AVALIAÇÃO DE PROCESSOS DE SEGURANÇA DA INFORMAÇÃO NA INTEGRAÇÃO DAS ÁREASDE CONTROLADORIA E DE TECNOLOGIA DA INFORMAÇÃO"**, apresentada pelo aluno Luiz Carlos Schneider, candidato ao título de Mestre em Ciências Contábeis. Após a apresentação, argüição e defesa, a Banca atribuiu os seguintes **conceitos**:

Prof. Dr. Angel Cobo – Univ. Cantabria — Conceito: APROV. PLEN.

Prof. Dr. Carlos Alberto Diehl - UNISINOS — Conceito: aprovado plenamente

Prof. Dr. Clóvis Antônio Kronbauer – UNISINOS — Conceito: APROVADO PLENAMENTE

A Dissertação obteve o **Conceito Final**: APP (Aprovado plenamente)

As alterações sugeridas pela Banca Examinadora são as seguintes:

_____

_____

_____

O aluno deverá apresentar a versão final do trabalho com as modificações propostas pela Banca Examinadora da Dissertação, no prazo máximo de 60 dias, mediante supervisão do Orientador.

São Leopoldo, 24 de abril de 2012.

Mestrando: Luiz Carlos Schneider — Assinatura: _____

Professor Orientador: Prof. Dr. Adolfo Alberto Vanti — Assinatura: _____

Membro: Prof. Dr. Angel Cobo — Assinatura: _____

Membro: Prof. Dr. Carlos Alberto Diehl — Assinatura: _____

Membro: Prof. Dr. Clóvis Antônio Kronbauer — Assinatura: _____

Secretária: Luciana Grimaldi Aquino — Assinatura: _____

AGRADECIMENTOS

Existem momentos em que os amigos contribuem decisivamente com as nossas escolhas, e nesta, quero agradecer aos amigos Scheila e Leandro pelo incentivo, vocês foram decisivos por eu ter chegado até aqui.

Ao meu orientador Professor Dr. Adolfo Alberto Vanti, pelos desafios propiciados e por suas valiosas contribuições para esta dissertação.

Aos colegas Gustavo e Rafael da Unisinos, pelas aulas e apoio na utilização do software Sphinx.

Ao meu colega de trabalho Fernando, por suas contribuições na elaboração dos gráficos.

Aos professores, colegas e colaboradores da equipe do PPGA/UNISINOS, pelo aprendizado e excelente ambiente acadêmico.

A Lojas Colombo S/A, por oportunizar o acesso as informações para que esta pesquisa fosse realizada.

Aos gestores entrevistados, Flori César Peccin e Agostinho Luiz Peroni pela atenção, compreensão e contribuições com esta pesquisa.

Ao meu amigo Luis Carlos Alberti, por ter me aberto as portas, sua contribuição foi muito importante para a realização desta pesquisa, mais uma vez obrigado.

Aos meus filhos Rafael e Guilherme, pelo carinho, amizade e respeito. Obrigado também pelo auxilio em algumas etapas desta pesquisa ao qual tive que recorrer a vocês.

Com especial carinho a minha esposa Simone, pelo amor, compreensão e por proporcionar um ambiente para que eu me dedicasse a este trabalho.

Por fim, agradeço a DEUS por me iluminar e propiciar mais este momento importante em minha vida.

“O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis.”

(José de Alencar)

RESUMO

O ambiente da informação nas organizações vem sendo afetado pela evolução continua das tecnologias e do ambiente dos negócios. A Controladoria como responsável pelos sistemas de informações que suportam a tomada de decisão nas organizações deve participar dos processos de segurança da informação. Por isto, a presente pesquisa avaliou os processos de segurança da informação integrando as áreas de Controladoria e de TI. Evidenciou-se o tipo de pesquisa metodológica como um estudo de caso exploratório de natureza aplicada. Mesmo que as análises estejam baseadas em gráficos e tabelas, o que enseja dados de natureza quantitativa, as técnicas de análise possuem predominância qualitativa realizada a partir de múltiplas fontes de coleta de dados, tais como, questionários e entrevistas, essas tratadas com o auxílio de *software* específico que contemplou as análises léxicas. Como resultado do estudo, foi elaborado um *framework* que promove a integração das áreas de Controladoria e de TI na avaliação dos processos de implementação de softwares tendo como foco os principais processos de negócio. O *framework* também contempla os achados da pesquisa quantos aos níveis de proteção de segurança da informação e de maturidade dos processos de TI o que possibilita a análise de eventuais riscos associados às práticas de proteção de segurança da informação e do modelo de governança de TI adotados na organização. Consequentemente, foram aprimorados os processos operacionais do trabalho conjunto dessas duas áreas e de controles do ambiente da informação.

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

ABSTRACT

The information environment in organizations has been affected by the continuing evolution of technology and business environment. The Controllership, as responsible for the information systems that support decision making in organizations, should participate in the information security process. Therefore, this study investigated the processes of information security through the integration the areas of Controllership and Information Technology (IT). The research methodology is demonstrated as an exploratory case study of an applied nature. Even though the analyzes were based on graphs and tables, which (may) entails quantitative data, analysis techniques have predominantly been of qualitative nature from multiple sources of data collection such as questionnaires and interviews. Such interviews were treated with the aid of specific software that included the lexical analyzer. As a result of the study, we designed a framework that promotes the integration of the Controllership and IT areas in the evaluation of software implementation processes focused on the core business processes of the Company. The framework also includes the findings from a survey on the levels of protection and the maturity of the information security of IT processes which enables the analysis of possible risks associated with the protection practices of information security and IT Governance model adopted in organization. As a consequence of this paper, the working operational processes of these two areas and the controls of the information environment of the Company were improved.

Keywords: Controllership. Information Technology. Information Security. Information Management. AHP.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

AC	Análise de Conteúdo
AHP	*Analytical Hierarchy Process*
AI	Aquisição e Implementação
AL	Análise Léxica
AQ	Aquisição, desenvolvimento e manutenção de sistemas de informação
BI	*Business Intelligence*
CA	Controle de acessos
CF	Conformidade
COBIT	*Control Objectives for Information and related Technology*
CPC	Comitê de Pronunciamentos Contábeis
DS	Entrega e Suporte
GA	Gestão de ativos
GC	Gestão da continuidade do negócio
GI	Gestão de incidentes de segurança da informação
GO	Gerenciamento das operações e comunicações
ISACA	*Information Systems Audit and Control Association*
ISO	*International Standardization Organization*
ITGI	*Information Technology Governance Institute*
ME	Monitoramento
OI	Organizando a segurança da informação
PL	Política de segurança da informação
PO	Planejamento e Organização
RH	Segurança em recursos humanos
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

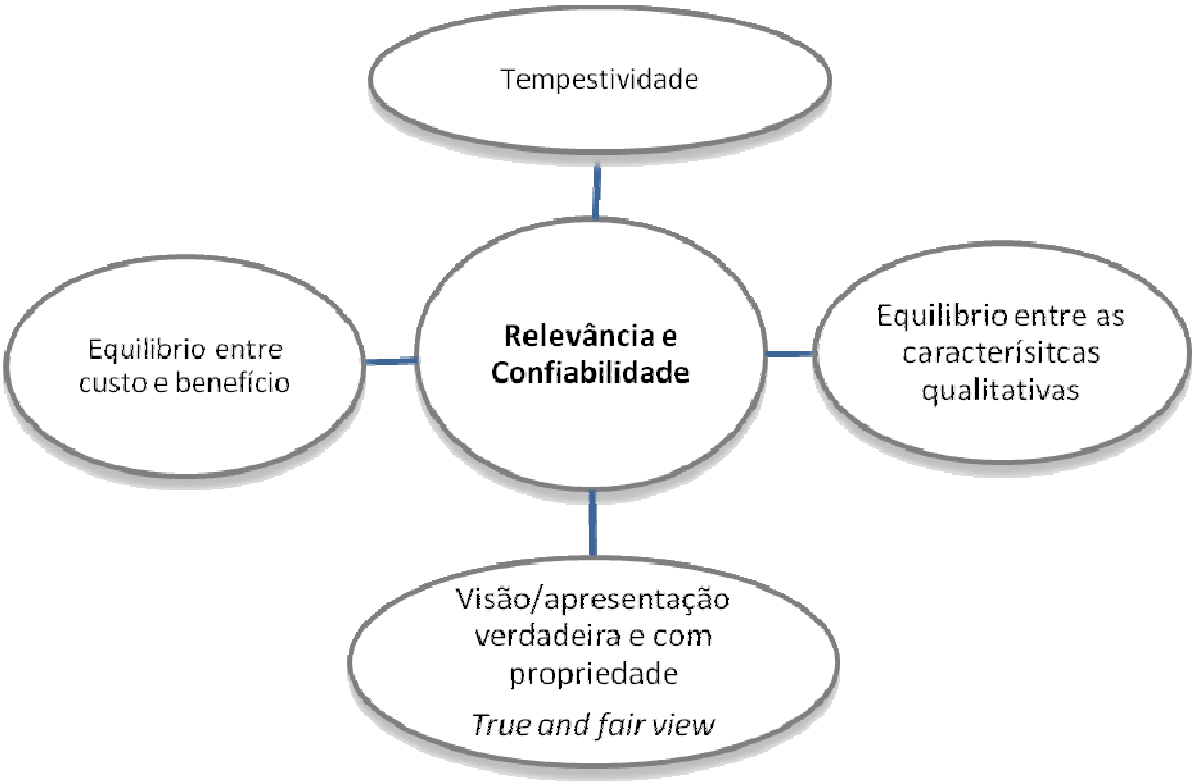
A evolução das tecnologias, as constantes transformações no ambiente dos negócios, as alterações de normatizações contábeis e das legislações fiscais e tributárias demandam implementações nos *softwares* utilizados na gestão das empresas, as quais refletem nos processos de segurança da informação. Têm-se, dessa forma, um ambiente de informações sensibilizado por esse cenário e, por outro lado, a necessidade dos gestores de tomar decisões mais ágeis e precisas visando à perpetuidade das organizações. Segundo o ITGI (2007), a complexidade do ambiente atual dos negócios gera nos executivos uma necessidade de informações condensadas e que estejam disponíveis no momento oportuno para a tomada de decisões ágeis e precisas relacionadas a valor, riscos e controles.

Nesse sentido, faz-se necessário que as áreas que respondem pelos sistemas de informações nas organizações adotem procedimentos sistemáticos de avaliação dos processos relacionados aos seus sistemas de informações, a fim 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 (CPC, 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 na época oportuna, pode ser necessário divulgá-la antes que todos os aspectos de uma transação ou evento sejam conhecidos, prejudicando assim a sua confiabilidade. No entanto, se para divulgar a informação a entidade aguardar até que todos os aspectos se tornem conhecidos, a informação pode ser altamente confiável, porém de pouca relevância para os usuários que tenham necessidade de tomar decisões nesse ínterim. Para atingir o adequado equilíbrio entre a relevância e a confiabilidade, o princípio básico consiste em identificar qual a melhor forma para satisfazer as necessidades do processo de decisão econômica dos usuários.

Na figura 1 apresenta-se os atributos envolvidos quanto ao tratamento das informações, segundo CPC 00 (2008, p. 15).

Figura 1 - Atributos da informação de acordo com o Comitê de Pronunciamentos Contábeis (CPC)



Fonte: Elaborado pelo autor com base no Pronunciamento Conceitual Básico (CPC, 2008)

Para a geração de informações relevantes, tempestivas e confiáveis, as organizações necessitam de um sistema de informações estruturado, o qual Laudon e Laudon (2007, p. 9) definem tecnicamente como sendo 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. Para O'Brien e Marakas (2007, p. 4), 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.

No que se refere ao processo de administração de dados e informações extraídos dos *softwares* nas empresas, este é de responsabilidade de uma área específica normalmente denominada TI – Tecnologia da Informação. Uma das atribuições da TI é de adotar as políticas de segurança de informações com base em instrumentos, por exemplo, a ISO 27002, que trata das recomendações de controles para a segurança da informação. No que tange à gestão dos processos

de TI, o modelo Cobit 4.1 conforme ITGI (2007) se relaciona através de um conjunto de documentos que caracterizam as melhores práticas e processos de negócios relativos à Tecnologia da Informação. A informação é um ativo essencial para os negócios de uma organização. Consequentemente, necessita ser adequadamente protegido (ISO 27002, 2007).

Para Kayworth e Whitten (2010), os processos de segurança da informação tornaram-se uma questão estratégica e de grande preocupação entre os executivos das empresas. A crescente dependência da internet, a globalização e novas regulamentações do governo obrigam as empresas a proteger os dados aumentando a consciência da necessidade de uma efetiva governança corporativa da segurança da informação. Para contribuir com esse processo de governança, o Cobit 4.1 estabelece cinco critérios para uma informação segura, conforme mostra a figura 2.

Figura 2 - Princípios básicos para uma informação segura

Fonte: Elaborado pelo autor com base (ITGI, 2007)

Ao considerar os atributos envolvidos no tratamento das informações constantes na figura 1 e os princípios básicos para uma informação segura apresentada na figura 2, bem como os processos de administração de dados e informações pela área de TI extraídos dos *softwares*, cabe discorrer sobre as responsabilidades da área de Controladoria na geração de informações para a tomada de decisão. Conforme Bazerman (2004), a tomada de decisão nas organizações está sujeita a fatores como a incerteza e o risco. Para reduzir o

índice de erros dos gestores em meio às situações adversas, o gerenciamento da informação se faz necessário na construção de cenários elaborados a partir de informações de qualidade.

Borinelli (2006 p. 136) aborda a função gerencial-estratégica da Controladoria que compreende as 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 principais funções as atividades de identificar, mensurar, analisar, avaliar, divulgar e controlar os diversos riscos envolvidos no negócio, bem como seus possíveis efeitos.

Segundo Carmen e Corina (2009), a Controladoria deve projetar e desenvolver um sistema de gestão orientado para a execução dos objetivos estratégicos da organização. Esse sistema deve contemplar um conjunto de informações relevantes para a organização, conectado com seus esforços de criação de valor e visando à sustentabilidade do negócio a longo prazo. Para tal, 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, o que permite a previsão de investimentos em estruturas, pessoas e mecanismos relacionados.

Dessa forma, os processos de geração de informações nas empresas, quando não administrados de forma integrada entre as áreas de Controladoria e de TI, podem propiciar um ambiente de retrabalhos, decisões equivocadas e intempestivas que conduzem a riscos financeiros, operacionais, tecnológicos e outros, os quais afetam seus ativos. Assim, torna-se necessário estabelecer um processo integrado dessas áreas (Controladoria x TI) na avaliação de processos de segurança de informações a fim de minimizar tais riscos à operação.

A Controladoria é a área responsável pelo sistema de informações da empresa, cabendo a ela adotar procedimentos que propiciem segurança ao ambiente informacional a fim de evitar que os diversos usuários da informação possam recebê-la com erro ou de forma intempestiva, influenciando o comportamento, a atitude e a decisão dos gestores. O posicionamento deste trabalho contempla a gestão holística, cujas áreas de Controladoria e TI atuam

nos processos de segurança da informação com a participação dos usuários, a fim de contribuir para a qualificação do sistema informacional da empresa.

A partir dessa contextualização, é possível então apresentar a questão problema do presente estudo: **Como avaliar os processos de segurança da informação integrando as áreas de Controladoria e de TI?**

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O objetivo deste trabalho é avaliar metodologicamente e de maneira aplicada os processos de segurança da informação integrando as áreas de Controladoria e de TI.

1.1.2 Objetivos Específicos

- identificar processos críticos e riscos de negócio;
- identificar a participação das áreas de Controladoria e Tecnologia da Informação nos processos críticos de negócio;
- avaliar as práticas de proteção de segurança de informações e níveis de maturidade nos processos de negócios;
- propor a criação de procedimentos integrados entre Controladoria e Tecnologia da Informação para tratamento dos processos de segurança das informações.

1.2 DELIMITAÇÃO DO TEMA

Faz parte do escopo central desta pesquisa que as áreas de Controladoria não necessariamente possuem essa denominação no organograma das empresas, mas exercem atividades atribuídas a Controladoria conforme estabelece o referencial teórico do presente estudo. Também considera-se que a área de Tecnologia da Informação não está subordinada à área de Controladoria e tem autonomia em suas ações.

No que se refere à linha de pesquisa, este estudo se delimita a área de Controle de Gestão e segurança e sistemas de informações vinculadas ao grupo de Administração de Tecnologia da Informação do Conselho Nacional de Desenvolvimento Científico e Tecnológico e a Universidad de Cantabria.

O tema Controladoria versa sobre os mais variados assuntos pertinentes à gestão nas organizações, da mesma forma, o tema Segurança de Informações, o qual abrange questões relacionadas a *hardware*, *software*, processos de gestão e de práticas de governança corporativa. Este estudo se delimita a analisar de forma específica as responsabilidades da Controladoria alinhadas aos seus objetivos e missão nas organizações quanto ao ambiente informacional, riscos eventuais a esse ambiente, advindos por processos que se relacionam com a segurança da informação.

Em relação ao tema Segurança de Informações, este estudo se delimita a analisar o grau de proteção, de acordo com critérios estabelecidos pela norma ISO/IEC 27002; e o nível de maturidade dos processos de TI, com base no Cobit 4.1 utilizando o modelo multicritério AHP. Ambos os temas são aplicados em um estudo de caso único.

Não foi objeto deste estudo analisar as relações políticas, pessoais ou de poder que fazem parte de qualquer contexto organizacional, e neste estudo em específico, para as áreas de Controladoria e de TI.

1.3 JUSTIFICATIVA

A informação é fator-chave para a tomada de decisão nas empresas. A Controladoria como área responsável por fornecer informações contábeis, financeiras e não financeiras ao processo de gestão deve atuar de forma participativa nas organizações, interligando os processos de geração de informações existentes entre as diversas áreas da empresa. Assim, o produto resultante, ou seja, a informação obtém os atributos necessários para atender a gestão da empresa, evitando que esta incorra em riscos operacionais.

A área de TI contribui com a utilização de seus instrumentos de segurança da informação para que sejam implementados requisitos que permitam normatizar a guarda e a disponibilidade da informação. A ISO 27002 (2007 p.x) relaciona o tema segurança da informação com a proteção da

informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Conforme o ITGI (2007), a alta direção das empresas tem percebido o significativo impacto que a informação tem no sucesso da organização e esperam um alto entendimento sobre a forma como a TI funciona e quanto ela está sendo bem administrada e, em particular, no quesito informações, se estas são gerenciadas a fim de atender às necessidades da gestão da empresa.

Dessa forma, uma atuação não integrada das áreas de Controladoria e TI nos processos que envolvem a geração, segurança e disponibilidade de informações, desde a etapa inicial de *inputs* de dados aos *softwares* utilizados pela empresa, onde o treinamento dos usuários para capacitá-los é fundamental para qualificar os sistemas de informações, podem gerar retrabalhos e incorrer em eventuais riscos operacionais. Assim, a integração das áreas de Controladoria e TI nos processos que envolvem a segurança da informação tende a ser benéfica para as empresas no que se refere à proteção e qualificação de um seus principais ativos: a informação.

Este estudo é relevante para o meio acadêmico e profissional em razão de evidenciar a necessidade de uma atuação integrada entre as áreas de Controladoria e TI nos processos de segurança da informação. As duas áreas possuem atuações e conhecimentos específicos que devem se complementar, visando à garantia dos atributos da informação para a tomada de decisão evitando riscos operacionais. Dessa forma, procura-se instigar a reflexão sobre a atuação conjunta e o compartilhamento do conhecimento entre as áreas e suas responsabilidades perante o sistema informacional nas organizações.

Como contribuição teórica, este estudo aborda temas relacionadas a área de Controle de Gestão e segurança e sistemas de informações vinculadas ao grupo de Administração de Tecnologia da Informação do Conselho Nacional de Desenvolvimento Científico e Tecnológico e a Universidad de Cantabria.

Ademais, os temas “Controladoria” e “Segurança de Informações” são amplamente estudados de forma separada, mas que ainda se identifica uma lacuna teórica na relação entre ambos.

1.4 ESTRUTURA DA DISSERTAÇÃO

Este estudo divide-se em cinco capítulos. No primeiro capítulo apresenta-se a introdução do estudo. Inicialmente faz-se a contextualização do tema, evidencia-se o objetivo geral e os específicos, a delimitação da pesquisa e relevância do estudo e, por último, a estrutura da dissertação.

No segundo capítulo apresentam-se os fundamentos teóricos do estudo. O referencial teórico foi desenvolvido de acordo com uma linha de raciocínio que pretende estabelecer a relação existente entre o papel estratégico da área de Controladoria e sua responsabilidade sobre o sistema de informações nas organizações, os processos de Segurança de Informações e o grau de proteção de acordo com as práticas da norma ISO/IEC 27002. Por fim, aborda-se o Cobit 4.1, seus requisitos de negócio, níveis de maturidade do Cobit 4.1 complementado pelo modelo multicritério AHP.

No terceiro capítulo, apresentam-se os aspectos metodológicos, como o critério para escolha do caso estudado, plano de coleta e tratamento dos dados, plano de análise dos dados, onde serão explicitados os procedimentos adotados nas etapas de coleta de dados (questionários e entrevistas), e, por último, as limitações da pesquisa.

No quarto capítulo, apresentam-se o caso estudado e a análise dos resultados com vistas a cumprir os objetivos de pesquisa, traçados no sentido de responder à questão problema.

Por fim, o quinto capitulo apresenta a conclusão sobre o estudo e recomendações para estudos futuros e a contribuição que o estudo pode trazer à academia, bem como, às organizações.

2 REFERENCIAL TEÓRICO

Neste capítulo apresenta-se o referencial teórico desenvolvido neste estudo, o qual aborda os temas Controladoria e Segurança de Informações.

Na seção que trata do tema Controladoria, aborda-se o ambiente contemporâneo dos negócios, os desafios para as áreas de Controladoria nas organizações, sua missão, seus objetivos e o seu objeto de estudo.

Na seção que trata do tema Segurança de Informações, aborda-se a importância do “ativo” informação, temas pertinentes a segurança da informação, a norma ISO/IEC 27002 e os critérios para analisar o nível de proteção das práticas de segurança de informação. Por fim, abordam-se o Cobit 4.1, os requisitos de negócio e o modelo multicritério AHP aplicado nos níveis de maturidade do Cobit. 4.1.

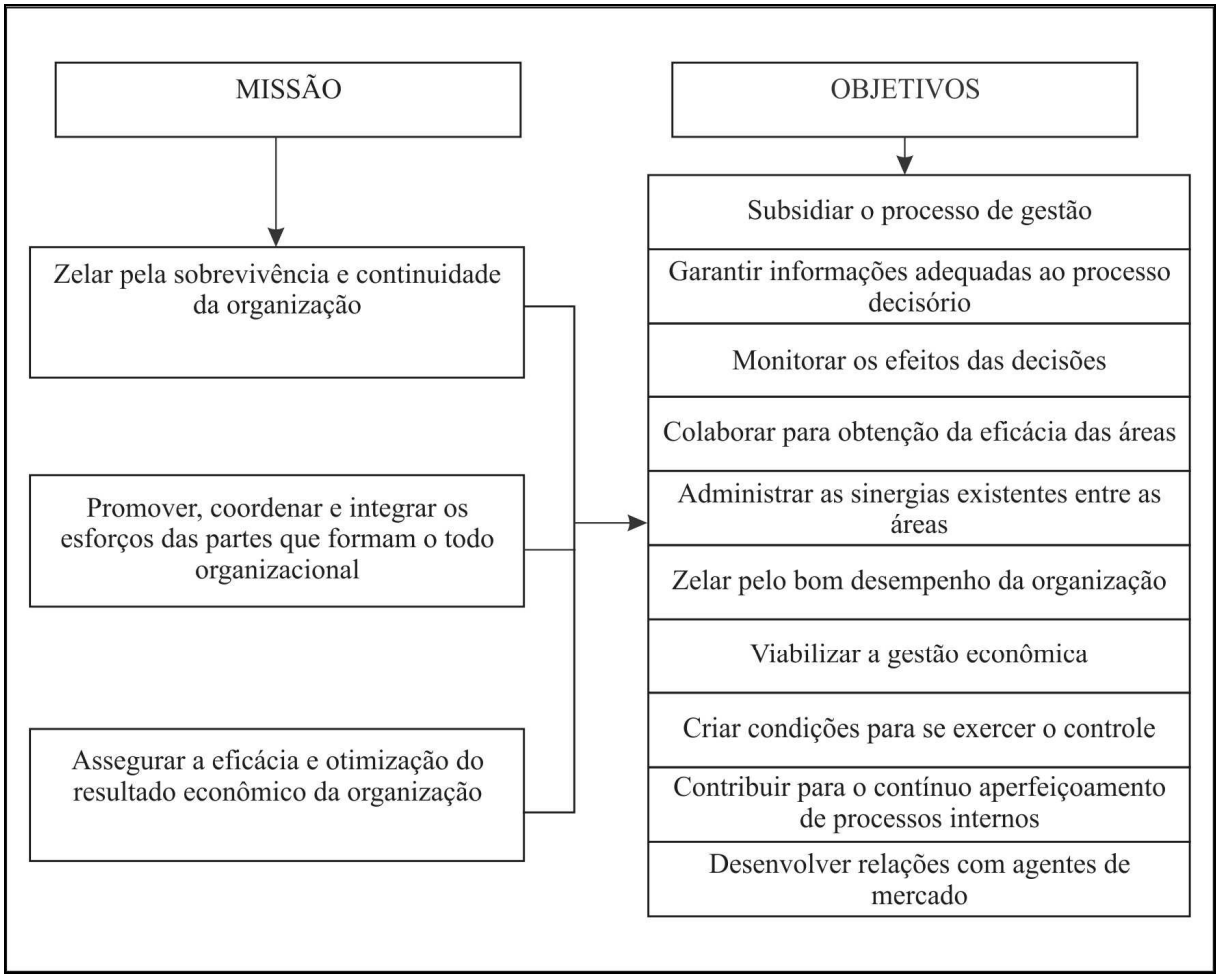
2.1 CONTROLADORIA

O ambiente contemporâneo dos negócios, onde a globalização e a concorrência estimulam a busca constante pela eficiência da gestão nas empresas, órgãos reguladores atuantes e o aquecimento do mercado de capitais no Brasil, desafiam a área de Controladoria a adotar uma postura mais participativa e integrada para 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 e Corina (2009) consideram que esta deve estar envolvida nos processos de decisões estratégicas da organização, fazendo o elo de ligação entre 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 disso, devem incentivar ações consistentes, apoiar e criar um conjunto de valores culturais integrados que produzam efeitos na mentalidade das pessoas direcionados aos objetivos da organização. Essa característica da informação é a que cria valor para a organização.

Em relação à missão e objetivos da Controladoria, Borinelli (2006) faz uma associação entre eles conforme apresenta-se na figura 3.

Figura 3 - Associação dos objetivos da Controladoria com sua missão



Fonte: Borinelli (2006, p. 208)

Percebe-se que a Controladoria diante dessa associação proposta por Borinelli quanto a objetivos e missão 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 oportunidades na continuidade da organização, na otimização do resultado econômico e financeiro.

Segundo Oliveira (2009), o papel da Controladoria é assessorar os diversos gestores da empresa, fornecendo informações relevantes e tempestivas para apoiar o processo decisório. A Controladoria tem a responsabilidade na modelagem, construção e manutenção do sistema de informações da

organização com o objetivo de possibilitar sempre as melhores decisões para a gestão econômica e financeira do negócio.

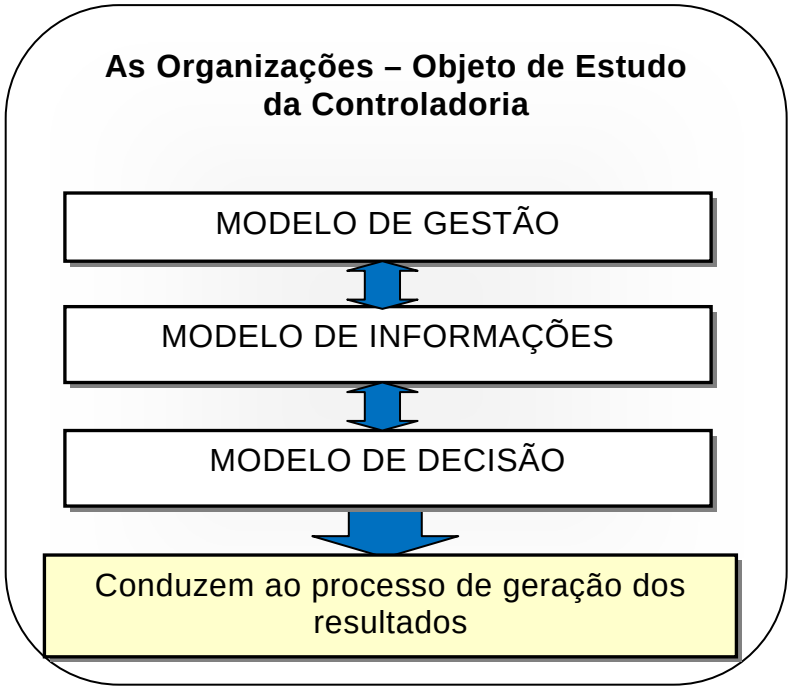
Padoveze e Bertolucci (2009) trazem a visão de Heckter e Willson sobre Controladoria,

> ao qual não cabe a ela o comando do navio, tarefa de responsabilidade do primeiro executivo; representa, entretanto, o navegador que cuida dos mapas de navegação. É sua finalidade manter informado o comandante quanto à distância percorrida, ao local em que se encontra e a velocidade da embarcação, à resistência encontrada, aos desvios de rota, aos recifes perigosos e aos caminhos traçados nos mapas, para que o navio chegue ao destino, ou seja, gerar resultados (PADOVEZE; BERTOLUCCI, 2009, p. 44).

Já Borinelli (2006, p. 109) cita que dentre os focos de atuação da controladoria existem as necessidades informacionais, consubstanciadas nos modelos de informação e de decisão.

Na figura 4, apresenta-se o objeto de estudo da controladoria e as relações entre si dos modelos de gestão, informação e decisão, que conduzem à geração de resultados.

Figura 4 - Objeto de estudo da Controladoria



Fonte: Adaptado de Borinelli (2006, p. 109)

Dessa forma, a interligação efetuada pelo modelo de informações entre os modelos de gestão e de decisão conduz ao processo de geração de

resultados, refletindo a responsabilidade da Controladoria perante a direção da empresa. Para Carmen e Corina (2009), a Controladoria como fonte privilegiada de informações, diante do ambiente complexo e dinâmico dos negócios, o que dificulta o processo decisório dos gestores, tem a responsabilidade de adaptar e aperfeiçoar permanentemente suas práticas e sistemas de informações visando atender as demandas dos tomadores de decisão. Dessa forma, contribui com informações adequadas às decisões que visam diminuir riscos. O gerenciamento de riscos é determinante na obtenção de resultados positivos, como também para a melhoria do prestígio do *controller* na empresa.

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. Dessa forma, entende-se que a Controladoria não pode delegar ou não participar dos processos de segurança da informação, pois ela é responsável pelos sistemas informacionais das organizações.

Para realizar operacionalmente as atribuições estabelecidas à Controladoria, esta deve atuar nas organizações como um elo de ligação entre as diversas áreas, apoiando sistemicamente o processo de geração de informações, apresentando estudos e as melhores alternativas econômicas aos gestores. Isso requer profissionais com conhecimentos teóricos e práticos em diversas áreas do conhecimento, pró-ativos, para que efetivamente na prática possa a área de Controladoria exercer a função atribuída pelas teorias. Segundo Oliveira (2009, p. 74), o profissional de Controladoria necessita de conhecimentos em diversas áreas e cita: contabilidade, economia, finanças, controles internos, orçamentos, tecnologia da informação, administração.

Na seção seguinte, aborda-se o tema segurança de informações.

2.2 SEGURANÇA DE INFORMAÇÕES

As informações para as empresas são atualmente um dos ativos mais relevantes e que muitas vezes fazem parte de suas vantagens competitivas. Portanto, preservá-las e disponibilizá-las no momento adequado faz parte de uma política eficaz de segurança de informações.

A segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (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, a conectividade através de redes e o armazenamento em meios digitais. Esses 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. 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 leva a implementações de segurança da informação mais eficaz. No entanto, a descentralização pode levar a problemas quando não se possui um programa de treinamento e conscientização desses usuários, medidas que devem fazer parte do planejamento das políticas de segurança da informação. Dessa forma, considera-se que empresas que adotam uma política corporativa e participativa nos processos de segurança de informação têm vantagens em relação às empresas que procuram concentrar suas políticas de segurança de informação em uma única área, a de tecnologia da informação.

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. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os funcionários da organização. Pode ser necessária também a participação de acionistas, fornecedores e clientes.

Para Eloff e Eloff (2003), as organizações devem adotar uma gestão holística da segurança da informação, propiciando mudanças de paradigmas, contribuindo para estabelecer um sistema de gestão da segurança da informação

a fim de proteger o ativo informação. O posicionamento deste trabalho contempla essa gestão holística, integrando as áreas de Controladoria e TI na avaliação dos processos de segurança da informação.

O ambiente organizacional, em decorrência de fatores internos e externos, afeta muitos processos de negócio, os quais passam por constantes alterações que requerem uma política de segurança de informação que vise evitar a ocorrências de riscos que possam comprometer a continuidade das empresas. Na estruturação da política de segurança de informação, um dos fatores-chave que devem ser considerados são os usuários. Nesse mesmo sentido, conforme Bulgurcu, Cavusoglu e Benbasat (2010), os usuários são os principais aliados das organizações nos esforços de reduzir os riscos relacionados à segurança da informação. Nessa linha, Spears e Barki (2010) afirmam que os usuários podem ser o recurso mais valioso na gestão de risco da segurança de informações. Para obter-se a eficácia nas políticas que visam prevenir, detectar ou minimizar eventuais riscos decorrentes de falhas de segurança de informações, as organizações necessitam inserir os usuários, para que estes estejam cientes e possam contribuir com essas políticas.

A ISO 27002 (2007) menciona que antes de considerar o tratamento de um risco, a organização deve definir os critérios para determinar se os riscos podem ou não ser aceitos. Para tal, existem três fontes principais de requisitos de segurança da informação que devem ser avaliados: (i) o impacto nos negócios devido a uma falha de segurança; (ii) a probabilidade da ocorrência de falhas, frente às vulnerabilidades encontradas e; (iii) a seleção dos controles de segurança da informação mais adequados à análise de riscos e vulnerabilidade. Riscos podem ser aceitos se, por exemplo, for avaliado que o risco é baixo ou que o custo do tratamento não é economicamente viável para a organização. Convém que tais decisões sejam registradas.

A norma ISO/IEC 27002 (2007) estabelece critérios que têm por objetivo analisar o nível de proteção das práticas de segurança da informação nas organizações. A aplicação desses critérios contribui com uma visão sistêmica sobre o tema segurança de informações, os quais foram aplicados na parte prático deste trabalho. A seguir, são descritos os critérios utilizados no presente estudo como apoio ao processo de coleta e análise dos dados:

- *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 (ISO/IEC 27002, p. 8);
- *OI*: organizando a segurança da informação, que tem por objetivo gerenciar a segurança da informação dentro da organização (ISO/IEC 27002, p. 10);
- *GA*: gestão de ativos, que tem por objetivo alcançar e manter a proteção adequada dos ativos da organização (ISO/IEC 27002, p. 21);
- *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 (ISO/IEC 27002, p. 25);
- *GO*: gerenciamento das operações e comunicações, que tem por objetivo garantir a operação segura e correta dos recursos de processamento da informação (ISO/IEC 27002, p. 40);
- *CA*: controle de acessos, que tem por objetivo controlar acesso à informação (ISO/IEC 27002, p. 65);
- *AQ*: aquisição, desenvolvimento e manutenção de sistemas de informação, que tem por objetivo garantir que segurança é parte integrante de sistemas de informação (ISO/IEC 27002, p. 84);
- *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 (ISO/IEC 27002, p. 98);
- *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 (ISO/IEC 27002, p. 103);

- *CF*: conformidade, que tem por objetivo evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação (ISO/IEC 27002, p. 108).

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 na seção 4.1.4.1 (p. 60), 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. Dessa forma, a norma ISO/IEC 27002 contempla diretrizes e princípios que contribuem no aprimoramento dos controles e, por conseguinte do ambiente da informação.

Para apoiar à gestão da área de TI tem-se o Cobit, um *framework* e uma base de conhecimentos para os processos de TI e seu gerenciamento, ao qual não contempla um padrão definitivo, o que permite que seja adaptado para cada empresa. A proposta do Cobit 4.1 (ITGI, 2007) é

> prover boas práticas através de um framework de domínios e processos e apresentar atividade em uma estrutura lógica gerenciável. Estas práticas visam ajudar a otimizar a TI, habilitando investimentos, garantindo a entrega de serviços, além de prover sua mensuração (ITGI, 2007, p. 7).

O Cobit auxilia na entrega de valor pela TI e busca identificar e gerir os riscos associados ao uso da tecnologia. O Cobit ajuda a reduzir *gaps* entre demandas do negócio, necessidade de controle e questões técnicas e busca garantir a integridade da informação e dos sistemas de informação (ISACA, 2011).

Conforme Tanuwijaya e Sarno (2010), o Cobit 4.1 tem por essência apoiar e atender as diferentes necessidades de gestão de TI preenchendo a lacuna entre processos de informação, riscos do negócio, controles e problemas técnicos buscando alinhar às estratégias de negócio.

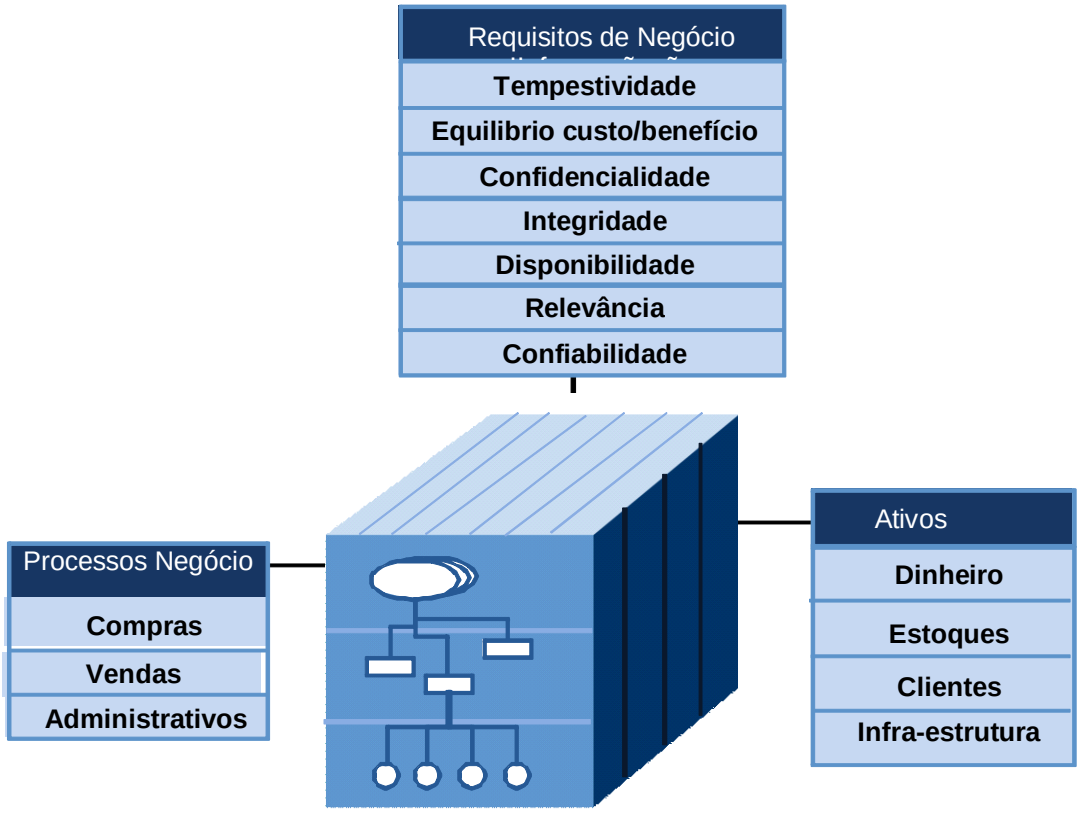
O Cobit propõe uma visão panorâmica de todos os processos de TI, e a ISO 27002 (2007), por sua vez, aborda os controles para a segurança da

informação. Conforme o ITGI (2007), o Cobit também propicia uma influência entre os diferentes usuários como alta direção, executivos de negócio, executivos de TI e auditores. Para atingir as melhores práticas de controles de processos, é primordial haver alinhamento e integração entre as diversas áreas da empresa.

Dessa forma, o modelo Cobit 4.1 pode contribuir com a implementação de uma cultura organizacional focada em processos, propiciando mapeamentos, níveis de maturidade e métricas que permitam apoiar o processo de gestão com ênfase em processos relevantes para a estratégia da organização.

A figura 5 apresenta os requisitos de negócio quanto aos critérios de informação do Cobit 4.1, interligados com os atributos das informações da Controladoria, relacionado-os a alguns processos de negócio e que podem afetar os ativos envolvidos, quando não adotada uma política de segurança da informação corporativa e eficaz.

Figura 5 - Critérios da informação integrando os atributos da informação da controladoria e requistos de negócio de segurança da informação do Cobit para minimizar riscos sobre ativos operacionais



Fonte: Elaborado pelo autor (adaptado cubo modelo Cobit 4.1. ITGI, 2007)

Os critérios da informação, relacionando conceitualmente os atributos da informação da Controladoria com base no CPC 00 (2008) (tempestividade, equilíbrio entre custo/benefício, confiabilidade, relevância) e os requisitos de negócio, conforme estabelece o Cobit 4.1 (efetividade, eficiência, confidencialidade, integridade, disponibilidade e confiabilidade), são descritos a seguir:

- *tempestividade*: o Cobit 4.1 (ITGI, 2007) denomina esse critério como sendo a efetividade da informação, onde a mesma deve estar disponível de forma precisa no prazo, na forma e no formato adequado. O CPC (2008) considera a tempestividade da informação aquela relevante e pertinente para o processo de negócio bem como a mesma sendo entregue em tempo, de maneira correta, consistente e utilizável;
- *equilíbrio custo/benefício*: o Cobit 4.1 (ITGI, 2007) denomina esse critério como sendo a eficiência da informação, onde a entrega da informação deve ser a mais produtiva e econômica através do melhor uso dos recursos. O CPC (2008) considera que os benefícios decorrentes da informação não devem exceder o custo de produzi-la;
- *confidencialidade*: no Cobit 4.1 (ITGI, 2007), a confidencialidade da informação está relacionada com a proteção de informações confidenciais para evitar a divulgação indevida. A Controladoria como gestora do processo de informações considera nos seus procedimentos de divulgação de informações o atributo confidencialidade para que a informação seja dirigida somente ao seu público-alvo;
- *integridade*: o Cobit 4.1 (ITGI, 2007) conceitua como sendo a informação completa, acurada e validada de acordo com os valores e expectativas do negócio. Conceitualmente para o CPC pode-se enquadrar a disponibilidade da informação no critério confiabilidade;
- *disponibilidade*: o Cobit 4.1 (ITGI, 2007) considera que a informação esteja disponível quando requerida pelo usuário. Também está ligada à salvaguarda dos recursos necessários e capacidades associadas.

Conceitualmente para o CPC pode-se enquadrar a disponibilidade da informação no critério tempestividade;

- *relevância*: esse critério é específico do CPC (2008, p. 11) onde

> as informações devem ser relevantes às necessidades dos usuários na tomada de decisões. As informações são relevantes quando podem influenciar as decisões econômicas dos usuários, ajudando-os a avaliar o impacto de eventos passados, presentes ou futuros ou confirmando ou corrigindo as suas avaliações anteriores.

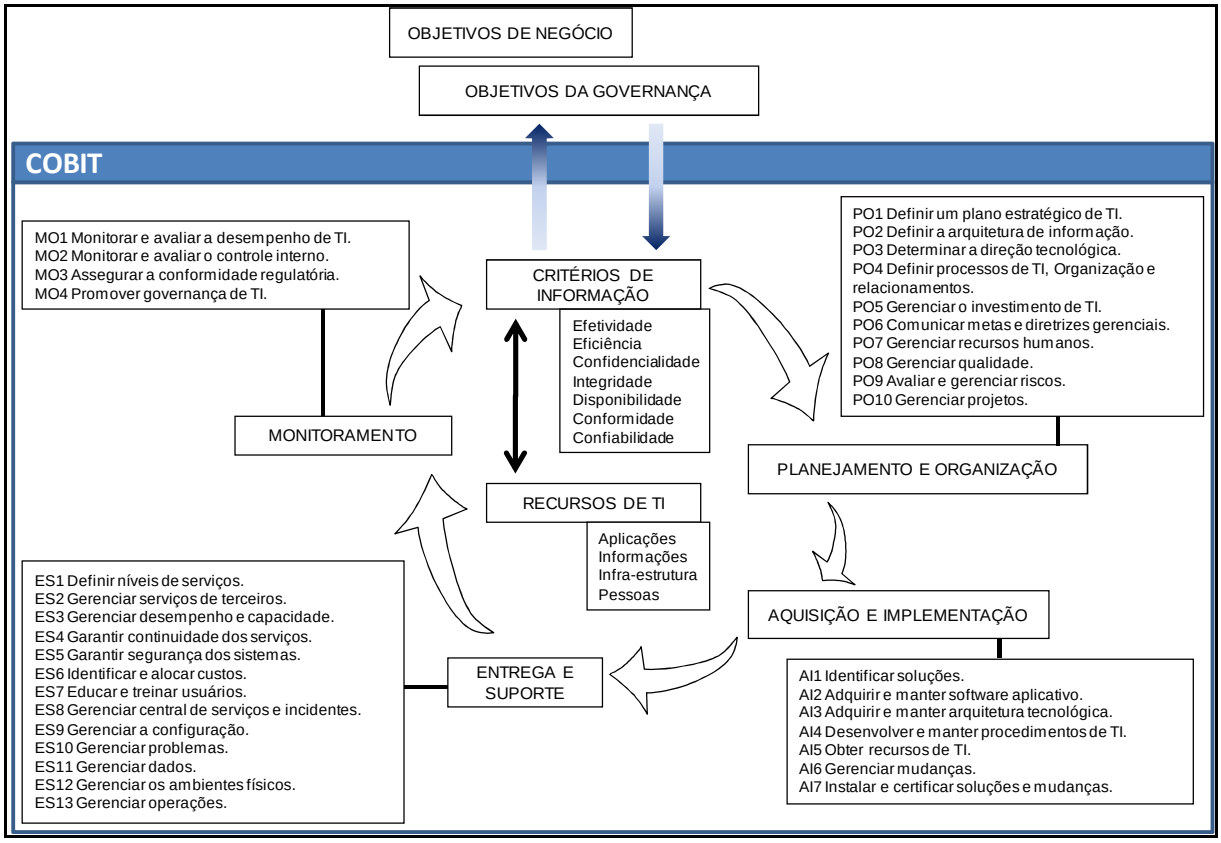
Conceitualmente para o Cobit 4.1 pode-se enquadrar algumas características do critério confiabilidade da informação;

- *confiabilidade*: o Cobit 4.1 (ITGI, 2007) considera a confiabilidade da informação quando estas são fornecidas de forma apropriada e precisa aos gestores para tomada de decisão a fim de exercer suas responsabilidades fiduciárias e de governança. O CPC (2008) considera a informação confiável quando esta estiver livre de erros ou vieses relevantes e representar adequadamente aquilo que se propõe a representar. Uma informação pode ser relevante, mas se contiver erros pode afetar o processo de tomada de decisão.

Percebe-se que os critérios da informação descritos e presentes na figura 5 tem correspondência entre os princípios básicos para uma informação segura considerada pela TI (figura 2), com os atributos das informações que a Controladoria baseia-se para fazer a gestão das informações aos usuários para tomada de decisão (figura 1). Dessa forma, a integração e utilização das ferramentas de TI, ISO 27002 e Cobit 4.1, o conhecimento técnico específico das áreas de TI e Controladoria nos processos de segurança da informação podem propiciar um ambiente de redução de retrabalhos e uma diminuição de riscos operacionais.

A visão geral do modelo Cobit 4.1 é apresentada na figura 6, na qual estão dispostos os 4 domínios contendo 34 processos genéricos, gerenciando os recursos de TI com objetivo de entregar informações para a área de negócios de acordo com os requerimentos de negócios e governança (ITGI, 2007).

Figura 6 - Visão geral do modelo COBIT 4.1



Fonte: ITGI (2007)

O Cobit 4.1 (ITGI, 2007) se divide em quatro domínios, conforme apresentado na figura 6. A seguir descreve-se o objetivo desses domínios:

1) *planejamento e organização*: esse domínio foca na identificação dos caminhos em que a TI pode melhor contribuir para a obtenção dos objetivos de negócio. Além disso, a visão estratégica necessita ser planejada, comunicada e gerenciada em diferentes perspectivas. Por fim, uma organização e uma infraestrutura tecnológica adequada devem ser definidas e implementadas;
2) *aquisição e implementação*: pretende identificar as soluções necessárias, utilizando o desenvolvimento ou aquisição e tê-las implementadas e integradas aos processos de negócio. Além disso, são consideradas mudanças e manutenção nos sistemas existentes, no contexto desse domínio;
3) *entrega e suporte*: está focado nos produtos reais dos serviços requeridos, desde operações tradicionais de segurança e aspectos de continuidade. Esse domínio inclui o processamento real de dados

pelos sistemas de aplicação, normalmente classificados em controles da aplicação;

4) *monitoramento*: tem como foco os processos de TI a serem avaliados, regularmente, nos aspectos de sua qualidade e conformidade com os requisitos de controle. Esse domínio direciona, ainda, a vigilância da gerência nos processos de controles da organização e fornece garantia independente pela auditoria interna ou externa.

Os quatro domínios se desdobram em 34 processos, e estes são compostos por atividades que permitem a execução. Estas bem executadas permitem atingir os objetivos propostos pelo modelo.

O Cobit 4.1 (ITGI, 2007, p. 8) suporta a gestão da área de TI estabelecendo as seguintes áreas como foco de atuação:

- *alinhamento estratégico*: foca em garantir a ligação entre os planos de negócios e de TI, definindo, mantendo e validando a proposta de valor de TI, alinhando as operações de TI com as operações da organização (ITGI, 2007, p. 8);
- *entrega de valor*: é a execução da proposta de valor de IT através do ciclo de entrega, garantindo que TI entrega os prometidos benefícios previstos na estratégia da organização, concentrado-se em otimizar custos e provendo o valor intrínseco de TI (ITGI, 2007, p. 8);
- *gestão de recursos*: refere-se à melhor utilização possível dos investimentos e o apropriado gerenciamento dos recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas. Questões relevantes referem se à otimização do conhecimento e infraestrutura (ITGI, 2007, p. 8);
- *gestão de riscos*: requer a preocupação com riscos pelos funcionários mais experientes da corporação, um entendimento claro do apetite de risco da empresa e dos requerimentos de conformidade, transparência sobre os riscos significantes para a organização e inserção do gerenciamento de riscos nas atividades da companhia (ITGI, 2007, p. 8);
- *mensuração de desempenho*: acompanha e monitora a implementação da estratégia, término do projeto, uso dos recursos,

> processo de performance e entrega dos serviços, usando, por exemplo, “*balanced scorecards*” que traduzem as estratégias em ações para atingir os objetivos, medidos através de processos contábeis convencionais (ITGI, 2007, p. 8).

No sentido de avaliar a execução das atividades, o estudo usa a técnica *Analytical Hierarchy Process* (AHP) para avaliar os níveis de maturidade o qual contempla a subjetividade do processo de análise dos processos de TI. O processo analítico hierárquico AHP é uma técnica de decisão multicritério iniciada por Saaty (1980) para solucionar problemas de planejamento de necessidades e alocação de recursos escassos.

Direciona-se, assim, o método AHP para atender à subjetividade de análise de importância agrupada de cada um dos aspectos que o Cobit 4.1 atende. Foi aplicado aos diferentes domínios em cada uma das áreas focais do Cobit 4.1 com uma preocupação de diminuir riscos operacionais ocasionados por processos fragilizados de TI. Dessa forma, enfatiza-se na análise dos resultados a área focal gestão de riscos.

O instrumento aplicado neste estudo foi desenvolvido a partir do trabalho de Vanti, Cobo e Rocha (2011) complementarmente ao questionário de níveis de maturidade do Cobit 4.1. As respectivas análises relacionadas aos níveis de maturidade nos diferentes domínios em cada uma das áreas focais do Cobit 4.1 na organização aparecem de maneira aplicada neste trabalho na seção 4.1.4.3, tendo como base as percepções dos gestores de TI.

No capítulo seguinte, aborda-se a metodologia de pesquisa a ser utilizada, cujo objetivo é apoiar a pesquisa e gerar as respostas ao problema apresentado.

3 METODOLOGIA DE PESQUISA

O presente estudo caracteriza-se pela utilização de abordagem qualitativa porque descreve a percepção dos respondentes ao problema proposto. Segundo Malhotra (2008), a pesquisa qualitativa resulta em dados primários porque é realizada com o propósito específico de levantar o problema em pauta. Ela é apropriada nas situações de incerteza, como quando os resultados conclusivos diferem das expectativas. Para Silva e Menezes (2001), a pesquisa qualitativa tem no seu ambiente natural a fonte direta para a coleta de dados, e o pesquisador é o instrumento principal.

No que se refere aos objetivos, a pesquisa se enquadra como uma pesquisa exploratória, no que se refere ao estudo da avaliação de processos de segurança da informação integrando as áreas de Controladoria e TI. Busca-se, portanto, conhecer de forma mais profunda o assunto que é pouco explorado, de modo a torná-lo mais claro e acessível para novas pesquisas. Quanto às pesquisas exploratórias, segundo Marconi e Lakatos (2007, p. 85), são investigações de pesquisa empírica cujo objetivo é a formulação de questões ou de um problema com a finalidade de desenvolver hipóteses, aumentar a familiaridade do pesquisador com o problema a fim de modificar ou clarificar conceitos.

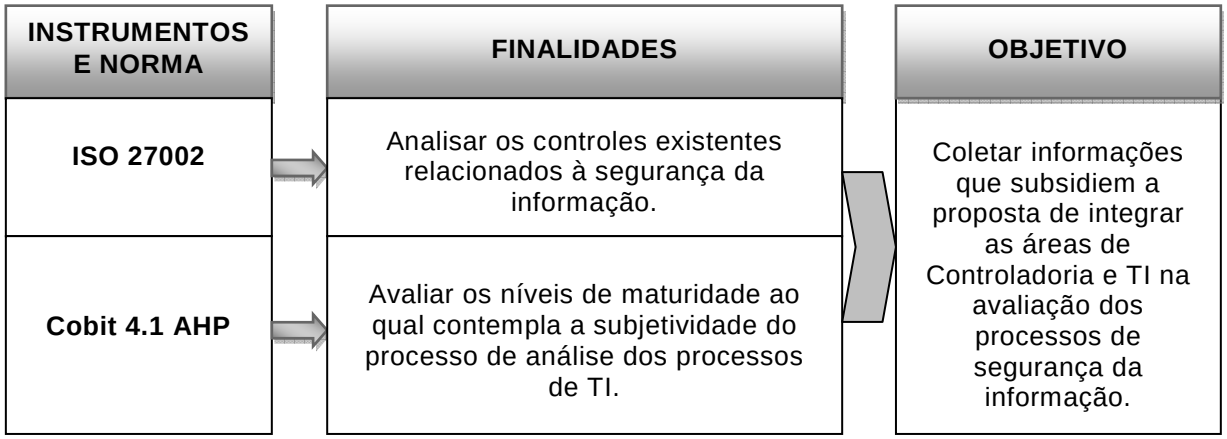
Como procedimentos técnicos utilizados, sendo o objetivo desta pesquisa relacionado com a integração das áreas de Controladoria e de TI nos processos de segurança de informação, um tema contemporâneo no seu contexto real, foi proposto um estudo de caso único, visando adquirir um conhecimento amplo e detalhado. De acordo com Yin (2010), os projetos de caso único exigem uma investigação cuidadosa do caso potencial a fim de minimizar equívocos e maximizar o acesso necessário à coleta de evidências do estudo de caso.

Para a realização do estudo de caso, utilizou-se o protocolo de estudo de caso que, segundo Yin (2010), tem por finalidade dar confiabilidade à pesquisa, dar foco e servir de suporte ao pesquisador na realização da coleta de dados do estudo de caso único. O protocolo de estudo de caso contempla uma visão geral do projeto do estudo; os procedimentos de campo; as questões de estudo de caso; e uma guia de para o relatório do estudo de caso.

No presente estudo, foram aplicados em uma triangulação os instrumentos da tecnologia da informação ISO/IEC 27002 e Cobit 4.1 com enfoque AHP para analisar os processos de segurança da informação, processos críticos ou riscos de negócio na organização estudada. Assim, obter informações que subsidiaram o objetivo do estudo de avaliação dos processos de segurança da informação integrando as áreas de Controladoria e de TI.

Na figura 7 apresenta-se as finalidades e objetivo desse procedimento técnico utilizado.

Figura 7 - Procedimentos técnicos complementares utilizados no estudo



Fonte: Elaborado pelo autor

Os procedimentos técnicos complementares que foram utilizados no estudo explicitam um fluxo, em que aplicaram-se questionários aos gestores participantes do estudo elaborados com base nos instrumentos ISO 27002 e Cobit 4.1 complementarmente com o modelo multicritério AHP, de forma que obteve-se a percepção dos mesmos quanto à gestão na organização no que refere-se aos níveis de controle e de maturidade dos processos de segurança da informação.

3.1 CRITÉRIOS PARA ESCOLHA DO CASO ESTUDADO

O presente estudo aborda um tema contemporâneo e inevitavelmente está relacionado ao fator humano, em que pessoas que irão colaborar com o presente estudo estarão sendo envolvidas. Entende-se que um fator importante é o de obter o consentimento prévio da empresa e das pessoas que estarão sendo inseridas no estudo. Ao permitir o acesso aos dados, informações, ou

estar presencialmente realizando um trabalho de campo, se faz necessário um elo de confiança entre o pesquisador e a organização a ser estudada.

Nesse sentido, Yin (2010, p. 100) cita que o pesquisador é responsável pela condução do seu estudo de caso e deve ter cuidados e sensibilidade especiais e envolve geralmente os seguintes aspectos:

- obter o consentimento informado de todas as pessoas envolvidas no estudo de caso, esclarecendo-as sobre os objetivos do estudo para que sua participação seja de forma voluntária;
- proteger os participantes do estudo de qualquer dano;
- proteger a privacidade e a confidencialidade dos que participam para que, não fiquem em posição desconfortável por eventuais solicitações de participação em estudos futuros, conduzido pelo próprio pesquisador ou outra pessoa;
- tomar precauções especiais para proteção de grupos específicos que possam ser vulneráveis (pessoas que têm acesso a informações privilegiadas).

A seleção da organização objeto do estudo de caso levou em consideração os seguintes critérios: a) empresa com sede no estado do Rio Grande do Sul; b) empresa de nacionalidade brasileira; c) empresa de destaque no seu segmento de atuação; d) possuir setores de Controladoria e de TI com subordinações independentes.

O primeiro critério refere-se à opção de se estudar uma empresa com sede no estado do Rio Grande do Sul, o que contribui para o agendamento entre o pesquisador residente nesse estado e a os participantes do estudo. O segundo e terceiro critérios referem-se à opção por empresa brasileira e de destaque no seu segmento de atuação, por entender-se que através da dinâmica de seus negócios pode propiciar elementos enriquecedores ao estudo. Por fim, o último critério é a existência no organograma da empresa de setores de Controladoria e de TI com subordinações independentes, fator principal para a realização do estudo.

O caso selecionado para estudo com base nos critérios descritos anteriormente nessa seção é as Lojas Colombo, do ramo varejista, fundada em

novembro de 1959, com sede na cidade de Farroupilha/RS. Possui atualmente uma rede de 357 lojas de varejo e três centros de distribuição.

O caso escolhido para ser estudado, conforme Yin (2010), é representativo, pois, ao possuir áreas estruturadas de Controladoria e de TI com subordinações independentes permite captar circunstâncias e as condições das atividades operacionais diárias e identificar processos que permitam aplicar a teoria do estudo podendo ser estendido a outras organizações.

3.2 PLANO DE COLETA E TRATAMENTO DE DADOS

A empresa objeto do estudo foi contatada em Outubro de 2010 pelo pesquisador, para apresentação da proposta de estudo aos gestores responsáveis pelas áreas de Controladoria, Contabilidade e de Tecnologia da Informação - TI da empresa. Para o processo de coleta de dados, a empresa designou o Gerente da área de TI como o contato principal entre o pesquisador e a empresa.

A definição desse gerente como elo entre a organização e o pesquisador é extremamente importante, pois tem conhecimento profundo de diversas áreas da empresa (25 anos de empresa), o que viabilizou todos os contatos e agendamentos de reuniões com os demais gestores participantes do processo de coleta de dados.

A etapa inicial de coleta de dados foi verificar junto aos gestores quais os principias 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, Contabilidade/ Fiscal e Supervisor de TI, para uma prévia análise, o primeiro instrumento de coleta de dados (anexo a) que se baseia na norma ISO/IEC 27002. A própria norma que serviu de suporte para o preenchimento das respostas. Posteriormente foi agendada uma reunião conjunta com todos os gestores, onde foram feitas a apresentação do instrumento, explicações sobre sua finalidade para a pesquisa e esclarecimento de dúvidas.

Esse primeiro instrumento contém 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. Nessa seleção, não estão inclusas as seções introdutórias (de 1 a 4) e a seção 9 que trata de segurança física e do ambiente por ser eminentemente técnica não relacionada ao presente estudo. As seções que tratam esse instrumento de coleta de dados são:

a) *política de segurança da informação*: verificar a existência de uma política de segurança da informação;
b) *organizando a segurança da informação*: verificar como ocorre o gerenciamento da segurança da informação dentro da organização;
c) *g*estão de ativos: verificar como a organização mantém e protege seus ativos;
d) *segurança em recursos humanos*: verificar 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*: verificar a gestão dos recursos de processamento e controles da informação;
f) *controle de acessos*: verificar gestão dos controles de acesso à informação;
g) *aquisição, desenvolvimento e manutenção de sistemas de informação*: verificar níveis de garantia de segurança aos sistemas de informação;
h) *gestão de incidentes de segurança da informação*: verificar o processo de comunicação e correção quando eventualmente existir incidentes com eventos de segurança da informação;
i) *gestão da continuidade do negócio*: verificar níveis de gestão que evitem interrupções das atividades de negócio;
j) *conformidade*: verificar o processo de gestão quanto a violações de obrigações legais, informações estatutárias, contratuais relacionadas a 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 (anexo b), 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. O entrevistado participa efetivamente do estudo, 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/Fiscal, 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 se necessário.

Na última etapa, desenvolveu-se o terceiro instrumento de coleta de dados AHP (anexo d) 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 feitas 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) complementarmente ao questionário de níveis de maturidade do Cobit 4.1 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 na figura 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.

Figura 8 - 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.

3.3 PLANO DE ANÁLISE DE DADOS

A análise de dados é a etapa onde o pesquisador inicia a classificação dos dados coletados no estudo, para tal deve adotar uma série de procedimentos ordenados que permitam qualificar esses dados a fim de gerar

evidências para o estudo. Segundo Yin (2010), um dos procedimentos da análise dos dados consiste em determinar prioridades de análise. Por sua vez, Malhotra (2008) destaca como essencial para a análise dos dados uma prévia preparação e organização dos dados coletados.

No que se refere à escolha da estratégia da análise dos dados, conforme Malhotra (2008), o pesquisador deve levar em conta todas as etapas anteriores e todos os aspectos da pesquisa a ser realizada, por exemplo, o problema de pesquisa e as características conhecidas dos dados.

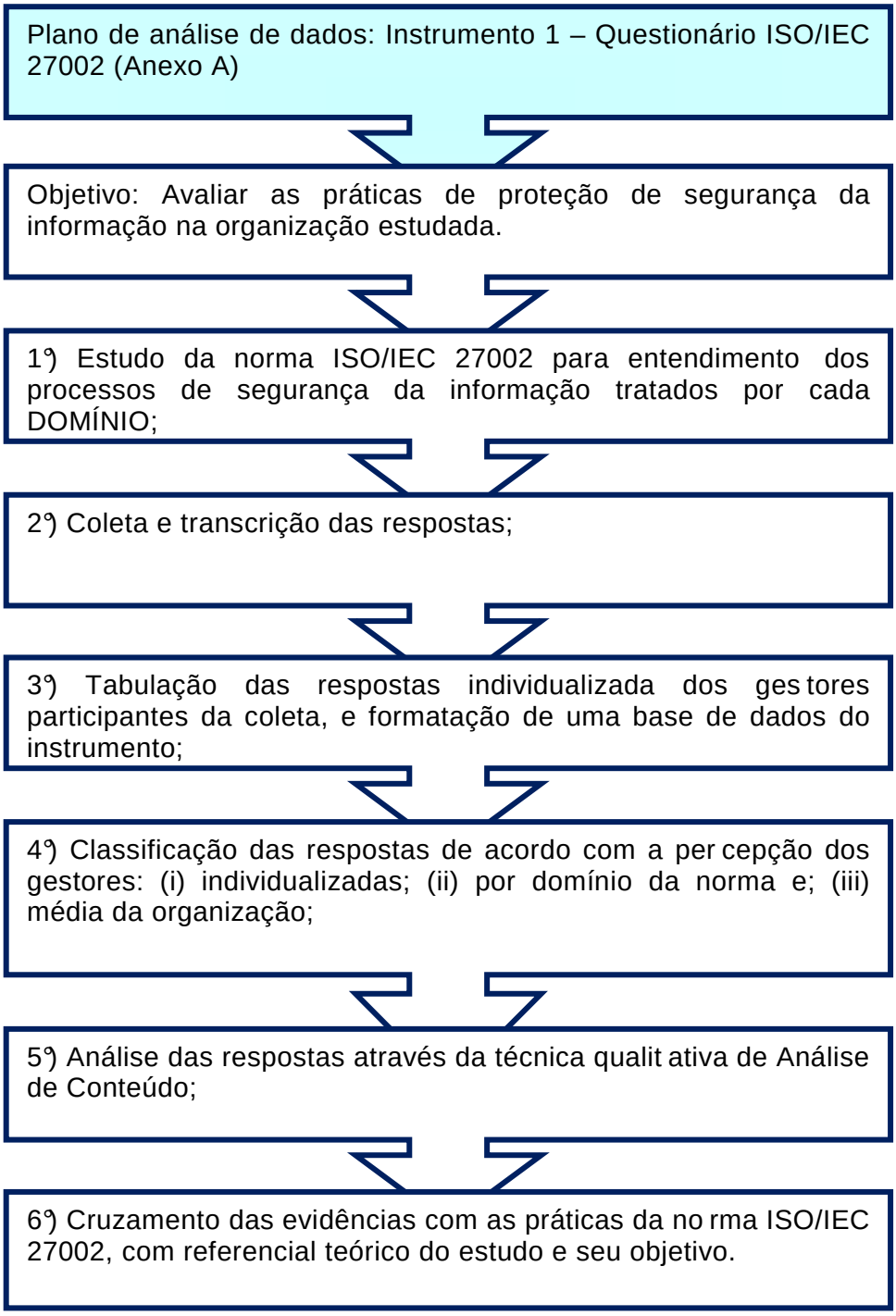
Yin (2010) propõe quatro estratégias para a análise dos dados: contar com proposições teóricas, desenvolver descrições de caso, usar dados quantitativos e qualitativos e examinar as explanações divergentes. Essas estratégias, segundo Yin (2010), podem ser usadas concomitantemente com as técnicas de análise de dados, quais sejam: combinação de padrão, a construção da explanação, a análise de séries temporais, os modelos lógicos e a síntese cruzada de dados.

Nas seções a seguir, são apresentadas as etapas adotadas no plano de análise dos dados para cada instrumento de coleta dos dados aplicados na organização.

3.3.1 Questionário – ISO/IEC 27002

A figura 9 apresenta as etapas adotadas no plano de análise dos dados quanto ao instrumento “questionário”, elaborado com base na norma ISO/IEC 27002 para analisar os controles existentes na organização relacionados à segurança da informação.

Figura 9 - Procedimentos do plano de análise de dados – Instrumento 1 – Questionário ISO/IEC 27002



Fonte: Elaborado pelo autor

A figura 9 explicita o fluxo do plano de análise dos dados para o instrumento elaborado com base na norma ISO/IEC 27002, e que propiciou a classificação e tabulação dos dados ao qual foram utilizados para subsidiar as análises quanto ao grau de proteção da informação na organização.

3.3.2 Entrevistas

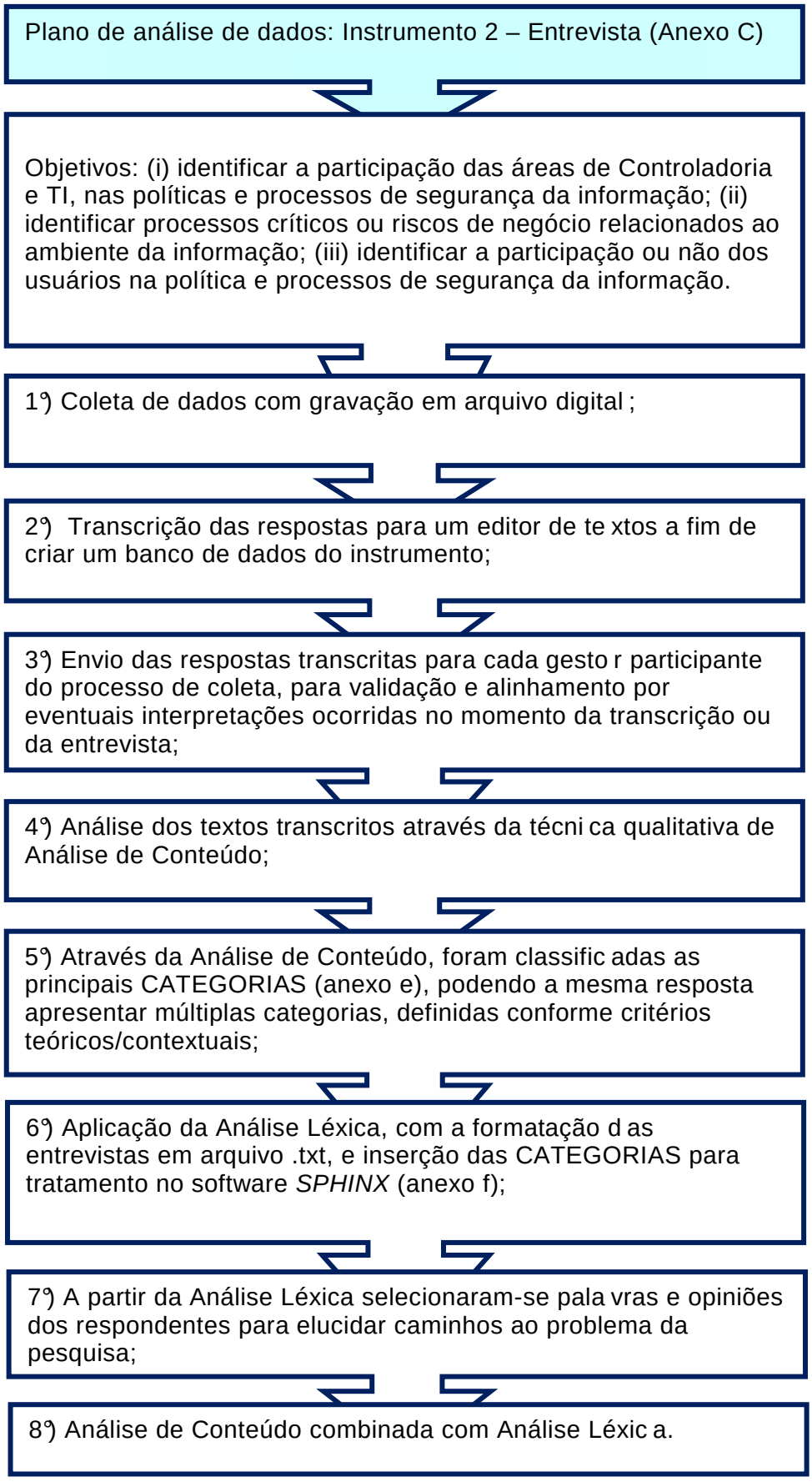
O segundo instrumento aplicado foi a entrevista (anexo c), que foi estruturada em três blocos de perguntas, cada bloco voltado a atender uma parte dos objetivos propostos pelo estudo. A seção I buscou informações gerais dos respondentes sobre possíveis fatores limitadores nos processos de integração entre as áreas de Controladoria e TI, a existência de processos que possibilitam essa integração e a atuação das áreas de Controladoria e TI nas alterações de softwares na organização.

Na seção II, buscou-se identificar junto aos respondentes qual política de segurança da informação adotada pela organização, a existência de procedimentos de análise crítica com a participação dos usuários nas alterações de *software*, a existência de treinamentos junto aos usuários do sistema, e o tratamento para os riscos em relação ao sistema informacional da organização.

Na seção III, objetivou-se identificar a atuação das áreas de Controladoria e TI na organização para comunicar a política de segurança da informação, o envolvimento juntos as demais áreas quanto às decisões sobre alterações de *software*, as necessidades de adequação dos *softwares* para geração de informações de apoio a tomada e decisão dos gestores. Por fim, a percepção dessas áreas quanto à inserção dos usuários nas políticas que visam prevenir, detectar ou minimizar eventuais riscos decorrentes de falhas de segurança de informações na empresa.

A figura 10 apresenta as etapas adotadas no plano de análise dos dados do instrumento “entrevista”.

Figura 10 - Procedimentos do plano de análise de dados – Instrumento 2 – Entrevistas



Fonte: Elaborado pelo autor

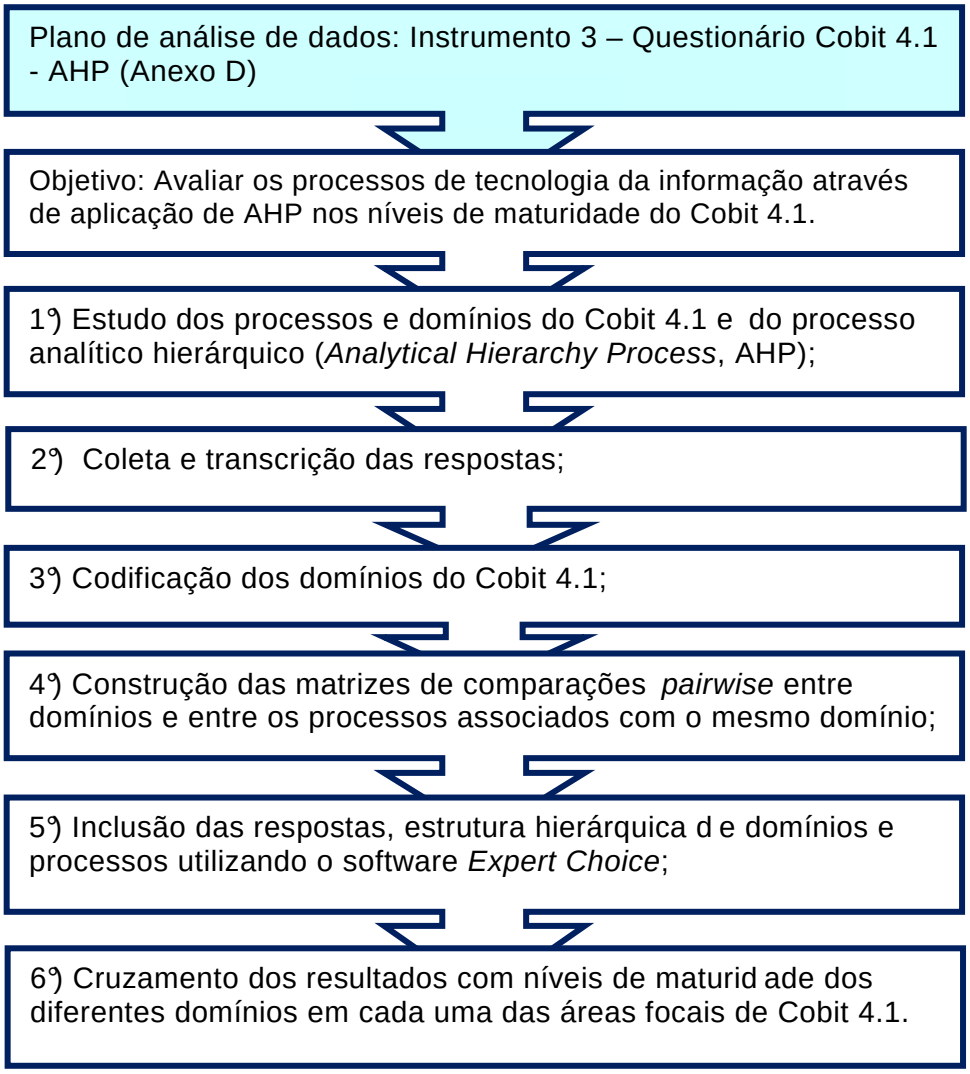
A figura 10 explicita o fluxo de análise dos dados da entrevista, e que propiciou a classificação, tabulação e categorização dos dados. Através da Análise Léxica, foram possíveis a determinação de prioridades nas análises quanto a política de segurança da informação e a atuação das áreas de Controladoria e de TI na avaliação dos processos de segurança da informação na organização.

3.3.3 Questionário – AHP

O terceiro instrumento aplicado foi o modelo multicritério AHP (anexo d), a partir da estruturação hierárquica que o modelo Cobit 4.1 propõe, para identificar os processos de TI com um maior grau de influência. Também foi considerado o objetivo de avaliar ou medir o grau de desenvolvimento de cada uma das áreas de foco definida pelo Cobit 4.1.

A figura 11 a seguir apresenta as etapas adotadas no plano de análise dos dados do instrumento questionário – AHP.

Figura 11 - Procedimentos do plano de análise de dados – Instrumento 3 – Questionário AHP



Fonte: Elaborado pelo autor

A figura 11 explicita o fluxo do plano de análise dos dados para o instrumento AHP elaborado complementarmente ao questionário de níveis de maturidade do Cobit 4.1, e que propiciou a geração dos dados utilizados para subsidiar as análises quanto aos níveis de maturidade obtidos por diferentes domínios em cada uma das áreas focais do Cobit 4.1 na organização.

3.4 LIMITAÇÕES DO MÉTODO

Qualquer método de pesquisa possui suas limitações, dentre elas as relacionadas ao fator humano. Do pesquisador, exige-se controle emocional “deste” e “sobre” as pessoas que invariavelmente participam do estudo. Para Yin

(2010), cada método tem suas vantagens e desvantagens peculiares relacionando três itens: a questão da pesquisa, o controle que o investigador tem sobre os eventos comportamentais reais e o enfoque sobre os fenômenos contemporâneos em oposição aos históricos.

Dentre as limitações do método de estudo de caso, pode-se citar o processo de elaboração da entrevista, em que tanto o pesquisador como o entrevistado pode incorrer em interpretações que afetem o resultado da pesquisa, contudo buscou-se dirimir as dúvidas junto aos entrevistados e efetuar os ajustes necessários. Outro fator limitante é a agenda dos entrevistados, por serem pessoas do *staff* da empresa, se faz necessário estabelecer um agendamento prévio.

No aspecto estudo de caso único, conforme Yin (2010), o mesmo é vulnerável, pois mais tarde o caso pode não vir a ser considerado no início. Outra limitação do estudo de caso único é que as conclusões do estudo não podem ser generalizadas para outras empresas, porém é possível de transferências para outros cenários organizacionais.

4 APRESENTAÇÃO DO CASO ESTUDADO E ANÁLISE DOS RESULTADOS

O objetivo deste capítulo é realizar a descrição e análise de dados do caso estudado. Primeiramente são apresentados a organização estudada, o organograma da empresa e os gestores que participaram dos processos de coleta de dados com as respectivas funções e responsabilidades. Posteriormente, apresentam-se os instrumentos de coleta de dados e, por fim, a análise dos dados obtidos através da aplicação dos questionários e entrevistas.

4.1 ORGANIZAÇÃO ESTUDADA

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.

Destacam-se como principais itens de comercialização as linhas de eletrodomésticos, vídeo, informática, móveis, comunicação, eletroportátil e áudio que representam 90% do seu faturamento. Seus principais fornecedores são a Whirlpool S/A, Sony Comércio e Indústria Ltda, LG Eletronics Ltda, Britania Eletrodomésticos S/A, Electrolux do Brasil S/A e Samsung Eletrônica Ltda. Atua em aproximadamente 256 municípios, tendo uma carteira de 5 milhões de clientes, sendo 2,1 milhões de clientes ativos.

Como premiações recentes, em 2010 a empresa conquistou o prêmio Top de Marketing Associação de Dirigentes de Vendas e Marketing do Brasil (ADVB-RS), obtido na categoria “varejo nacional”. O prêmio foi concedido em decorrência dos constantes investimentos em inovação ao longo dos seus 52 anos e a antecipação das tendências e cenários como lojas Premium, web, m-commerce (vendas através de smartphones), televendas, ponto de venda de saldos, lojas convencionais de shopping center e de rua.

4.1.1 Estratégia Institucional

Para manter-se competitiva em um ambiente de alta concorrência, bem como de oportunidades, a empresa estabeleceu no seu Planejamento Estratégico concentrar investimentos no cliente, através de serviços que promovam sua satisfação através da diferenciação frente à concorrência. Nesse contexto, a empresa encontrou nos serviços oportunidades de agregar valor a sua marca e ao seu negócio. Comercializando *commodities*, onde produto e marca são iguais para todas as lojas do ramo, busca agregar valor apresentando serviços cujo valor seja percebido pelo cliente. Dessa forma, oferta uma gama de serviços quais sejam: (i) seguro prestação; (ii) lista de casamento; (iii) habilitação de celulares; (iv) cheque-presente; (v) catálogo eletrônico; (vi) central de atendimento ao cliente; (vii) garantia máxima Colombo; (viii) assistência técnica; (ix) logística; (x) central de montagem; (xi) crédito flexível; (xii) cartão de crédito Colombo; (xiii) consórcio Colombo; e, (xiv) Credifar S/A - Crédito, Financiamento e Investimento.

Todos os produtos e serviços oferecidos pelas Lojas Colombo S/A, estão disponíveis aos clientes através dos seguintes canais de distribuição:

- Lojas de Rua e Shopping;
- Colombo Pneus;
- Colombo Virtual Shop;
- Colombo Mega Store;
- Colombo Home Store;
- <www.colombo.com.br>;
- Televendas – 0800;
- Programa Colombo Shop – Televisivo.

No quadro 1 apresentam-se a visão, a missão, os valores e o código de ética das Lojas Colombo S/A.

Quadro 1 - Visão, Missão, Valores e Código de Ética da Organização

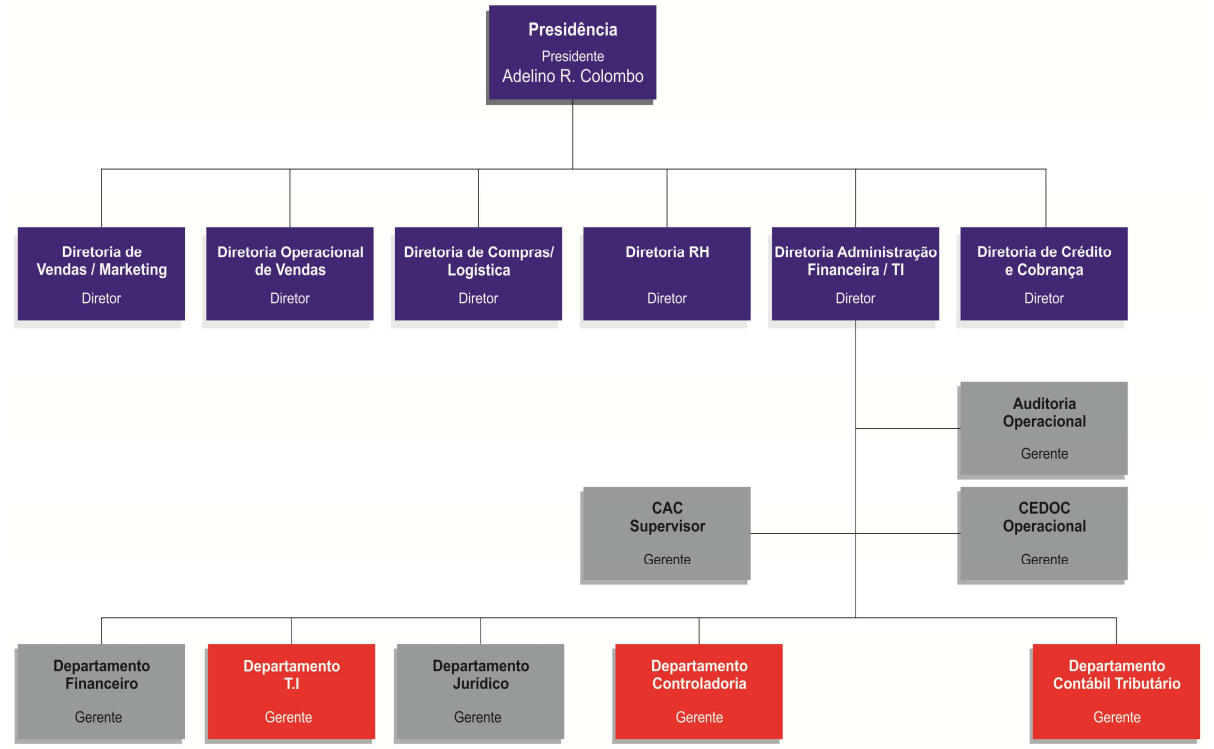
Visão	- Construir um novo ciclo de 50 anos.
Missão	- Viabilizar a realização de sonhos e bem estar, construindo relacionamentos duradouros, oferecendo bens e serviços de forma sustentável.
Valores	- Foco no resultado; - Foco no cliente e excelência no atendimento; - Qualidade nos processos; - Capacitação e aprendizado contínuo; - Profissionalismo e ética nas relações; - Respeito, coerência e espírito de equipe; - Confiança e credibilidade; - Assertividade e pró-atividade.
Código de Ética	- Respeito ao ser humano e aos seus direitos; - Cumprimento de acordos firmados; - Compromisso com a verdade e transparência nas relações; - Respeito às leis e regulamentos; - Sigilo das estratégias e informações da empresa; - Coerência entre discurso e ação; - Assegurar adequada relação custo x benefício a nossos clientes; - Aprimoramento continuado; - A equipe como base de geração de resultados;

Fonte: Elaborado pelo autor com base nas informações fornecidas pela empresa

4.1.2 Organograma da Empresa, Gestores Participantes do Estudo e Processos de Negócio

Nessa seção, apresentam-se o organograma da empresa Lojas Colombo S/A e os cargos dos gestores das áreas de TI, Controladoria e Contabilidade/Fiscal que participaram do presente estudo com suas respectivas funções e responsabilidades. Por fim, os principais processos de negócio na organização de acordo com os gestores entrevistados.

Figura 12 - Organograma da empresa - Lojas Colombo S/A



Fonte: Planejamento estratégico da empresa

O organograma anteriormente representado evidencia as posições das áreas de TI, Controladoria e Contabilidade/Fiscal na organização. A seguir, descrevem-se as funções e responsabilidades dos gestores que participaram dos processos de coleta de dados.

- *Gerente de Departamento de Contabilidade/Fis*cal: (i) gerir os processos de apuração dos balancetes/resultados mensais e balanços anuais, de acordo com legislação, normas e práticas contábeis; (ii) gerir os processos de apuração de impostos e tributos mensais e anuais, de acordo com a legislação normas e práticas fiscais; (iii) planejar os registros e controles dos atuais e novos processos/operações da Companhia, em conformidade com as práticas contábeis; (iv) qualificar os processos organizacionais de sua área de atuação, identificando e promovendo inovações e soluções diferenciadas, validando a aplicabilidade de novas tecnologias, conhecimentos e práticas; (v) participar dos processos de planejamento e tomada de decisão da Empresa, desenvolvendo estudos e novos cenários; (vi) acompanhar fiscalizações tributárias,

auditorias externas, bem como desenvolver as demonstrações financeiras e contábeis da Companhia; (vii) gerir o processo de planejamento tributário, em conformidade com as diretrizes da gestão e avaliação da legislação vigente; e, (viii) manter-se atualizado em relação às mudanças na legislação fiscal, normas e práticas contábil, visando apontar oportunidades de ganhos tributários, bem como orientar as demais áreas quanto aos procedimentos fiscais;

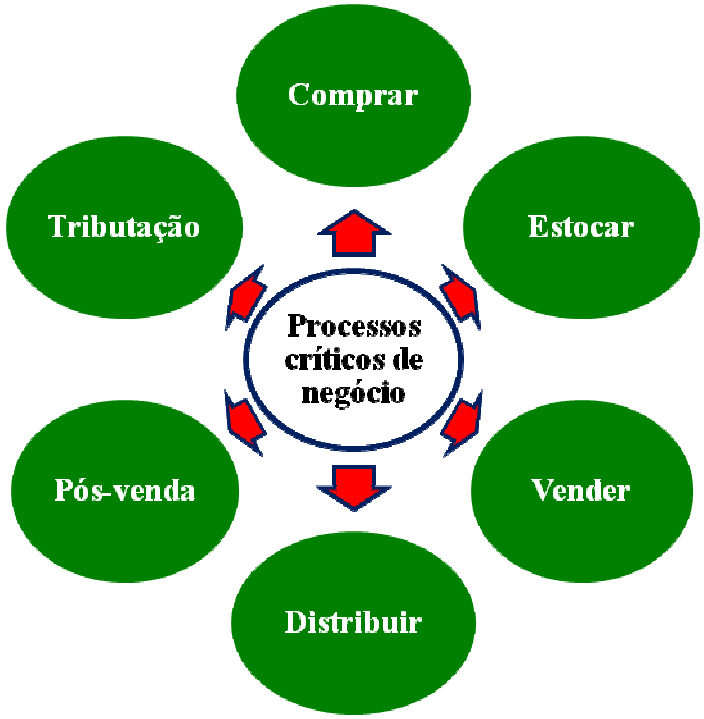
- *Gerente de Departamento de Controladoria*: (i) gerenciar o processo orçamentário anual e submeter para avaliação da alta administração; (ii) acompanhar que os valores orçamentários sejam executados a fim de garantir a rentabilidade prevista; (iii) apresentar os resultados para direção e gestores de área, demonstrando as variações entre o previsto e realizado, auxiliando na tomada de decisões; (iv) desenvolver estudos de viabilidade, aquisição e venda (imobilizados, produtos, bens, etc.) conforme demanda da alta administração da Companhia;
- *Gerente de Departamento de TI*: (i) direcionar, desenvolver e conduzir as ações relacionadas ao Planejamento Estratégico de TI; (ii) definir a arquitetura lógica e física da infraestrutura, com sistemas operacionais adequados e gerenciamento da implantação (definição do cronograma, recursos utilizados, gerência de tempo, etc.); (iii) gerenciar as questões relacionadas a treinamento/capacitação, gestão da performance, seleção de pessoas, remuneração e carreira, bem como pelos indicadores de resultados da equipe de TI; (iv) especificar, implementar e monitorar o plano de contingência e desastre, em conformidade com as melhores práticas de TI; (v) estudar e propor processos para adequação dos sistemas de informação aos objetivos de negócio da empresa; (vi) controlar os indicadores estratégicos e orçamentários da área de TI; (vii) contratar e gerenciar serviços terceirizados em desenvolvimento de *software* e infraestrutura, utilizando as melhores práticas em gerência de aquisições; (viii) responder pela aprovação e aquisição de equipamentos de TI; (ix) atuar e fomentar perante a sua equipe a realização de pesquisa, geração, desenvolvimento e implantação de novas soluções de

tecnologia; e, (x) atuar e fomentar perante a sua equipe a prestação de serviços de consultoria interna para as soluções de tecnologia aplicadas aos usuários;

- *Supervisor de Departamento de TI*: (i) realizar a gestão dos processos e equipes vinculadas aos serviços de TI, visando atender as solicitações e seu posterior planejamento para resoluções; (ii) responder por elaboração, análise e indicadores das métricas de atendimento dos serviços de TI na forma de otimizá-los; (iii) garantir a contínua evolução da base de conhecimento (conjunto de documentações e serviços) de TI; (iv) participar da proposta de planejamento orçamentário juntamente com o gerente da área, bem como, controlar a execução orçamentária, e (v) participar do comitê de mudanças da área, analisando o impacto que as mudanças ocasionarão no ambiente de TI.

Na figura 13 apresentam-se os processos críticos de negócio na organização estudada de acordo com os gestores entrevistados.

Figura 13 - Processos críticos de negócio



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

Na seção seguinte, apresenta-se a coleta de dados do presente estudo.

4.1.3 Coleta de Dados

A coleta de dados compreendeu as etapas que são descritas na continuação.

Etapa 1: Verificação do nível de proteção das práticas de segurança

A primeira etapa de coleta de dados foi a aplicação do **instrumento 1**, questionário para verificar o nível de proteção das práticas de segurança recomendadas pela ISO/IEC 27002. Esse instrumento foi aplicado ao Gerente e Supervisor da área de Tecnologia da Informação – TI e pelos Gerentes das áreas de Contabilidade e de Controladoria a fim de avaliarem-se as percepções sobre as práticas de segurança da informação na organização. Para uma melhor interpretação das práticas, foi enviado juntamente com o questionário a norma ISO/IEC 27002.

Domínios da norma (mantido início no item 5 devido que o intervalo de 1 a 4 que é somente introdutório e não considerado o item 9 ao qual trata de segurança física e do ambiente por ser eminentemente técnico):

- *(PL)*: política de segurança da informação;
- *(OI)*: organizando a segurança da informação;
- *(GA)*: gestão de ativos;
- *(RH)*: segurança em recursos humanos;
- *(GO)*: gerenciamento das operações e comunicações;
- *(CA)*: controle de acessos;
- *(AQ)*: aquisição, desenvolvimento e manutenção de sistemas de informação;
- *(GI)*: gestão de incidentes de segurança da informação;
- *(GC)*: gestão da continuidade do negócio;
- *(CF)*: conformidade.

Esse instrumento contempla níveis de proteção das práticas de segurança da informação descritos a seguir. Os gestores classificaram o nível de proteção para cada domínio na organização.

- *proteção inadequada*: não existe nenhum esforço para implementação dos controles recomendados. Produtos e equipamentos certificados não têm qualquer influência na classificação das seções nesse nível;
- *proteção mínima*: a organização adota o mínimo de controles recomendados. Produtos e equipamentos certificados não têm qualquer influência na classificação das seções nesse nível;
- *proteção razoável*: a maioria dos controles são implementados e devem satisfazer os requisitos com base em procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso;
- *proteção adequada*: implementa todos os controles recomendados pelo domínio. Sempre que possível, é obrigatório o uso de produtos e equipamentos certificados;
- *não aplicável*: considerando o segmento ou estrutura da empresa, tal controle não se aplica.

Os gráficos com os resultados da coleta de dados podem ser observados na seção 4.1.4.1 que trata da análise dos dados. As respostas dos questionários podem ser observadas no “anexo a”.

Etapa 2: Entrevista

A segunda etapa de coleta de dados foi a aplicação do instrumento 2, entrevista (anexo c), aplicada aos Gerentes de TI, Controladoria e Contabilidade/Fiscal. A entrevista foi estruturada em três blocos de perguntas, cada bloco voltado a atender aos objetivos propostos pelo estudo para verificar possíveis processos que remetam à integração das áreas de Controladoria e de TI. O objetivo dessa etapa foi o colher subsídios da atuação corporativa destas áreas (Controladoria e TI), ações desencadeadas que sustentem as políticas e normas de segurança da informação, processos principais do negócio e os controles sobre eventuais riscos. Por fim, colher subsídios para o desenvolvimento de um *frame* que demonstre a atuação integrada das áreas de Controladoria e de TI nos processos de avaliação de segurança de informações.

Os dados gerados nessa etapa foram incluídos no *software SPHINX*, que contempla as análises léxicas e de conteúdo, gerando mapas que podem ser observados na seção 4.1.4.2, que trata da análise dos dados.

Etapa 3: Verificação do nível de maturidade processos de TI – AHP

A terceira etapa da coleta de dados foi a aplicação do instrumento 3 (anexo d e página 42), questionário para verificar o nível de maturidade dos processos de TI com base no modelo multicritério AHP direcionado especificamente aos níveis de maturidade co Cobit 4.1. Esse instrumento foi aplicado ao Gerente e Supervisor da área de Tecnologia da Informação – TI a fim de avaliar suas percepções sobre os níveis de maturidade nos diferentes domínios em cada uma das áreas focais de Cobit 4.1 na organização. Para uma melhor interpretação do instrumento, foi efetuada reunião presencial com os gestores para elucidar eventuais dúvidas e esclarecer os objetivos do respectivo instrumento de coleta. Os dados gerados nessa etapa foram incluídos no *software Expert Choice,* ferramenta que implementa a metodologia AHP e podem ser observados na seção 4.1.4.3 que trata da análise dos dados.

Na continuação, inicia-se a seção de análise dos dados. A mesma contempla as análises do nível de proteção das práticas de segurança da informação com base na ISO/IEC 27002, análises das entrevistas a partir dos mapas gerados pelo software *SPHINX* e, por fim, as análises do grau de maturidade nos diferentes domínios em cada uma das áreas focais de Cobit 4.1 com base no modelo multicritério AHP na organização estudada.

4.1.4 Análise dos Dados

Esta seção objetiva apresentar os resultados encontrados por meio dos questionários e entrevista aplicados. As análises do questionário com base na norma ISO/IEC 27002 serviram como diagnóstico do grau de proteção das práticas de segurança da informação, a entrevista segue de acordo com as seções definidas no instrumento de pesquisa com base nos resultados da análise léxica e de conteúdo. As análises do questionário AHP complementar ao Cobit 4.1 serviram para avaliar os níveis de maturidade nos diferentes domínios em cada uma das áreas focais de Cobit 4.1. No que se refere à avaliação de

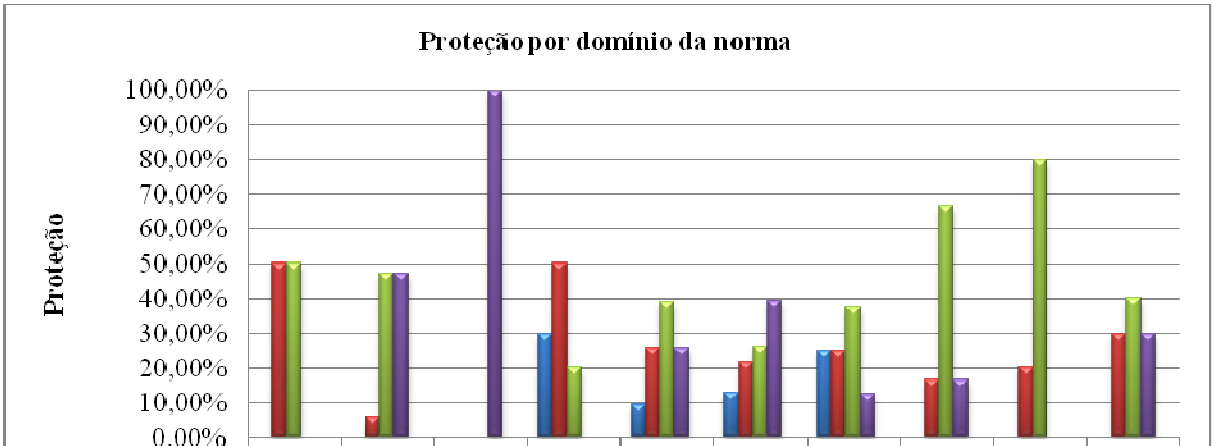
processos de segurança da informação integrando as áreas de Controladoria e de TI, verificou-se procedimentos existentes nesse sentido e oportunidades de aprimorar e sistematizar esse processo.

4.1.4.1 Análise do Nível de Proteção das Práticas de Segurança da Informação com Base na ISO/IEC 27002 - Instrumento 1

Nesta seção, apresentam-se os gráficos gerados a partir da coleta de dados do instrumento 1 e as análises de acordo com a percepção de cada respondente ao grau de proteção referente às práticas da norma ISO/IEC 27002 conforme os domínios utilizados no presente estudo. A ISO/IEC 27002 estabelece as diretrizes e princípios gerais para iniciar, implementar, manter e aperfeiçoar a gestão da segurança da informação em uma organização.

O primeiro gráfico de proteção da informação foi respondido pelo Gerente do Departamento de TI, conforme representação na continuidade.

Figura 14 - Proteção dos domínios da ISO/IEC 270002 na empresa pesquisada – Gerente Departamento de TI



	(PL)	(OI)	(GA)	(RH)	(GO)	(CA)	(AQ)	(GI)	(GC)	(CF)
1 - Inadequada	0,00%	0,00%	0,00%	30,00%	9,68%	13,04%	25,00%	0,00%	0,00%	0,00%
2 - Mínima	50,00%	5,88%	0,00%	50,00%	25,81%	21,74%	25,00%	16,67%	20,00%	30,00%
3 - Razoável	50,00%	47,06%	0,00%	20,00%	38,71%	26,09%	37,50%	66,67%	80,00%	40,00%
4 - Adequada	0,00%	47,06%	100,00%	0,00%	25,81%	39,13%	12,50%	16,67%	0,00%	30,00%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%

Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 14 evidencia os resultados do grau de proteção referente às práticas da norma ISO/IEC 27002, aplicado junto ao Gerente de

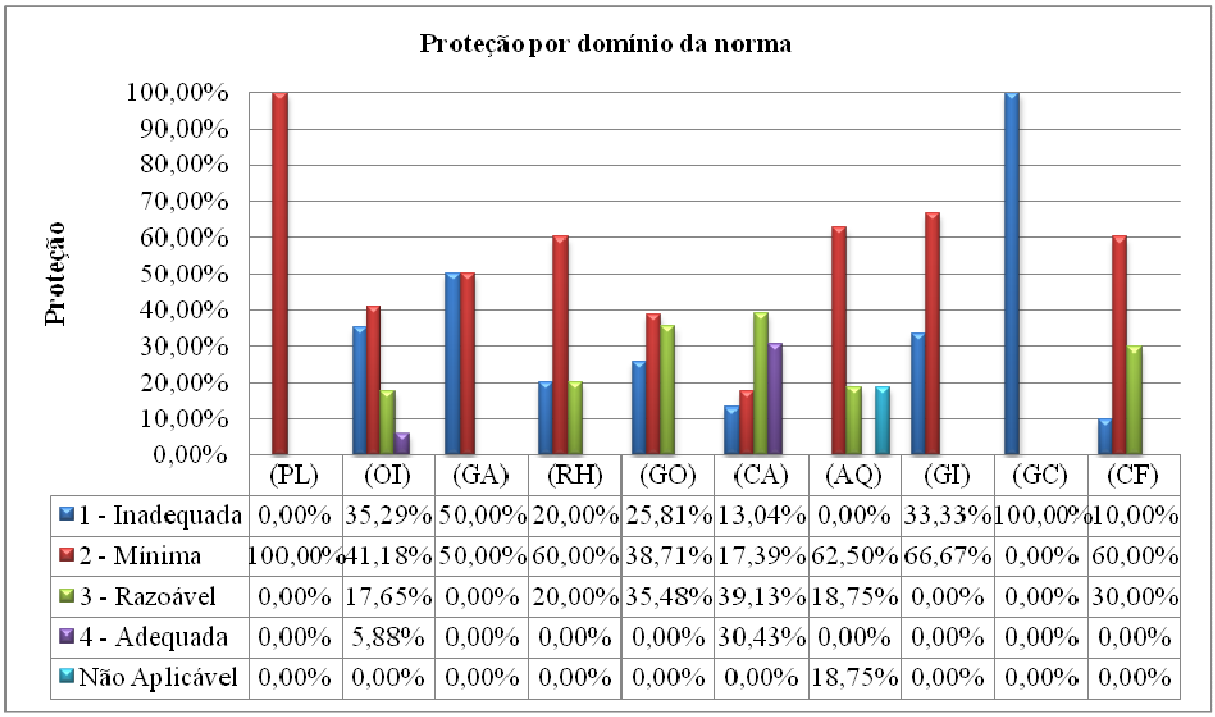
Departamento de TI. Com ele é possível visualizar que o domínio de proteção da informação mais significativo encontrado é o de GA – Gestão de Ativos, que está 100% adequado.

Os domínios de proteção da informação, OI – Organizando a Segurança da Informação, GO - Gerenciamento das operações e comunicações, CA - Controle de acessos, GI - Gestão de incidentes de segurança da informação, GC - Gestão da continuidade do negócio e CF – Conformidade são classificados de razoáveis para adequado.

Os domínios de proteção da informação, PL - Política de segurança da informação, RH - Segurança em recursos humanos, AQ - Aquisição, desenvolvimento e manutenção de sistemas de informação, foram classificados como os mais frágeis na organização quanto a grau de proteção da informação de acordo com a percepção do Gerente de Departamento de TI.

O segundo gráfico de proteção da informação foi respondido pelo Supervisor do Departamento de TI, conforme representação na continuidade.

Figura 15 - Proteção dos domínios da ISO/IEC 270002 na empresa pesquisada – Supervisor Departamento de TI



	(PL)	(OI)	(GA)	(RH)	(GO)	(CA)	(AQ)	(GI)	(GC)	(CF)
1 - Inadequada	0,00%	35,29%	50,00%	20,00%	25,81%	13,04%	0,00%	33,33%	100,00%	10,00%
2 - Mínima	100,00%	41,18%	50,00%	60,00%	38,71%	17,39%	62,50%	66,67%	0,00%	60,00%
3 - Razoável	0,00%	17,65%	0,00%	20,00%	35,48%	39,13%	18,75%	0,00%	0,00%	30,00%
4 - Adequada	0,00%	5,88%	0,00%	0,00%	0,00%	30,43%	0,00%	0,00%	0,00%	0,00%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	18,75%	0,00%	0,00%	0,00%

Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

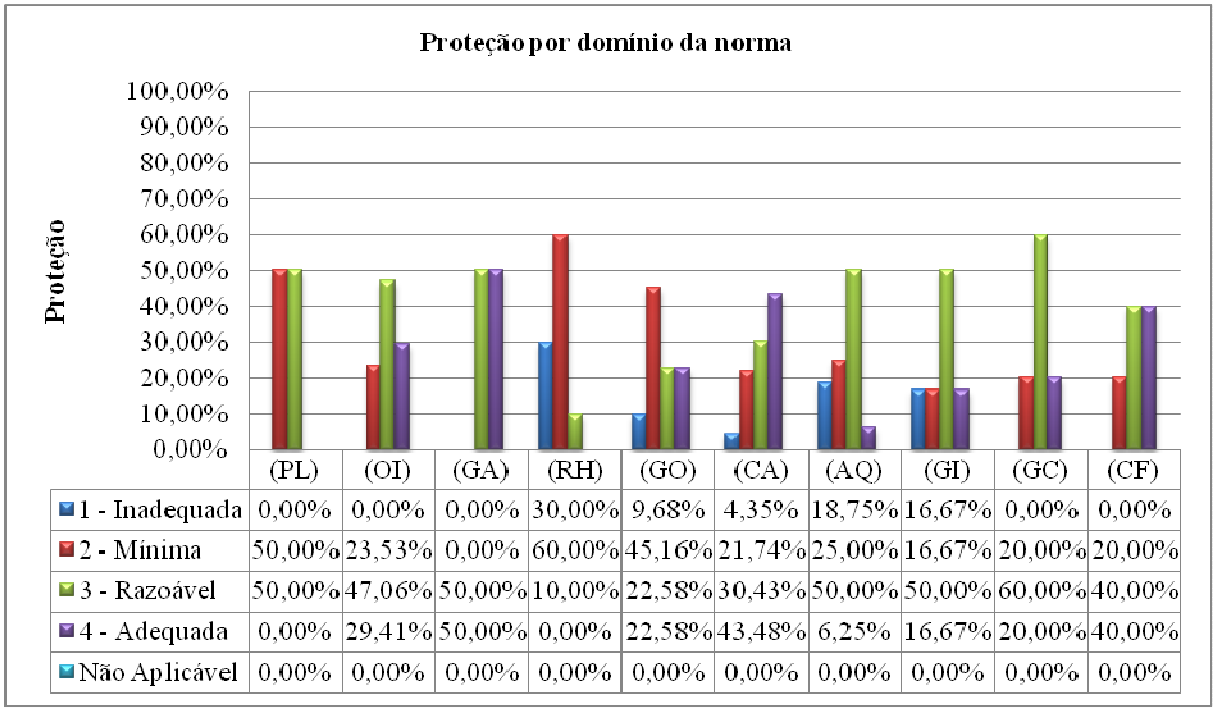
O gráfico da figura 15 evidencia os resultados do grau de proteção referente às práticas da norma ISO/IEC 27002, aplicado junto ao Supervisor de

Departamento de TI. Com ele é possível visualizar que o domínio de proteção da informação mais significativo encontrado é o de CA - Controle de acessos, classificado entre razoável e adequado.

Os domínios de proteção da informação, PL - Política de segurança da informação, OI – Organizando a Segurança da Informação, GA – Gestão de Ativos, RH - Segurança em recursos humanos, GO - Gerenciamento das operações e comunicações, AQ - Aquisição, desenvolvimento e manutenção de sistemas de informação, GI - Gestão de incidentes de segurança da informação, GC - Gestão da continuidade do negócio e CF – Conformidade, são classificados como mínimos ou inadequados quanto ao grau de proteção da informação de acordo com a percepção do Supervisor de Departamento de TI.

O terceiro gráfico de proteção da informação foi respondido pelo Gerente do Departamento de Contabilidade/Fiscal, conforme representação na continuidade.

Figura 16 - Proteção dos domínios da ISO/IEC 270002 na empresa pesquisada – Gerente Departamento de Contabilidade/Fiscal



	(PL)	(OI)	(GA)	(RH)	(GO)	(CA)	(AQ)	(GI)	(GC)	(CF)
1 - Inadequada	0,00%	0,00%	0,00%	30,00%	9,68%	4,35%	18,75%	16,67%	0,00%	0,00%
2 - Mínima	50,00%	23,53%	0,00%	60,00%	45,16%	21,74%	25,00%	16,67%	20,00%	20,00%
3 - Razoável	50,00%	47,06%	50,00%	10,00%	22,58%	30,43%	50,00%	50,00%	60,00%	40,00%
4 - Adequada	0,00%	29,41%	50,00%	0,00%	22,58%	43,48%	6,25%	16,67%	20,00%	40,00%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%

Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

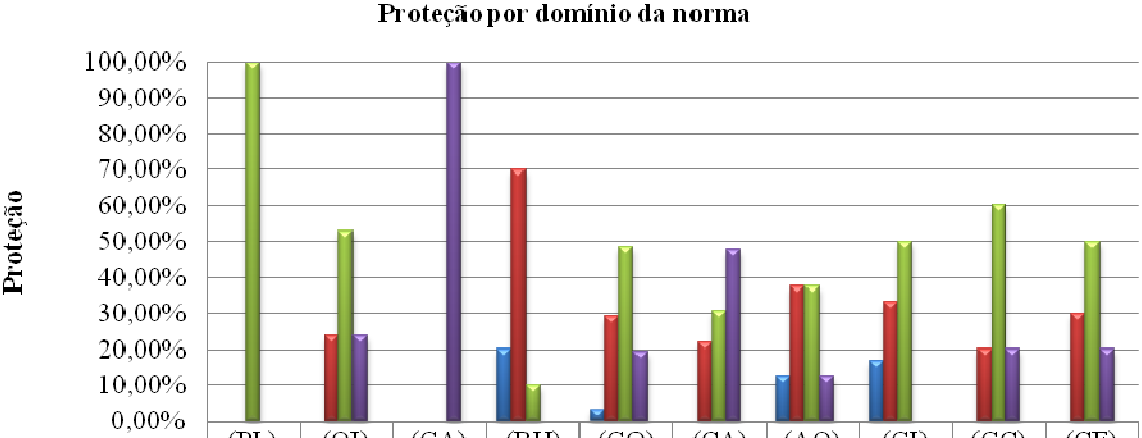
O gráfico da figura 16 evidencia os resultados do grau de proteção referente às práticas da norma ISO/IEC 27002, aplicado junto ao Gerente de Departamento de Contabilidade/Fiscal. Com ele é possível visualizar que os

domínios de proteção da informação, OI – Organizando a Segurança da Informação, GA – Gestão de Ativos, CA - Controle de acessos, GI - Gestão de incidentes de segurança da informação, GC - Gestão da continuidade do negócio e CF – Conformidade, são classificados entre razoável e adequado.

Os domínios de proteção da informação, PL - Política de segurança da informação, RH - Segurança em recursos humanos, GO - Gerenciamento das operações e comunicações, AQ - Aquisição, desenvolvimento e manutenção de sistemas de informação, são classificados como mais frágeis na organização quanto ao grau de proteção da informação de acordo com a percepção do Gerente de Departamento de Contabilidade/Fiscal.

O quarto gráfico de proteção da informação foi respondido pelo Gerente do Departamento de Controladoria, conforme representação na continuidade.

Figura 17 - Proteção dos domínios da ISO/IEC 270002 na empresa pesquisada – Gerente Departamento de Controladoria



	(PL)	(OI)	(GA)	(RH)	(GO)	(CA)	(AQ)	(GI)	(GC)	(CF)
1 - Inadequada	0,00%	0,00%	0,00%	20,00%	3,23%	0,00%	12,50%	16,67%	0,00%	0,00%
2 - Mínima	0,00%	23,53%	0,00%	70,00%	29,03%	21,74%	37,50%	33,33%	20,00%	30,00%
3 - Razoável	100,00%	52,94%	0,00%	10,00%	48,39%	30,43%	37,50%	50,00%	60,00%	50,00%
4 - Adequada	0,00%	23,53%	100,00%	0,00%	19,35%	47,83%	12,50%	0,00%	20,00%	20,00%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%

Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 17 evidencia os resultados do grau de proteção referente às práticas da norma ISO/IEC 27002, aplicado junto ao Gerente de Departamento de Controladoria. Com ele é possível visualizar que o domínio de proteção da informação mais significativo encontrado é o de GA – Gestão de Ativos, que está 100% adequado.

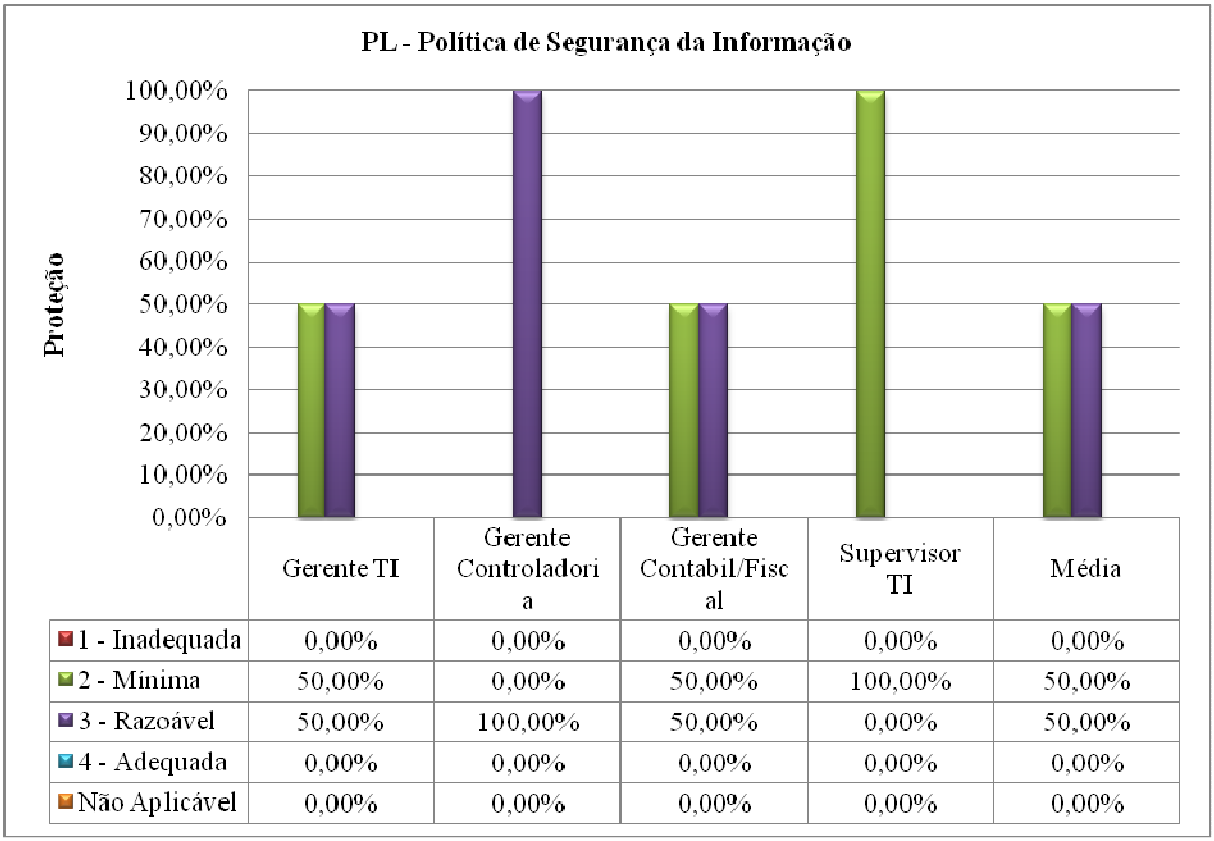
Os domínios de proteção da informação, OI – Organizando a Segurança da Informação, CA - Controle de acessos, GC - Gestão da continuidade do negócio e CF – Conformidade, são classificados de razoáveis para adequado.

O domínio de proteção da informação, PL - Política de segurança da informação, foi classificado 100% como razoável. Os domínios de proteção da informação, RH - Segurança em recursos humanos, GO - Gerenciamento das operações e comunicações, AQ - Aquisição, desenvolvimento e manutenção de sistemas de informação, GI - Gestão de incidentes de segurança da informação, são classificados como mais frágeis na organização quanto ao grau de proteção da informação de acordo com a percepção do Gerente de Departamento de Controladoria.

Na continuidade, são apresentados os gráficos individualizados por DOMÍNIO, na percepção de cada gestor e na média da organização, ao considerar no conjunto, as respostas efetuadas pelos respondentes no que se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002.

O gráfico a seguir se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio PL – Política de Segurança da Informação, de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 18 - Proteção do domínio PL – Política de Segurança da Informação – ISO/IEC 27002



	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	0,00%	0,00%	0,00%	0,00%	0,00%
2 - Mínima	50,00%	0,00%	50,00%	100,00%	50,00%
3 - Razoável	50,00%	100,00%	50,00%	0,00%	50,00%
4 - Adequada	0,00%	0,00%	0,00%	0,00%	0,00%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

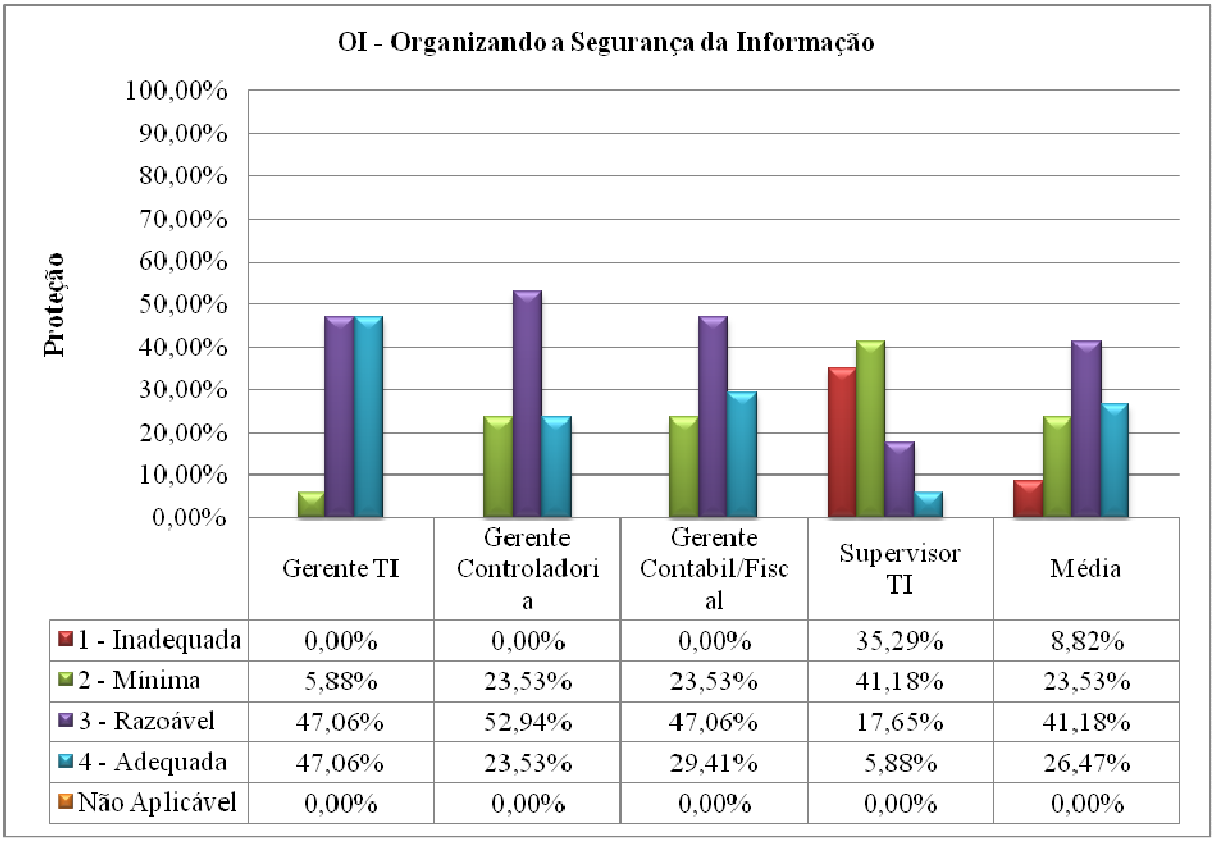
Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 18 evidencia que o Gerente de Controladoria considera como 100% razoável o grau de proteção referente às práticas da norma ISO/IEC 27002 para do domínio PL – Política de Segurança da Informação. Diferentemente das percepções dos Gerentes de TI e de Contabilidade/Fiscal que consideram entre razoável e mínima. O Supervisor de TI considera 100% como sendo nível mínimo de proteção da segurança da informação.

Ao considerar no conjunto as respostas efetuadas pelos respondentes, a média desse domínio está entre razoável e mínima na organização.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio OI – Organizando a Segurança da Informação de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 19 - Proteção do domínio OS – Organizando a Segurança da Informação – ISO/IEC 27002



	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	0,00%	0,00%	0,00%	35,29%	8,82%
2 - Mínima	5,88%	23,53%	23,53%	41,18%	23,53%
3 - Razoável	47,06%	52,94%	47,06%	17,65%	41,18%
4 - Adequada	47,06%	23,53%	29,41%	5,88%	26,47%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

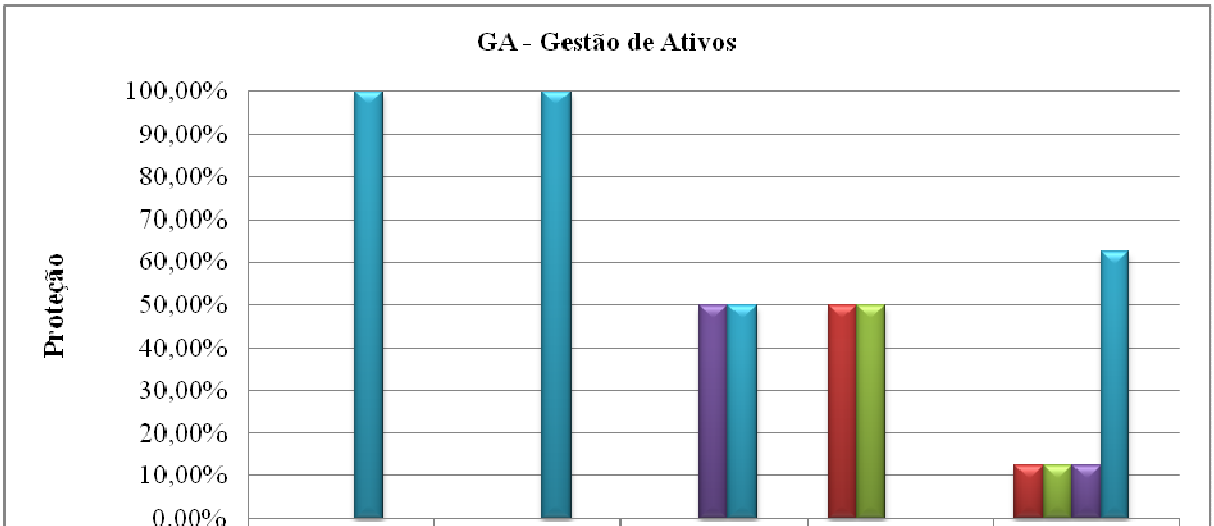
Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 19 evidencia que os Gerentes de TI, de Controladoria e de Contabilidade/Fiscal consideram como sendo razoável e ou adequada o grau de proteção para do domínio OI – Organizando a Segurança da Informação. A percepção do Supervisor de TI considera como sendo de mínima ou inadequada.

Ao considerar no conjunto, as respostas efetuadas pelos respondentes a média desse domínio é razoável na organização.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio GA – Gestão de Ativos, de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 20 - Proteção do domínio GA – Gestão de Ativos – ISO/IEC 27002



	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	0,00%	0,00%	0,00%	50,00%	12,50%
2 - Mínima	0,00%	0,00%	0,00%	50,00%	12,50%
3 - Razoável	0,00%	0,00%	50,00%	0,00%	12,50%
4 - Adequada	100,00%	100,00%	50,00%	0,00%	62,50%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

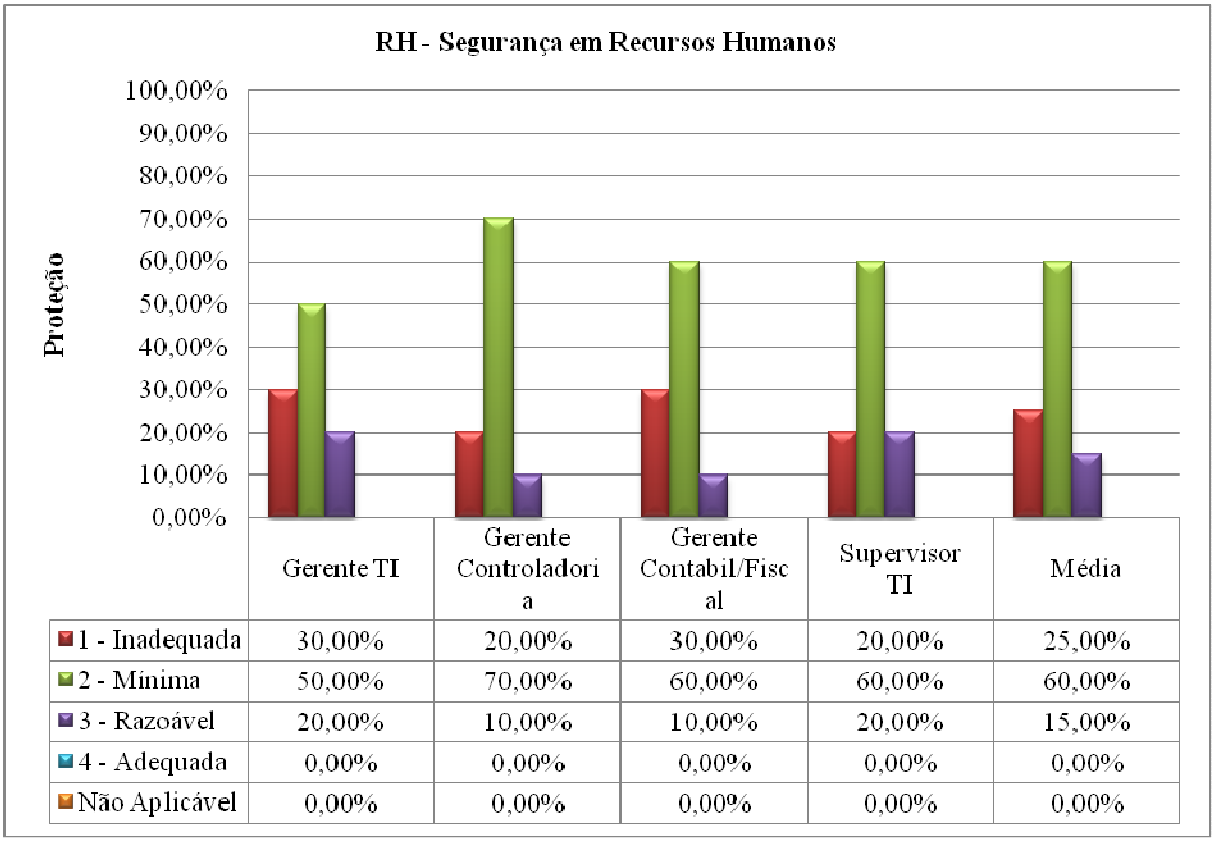
Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 20 evidencia que os Gerentes de TI e de Controladoria consideram como sendo 100% adequada o grau de proteção para do domínio GA – Gestão de Ativos. A percepção do Gerente Contábil/Fiscal considera entre razoável e adequada. O Supervisor de TI considera como sendo mínima ou inadequada.

Ao considerar no conjunto, as respostas efetuadas pelos respondentes a média desse domínio é de adequada na organização.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio RH – Segurança em Recursos Humanos**,** de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 21 - Proteção do domínio RH – Segurança em Recursos Humanos – ISO/IEC 27002



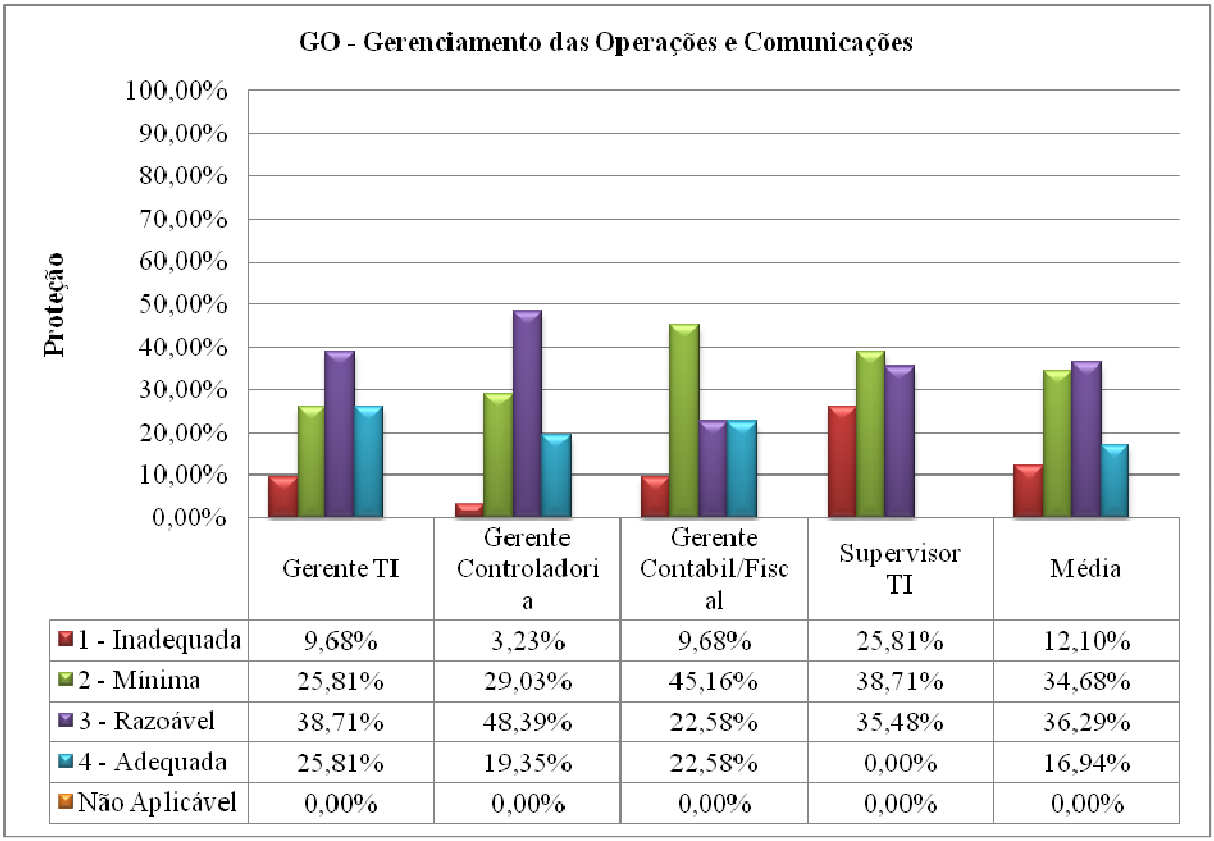
	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	30,00%	20,00%	30,00%	20,00%	25,00%
2 - Mínima	50,00%	70,00%	60,00%	60,00%	60,00%
3 - Razoável	20,00%	10,00%	10,00%	20,00%	15,00%
4 - Adequada	0,00%	0,00%	0,00%	0,00%	0,00%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 21 evidencia que as percepções dos gestores quanto ao grau de proteção para o domínio RH – Segurança em Recursos Humanos, na organização, é mínima.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio GO – Gerenciamento das Operações e Comunicações**,** de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 22 - Proteção do domínio GO – Gerenciamento das Operações e Comunicações – ISO/IEC 27002



	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	9,68%	3,23%	9,68%	25,81%	12,10%
2 - Mínima	25,81%	29,03%	45,16%	38,71%	34,68%
3 - Razoável	38,71%	48,39%	22,58%	35,48%	36,29%
4 - Adequada	25,81%	19,35%	22,58%	0,00%	16,94%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

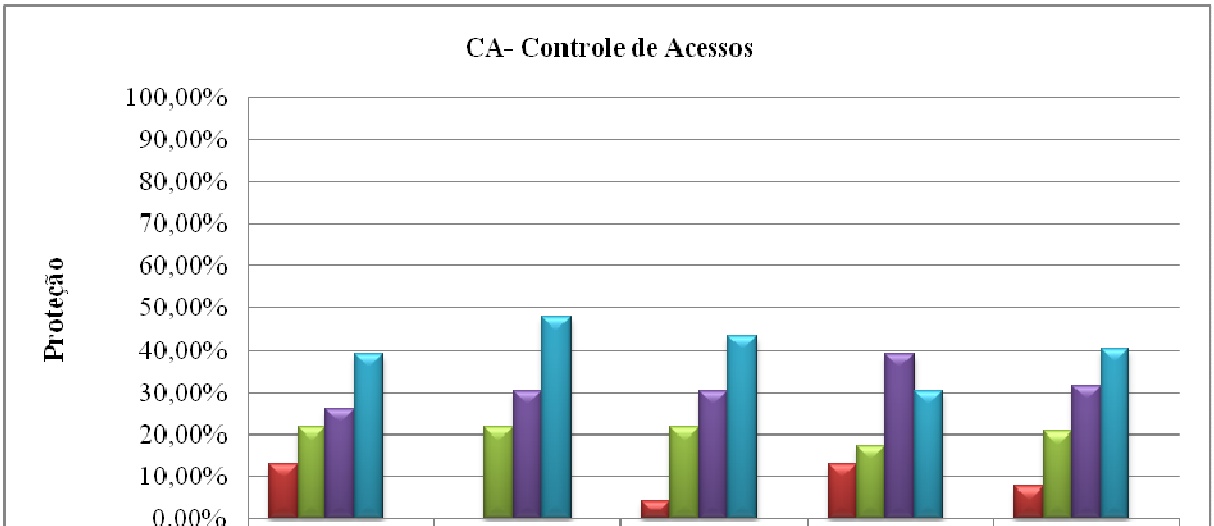
Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 22 evidencia que os Gerentes de TI e de Controladoria percebem como razoável o grau de proteção para do domínio GO – Gerenciamento das Operações e Comunicações. O Gerente Contábil/Fiscal considera como mínima. O Supervisor de TI considera entre razoável e mínima.

Ao considerar no conjunto, as respostas efetuadas pelos respondentes a média desse domínio está entre razoável e mínima na organização.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio CA – Controle de Acessos**,** de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 23 - Proteção do domínio CA – Controle de Acessos – ISO/IEC 27002



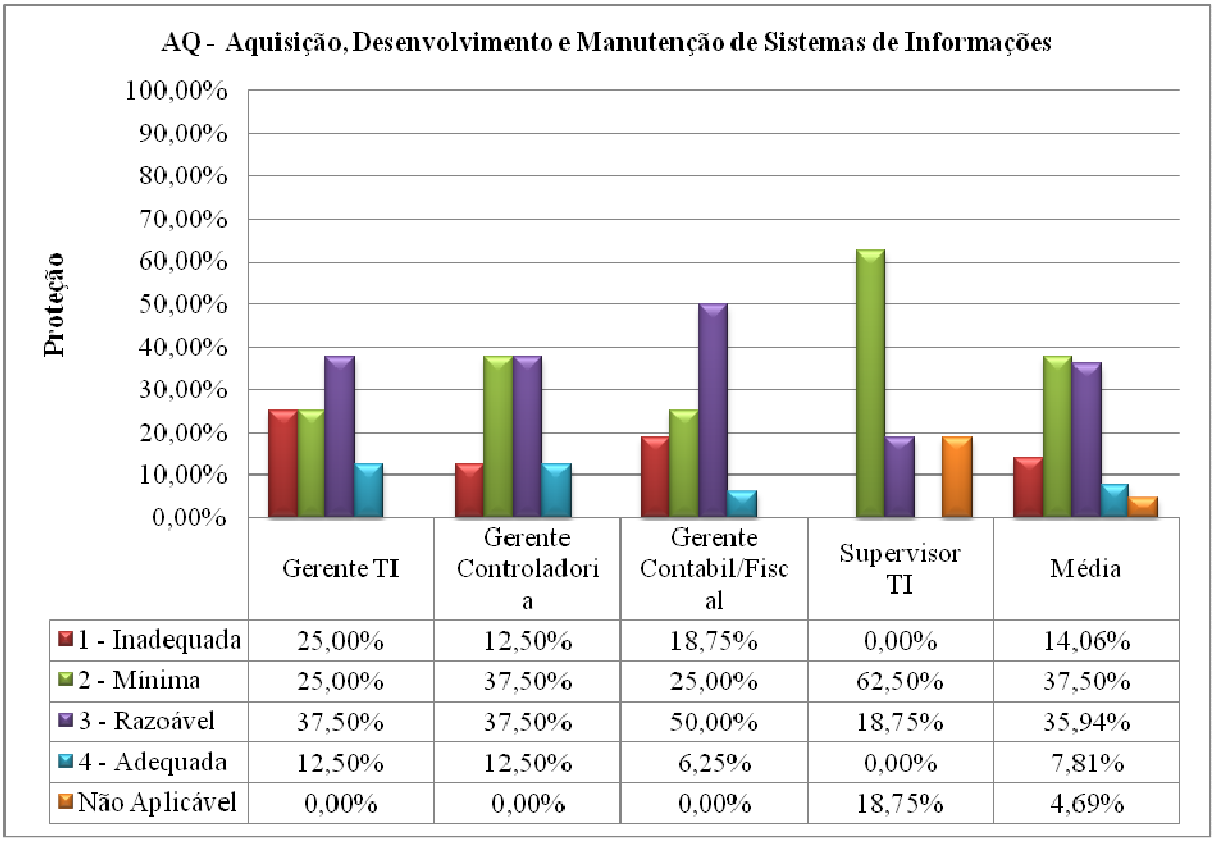
	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	13,04%	0,00%	4,35%	13,04%	7,61%
2 - Mínima	21,74%	21,74%	21,74%	17,39%	20,65%
3 - Razoável	26,09%	30,43%	30,43%	39,13%	31,52%
4 - Adequada	39,13%	47,83%	43,48%	30,43%	40,22%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 23 evidencia que as percepções dos gestores quanto ao grau de proteção para o domínio CA – Controle de Acessos, na organização, é de razoável a adequada.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio AQ – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações**,** de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 24 - Proteção do domínio AQ – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações – ISO/IEC 27002



	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	25,00%	12,50%	18,75%	0,00%	14,06%
2 - Mínima	25,00%	37,50%	25,00%	62,50%	37,50%
3 - Razoável	37,50%	37,50%	50,00%	18,75%	35,94%
4 - Adequada	12,50%	12,50%	6,25%	0,00%	7,81%
Não Aplicável	0,00%	0,00%	0,00%	18,75%	4,69%

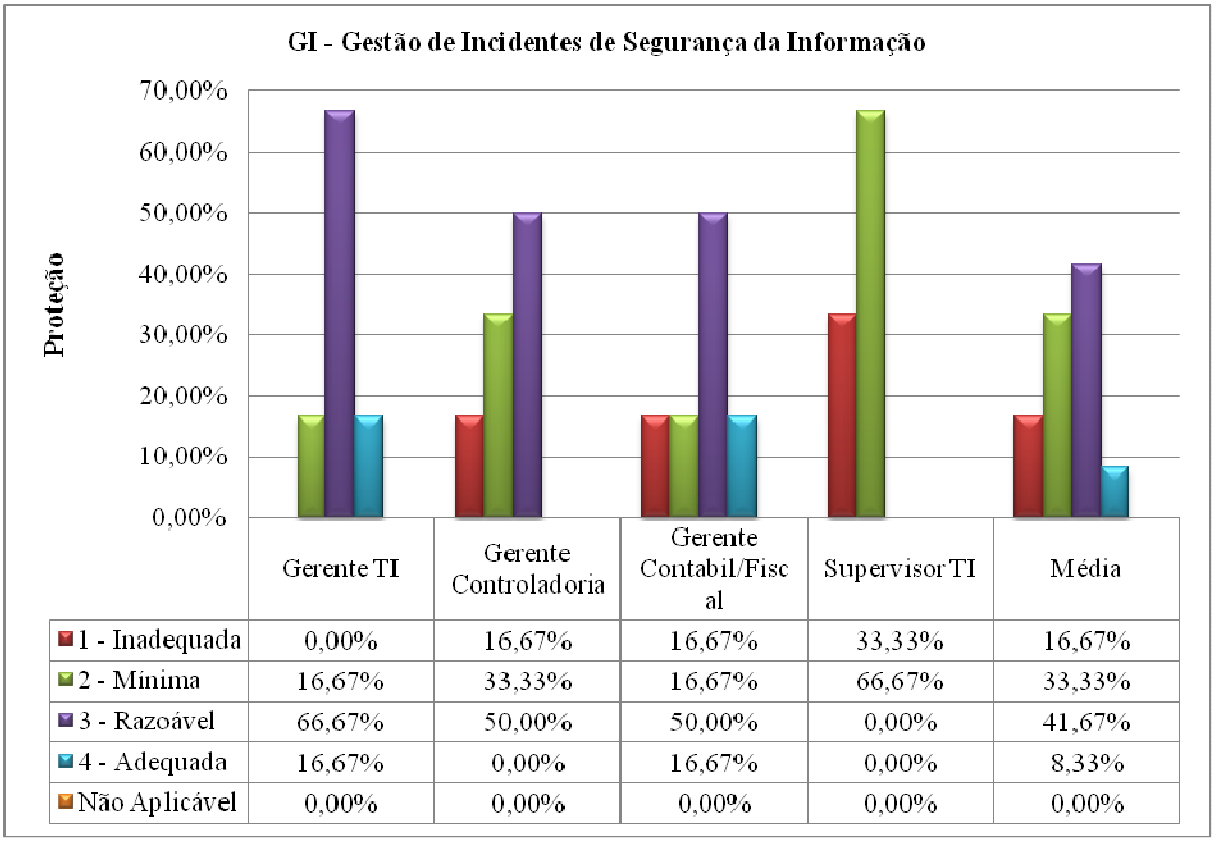
Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 24 evidencia que os Gerentes de TI e de Controladoria percebem entre razoável e mínima o grau de proteção para do domínio AQ – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações. O Gerente Contábil/Fiscal considera razoável. O Supervisor de TI considera mínima.

Ao considerar no conjunto, as respostas efetuadas pelos respondentes a média desse domínio está entre razoável e mínima na organização.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio GI – Gestão de Incidentes de Segurança da Informação**,** de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 25 - Proteção do domínio GI – Gestão de Incidentes de Segurança da Informação – ISO/IEC 27002



	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	0,00%	16,67%	16,67%	33,33%	16,67%
2 - Mínima	16,67%	33,33%	16,67%	66,67%	33,33%
3 - Razoável	66,67%	50,00%	50,00%	0,00%	41,67%
4 - Adequada	16,67%	0,00%	16,67%	0,00%	8,33%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

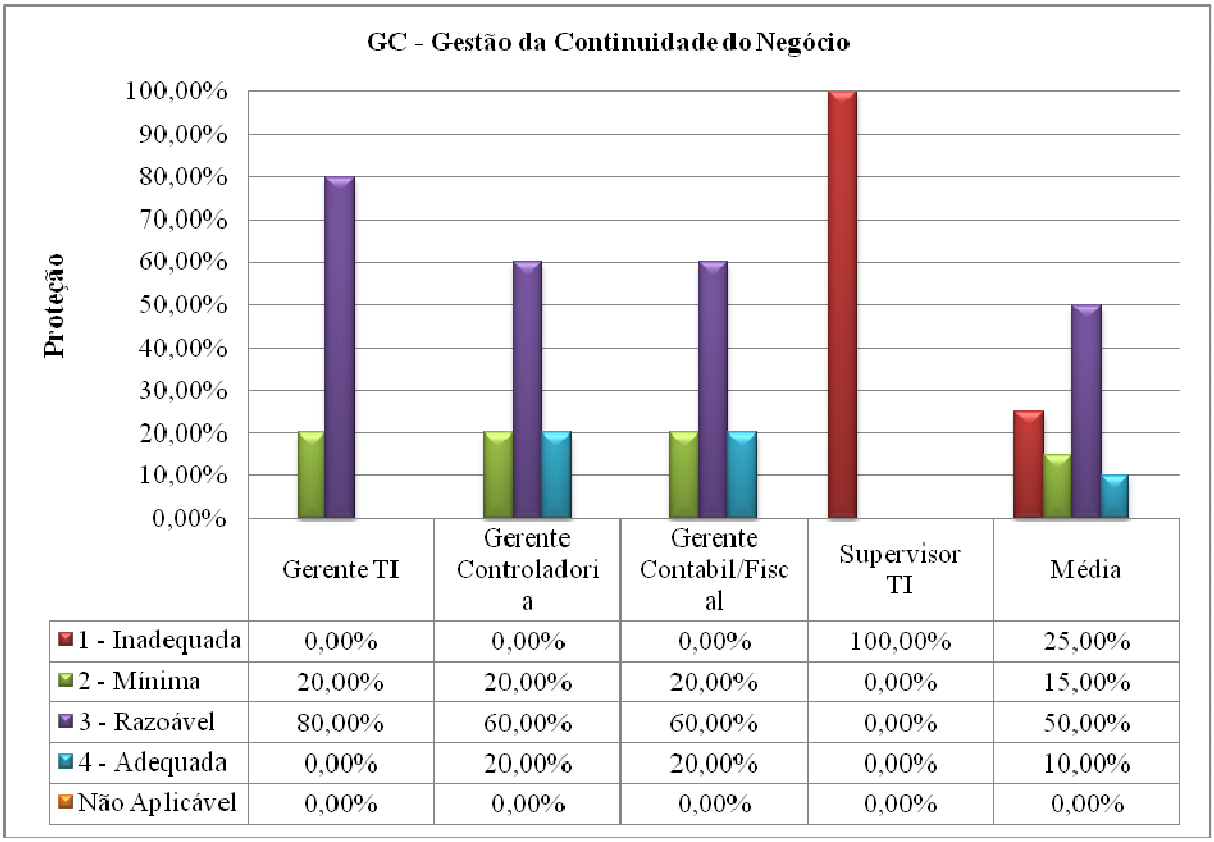
Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 25 evidencia que o Gerente de TI considera razoável o grau de proteção para o domínio GI – Gestão de Incidentes de Segurança da Informação. O Gerente de Controladoria considera como sendo 50% razoável e os demais 50% entre mínima e inadequada. Para Contabilidade/Fiscal, prevalece como sendo razoável. O Supervisor de TI considera como mínima o grau de proteção da segurança da informação para esse domínio.

Ao considerar no conjunto, as respostas efetuadas pelos respondentes a média desse domínio está razoável na organização.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio GC – Gestão da Continuidade do Negócio**,** de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 26 - Proteção do domínio GC – Gestão da Continuidade – ISO/IEC 27002



	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	0,00%	0,00%	0,00%	100,00%	25,00%
2 - Mínima	20,00%	20,00%	20,00%	0,00%	15,00%
3 - Razoável	80,00%	60,00%	60,00%	0,00%	50,00%
4 - Adequada	0,00%	20,00%	20,00%	0,00%	10,00%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

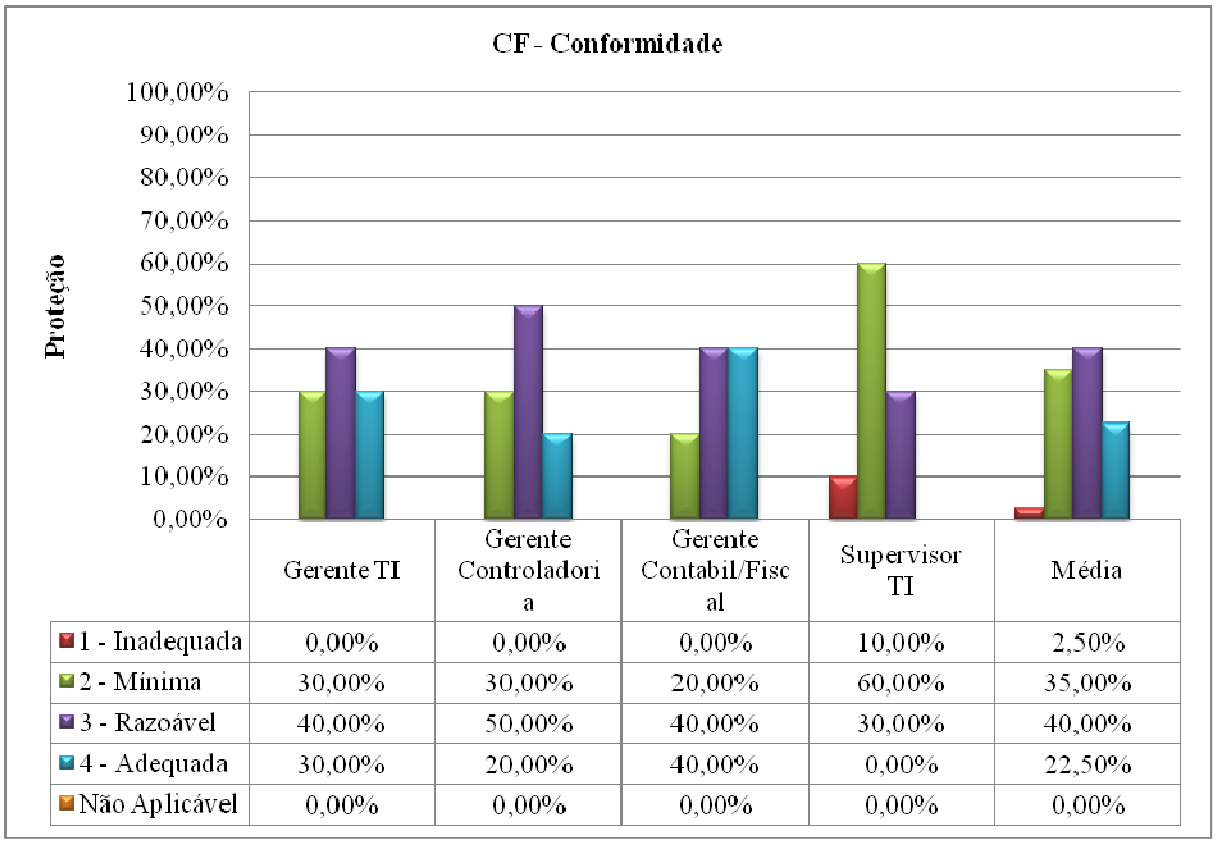
Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 26 evidencia que a percepção dos Gerentes de TI, Controladoria e Contabilidade/Fiscal é de que está razoável o grau de proteção para o domínio GC – Gestão da Continuidade do Negócio. Diferentemente da percepção do Supervisor de TI, o qual considera como sendo 100% inadequada o grau de proteção da segurança da informação para esse domínio.

Ao considerar no conjunto, as respostas efetuadas pelos respondentes a média desse domínio está razoável na organização.

O gráfico representado na continuidade se refere ao grau de proteção quanto às práticas da norma ISO/IEC 27002 do domínio CF – Conformidade**,** de acordo com a percepção dos gestores e na média por nível do domínio na empresa ao considerar no conjunto as respostas efetuadas pelos respondentes.

Figura 27 - Proteção do domínio CF – Conformidade – ISO/IEC 27002



	Gerente TI	Gerente Controladoria	Gerente Contabil/Fiscal	Supervisor TI	Média
1 - Inadequada	0,00%	0,00%	0,00%	10,00%	2,50%
2 - Mínima	30,00%	30,00%	20,00%	60,00%	35,00%
3 - Razoável	40,00%	50,00%	40,00%	30,00%	40,00%
4 - Adequada	30,00%	20,00%	40,00%	0,00%	22,50%
Não Aplicável	0,00%	0,00%	0,00%	0,00%	0,00%

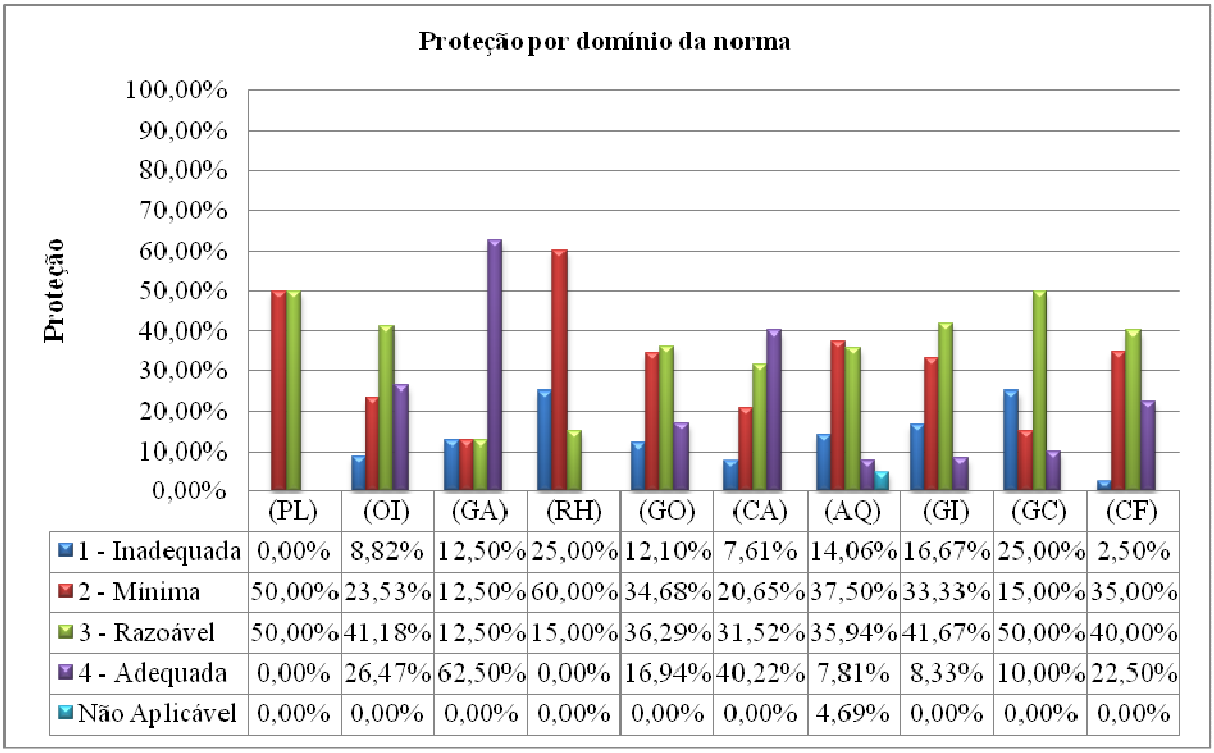
Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 27 evidencia que o Gerente de TI e de Controladoria consideram como razoável o grau de proteção para o domínio CF – Conformidade. O Gerente de Contabilidade/Fiscal considera entre razoável e adequada. Diferentemente é a percepção do Supervisor de TI, o qual considera como mínima o grau de proteção da segurança da informação para esse domínio.

Ao considerar no conjunto, as respostas efetuadas pelos respondentes a média desse domínio está razoável na organização.

Por fim, apresenta-se o gráfico 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, conforme representação na continuidade.

Figura 28 - 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%

Fonte: Elaborado pelo autor a partir dos dados do questionário da norma ISO/IEC 27002

O gráfico da figura 28 evidencia os resultados do grau de proteção médio da organização referente às práticas da norma ISO/IEC 27002. 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 à documentação da política de segurança da informação.

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 - é citads 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.

Dessa 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, princípios básicos para uma informação segura (Cobit 4.1. ITGI, 2007) e atributos da informação da Controladoria (CPC 00, 2008) possam ser afetados.

Isso se denota na percepção dos gestores, conforme respostas ao primeiro instrumento de coleta (anexo a), que consideram que a organização estabelece controles mínimos no que refere-se a: (i) documentação da política de segurança da informação (PL); (ii) papéis 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 da afetação do 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 o controle.

Para Eloff e Eloff (2003), o tema gestão em segurança da informação pode ser abordado sob várias perspectivas; estrategicamente, abordando questões de governança de TI, políticas e problemas de gestão. Outra perspectiva é com foco nos usuários, abordando questões como a cultura de segurança, sensibilização, formação e ética.

A gestão em segurança da informação pode ser eficaz quando abordada de forma integrada nas perspectivas gerencial, técnica e de pessoas. Segundo Spears e Barki (2010), no que se refere à gestão em segurança da informação com ênfase nas pessoas, quando existe processos de desenvolvimento ou alteração de sistemas em que os usuários são envolvidos, os resultados têm sido positivos nas organizações, gerando satisfação e comprometimento.

Na seção seguinte, apresenta-se a análise do segundo instrumento de coleta de dados, a entrevista.

4.1.4.2 Análise das Entrevistas - Instrumento 2

Nesta seção, apresentam-se as análises das entrevistas a partir da Análise de Conteúdo combinada com a Análise Léxica a partir de informações extraídas do *software Sphinx,* que consiste em observar a frequência das palavras para extrair, as que tenham conteúdo no texto. Participaram dessa entrevista os Gerentes de Departamento de TI, Controladoria e Contabilidade/Fiscal.

As respostas dos entrevistados foram primeiramente classificadas conforme sua CATEGORIA (podendo uma mesma resposta apresentar múltiplas categorias), definidas conforme critérios teóricos e contextuais. As CATEGORIAS selecionadas são descritas a seguir:

- alinhamento da comunicação entre usuários chaves, áreas de Controladoria e TI;
- *Business Intelligence – BI* (Sistema de Informações para tomada de decisão);
- controle do processo de alterações de software com especificações de necessidades, objetivos e retorno esperados;
- criar comitê composto pelas áreas de Controladoria e TI para analisar mudanças de software que afetam o negócio;
- direção da empresa influenciando as áreas de gestão com foco nos pilares (processos principais) do negócio – projeto corporativo;
- fatores limitadores da integração entre as áreas de Controladoria e TI;
- gestão holística em Segurança da Informação;
- homologação das alterações de software junto ao usuário solicitante;
- modelagem do sistema informacional da empresa;
- participação usuários nos processos de segurança e disponibilidade de informações;
- políticas e normas de segurança da informação (Controle de acesso, perfis usuários, etc...);
- processos principais da empresa: comprar, estocar, vender, distribuir, pós-venda e tributação;
- requisitos/atributos da informação (Tempestividade, Confiabilidade, Relevância, etc.);
- riscos (Ganhos ou perdas) econômicos e financeiros;
- riscos de integridade das informações – vulnerabilidade;
- treinamentos contínuos e de conscientização junto aos usuários chaves das demais áreas da empresa.

Através da AL, os dados gerados foram cruzados com as categorias classificadas na etapa de análise de conteúdo para fornecerem indícios e evidências sobre o conteúdo do texto.

As análises iniciam a partir da tabela 1, onde são apresentadas as 12 palavras de acordo com a AL que tiveram maior frequência nas respostas dos gestores entrevistados. Na seção 4.2.4.2.1, apresenta-se o mapa da AL, o qual contempla as palavras relacionadas às respostas de cada gestor entrevistado.

Posteriormente na seção 4.2.4.2.2, apresentam-se os mapas (analisados em partes) da AL cruzando com as CATEGORIAS selecionadas através da AC. Por fim na seção 4.2.4.2.3 apresenta-se o mapa da AL cruzando as categorias com as respostas dos gestores entrevistados.

Tabela 1 - Léxicos mais frequentes por gestor entrevistado

Gerente de Contabilidade/Fiscal			Gerente de Controladoria			Gerente de TI			Total
Análise Léxica	Freq.	%	Análise Léxica	Freq.	%	Análise Léxica	Freq.	%	% Citação
Alinhada	**13**	**50,00%**	**Alinhada**	**8**	**30,80%**	Alinhada	5	19,20%	100%
Alteração	11	30,60%	**Alteração**	**13**	**36,10%**	Alteração	12	33,30%	100%
Ambiente	**10**	**37,00%**	Ambiente	8	29,60%	Ambiente	9	33,30%	100%
Áreas	**20**	**36,40%**	Áreas	15	27,30%	**Áreas**	**20**	**36,40%**	100%
Decisão	9	34,60%	Decisão	6	23,10%	**Decisão**	**11**	**42,30%**	100%
Informação	**24**	**35,80%**	**Informação**	**22**	**32,80%**	Informação	21	31,30%	100%
Resultado	**13**	**48,10%**	Resultado	6	22,20%	Resultado	8	29,60%	100%
Risco	9	33,30%	Risco	7	25,90%	**Risco**	**11**	**40,70%**	100%
Segura	13	34,20%	Segura	11	28,90%	Segura	14	36,80%	100%
Sistema	**17**	**37,80%**	**Sistema**	**14**	**31,10%**	Sistema	14	31,10%	100%
TI	**18**	**36,00%**	TI	14	28,00%	**TI**	**18**	**36,00%**	100%
Usuário	13	27,70%	**Usuário**	**18**	**38,30%**	Usuário	16	34,00%	100%

Fonte: Elaborado pelo autor a partir dos dados do Sphinx Léxica versão 5.0

Essa tabela anteriormente representada evidencia que a palavra alinhada (que remete ao alinhamento da comunicação entre as áreas de Controladoria e de TI na organização) foi observada em 50% das respostas do Gerente Contabilidade/Fiscal, seguindo de resultado com 48%. As palavras, sistema, ambiente (que remete ao ambiente organizacional), áreas (que remetem as áreas de Controladoria, TI e demais áreas da organização), TI e informação também foram citadas com relativa frequência nas respostas desse gestor. Essas palavras com maior frequência evidenciam a percepção do gestor quanto à importância do alinhamento entre as áreas e do ambiente organizacional como processos de aproximação das áreas de TI e Controladoria. Isso se evidencia nas respostas do entrevistado.

> *[...] falta de alinhamento quanto à visão de negócio, de priorizar os objetivos gerais e estratégicos da empresa em detrimento das necessidades específicas das áreas. Isto reflete na distância entre o conhecimento das necessidades da gestão e a sua aplicação de forma técnica e operacional [...]* (Ao responder sobre os fatores limitadores nos processos de integração entre as áreas de Controladoria e TI nas alterações de *software*).

> *[...] análises conjuntas entre as áreas de TI e Controladoria sobre os principais processos que tem efeito no resultado da empresa permite um alinhamento das ações de cada área de forma integrada [...]* (Ao responder sobre os processos que possibilitam a integração das áreas de Controladoria e TI).

Os trechos anteriores, extraídos da transcrição da entrevista com o Gerente de Contabilidade/Fiscal da empresa estudada, reiteram as afirmações feitas anteriormente.

Para o Gerente de Controladoria, evidencia-se a palavra usuário como a mais observada nas respostas com 38,3%. As palavras alteração (que remete a alterações de *software*), informação, sistema e alinhada também foram citadas com relativa frequência nas respostas desse gestor. Essas palavras com maior frequência evidenciam a percepção do gestor quanto à importância do alinhamento com os usuários em processos de segurança da informação, por exemplo, alterações de *software*, e a preocupação com a qualidade do sistema de informações da empresa. Isso se evidencia nas respostas do entrevistado.

> *[...] É necessário conhecer o negócio da empresa, pois somente o conhecimento em linguagens de programação limita a integração, podendo ser um fator de retrabalhos em decorrência do fator comunicação entre usuário solicitante de alterações, técnico de TI e a linguagem de negócio da Controladoria. Existindo este alinhamento entende-se que pode-se restringir o número de alterações nos sistemas, porque muitas delas, constata-se que não ajudam na melhoria da atividade da empresa [...]* (Ao responder sobre os fatores limitadores nos processos de integração entre as áreas de Controladoria e TI nas alterações de *software*).

> *[...] Através de uma atuação de validação junto ao usuário chave solicitante da alteração e a equipe da TI. Muitas alterações são demandas para a TI e que não passam por um filtro de validar se estão claras suas contribuições para o negócio da empresa. Se este processo existir sistematicamente, muitas alterações não serão feitas, pois não contribuem com os principais processos ligados ao negócio da empresa e podem-se evitar possíveis vulnerabilidades nos sistemas de informações da empresa [...]* (Ao responder sobre como a Controladoria poderia atuar para evitar possíveis vulnerabilidades no sistema de informação advindos das alterações de *software*).

Os trechos anteriores, extraídos da transcrição da entrevista com o Gerente de Controladoria da empresa estudada, reiteram as afirmações feitas anteriormente.

Para o Gerente de TI, evidencia-se a palavra decisão (que remete ao processo de tomada de decisão na organização) como a mais observada nas

respostas com 42,3%. As palavras risco, áreas e TI também foram citadas com relativa frequência nas respostas desse gestor. Essas palavras com maior frequência evidenciam a percepção do gestor quanto à importância da participação da TI junto às áreas nas solicitações de alterações de *software* que possam afetar o sistema de informações da organização, evitando riscos a partir de decisões equivocadas. Isso se evidencia nas respostas do entrevistado.

> *[...] alterações de sistemas com um processo de análise insuficiente e sem o envolvimento adequado das áreas pode disseminar informações erradas a partir do sistema de informações da empresa para a direção, conselho de administração gerando tomada de decisões equivocadas [...]* (Ao responder sobre como a Controladoria poderia atuar para evitar possíveis vulnerabilidades no sistema de informação advindos das alterações de *software*).

> *[...] Agregar os conhecimentos de áreas que trabalham com a informação, a TI pensando na estrutura física, nas políticas e procedimentos de um processo da segurança da informação eficiente. A Controladoria, visando formatar informações para tomada de decisão permite que se analise e avalie riscos de continuidade de negócio de uma forma mais holística, contribuindo para mitigar riscos [...]* (Ao responder sobre o envolvimento das áreas de Controladoria e TI nas análises e avaliações de riscos de continuidade do negócio no que se refere ao processamento, geração e segurança da informação).

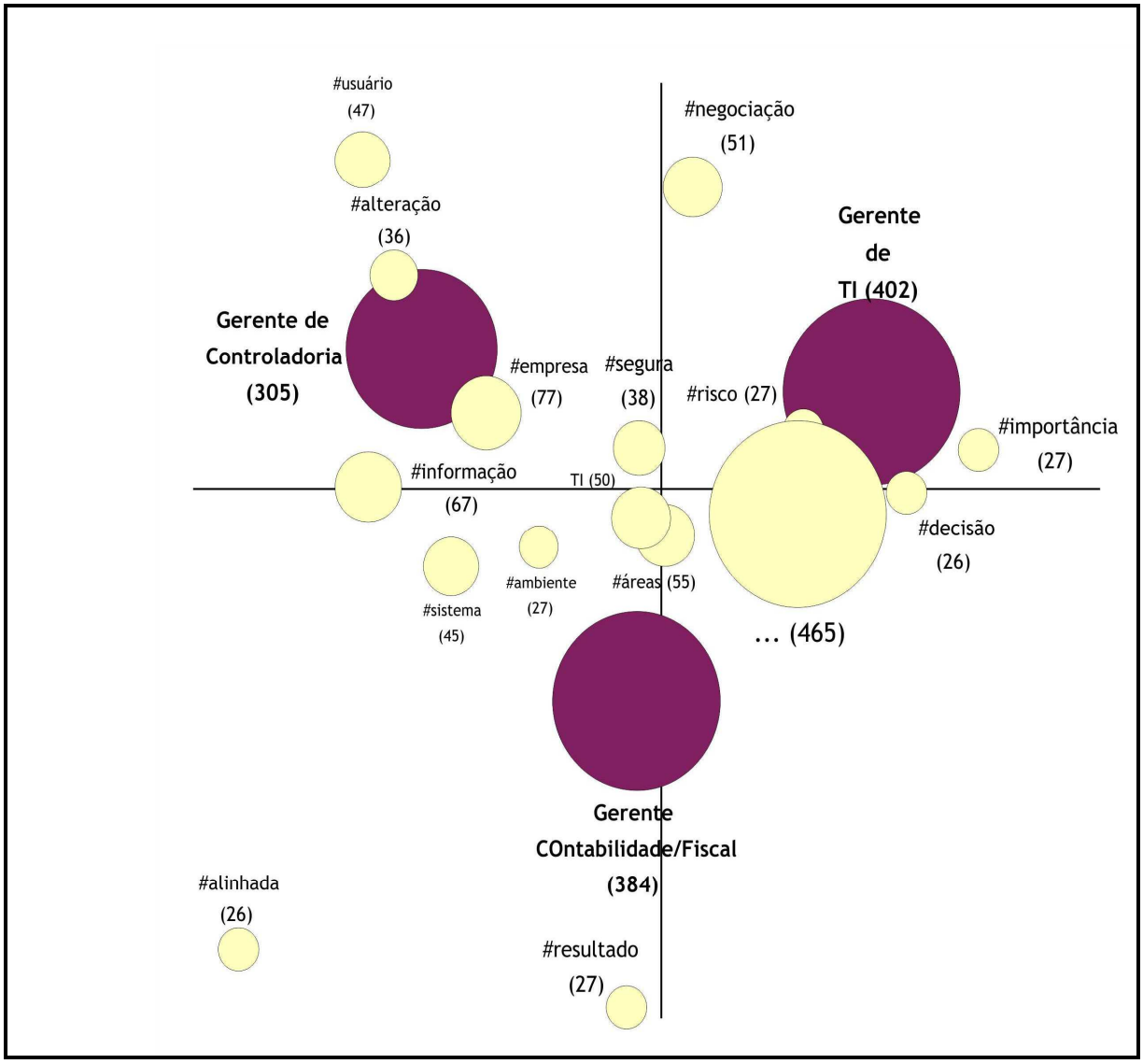
Os trechos anteriores, extraídos da transcrição da entrevista com o Gerente de Controladoria da empresa estudada, reiteram as afirmações feitas anteriormente.

Nas seções a seguir, apresentam-se os mapas resultantes da análise léxica, com uso do software SPHINX, das perguntas relacionadas na seção I, II e III do instrumento de pesquisa (anexo a) e traz a frequência das palavras relacionadas às respostas de cada gestor entrevistado, cruzamento com as categorias selecionadas através da AC, e estas com as respostas dos gestores a cada questionamento. Para facilitar a visualização, os mapas serão analisados em partes. Os mapas completos estão disponíveis no anexo f.

4.1.4.2.1 Análise Léxica por Gestor

O primeiro mapa traz a frequência das palavras relacionadas às respostas de cada gestor entrevistado, conforme representação na continuidade.

Figura 29 - Visualização mapa fatorial – Léxicos *versus* respostas por gestor



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 análises entre os léxicos relacionados às respostas de cada gestor. Percebe-se, por exemplo, a aproximação entre os léxicos, alteração (que remete a alterações de *software*), empresa, usuário e informação muito próximas à categoria Gerente de Controladoria.

Isso demonstra que a Controladoria responde pelas informações para tomada de decisão na organização, tendo a preocupação com processos de segurança de informações como, por exemplo, alteração de *software*, que possam afetar os requisitos da informação, por exemplo, a tempestividade, o equilíbrio custo/benefício, a relevância, a confidencialidade, a integridade, a disponibilidade, a relevância e a confiabilidade da informação. Também é

considerado o aspecto do envolvimento e alinhamento da comunicação com usuários, esses fatores podem contribuir na minimização de riscos para a empresa. Isto se evidencia nas respostas do entrevistado.

> *[...] A Controladoria tem preocupação com relação aos impactos das alterações nos softwares que podem afetar a lucratividade da empresa. Se estas alterações tem influência nos custos das mercadorias, nos controles dos estoques, afetam margens de contribuição deve ter atuação da Controladoria. A Controladoria deve apoiar a TI para filtrar e aprofundar as análises sobre alterações de software [...]* (Ao responder sobre como se daria a participação de Controladoria e TI nas restrições sobre mudanças em pacotes de *software*).
>
> *[...] a área de Controladoria é responsável pelas informações que permeiam e dão suporte a tomada de decisões dos gestores. Desta forma, a Controladoria deve validar junto a TI as informações destinadas aos usuários, estabelecer um alinhamento na comunicação das informações estratégicas que podem impactar em riscos de negócio [...]* (Ao responder sobre o envolvimento das áreas de Controladoria e TI nas análises e avaliações de riscos de continuidade do negócio no que se refere ao processamento, geração e segurança da informação).
>
> *[...] O envolvimento dos usuários com as políticas e normas de segurança da informação propicia um ambiente de maior segurança. Ao transmitir aos usuários o entendimento da complexidade de um ambiente de informação na empresa, e que ele deve contribuir com sugestões para a melhoria deste ambiente, propicia a sua integração com as políticas e normas de segurança da informação ao qual irá gerar um alinhamento aos requisitos de segurança da informação [...]* (Ao responder sobre o entendimento de que a participação e envolvimento dos usuários com as políticas e normas de segurança da informação contribuem com os requisitos de segurança da informação).
>
> *[...] Relevância, tempestividade e confiabilidade. A informação disponibilizada deve estar correta para o usuário. Quando a Controladoria fornece uma informação, esta deve prever estes requisitos [...]* (Ao responder sobre quais os requisitos/atributos considerados pelas áreas de Controladoria e de TI quanto à informação disponibilizada aos seus diversos usuários).

Os trechos anteriores, extraídos da transcrição da entrevista com o Gerente de Controladoria da empresa estudada, reiteram as afirmações feitas anteriormente.

Para a categoria Gerente de Contabilidade/Fiscal, percebe-se a aproximação dos léxicos, ambiente (que remete ao ambiente organizacional), áreas (que remetem as áreas de Controladoria, TI e demais áreas da organização), TI, sistema e resultado.

Isso demonstra que a Contabilidade/Fiscal na empresa entende que os procedimentos de alteração de sistema devem ser analisados pela área de TI, e que devem-se priorizar os que estão relacionados aos objetivos do negócio. Também, a participação da área de Controladoria é importante para contribuir nas análises de impacto para o negócio juntamente com o usuário-chave da área solicitante. Se isso não ocorre, o resultado da empresa pode ser afetado por retrabalhos ou decisões equivocadas advindas por alteração de software. Isso se evidencia nas respostas do entrevistado.

> [...] A Controladoria, por possuir uma visão sistêmica do negócio, pode contribuir com a área de TI a priorizar o desenvolvimento ou alterações nos softwares alinhados com as prioridades estabelecidas no planejamento estratégico, aumentando a assertividade e a qualidade dos dados, transformando a informação útil e precisa para o processo decisório da empresa (diretoria e áreas de gestão) [...] (Ao responder sobre os processos que possibilitam a integração das áreas de Controladoria e TI).

> [...] Envolver os usuários chaves para validar alterações de software, estabelecer uma cultura de arquitetura de processos na empresa, onde especifique as fases a serem cumpridas como, por exemplo, avaliação econômica e financeira do projeto de alteração demandado e se, o mesmo está alinhado com o negócio da empresa. Implementar solicitações de alterações através de um formulário ou documento.... desta forma, entende-se que se minimizariam retrabalhos que impactam nas informações geradas pela Controladoria [...] (Ao responder como a TI poderia atuar para evitar possíveis retrabalhos advindos de erros nas alterações de sistemas/*softwares* que impactam nas atividades operacionais da Controladoria).

Os trechos anteriores, extraídos da transcrição da entrevista com o Gerente de Contabilidade/Fiscal da empresa estudada, reiteram as afirmações feitas anteriormente.

Para a categoria Gerente de TI, percebe-se a aproximação dos léxicos, risco, decisão, importância (que remetem ao sentido de importância para a organização, dos processos de segurança da informação e envolvimento das áreas/usuários), negociação e diversos, estes de menor expressão ao qual não aparecem no mapa, porém aglutinados, foram vinculados à categoria do Gerente de TI. Isso demonstra que a área de TI na empresa atua em processos de segurança da informação, nesse contexto citando, alterações de *software* que afetem o ambiente informacional na organização, as quais possam gerar riscos através de retrabalhos e decisões equivocadas advindas por informações errôneas do sistema informacional. Esse processo de alteração de *software*

requer negociação e envolvimento das áreas/usuários solicitantes. O que se evidencia nas respostas do entrevistado.

> *[...] Um ciclo normal, num processo de alteração de software, consiste inicialmente pela solicitação de alteração de software pelo usuário. A TI procede o entendimento técnico e aprova com o usuário solicitante. Na etapa de homologação existem as principais dificuldades, pois gerar um ambiente fidedigno de testes e envolver as áreas ou usuários chaves é o grande desafio antes de colocar em operação. Portanto, proporcionar um ambiente fidedigno, envolvendo os usuários chaves espera-se qualificar o processo de entrega de TI minimizando retrabalhos e por conseguinte resultando em ganhos financeiros [...]* (Ao responder como a TI poderia atuar para evitar possíveis retrabalhos advindos de erros nas alterações de sistemas/*softwares* que impactam nas atividades operacionais da Controladoria).
>
> *[...] São procedimentos que envolvem a TI e o cliente solicitante da alteração, no qual a TI contata o seu cliente para verificar se as alterações atenderam suas expectativas. Alterações solicitadas e documentadas que possam afetar clientes, produtos ou margem de lucro, recebe uma análise preliminar para avaliar possíveis efeitos que podem afetar tomadas de decisão e evitar riscos ao negócio. Citamos, por exemplo, alterações que afetem a qualidade dos estoques, as margens dos produtos, a imagem da empresa perante a nossa cadeia de valor [...]* (Ao responder sobre quais os procedimentos na organização de análise crítica técnica das aplicações após mudanças no sistema operacional).

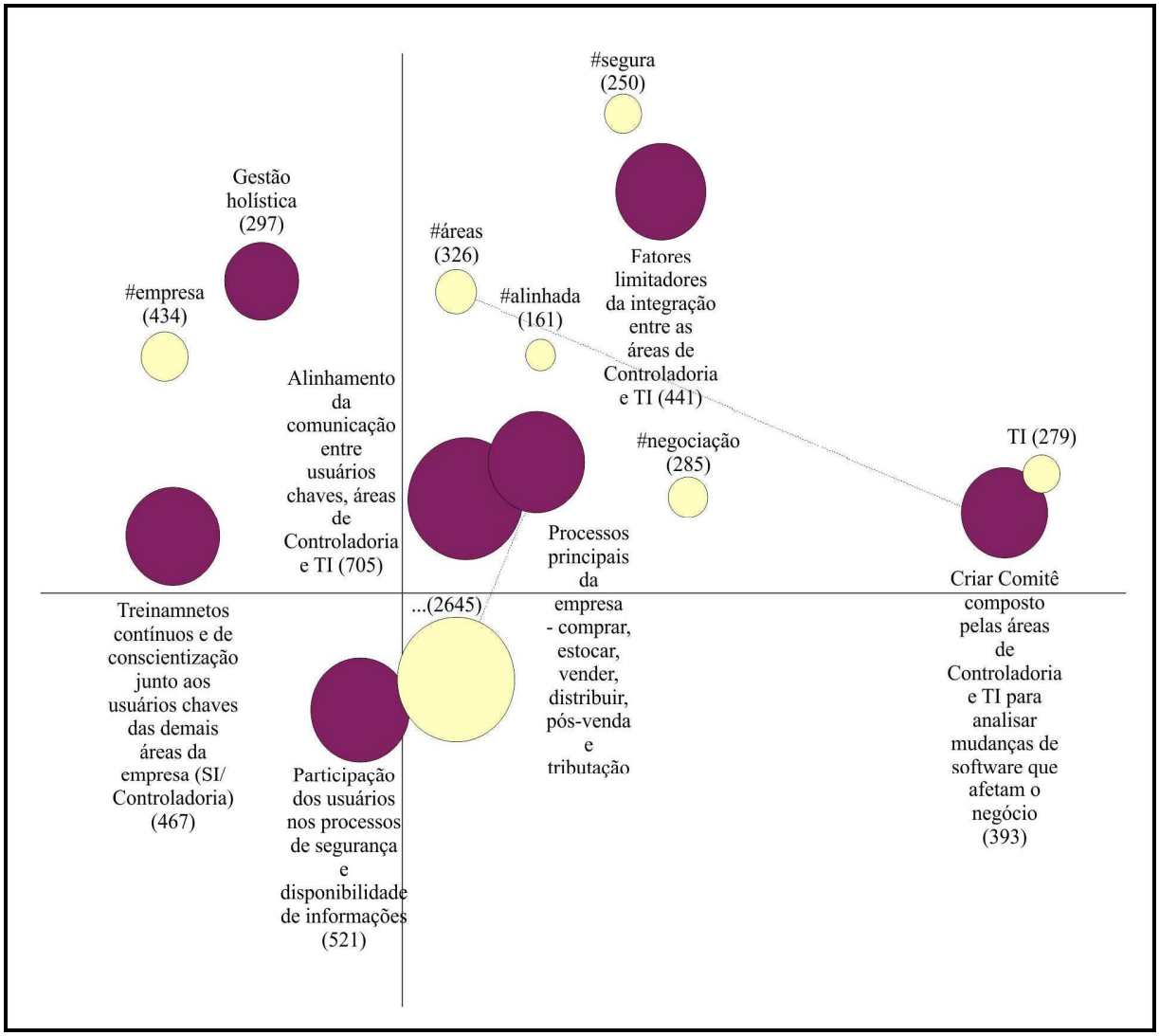
Os trechos anteriores, extraídos da transcrição da entrevista com o Gerente de TI da empresa estudada, reiteram as afirmações feitas anteriormente.

Na seção seguinte apresentam-se os mapas resultantes da análise léxica cruzando com as categorias selecionadas através da AC. Para facilitar a visualização, o mapa será analisado em partes. O mapa completo está disponível no anexo f.

4.1.4.2.2 Análise Léxica Cruzando com Categorias

A primeira parte do mapa traz a visualização da região central contendo frequência das palavras relacionadas às categorias, conforme representação na continuidade.

Figura 30 - Visualização parte mapa fatorial – Léxicos *versus* Categorias



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

A partir da visualização da região central do mapa fatorial anteriormente representado, evidenciam-se variáveis que permitem análises entre os léxicos relacionados às categorias e entre estas, selecionadas nas entrevistas, através da AC.

Podem ser observadas a aproximação do léxico TI e a relação de grande significância do léxico, áreas com a categoria Criar Comitê composto pelas áreas de Controladoria e TI para analisar alterações de software que afetam o negócio. Dessa forma, evidencia-se que a área de TI na organização sinaliza a necessidade de se criar um comitê entre as áreas de Controladoria e TI para analisar conjuntamente as solicitantes as alterações de *software*. Ao mesmo tempo, esse processo poderia possibilitar a integração dessas áreas. Isso pode ser evidenciado na resposta do Gerente de TI da organização.

> [...] Entende-se que o alinhamento da linguagem entre as áreas de Controladoria e de TI seria um processo que possibilitaria a aproximação das áreas. Este processo tende a gerar o entendimento do negócio. Para a realização deste alinhamento, poderíamos criar uma linha ou canal de comunicação, onde a TI juntamente com a Controladoria através de um comitê, passaria a analisar as mudanças de software que afetam o negócio. Contemplando alterações relevantes que afetam o negócio, haveria um processo de homologação. Após, efetuar-se-ia a alteração de software [...] (Ao responder sobre quais seriam os processos que possibilitam a aproximação das áreas de Controladoria e TI).

O trecho anterior, extraído da transcrição da entrevista com o Gerente de TI da empresa estudada, reiteram as afirmações feitas anteriormente.

Observa-se também que a categoria Fatores limitadores da integração entre as áreas de Controladoria e de TI tem muito próximo os léxicos áreas, alinhada (que remete ao alinhamento da comunicação entre as áreas de Controladoria e de TI na organização), segura (que remete a segurança da informação) e negociação. Isso evidencia que, o alinhamento da comunicação entre as áreas de Controladoria e de TI, a negociação e envolvimento das demais áreas da empresa em processos de alteração de *software* podem ser fatores limitadores de integração entre as áreas de Controladoria e de TI na organização. Da mesma forma, esses fatores estão sendo considerados como ações que podem contribuir para o negócio e o ambiente de segurança da informação.

Existe também uma aproximação entre as categorias, Alinhamento da comunicação entre usuários-chave, áreas de Controladoria e de TI, Processos principais da empresa: (i) comprar; (ii) estocar; (iii) vender; (iv) distribuir; (v) pós venda; (vi) tributação e Participação dos usuários nos processos de segurança e disponibilidade de informações, demonstrando que processos de segurança da informação, citado como exemplo, alterações de *software*, para surtirem os efeitos desejados e não afetarem o ambiente da informação, estão intimamente ligadas à necessidade de alinhamento da comunicação entre as áreas de Controladoria, TI, envolvimento dos usuários e atenção nos reflexos que possam afetar os principais processos críticos da empresa, evitando riscos econômico e financeiros para a organização. Como processos críticos e riscos de negócio para a organização, foram citados os processos de comprar, estocar, vender, distribuir, pós-venda e tributação.

Analisando as demais categorias visualizadas no mapa fatorial, fica evidenciado que Gestão holística em segurança da informação e Treinamentos contínuos e de conscientização junto aos usuários-chave das demais áreas da empresa e o léxico empresa estão próximas. Isso demonstra que, ao adotar um processo contínuo de treinamentos junto aos usuários, liderados tecnicamente pelas áreas de Controladoria e de TI, propiciando um ambiente de interação e de participação das demais áreas da empresa, contribuiria com a segurança da informação. Esse processo ainda carece de execução plena na organização, assim sendo, eventualmente ocorrem retrabalhos e um ambiente passível de riscos operacionais. Isto pode ser evidenciado na resposta dos entrevistados.

> *[...] A implementação deveria se dar através de treinamentos contínuos. Estes processos devem ser liderados pelas áreas de Controladoria e de TI, aos quais devem elaborar o material técnico para o treinamento. Nos treinamentos seriam abordados aspectos técnicos da segurança da informação por parte da TI e as questões de negócio quanto à informação para tomada de decisão por parte da Controladoria. Desta forma, entende-se que a conscientização dos usuários faria parte da cultura da organização, se tornando fator chave nos processos de segurança e disponibilidade de informações dentro dos critérios necessários para a tomada de decisão [...]* (Ao responder 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).

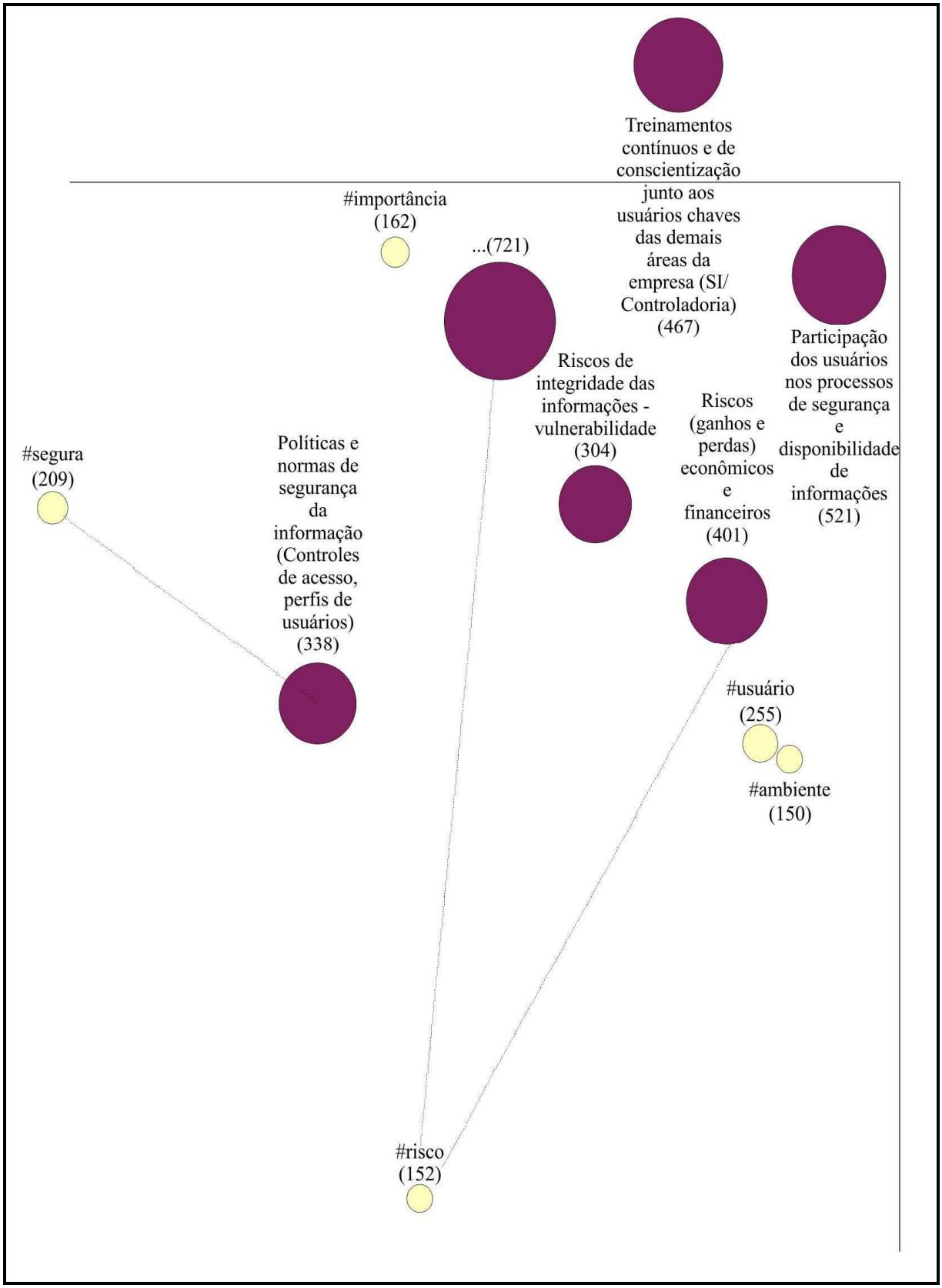
> *[...] A gestão holística é extremamente relevante para as áreas de Controladoria e de TI. Nos processos atuais essa prática é incipiente, devido à falta de treinamentos, a rotatividade e disseminação da conscientização dos usuários. Uma política de segurança da informação para ser eficaz tem nos usuários seu principal aliado, e atualmente o cenário é de que estes usuários atuam operacionalmente de forma muito pontual, devido à falta de treinamentos [...]* (Ao responder se as áreas de Controladoria e de TI consideram relevante adotar uma gestão holística para tornar as implementações de segurança da informação mais eficazes).

> *[...] A gestão holística está vinculada as ações que possibilitam integrar as áreas aos objetivos da empresa, conectando as implementações de segurança da informação. Permite visualizar e analisar o status atual da empresa, projetando o que se pretende implementar para buscar a eficácia em qualquer implementação que envolva a segurança da informação. Ainda temos um cenário de departamentalização muito forte, que muitas vezes se preocupam somente com seu universo, com suas informações [...]* (Ao responder se as áreas de Controladoria e de TI consideram relevante adotar uma gestão holística para tornar as implementações de segurança da informação mais eficazes).

Os trechos anteriores, extraídos da transcrição das entrevistas com os gestores da empresa estudada, reiteram as afirmações feitas anteriormente.

A segunda parte do mapa traz a visualização que contém a frequência das palavras relacionadas às categorias também relevantes para o estudo, conforme representação na continuidade.

Figura 31 - Visualização parte mapa fatorial – Léxicos *versus* Categorias



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

A partir da visualização da região do mapa fatorial anteriormente representado, evidenciam-se variáveis que permitem análises entre os léxicos relacionados às categorias e entre estas, selecionadas nas entrevistas através da AC.

Pode ser observada a aproximação entre as categorias Riscos de integridade das informações – vulnerabilidade, Riscos econômicos e financeiros, Participação dos usuários nos processos de segurança da informação e Treinamentos contínuos e de conscientização aos usuários-chave e dessas categorias, com os léxicos usuários, ambiente (que remete ao ambiente organizacional) e risco. Dessa forma, evidencia-se que ações de inserção e de conscientização dos usuários na política de segurança da informação aliadas a treinamentos contínuos contribuem para minimizar riscos ao ambiente informacional, quer por acessos indevidos ou por alterações de *software*. A existência eventual de vulnerabilidades no sistema informacional da organização pode gerar riscos econômicos e financeiros para a organização. Isso pode ser evidenciado nas respostas dos entrevistados.

> *[...] A informação é um ativo importante para a empresa. Para evitar riscos de vazamento de informações devem-se ter políticas e procedimentos claros sobre acesso e trabalhar continuamente a conscientização dos usuários. Muitas informações são valiosas para o mercado, por exemplo, uma base de 5 milhões de clientes, quanto vale no mercado? Se eventualmente, um usuário com acesso indevido à base de informações pode gerar um risco intangível para a empresa. Informações relevantes devem ser identificadas pela empresa e determinar seu acesso a um número de usuários restrito, conscientizá-los [...]* (Ao responder sobre quais os procedimentos adequados para evitar o risco de vazamento de informações relevantes).

> [...] Adotando uma política de controle sobre o fluxo de informações estratégicas da empresa que contemple responsabilidades. Na política, contemplar a segmentação de controle de acesso por usuário atrelado ao perfil de usuário vinculado a função ou cargo. Disseminar a conscientização corporativa e comunicar os parceiros externos sobre tal política, pois muitas negociações estratégicas que tem impacto no negócio são sigilosas [...] (Ao responder sobre quais os procedimentos adequados para evitar o risco de vazamento de informações relevantes).

> *[...] A importância estratégica da segurança da informação é considerada um requisito básico. A segurança física é de responsabilidade da área de TI com apoio de uma auditoria para analisar de forma sistemática se estão sendo adotadas as melhores práticas de segurança da informação como, por exemplo, acessos adequados, realização de backups das informações. A Controladoria por municiar com informações a tomada de decisões dos gestores, em especial as decisões estratégicas do conselho de administração e diretoria, atua para que o ambiente da informação seja seguro e estável [...]* (Ao responder sobre qual a percepção das áreas de Controladoria e de Ti em relação ao tema segurança da informação e sua importância estratégica para a empresa).

> *[...] o ambiente da informação, a segurança da informação, está interligado com a credibilidade das áreas de TI e Controladoria que são as gestoras do ambiente informacional na empresa [...]* (Ao responder sobre qual a percepção das áreas de Controladoria e de Ti em relação ao tema segurança da informação e sua importância estratégica para a empresa).

Os trechos anteriores, extraídos da transcrição das entrevistas com os gestores da empresa estudada, reiteram as afirmações feitas anteriormente.

Observa-se também que a categoria Políticas e normas de segurança da informação possui uma relação de grande significância com o léxico segura (que remete a segurança do ambiente da informação). Isso evidencia que as políticas e normas de segurança da informação que a organização adota estão intimamente relacionadas à proteção do ambiente da informação. Além disto, aponta que as decisões das políticas de segurança na organização devem privilegiar a inserção e envolvimento dos usuários. O que pode ser evidenciado nas respostas dos entrevistados.

> *[...] A inserção dos usuários e sua responsabilidade no contexto global da empresa seria um fator primordial nas políticas de segurança da informação para as empresas [...]* (Ao responder sobre de que forma poderia ser implementado um processo de conscientização, educação e treinamento em segurança da informação nas áreas da empresa?).

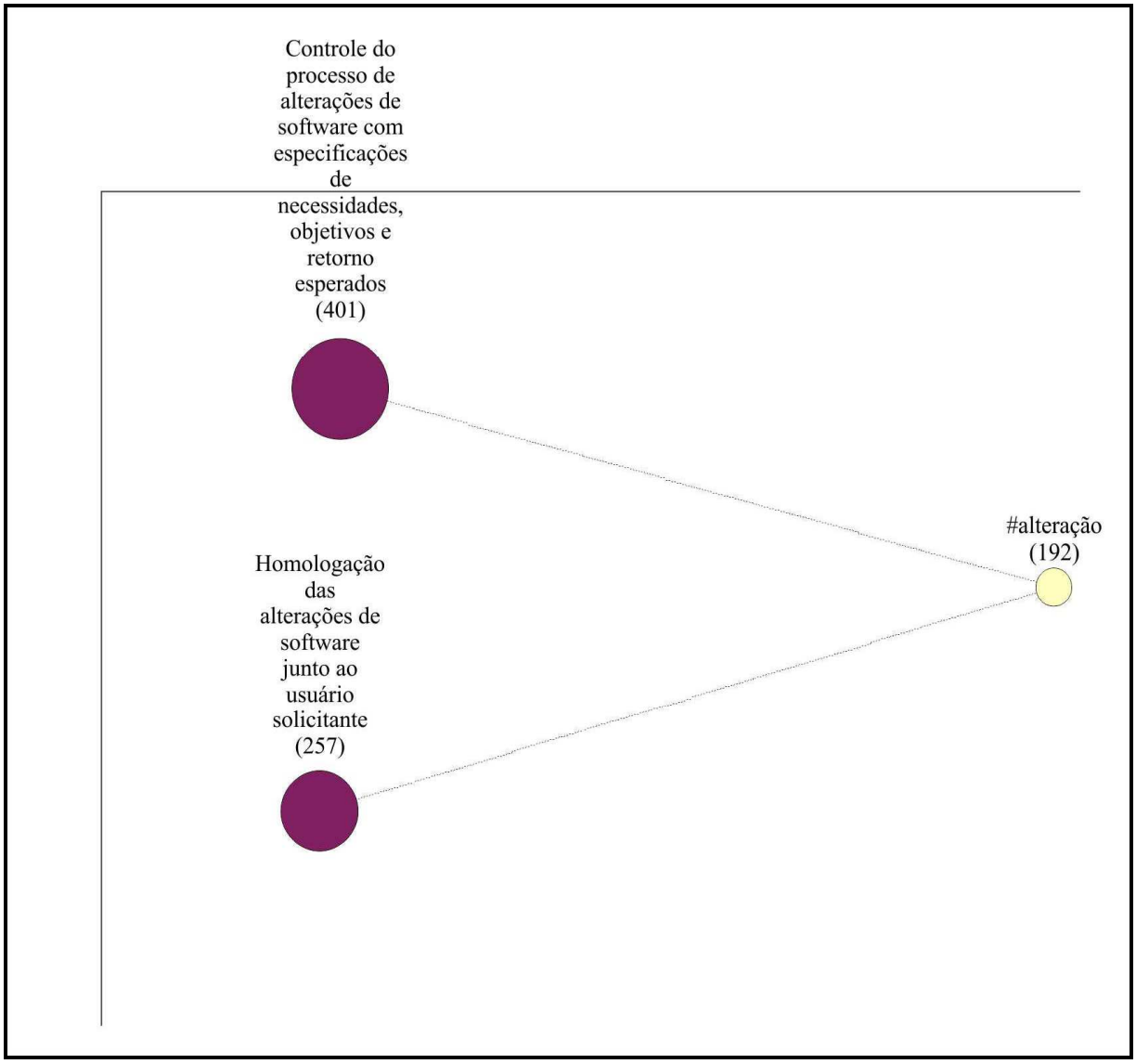
> *[...] O processo de conscientizar os usuários de que as informações geradas por eles são extremamente importantes para as decisões tomadas na empresa, fazendo-se sentir como parte integrante do processo, gera comprometimento e maior zelo e deve estar contemplado nos treinamentos e na forma de comunicar isto a nível corporativo. Assim, entende-se que estas ações contribuem para solidificar as políticas de segurança da informação [...]* (Ao responder sobre qual o entendimento sobre a participação das áreas de Controladoria e de TI na elaboração de treinamentos para usuários a fim de garantir a segurança de informações).

> *[...] O envolvimento e a participação de usuários nas políticas de segurança da informação contribuem de forma decisiva para a sua eficácia. Os processos que permeiam a empresa tem verticalidade, eles nascem numa área e interligam-se com as demais áreas da empresa. Para ter este envolvimento e participação se faz necessário treinamento de forma sistemática com uma comunicação clara do que realmente é importante. O usuário é uma das peças chaves para o sucesso de uma política de segurança da informação [...]* (Ao responder se é entendimento que a participação e envolvimento dos usuários com as políticas e normas de segurança da informação contribuem com os requisitos de segurança da informação).

Os trechos anteriores, extraídos da transcrição das entrevistas com os gestores da empresa estudada, reiteram as afirmações feitas anteriormente.

A última visualização do mapa referente cruzamento dos léxicos com as categorias é representado na continuidade.

Figura 32 - Visualização parte mapa fatorial – Léxicos *versus* Categorias



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

A partir da visualização de parte do mapa fatorial anteriormente representado, evidenciam-se variáveis que permitem análises entre o léxico alteração (que remete a alterações de *software*) e as categorias Controle do processo de alterações de *software* com especificações de necessidades, objetivos e retorno esperados e Homologação das alterações de *software* junto ao usuário solicitante.

Essa relação de grande significância evidencia que a organização atua no ambiente de controle sobre solicitações de alterações de *software* e na homologação junto ao usuário solicitante. Esse processo se realiza através de ferramentas de TI como, por exemplo, registros de log de auditoria e na inserção dos usuários. Posteriormente ao desenvolvimento da alteração os usuários

participam e validam o desenvolvimento alinhando às suas expectativas. Contudo, a empresa não tem procedimentos formais descritos para esse processo.

> *[...] O fluxo de uma alteração passa pelo controle sobre as versões de softwares, para identificar a área solicitante, analisar juntamente com o usuário solicitante as alterações solicitadas. Após desenvolve-se as alterações, faz-se os testes. Porém, o ambiente de testes pode não refletir adequadamente o ambiente oficial gerando falhas ao quais somente serão percebidas após entrada no ambiente oficial. Com os registros (log) de auditoria, permite identificar qual era a versão anterior do programa e imediatamente substituir a versão do programa com erro. A área de TI consegue através do log, identificar qual usuário e área solicitou a alteração, qual o programador que fez a alteração, ou seja, contribui com a gestão da área de TI [...]* (Ao responder na percepção da TI de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área).
>
> *[...] É entendimento que a responsabilidade da homologação é do usuário final, pois, a TI faz o processo de desenvolvimento do software a partir da solicitação do usuário, analisa, aprova juntamente com o usuário, faz os testes, denominados de "testes unitários". Quando a TI entende que está adequado, disponibiliza para o ambiente de homologação onde o usuário chave solicitante analisa se os objetivos foram atingidos pelas alterações solicitadas. Importante que a Controladoria participe deste processo principalmente em alterações que afetem os pilares do negócio da empresa quais sejam clientes, produtos e margens de lucro [...]* (Ao responder se após as alterações no sistema operacional, entende-se que se deve efetuar testes envolvendo usuários responsáveis pela gestão de informações para validar tais alterações).
>
> *[...] Os usuários responsáveis devem participar desde o início do processo de alterações no sistema operacional. Devem realizar as definições de escopo das alterações, estabelecer possíveis efeitos estruturais não planejados. Participar dos testes necessários para identificar possíveis falhas no desenvolvimento efetuado pela equipe técnica da TI até o processo de homologação das alterações [...]* (Ao responder se após as alterações no sistema operacional, entende-se que devem-se efetuar testes envolvendo usuários responsáveis pela gestão da informações para validar tais alterações).

Os trechos anteriores, extraídos da transcrição das entrevistas com os gestores da empresa estudada, reiteram as afirmações feitas anteriormente.

Na seção seguinte, apresenta-se o mapa resultante da análise léxica por gestor cruzando com as categorias selecionadas através da AC.

A partir das análises de temas como alinhamento da comunicação, envolvimento de usuários-chave, treinamentos, criação de comitê e gestão holística na segurança da informação são relacionados a fatores que podem contribuir com a integração das áreas de Controladoria e TI para aprimorar

processos de alteração de *software*, requer primeiramente a compreensão da gestão sobre quais ações podem ser implementadas.

Segundo Bulgurcu, Cavusoglu e Benbasat (2010), é importante os gestores compreenderem quais fatores motivam os usuários a cumprir com as políticas de segurança da informação, a partir dessa compreensão, diagnosticar deficiências para fornecer meios que as minimizem. Para Spears e Barki (2010), os gestores em segurança da informação podem aproveitar a conformidade regulamentar como uma oportunidade para envolver usuários e aumentar a consciência organizacional em segurança da informação, alinhando a política de segurança aos objetivos de negócios.

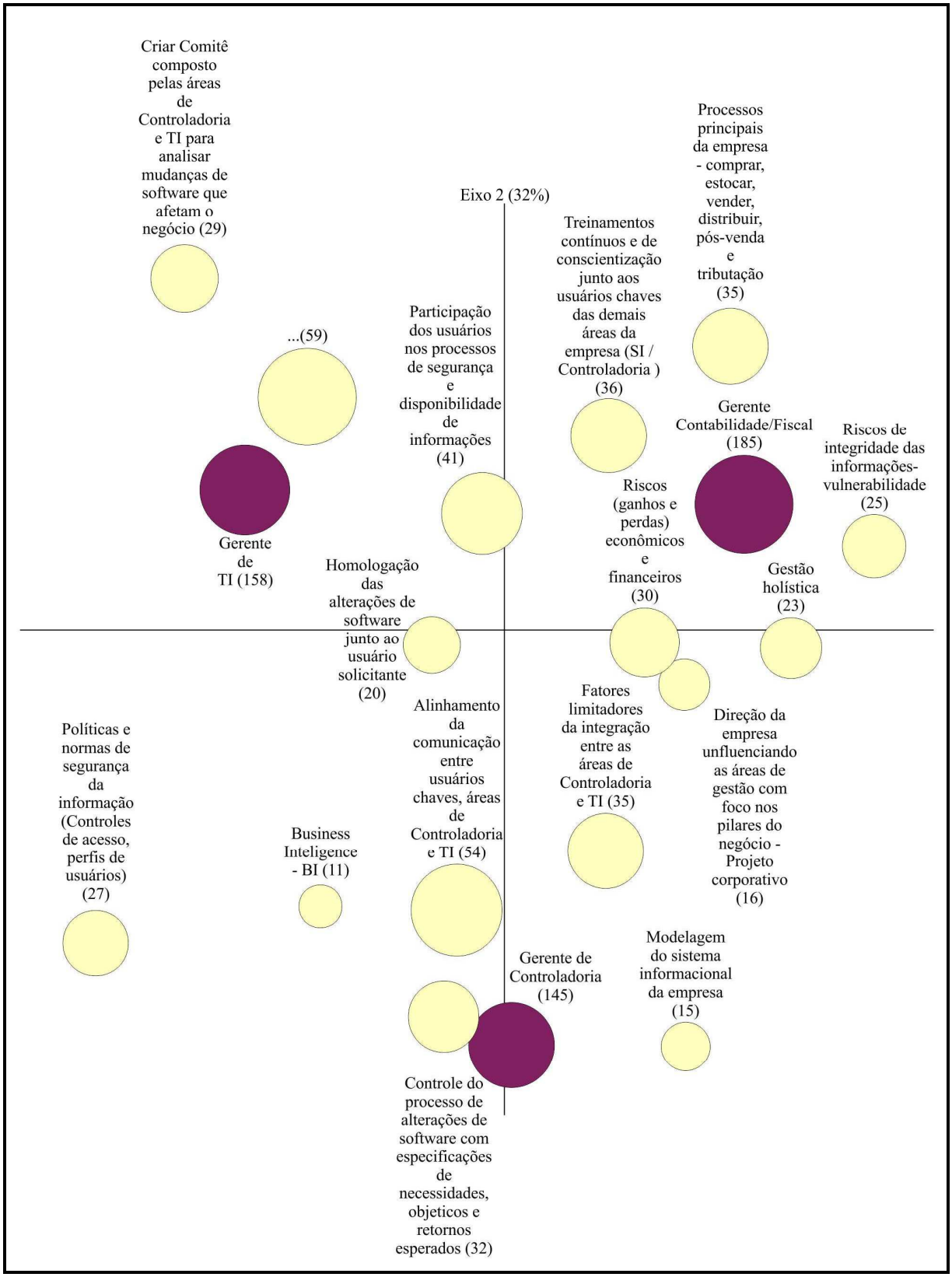
Conforme Eloff e Eloff (2003), as organizações devem adotar uma gestão holística da segurança da informação, propiciando mudanças de paradigmas, contribuindo para estabelecer um sistema de gestão da segurança de informações a fim de proteger o ativo informação. Cabe a Controladoria contribuir com esse processo através de uma atuação participativa, estimulando a interação das áreas e o comprometimento dos usuários com o sistema de informações da empresa. Nesse sentido, Borinelli (2006, p. 208) cita que a Controladoria tem como uma de suas missões a de promover, coordenar e integrar os esforços das partes que formam o todo organizacional.

Na seção seguinte, apresenta-se o mapa resultante da análise léxica cruzando as categorias com as respostas dos gestores.

4.1.4.2.3 Análise Léxica por Gestor Cruzando com Categorias

A visualização do mapa contém frequência a partir da análise léxica das respostas dos gestores relacionadas às categorias, conforme representação na continuidade.

Figura 33 - Visualização mapa fatorial – Categorias por Gestor



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 as categorias de acordo com a

percepção de cada gestor dentro da sua área de atuação relacionadas 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 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, a categoria alinhamento da comunicação entre usuários-chave, áreas de Controladoria e TI é um fator que pode contribuir ou limitar a integração das áreas de Controladoria, porém minimiza eventos que afetem o sistema de informações na organização. Quanto aos processos de segurança da informação, relacionam-se as categorias: (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. As categorias; modelagem do sistema informacional da empresa e *Business Intelligence – BI* foram citadas 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, previsto x realizado 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/Fiscal relaciona a categoria 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, as categorias 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 da empresa podem 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).

Na seção seguinte apresenta-se a análise do terceiro instrumento de coleta de dados, o questionário Cobit 4.1 – AHP.

4.1.4.3 Análise do Questionário Cobit – AHP – Instrumento 3

Para cada uma das áreas de foco, implementou-se uma estrutura hierárquica de domínios e processos utilizando o *software Expert Choice* (ver figuras 34 e 35), com o qual foram calculados os pesos associados a cada processo (ver tabela 2).

Figura 34 - Estrutura hierárquica do modelo Cobit 4.1

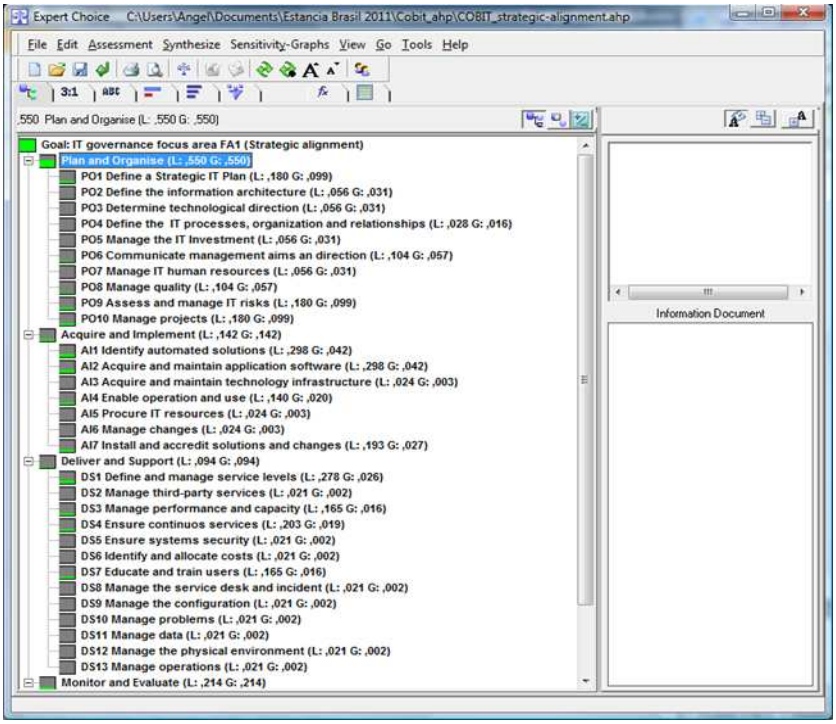
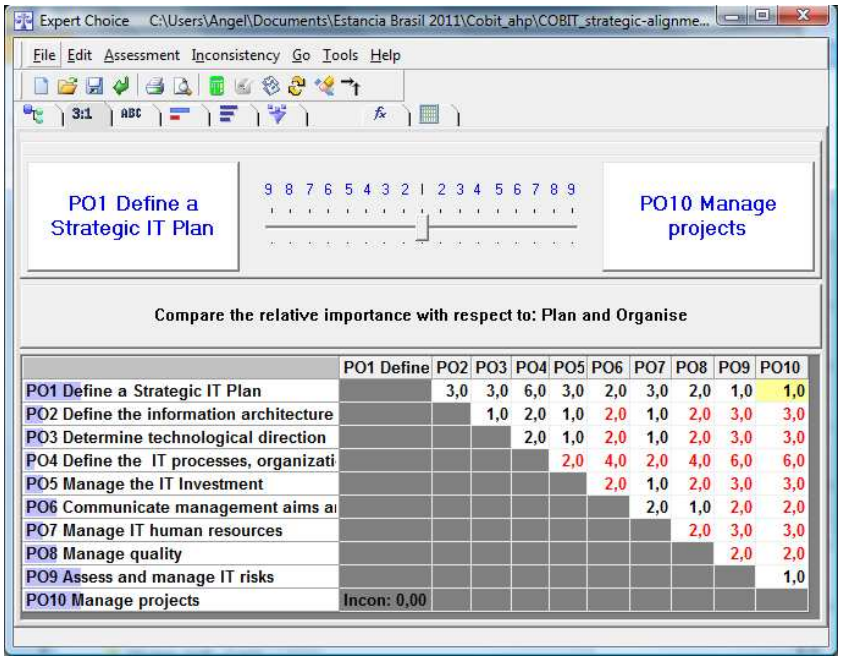


Figura 35 - Comparações *pairwise* dos processos



Os pesos associados a cada processo (ver tabela 3) correspondem a valores dos processos e domínios em diferentes áreas focais, definidos após a definição das matrizes de comparação.

Tabela 2 - Valores de peso de processos e domínios em diferentes áreas focais após a definição das matrizes de comparação

Dominios / Áreas Focais	Alinhamento Estratégico		Entrega de Valor		Gestão de Recursos		Gestão de RISCOS		Mensuração Desempenho	
Planejamento e Organização		**0,55**		**0,119**		**0,271**		**0,3**		**0,188**
PO1	0,18	0,099	0,019	0,002	0,162	0,044	0,127	0,038	0,028	0,005
PO2	0,056	0,031	0,122	0,014	0,102	0,028	0,047	0,014	0,028	0,005
PO3	0,056	0,031	0,159	0,019	0,214	0,058	0,079	0,024	0,028	0,005
PO4	0,028	0,016	0,019	0,002	0,105	0,029	0,079	0,024	0,028	0,005
PO5	0,056	0,031	0,256	0,03	0,105	0,029	0,012	0,004	0,26	0,049
PO6	0,104	0,057	0,019	0,002	0,015	0,004	0,168	0,05	0,028	0,005
PO7	0,056	0,031	0,019	0,002	0,105	0,029	0,047	0,014	0,22	0,041
PO8	0,104	0,057	0,159	0,019	0,015	0,004	0,079	0,024	0,028	0,005
PO9	0,18	0,099	0,019	0,002	0,015	0,004	0,237	0,071	0,028	0,005
PO10	0,18	0,099	0,211	0,025	0,162	0,044	0,127	0,038	0,323	0,061
Aquisição e Implementação		**0,142**		**0,261**		**0,191**		**0,08**		**0,063**
AI1	0,298	0,042	0,167	0,044	0,135	0,026	0,251	0,02	0,067	0,004
AI2	0,298	0,042	0,167	0,044	0,018	0,003	0,251	0,02	0,067	0,004
AI3	0,024	0,003	0,018	0,005	0,135	0,026	0,025	0,002	0,067	0,004
AI4	0,14	0,02	0,098	0,026	0,081	0,015	0,173	0,014	0,067	0,004
AI5	0,024	0,003	0,098	0,026	0,278	0,053	0,025	0,002	0,067	0,004
AI6	0,024	0,003	0,285	0,074	0,218	0,041	0,025	0,002	0,067	0,004
AI7	0,193	0,027	0,167	0,044	0,135	0,026	0,251	0,02	0,6	0,038
Entrega e Suporte		**0,094**		**0,451**		**0,418**		**0,425**		**0,375**
DS1	0,278	0,026	0,119	0,054	0,14	0,058	0,011	0,005	0,233	0,087
DS2	0,021	0,002	0,071	0,032	0,051	0,021	0,082	0,035	0,099	0,037
DS3	0,165	0,016	0,045	0,02	0,081	0,034	0,055	0,023	0,099	0,037
DS4	0,203	0,019	0,119	0,054	0,081	0,034	0,131	0,056	0,144	0,054
DS5	0,021	0,002	0,01	0,005	0,01	0,004	0,194	0,082	0,014	0,005
DS6	0,021	0,002	0,045	0,02	0,081	0,034	0,011	0,005	0,099	0,037
DS7	0,165	0,016	0,071	0,032	0,051	0,021	0,055	0,023	0,014	0,005
DS8	0,021	0,002	0,071	0,032	0,01	0,004	0,011	0,005	0,099	0,037
DS9	0,021	0,002	0,119	0,054	0,14	0,058	0,082	0,035	0,014	0,005
DS10	0,021	0,002	0,119	0,054	0,01	0,004	0,082	0,035	0,144	0,054
DS11	0,021	0,002	0,19	0,086	0,214	0,089	0,194	0,082	0,014	0,005
DS12	0,021	0,002	0,01	0,005	0,051	0,021	0,082	0,035	0,014	0,005
DS13	0,021	0,002	0,01	0,005	0,081	0,034	0,011	0,005	0,014	0,005
Monitoramento		**0,214**		**0,169**		**0,12**		**0,195**		**0,375**
ME1	0,224	0,048	0,219	0,037	0,373	0,045	0,14	0,027	0,45	0,169
ME2	0,035	0,008	0,309	0,052	0,049	0,006	0,2	0,039	0,05	0,019
ME3	0,37	0,079	0,034	0,006	0,049	0,006	0,33	0,064	0,05	0,019
ME4	0,37	0,079	0,438	0,074	0,53	0,064	0,33	0,064	0,45	0,169

Os pesos anteriormente apresentados permitem avaliar o nível de importância de cada processo para atingir o objetivo global de alcançar um modelo de governança de TI eficaz e eficiente na área focal selecionada, sendo que, neste trabalho, enfatiza-se a área focal relacionada a RISCO.

Duas entrevistas foram realizadas com o Gerente e Supervisor de TI da empresa. Ambos os gestores foram convidados a realizar uma estimativa do nível de maturidade em sua organização para cada um dos 34 processos definidos no Cobit. Utilizou-se então a escala 0-1 de maturidade e diretrizes de avaliação conforme critérios definidos pelo Cobit. A correspondência entre a escala de 0-1 utilizada e os níveis de maturidade é mostrada na tabela 3.

Tabela 3 - Níveis de maturidade de processos de TI – Cobit 4.1

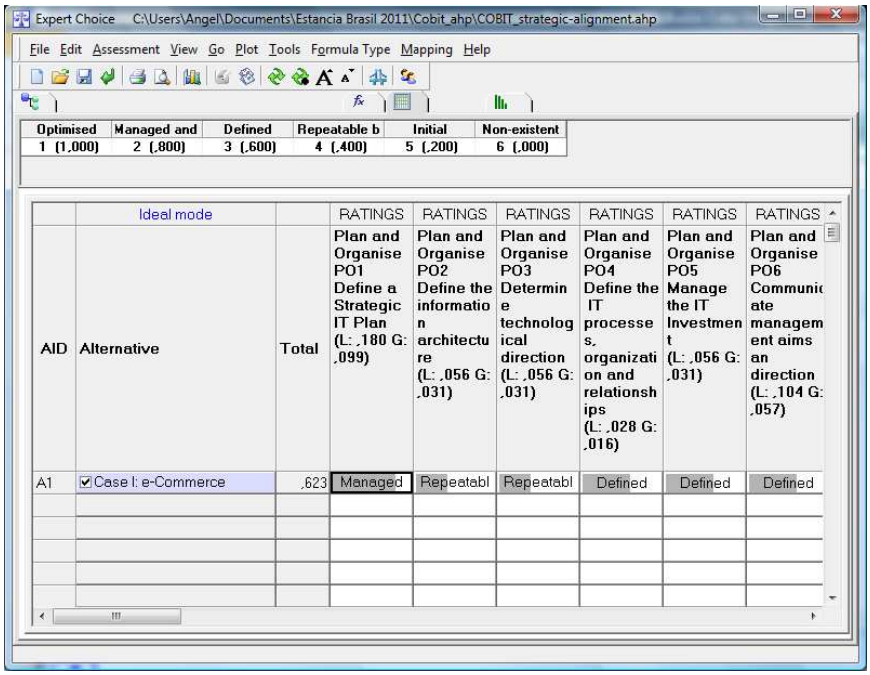
GRAU DE MATURIDADE COBIT	**NÍVEL NA ESCALA PROPOSTO NO MODELO**
0 – Inexistente	0.0
1 – Inicial	0.2
2 – Repetitivo, mas intuitivo	0.4
3 – Definido	0.6
4 – Gerenciado e mensurável	0.8
5 – Otimizado	1.0

O grau de maturidade do Cobit de acordo com o nível na escala proposto no modelo demonstra o estágio da organização. Estes são descritos a seguir:

- *0.0 – Inexistente*: gerenciamento de processos não aplicados;
- *0.2 – Inicial*: processos são iniciais, específicos e desorganizados;
- *0.4 – Repetitivo, mas intuitivo*: processos seguem um caminho padrão;
- *0.6 – Definido*: processos são documentados e comunicados;
- *0.8 – Gerenciado e mensurável*: processos são monitorados e medidos;
- *1.0* – boas práticas são seguidas e automatizadas.

A figura 36 mostra a introdução das respostas ao questionário no *software Expert Choice.*

Figura 36 - Inclusão de níveis de maturidade



Para estabelecer uma avaliação de consenso entre os dois gestores entrevistados, considerou-se a média geométrica de suas respostas e aplicando a ponderação obtida pelo modelo AHP foi possível obter um diagnóstico da situação atual da empresa, em relação à eficácia do modelo de governança de TI utilizados. A tabela 4 resume os níveis obtidos por diferentes domínios em cada uma das áreas focais de Cobit. Como visto, o domínio com um nível claramente mais elevado de desenvolvimento é o de AI (Aquisição e Implementação). Os outros domínios não alcançam o nível de maturidade “Definido” do Cobit 4.1.

Tabela 4 - Estudo de caso. Níveis de maturidade dos domínios x áreas focais

Domínios / Áreas Focais	Alinh. Estrat.	Entrega Valor	Gestão Recursos	**Gestão RISCOS**	Mensur. Desemp.	Média
PO: Planej. e Organiz.	0,531	0,458	0,482	**0,527**	0,455	0,491
AI:Aquis. e Implement.	**0,688**	**0,737**	**0,743**	**0,688**	**0,752**	**0,722**
DS: Entrega e Suporte	0,574	0,572	0,589	**0,532**	0,656	0,585
ME: Monitoramento	0,458	0,527	0,556	**0,450**	0,571	0,512

Fonte: Elaborado pelo autor com base nos dados fornecidos pelo questionário Cobit – AHP e Software Expert Choice

Ponderando os níveis de maturidade de pesos globais atribuídos pelo modelo AHP para cada processo, obtém-se o nível de maturidade global de cada

área focal. Com esses resultados, este trabalho enfatiza então o alcançado com a área focal de Gestão de Riscos e o Domínio de Aquisição e Implementação, já que são estes os mais percebidos pelas respostas dos gestores quanto ao nível de Maturidade Cobit - AHP.

A área focal gestão de riscos apresenta para o domínio ME o menor nível de desenvolvimento estando classificado em repetitivo, mas intuitivo (0.4), cujos processos seguem um caminho padrão. Os domínios PO e DS o nível de maturidade na organização estão entre repetitivo, mas intuitivo e definido (0.5) onde os processos não estão totalmente documentados e comunicados. O domínio com nível mais elevado de desenvolvimento é AI (0.68) classificado como definido onde os processos são documentados e comunicados. O domínio AI para todas as áreas focais os processos são documentados e comunicados.

Os resultados indicam que a organização atua na área focal de gestão de riscos no nível de documentação e comunicação sobre os riscos relativos á soluções necessárias aos processos de negócio, quer originados de aquisição, desenvolvimento ou manutenção nos sistemas já existentes.

Na seção seguinte, apresentam-se a conclusão do estudo e as recomendações de estudos futuros relacionados à integração das áreas Controladoria e da TI.

5 CONCLUSÃO E RECOMENDAÇÕES

5.1 CONCLUSÃO

A gestão da informação no ambiente atual dos negócios pode ser fator diferencial para as organizações manterem-se competitivas, pois tendem a propiciar uma melhor decisão.

Para Mithas, Ramasubbu e Sambamurthy (2011) a gestão da informação desempenha papel importante no desenvolvimento de outras capacidades que influenciam positivamente nos diversos processos organizacionais, contribuindo com a eficácia e no desempenho da organização.

Dessa forma, a informação é um ativo essencial para os negócios de uma organização. Consequentemente, necessita ser adequadamente protegida (ISO 27002, 2007). Relacionado à proteção da informação se faz necessário que as organizações adotem uma gestão de segurança da informação. Eloff e Eloff (2003, p. 135) citam que a gestão em segurança da informação deve contemplar pessoas, fundamentais para o sucesso de qualquer programa de segurança da informação, bem como a adoção de um código de práticas de segurança da informação com a identificação dos principais processos de negócio. 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 refere 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, p. 278) cita que é função da Controladoria o desenho, desenvolvimento e manutenção dos sistemas de informações, sem envolver-se com a parte de infraestrutura e tecnologia da informação. Já Wilkin e Chenhall (2010) abordam o ambiente crescente de conscientização sobre o papel da TI quanto aos aspectos de captura, armazenamento, manipulação e apresentação dos dados para apoiar os sistemas de informações.

Ao longo deste estudo, procurou-se demonstrar a importância da informação e da segurança da informação no ambiente atual dos negócios, bem como as responsabilidades especificas e complementares das áreas de Controladoria e de TI sobre os sistemas de informações nas organizações. Isso relacionado ao objetivo geral deste estudo de avaliar os processos de segurança da informação integrando as áreas de Controladoria e de TI.

O primeiro objetivo específico estabelecido para a pesquisa foi identificar processos críticos e riscos de negócio na empresa estudada, e para tal foram aplicados questionários com base na norma ISO 27002 que estabelece as práticas de gestão da segurança da informação na organização e entrevistas. No quadro 2, é possível verificar os processos críticos percebidos quanto às práticas de segurança da informação na organização.

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: Elaborado pelo autor com base nas respostas dos gestores ao questionário – ISO/IEC 27002

Dentro desse mesmo objetivo, quanto às entrevistas realizadas, os gestores identificaram os seguintes processos críticos e riscos de negócio para a organização: (i) comprar; (ii) vender; (iii) entregar; (iv) estocar; (v) logística; e (vi) tributário.

O segundo objetivo específico estabelecido para a pesquisa foi identificar a participação das áreas de Controladoria e Tecnologia da Informação nos

processos críticos de negócio na empresa estudada, para o que foram elaboradas questões relativas à atuação das áreas nesses processos.

Em relação às práticas de segurança da informação, constatou-se que a partir da visão integrada das áreas, o domínio de segurança em recursos humanos deve ser aprimorado. As áreas carecem de uma atuação mais efetiva nos processos relacionados a esse domínio. Para os demais domínios, verificou-se uma gestão em nível técnico e operacional. Quanto aos principais processos de negócio da empresa (compras, vendas, estocagem, margem de lucro dos produtos, tributação), Controladoria e TI participam ou tomam conhecimento das definições das diretrizes políticas e operacionais na organização. Também se constatou que essas áreas efetuam treinamentos de alinhamento técnico junto às demais áreas, contudo, os respondentes entendem que esse processo pode ser aprimorado através da elaboração de um calendário formal, o que possibilitaria aprimorar os processos operacionais do trabalho conjunto das áreas.

O terceiro objetivo específico estabelecido para a pesquisa foi avaliar as práticas de proteção de segurança de informações e níveis de maturidade nos processos de negócios. Visando responder ao objetivo, foram compilados os dados obtidos através de dois questionários, um elaborado com base na norma ISO 27002 para avaliar as práticas de proteção de segurança de informações e outro com base no modelo multicritério AHP para avaliar os níveis de maturidade na organização.

Constatou-se, na visão integrada dos gestores de Controladoria, TI e Contábil/Fiscal, que as práticas de proteção da informação de acordo com a ISO 27002 na organização 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 esses 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, seno que 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.

A que se considerar que em um ambiente afetado por constantes alterações torna-se complexo para qualquer organização se cercar de ferramentas que garantam um ambiente em que resulte a avaliação dos processos de segurança da informação como totalmente adequados.

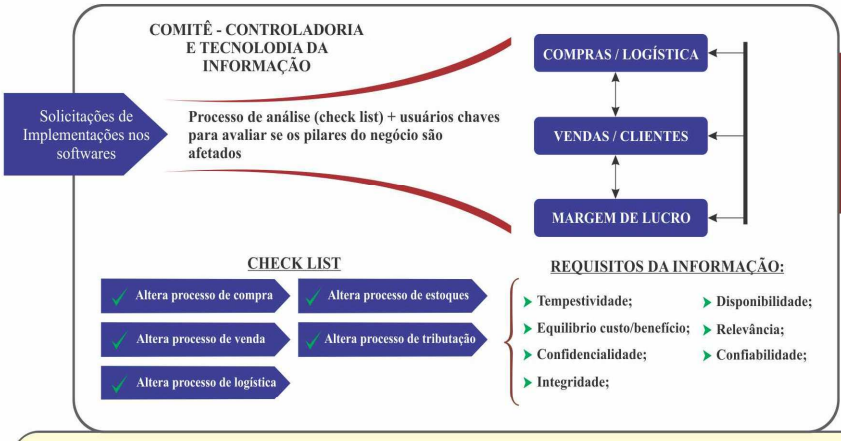
Quanto aos níveis de maturidade nos processos utilizando o modelo multicritério AHP aplicado aos diferentes domínios em cada uma das áreas focais do Cobit 4.1, constatou-se que na visão dos gestores de TI o domínio AI (Aquisição e Implementação) tem um nível claramente mais elevado de desenvolvimento na organização. Isso permite concluir que a área de TI atua com maior intensidade na identificação de soluções para os processos de negócios da organização. Em relação à área focal de gestão de riscos, constatou-se também que o domínio AI (Aquisição e Implementação) é o mais elevado em níveis de maturidade. Para os demais domínios, os processos de gestão de riscos seguem um caminho padrão e não estão totalmente documentados e comunicados.

O quarto objetivo específico estabelecido para a pesquisa foi propor a criação de procedimentos integrados entre Controladoria e Tecnologia da Informação para tratamento dos processos de segurança das informações. Como resultado, na figura 37, apresenta-se um *framework,* o qual integra as áreas de Controladoria e de TI nas avaliações do processo de solicitações de implementações nos *softwares* demandadas por usuários. Esse *framework* foi elaborado em conjunto com os gestores após a análise dos dados coletados, tendo como finalidade apoiar a operacionalização e a formalização desse processo na organização.

O *framework* também contempla quadros com os resultados gerados por este trabalho a partir das aplicações dos instrumentos ISO/IEC 27002,

entrevistas e Cobit – AHP e que suportaram o atendimento dos objetivos estabelecidos pelo estudo.

Figura 37 - Framework integração Controladoria e TI na avaliação de processos de segurança da informação



Avaliação dos Processos de Segurança da Informação - ISO 27002
Visão Integrada - Controladoria e TI

DOMÍNIO ISO 27002 / NÍVEIS	INADEQUADA	MINÍMA	RAZOÁVEL	ADEQUADA	N/A
Política de Segurança da Informação	0%	50,00%	50,00%	0%	0%
Organizando a Segurança da Informação	8,82%	23,53%	41,18%	26,47%	0%
Gestão de Aditivos	12,50%	12,50%	12,50%	62,50%	0%
Segurança em Recursos Humanos	25,00%	60,00%	15,00%	0%	0%
Gerenciamento das Operações e Comunicações	12,10%	34,68%	36,29%	16,94%	0%
Controle de Acesso	7,61%	20,65%	31,52%	40,22%	0%
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações	14,06%	37,50%	35,94%	7,81%	4,69%
Gestão de Incidentes de Segurança da Informação	16,67%	33,33%	41,67%	8,33%	0%
Gestão de Continuidade de Negócio	25,00%	15,00%	50,00%	10,00%	0%
Conformidade	2,50%	35,00%	40,00%	22,50%	0%

Analise qualitativa das entrevistas - *SPHINX* - Integração Controladoria X TI

GESTORES ENTREVISTADOS	CATEGORIAS VINCULADAS AS RESPOSTAS DOS GESTORES				
Gerente de TI	Criar Comitê	Participação usuários	Homologação alterações		
Gerente de Controladoria	Alinhamento comunicação	Controles processo alter. software	Políticas e normas seg. informação	BI - modelador sist. informações	
Gerente Contábil Fiscal	Treinamentos	Riscos econômico financeiros	Riscos de integridade informações	Direção empresa influ. seg. inform.	Foco princip. proces. empresa

Níveis de maturidade nos domínios em cada uma das áreas focais do Cobit 4.1 - AHP

CLASSIFICAÇÕES	Inexistente	Inicial	Repetitivo mas intuitivo	Definido	Gerenciado e mensurável	Otimizado
Grau de maturidade - Cobit	0	1	2	3	4	5
Nível na escala prop. modelo	0.0	0.2	0.4	0.6	0.8	1.0
DOMÍNIOS / ÁREAS FOCAIS	**Alinhamento estratégico**	**Entrega de valor**	**Gestão de recursos**	**Gestão de RISCOS**	**Mensuração e desempenho**	**Média**
PO - Planej. e Organização	0.5	0.5	0.5	0.5	0.5	0.5
AI - Aquis. e Implementação	0.7	0.7	0.7	0.7	0.8	0.7
DS - Entrega e Suporte	0.6	0.6	0.6	0.5	0.7	0.6
ME - Monitoramento	0.5	0.5	0.6	0.5	0.6	0.5

Fonte: Elaborado pelo autor com base no estudo de caso

A visualização do *framework* anteriormente representado deve ser entendida da seguinte forma: O primeiro quadro representa a atuação integrada das áreas de Controladoria e de TI nas avaliações dos processos de segurança da informação sobre implementações nos *softwares* que possam impactar de forma relevante a tomada de decisões dos gestores e consequentemente tem reflexos nos resultados da empresa. O foco de atuação recai sobre os processos principais da empresa, ao qual envolvem: (i) compra; (ii) vender; (iii) entregar; (iv) estocar; e (v) tributação.

O processo de integração das áreas estrutura-se a partir de um comitê formado por profissionais de ambas as áreas (Controladoria e TI) tendo como suporte ferramentas de tecnologia da informação que sinalizem adaptações nos processos definidos e parametrizados. Esse comitê responde pela implementação de políticas técnicas e de gestão corporativas, que estabelece os procedimentos e responsabilidades sobre demandas de solicitações, *chek list* técnico e restrições. Todo esse processo é previamente alinhado com a alta administração.

No segundo quadro do *framework*, visualizam-se os resultados da adequação da segurança da informação de acordo com a ISO/IEC 27002 ao considerar a percepção integrada dos gestores das áreas de Controladoria e de TI.

No terceiro quadro, apresentam-se os resultados das principais “categorias” associadas às respostas das entrevistas a partir das análises qualitativas de conteúdo e através do *software SPHINX.* Estas contribuíram para a elaboração do primeiro quadro do *framework* da atuação integrada das áreas de TI e Controladoria. Constata-se que cada gestor tem uma percepção das ações que podem contribuir na avaliação nos processos de segurança da informação na organização integrando as áreas de Controladoria e de TI.

Observa-se que para o 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/Fiscal, 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**.

No último quadro do *framework,* visualizam-se os resultados dos níveis de maturidade nos domínios e áreas focais de acordo com o Cobit – AHP com destaque para o domínio AI (Aquisição e Implementação), o qual apresenta um nível claramente mais elevado de desenvolvimento na organização e a área focal de gestão de riscos.

Ressalta-se que os gestores participantes do estudo estão conscientes da importância de todas as práticas, procedimentos e objetivos de avaliação dos processos que envolvem a segurança e os sistemas de informação na organização. Dessa forma, é oportuno afirmar que as áreas trabalham nesse sentido, orientada pela alta administração para a implementação de melhorias continuas visando à qualificação do ambiente informacional da organização.

Assim sendo, a implementação dos procedimentos estabelecidos no framework promove a integração das áreas de Controladoria e de TI na avaliação dos processos de segurança da informação dentre esses, os de implementações nos softwares demandadas pelos usuários. O *framework* também apresenta o diagnóstico quantos aos níveis de proteção de segurança da informação e de maturidade dos processos de TI o que possibilita a análise de eventuais riscos associados às práticas de proteção de segurança da informação e do modelo de governança de TI adotados na organização. Consequentemente, aprimoraram-se os processos operacionais do trabalho conjunto dessas duas áreas e de controles do ambiente da informação.

5.2 RECOMENDAÇÕES

Como sugestão de temas para novas pesquisas ou aprofundamento dessa mesma pesquisa, cita-se os seguintes:

a) Realização de pesquisas similares com outras organizações do mesmo setor ou de outros setores empresariais;

b) Realização de pesquisas com a utilização da técnica AHP como ferramenta de apoio aos processos de gestão da área de Controladoria;
c) Realização de pesquisas que relacionem a integração de processos de Governança Corporativa, Governança de TI e Controladoria.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas. **Norma brasileira ISO/IEC 27002, 2007**. Rio de Janeiro: ABNT, 2007.

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

ATKINSON, A. A. et al. **Contabilidade gerencial**. São Paulo: Atlas, 2008.

BAZERMAN, M. H. **Processo decisório**: para cursos de administração, economia e MBAs. Rio de Janeiro: Elsevier, 2004.

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

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information security policy campliance: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly Executive**, v. 34, n. 3, set. 2010.

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.

CPC - Comitê de Pronunciamentos Contábeis. **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 cecurity management: a new paradigm. **Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on enablement through technology**, p. 130-136, 2003.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2009.

ISACA. Disponível em: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Assessment-Process-CAP-COBIT-41-Process-Assessment-Model-Exposure-Draft.aspx>. Acesso em: 30 nov. 2011.

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.

JUNG, C. F. Metodologia científica: ênfase em pesquisa tecnológica. 3. ed. rev. e ampl. 2003. Disponível em: <http://www.jung.pro.br>. Acesso em: 28 fev. 2011.

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

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

MALHOTRA, Naresh K. **Introdução à pesquisa de marketing**. São Paulo: Pearson Prentice Hall, 2008.

MARCONI, M. A.; LAKATOS, E. M. **Metodologia científica**. São Paulo: Atlas, 2000.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de pesquisa**. 6. ed. São Paulo: Atlas, 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.

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

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

OLIVEIRA, A. B. S. **Controladoria**: fundamentos do controle empresarial. São Paulo: Saraiva, 2009.

PADOVEZE, C. L.; BERTOLUCCI, R. G. **Gerenciamento do risco corporativo em controladoria – Enterprise Risk Management (ERM)**. São Paulo: Cengage Learning, 2009.

SAATY, T. L. **The analytical hierarchy process**: planning, priority setting, resource allocation. New York: Mc Graw-Hill, 1980.

SILVA, E. L.; MENEZES, E. M. Metodologia da pesquisa e elaboração de dissertação. Florianópolis: UFSC / PPGEP / LED, 2001.

SPEARS, J. L.; BARKI, H. User participation inf information systems security risk management. **MIS Quarterly Executive**, v. 34, n. 3, set. 2010.

TANUWIJAYA, H.; SARNO, R. Comparation of cobit maturity model and structural equation model for measuring the alignment between university academic regulations and information technology goals. **IJCSNS International Journal of Computer Science and Network Security**, v. 10, n. 6, Jun. 2010.

VANTI, A. A.; COBO, A.; ROCHA, R. Avaliação de modelo de governança de TI com o uso de FAHP. São Paulo: Contecsi / USP, 2011.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 3. ed. São Paulo: Atlas, 2000.

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.

YIN, R. K. **Estudo de caso**: planejamento e métodos. 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.

ANEXOS

ANEXO A – AVALIAÇÃO DAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO - ISO/IEC 27002

Avaliador: Agostinho Luiz Peroni
Data: 18/08/2011

O instrumento a seguir tem por objetivo avaliar a adequação aos controles relacionados à segurança da informação considerando a norma ISO/IEC 27002. De acordo com o código de prática à gestão da segurança da informação considerando os seguintes níveis:

Proteção Inadequada: Não existe nenhum esforço para implementação dos controles recomendados. Produtos e equipamentos certificados não tem qualquer influência na classificação das seções neste nível;

Proteção mínima: A organização adota o mínimo de controles recomendados. Produtos e equipamentos certificados não tem qualquer influência na classificação das seções neste nível;

Proteção razoável: A maioria dos controles são implementados e devem satisfazer os requisitos com base em procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso;

Proteção adequada: Implementa todos os controles recomendados pelo domínio. Sempre que possível é obrigatório o uso de produtos e equipamentos certificados;

Não aplicável: Considerando o segmento ou estrutura da empresa, tal controle não se aplica.

Quadro de análise:

Marque com um “x” na coluna que você considera que a respectiva prática de segurança se encontra:

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
1 - Política da Segurança da Informação. ISO 27002 – Página 8	0	0	2	0	0
1.1 - Documento da política de segurança da informação;			x		
1.2 - Análise crítica da política de segurança da informação			x		
2 - Organizando a Segurança Informação. ISO 27002 – Página 10	0	4	9	4	0
2.1 - Comprometimento da direção com a segurança da informação no processo crítico de gestão comercial;		x			
2.2 - Coordenação da segurança da informação em transações relacionadas aos custos comerciais;			x		
2.3 - Processo de autorização para os recursos de processamento da informação em transações comerciais;				x	
2.4 - Acordos de confidencialidade na definição de política de preços;		x			
2.5 - Acordos de confidencialidade na definição de prazos;		x			
2.6 - Acordos de confidencialidade no estabelecimento de descontos;			x		
2.7 - Acordos de confidencialidade em negociações de compra de mercadorias para comercialização;			x		
2.8 - Contato com departamentos de controladoria, contabilidade, cobrança, vendas e marketing;				x	
2.9 - Contato com grupos de vendedores e representantes;		x			
2.10 - Contato com grupos de filiais;			x		
2.11 - Análise crítica independente de segurança da informação envolvendo operações comerciais;				x	
2.12 - Identificação dos riscos de segurança da informação relacionados às filiais nos processos de gestão de estoques;			x		
2.13 - Identificação dos riscos de segurança de informação relacionados às filiais nos processos de gestão de vendas;			x		
2.14 - Identificação dos riscos de segurança da informação relacionados às filiais nos processos de gestão financeira;				x	
2.15 - Identificando a segurança da informação, quando tratando com os fornecedores;			x		
2.16 - Identificando a segurança da informação, quando tratando com clientes;			x		

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
2.17 - Identificando segurança da informação nos acordos com financeiras e escritórios de cobrança;			x		
3 - Gestão de ativos (GA). ISO 27002 – Página 21	0	0	0	4	0
3.1 - Inventário dos ativos: estoques, patrimônio, financeiro.				x	
3.2 - Proprietário dos ativos - Atribuição de Responsáveis.				x	
3.3 - Recomendações para classificação (Confidencialidade, Integridade, Disponibilidade, Efetividade e Eficiência).				x	
3.4 - Rótulos e tratamento da informação;				x	
4 - Segurança em recursos humanos. ISO 27002 – Página 25	2	7	1	0	0
4.1 - Papéis e responsabilidades nos processos de vendas;		x			
4.2 - Papéis e responsabilidades nos processos de compras;		x			
4.3 - Processo de seleção funcional para gestão de sistemas de custos comerciais;		x			
4.4 - Processo de seleção funcional para gestão de sistemas financeiros (Cobrança, Baixa de Títulos);	x				
4.5 - Termos e condições de contratação;		x			
4.6 - Conscientização, educação e treinamento em segurança da informação;	x				
4.7 - Processo disciplinar quanto a acesso a sistemas, utilização de equipamentos fora da empresa, informações privilegiadas e tráfego de informações;		x			
4.8 - Encerramento de atividades do uso do sistema de gestão de custos, formação de preços		x			
4.9 - Encerramento de atividades do uso do sistema de gestão de financeira (Controladoria, Contabilidade, Cobrança e Financeiro)			x		
4.10 - Processo de gestão de direitos de acesso (interno e externo).		x			
5 - Gerenciamento das operações e comunicações. ISO 27002 – Página 40	1	9	15	6	0
5.1 - Documentação dos procedimentos de operação de sistemas de custos comerciais em aplicativos Office;			x		
5.2 - Controles internos sobre as operações de custos comerciais e formação de preços;			x		
5.3 - Gestão de mudanças em operações que impactam em custos comerciais;		x			
5.4 - Separação dos recursos de formação de custos, formação de preços e de confirmação de margens de lucro;				x	
5.5 Eficiências na entrega de serviços;			x		
5.6 Monitoramento e análise crítica de serviços terceirizados;		x			
5.7 Gerenciamento de mudanças para serviços terceirizados;			x		

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
5.8 Gestão de capacidade de transporte e armazenamento;			x		
5.9 Controle aceitação de sistemas;		x			
5.10 Controles codificados e de rastreabilidade de mercadorias;		x			
5.11 Cópias de segurança das informações;			x		
5.12 Controles e segurança dos serviços de redes;			x		
5.13 Gerenciamento de mídias removíveis;		x			
5.14 Descarte de mídias;		x			
5.15 Procedimentos para tratamento de informação;			x		
5.16 Segurança da documentação dos sistemas;				x	
5.17 Políticas e procedimentos para troca de informações;			x		
5.18 Acordos para a troca de informações;				x	
5.19 Mensagens eletrônicas;			x		
5.20 Transações on-line;				x	
5.21 Registros de auditoria;	x				
5.22 Monitoramento do uso do sistema;			x		
5.23 Proteção das informações dos registros (log);		x			
5.24 Registros (log) de administrador e operador;		x			
5.25 Registros (log) de falhas;				x	
5.26 Controles internos sobre as operações de compras e controles de estoques;			x		
5.27 Gestão de mudanças em operações que impactam em compras e controles de estoques;		x			
5.28 Gestão de mudanças em operações que impactam em controles financeiros;				x	
5.29 Controles internos sobre as operações financeiras;			x		
5.30 Gestão de mudanças em operações que impactam nos processos de elaboração de informações estratégicas da Controladoria;			x		
5.31 Controles internos sobre processos de elaboração de informações estratégicas da Controladoria;			x		
6 - Controle de acessos. ISO 27002 – Página 65	0	5	7	11	0
6.1 Política de controle de acesso;		x			
6.2 Registro de usuário;			x		
6.3 Gerenciamento de privilégios;				x	
6.4 Análise crítica dos direitos de acesso de usuário;			x		
6.5 Uso de senhas;				x	
6.6 Equipamento de usuário sem monitoração;		x			
6.7 Política de mesa limpa e tela limpa;			x		
6.8 Política de uso dos serviços de rede;				x	
6.9 Autenticação para conexão externa do usuário;				x	

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
6.10 Identificação de equipamento em redes;				x	
6.11 Proteção e configuração de portas de diagnóstico remotas;				x	
6.12 Segregação de redes;				x	
6.13 Controle de conexão de rede;				x	
6.14 Controle de roteamento de redes;			x		
6.15 Procedimentos seguros de entrada no sistema (log-on);				x	
6.16 Sistema de gerenciamento de senha;		x			
6.17 Uso de utilitários de sistema;				x	
6.18 Desconexão de terminal por inatividade;			x		
6.19 Limitação de horário de conexão;		x			
6.20 Restrição de acesso à informação;			x		
6.21 Isolamento de sistemas sensíveis;		x			
6.22 Computação e comunicação móvel;			x		
6.23 Trabalho remoto.				x	
7 - Aquisição, desenvolvimento e manutenção de sistemas de informação. ISO 27002 – Página 84	2	6	6	2	0
7.1 Análise e especificação dos requisitos de segurança;			x		
7.2 Validação dos dados de entrada;			x		
7.3 Controle do processamento interno;		x			
7.4 Treinamento usuários com a participação das áreas envolvidas;		x			
7.5 Validação de informações de saída;			x		
7.6 Política para o uso de controles criptográficos;		x			
7.7 Gerenciamento de chaves;			x		
7.8 Controle de software operacional;			x		
7.9 Proteção dos dados para teste de sistema;		x			
7.10 Controle de acesso ao código-fonte de programa;				x	
7.11 Procedimentos para controle de mudanças;				x	
7.12 Análise crítica técnica das aplicações após mudanças no sistema operacional;	x				
7.13 Restrições sobre mudanças em pacotes de software;	x				
7.14 Vazamento de informações;		x			
7.15 Desenvolvimento terceirizado de software;		x			
7.16 Controle de vulnerabilidades técnicas.			x		
8 - Gestão de incidentes de segurança da informação. ISO 27002 – Página 98	1	2	3	0	0
8.1 Notificação de eventos de segurança da informação;	x				
8.2 Notificando fragilidades de segurança da informação;		x			
8.3 Responsabilidades e procedimentos;			x		
8.4 Aprendendo com os incidentes de segurança da informação;			x		

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
8.5 Coleta de evidências;		x			
8.6 Grau de participação das áreas envolvidos nos processos de geração de informações.			x		
9 - Gestão da continuidade do negócio. ISO 27002 – Página 103	0	1	3	1	0
9.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio;			x		
9.2 Continuidade de negócios e análise/avaliação de riscos;		x			
9.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação;				x	
9.4 Estrutura do plano de continuidade do negócio;			x		
9.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.			x		
10 – Conformidade. ISO 27002 – Página 108	0	3	5	2	0
10.1 Identificação da legislação vigente;				x	
10.2 Direitos de propriedade intelectual;			x		
10.3 Proteção de registros organizacionais;			x		
10.4 Proteção de dados e privacidade de informações pessoais;			x		
10.5 Prevenção de mau uso de recursos de processamento da informação;		x			
10.6 Regulamentação de controles de criptografia;				x	
10.7 Conformidade com as políticas e normas de segurança da informação;			x		
10.8 Verificação da conformidade técnica;			x		
10.9 Controles de auditoria de sistemas de informação;		x			
10.10 Proteção de ferramentas de auditoria de sistemas de informação.		x			

Avaliador: Luis Carlos Alberti
Data: 19/08/2011

O instrumento a seguir tem por objetivo avaliar a adequação aos controles relacionados à segurança da informação considerando a norma ISO/IEC 27002. De acordo com o código de prática à gestão da segurança da informação considerando os seguintes níveis:

Proteção Inadequada: Não existe nenhum esforço para implementação dos controles recomendados. Produtos e equipamentos certificados não tem qualquer influência na classificação das seções neste nível;
Proteção mínima: A organização adota o mínimo de controles recomendados. Produtos e equipamentos certificados não tem qualquer influência na classificação das seções neste nível;
Proteção razoável: A maioria dos controles são implementados e devem satisfazer os requisitos com base em procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso;
Proteção adequada: Implementa todos os controles recomendados pelo domínio. Sempre que possível é obrigatório o uso de produtos e equipamentos certificados;
Não aplicável: Considerando o segmento ou estrutura da empresa, tal controle não se aplica.

Quadro de análise:

Marque com um “x” na coluna que você considera que a respectiva prática de segurança se encontra:

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
1 - Política da Segurança da Informação. ISO 27002 – Página 8	0	1	1	0	0
1.1 - Documento da política de segurança da informação;		x			
1.2 - Análise crítica da política de segurança da informação			x		
2 - Organizando a Segurança Informação. ISO 27002 – Página 10	0	1	8	8	0
2.1 - Comprometimento da direção com a segurança da informação no processo crítico de gestão comercial;				x	
2.2 - Coordenação da segurança da informação em transações relacionadas aos custos comerciais;				x	
2.3 - Processo de autorização para os recursos de processamento da informação em transações comerciais;				x	
2.4 - Acordos de confidencialidade na definição de política de preços;			x		
2.5 - Acordos de confidencialidade na definição de prazos;			x		
2.6 - Acordos de confidencialidade no estabelecimento de descontos;		x			
2.7 - Acordos de confidencialidade em negociações de compra de mercadorias para comercialização;			x		
2.8 - Contato com departamentos de controladoria, contabilidade, cobrança, vendas e marketing;				x	
2.9 - Contato com grupos de vendedores e representantes;			x		
2.10 - Contato com grupos de filiais;			x		
2.11 - Análise crítica independente de segurança da informação envolvendo operações comerciais;				x	
2.12 - Identificação dos riscos de segurança da informação relacionados às filiais nos processos de gestão de estoques;			x		
2.13 - Identificação dos riscos de segurança de informação relacionados às filiais nos processos de gestão de vendas;			x		
2.14 - Identificação dos riscos de segurança da informação relacionados às filiais nos processos de gestão financeira;				x	
2.15 - Identificando a segurança da informação, quando tratando com os fornecedores;			x		
2.16 - Identificando a segurança da informação, quando tratando com clientes;				x	

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
2.17 - Identificando segurança da informação nos acordos com financeiras e escritórios de cobrança;				x	
3 - Gestão de ativos (GA). ISO 27002 – Página 21	0	0	0	4	0
3.1 - Inventário dos ativos: estoques, patrimônio, financeiro.				x	
3.2 - Proprietário dos ativos - Atribuição de Responsáveis.				x	
3.3 - Recomendações para classificação (Confidencialidade, Integridade, Disponibilidade, Efetividade e Eficiência).				x	
3.4 - Rótulos e tratamento da informação;				x	
4 - Segurança em recursos humanos. ISO 27002 – Página 25	3	5	2	0	0
4.1 - Papéis e responsabilidades nos processos de vendas;		x			
4.2 - Papéis e responsabilidades nos processos de compras;		x			
4.3 - Processo de seleção funcional para gestão de sistemas de custos comerciais;	x				
4.4 - Processo de seleção funcional para gestão de sistemas financeiros (Cobrança, Baixa de Títulos);	x				
4.5 - Termos e condições de contratação;	x				
4.6 - Conscientização, educação e treinamento em segurança da informação;		x			
4.7 - Processo disciplinar quanto a acesso a sistemas, utilização de equipamentos fora da empresa, informações privilegiadas e tráfego de informações;			x		
4.8 - Encerramento de atividades do uso do sistema de gestão de custos, formação de preços		x			
4.9 - Encerramento de atividades do uso do sistema de gestão de financeira (Controladoria, Contabilidade, Cobrança e Financeiro)		x			
4.10 - Processo de gestão de direitos de acesso (interno e externo).			x		
5 - Gerenciamento das operações e comunicações. ISO 27002 – Página 40	3	8	12	8	0
5.1 - Documentação dos procedimentos de operação de sistemas de custos comerciais em aplicativos Office;		x			
5.2 - Controles internos sobre as operações de custos comerciais e formação de preços;			x		
5.3 - Gestão de mudanças em operações que impactam em custos comerciais;				x	
5.4 - Separação dos recursos de formação de custos, formação de preços e de confirmação de margens de lucro;				x	
5.5 Eficiências na entrega de serviços;			x		
5.6 Monitoramento e análise crítica de serviços terceirizados;			x		
5.7 Gerenciamento de mudanças para serviços terceirizados;				x	

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
5.8 Gestão de capacidade de transporte e armazenamento;			x		
5.9 Controle aceitação de sistemas;			x		
5.10 Controles codificados e de rastreabilidade de mercadorias;		x			
5.11 Cópias de segurança das informações;			x		
5.12 Controles e segurança dos serviços de redes;				x	
5.13 Gerenciamento de mídias removíveis;				x	
5.14 Descarte de mídias;		x			
5.15 Procedimentos para tratamento de informação;			x		
5.16 Segurança da documentação dos sistemas;		x			
5.17 Políticas e procedimentos para troca de informações;	x				
5.18 Acordos para a troca de informações;	x				
5.19 Mensagens eletrônicas;				x	
5.20 Transações on-line;				x	
5.21 Registros de auditoria;	x				
5.22 Monitoramento do uso do sistema;				x	
5.23 Proteção das informações dos registros (log);		x			
5.24 Registros (log) de administrador e operador;		x			
5.25 Registros (log) de falhas;		x			
5.26 Controles internos sobre as operações de compras e controles de estoques;			x		
5.27 Gestão de mudanças em operações que impactam em compras e controles de estoques;			x		
5.28 Gestão de mudanças em operações que impactam em controles financeiros;			x		
5.29 Controles internos sobre as operações financeiras;		x			
5.30 Gestão de mudanças em operações que impactam nos processos de elaboração de informações estratégicas da Controladoria;			x		
5.31 Controles internos sobre processos de elaboração de informações estratégicas da Controladoria;			x		
6 - Controle de acessos. ISO 27002 – Página 65	3	5	6	9	0
6.1 Política de controle de acesso;			x		
6.2 Registro de usuário;		x			
6.3 Gerenciamento de privilégios;			x		
6.4 Análise crítica dos direitos de acesso de usuário;	x				
6.5 Uso de senhas;	x				
6.6 Equipamento de usuário sem monitoração;		x			
6.7 Política de mesa limpa e tela limpa;	x				
6.8 Política de uso dos serviços de rede;				x	
6.9 Autenticação para conexão externa do usuário;				x	
6.10 Identificação de equipamento em redes;				x	

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
6.11 Proteção e configuração de portas de diagnóstico remotas;				x	
6.12 Segregação de redes;				x	
6.13 Controle de conexão de rede;				x	
6.14 Controle de roteamento de redes;				x	
6.15 Procedimentos seguros de entrada no sistema (log-on);			x		
6.16 Sistema de gerenciamento de senha;		x			
6.17 Uso de utilitários de sistema;			x		
6.18 Desconexão de terminal por inatividade;				x	
6.19 Limitação de horário de conexão;		x			
6.20 Restrição de acesso à informação;		x			
6.21 Isolamento de sistemas sensíveis;			x		
6.22 Computação e comunicação móvel;			x		
6.23 Trabalho remoto.				x	
7 - Aquisição, desenvolvimento e manutenção de sistemas de informação. ISO 27002 – Página 84	4	4	6	2	0
7.1 Análise e especificação dos requisitos de segurança;			x		
7.2 Validação dos dados de entrada;			x		
7.3 Controle do processamento interno;		x			
7.4 Treinamento usuários com a participação das áreas envolvidas;		x			
7.5 Validação de informações de saída;		x			
7.6 Política para o uso de controles criptográficos;			x		
7.7 Gerenciamento de chaves;			x		
7.8 Controle de software operacional;			x		
7.9 Proteção dos dados para teste de sistema;		x			
7.10 Controle de acesso ao código-fonte de programa;				x	
7.11 Procedimentos para controle de mudanças;				x	
7.12 Análise crítica técnica das aplicações após mudanças no sistema operacional;	x				
7.13 Restrições sobre mudanças em pacotes de software;	x				
7.14 Vazamento de informações;	x				
7.15 Desenvolvimento terceirizado de software;			x		
7.16 Controle de vulnerabilidades técnicas.	x				
8 - Gestão de incidentes de segurança da informação. ISO 27002 – Página 98	0	1	4	1	0
8.1 Notificação de eventos de segurança da informação;		x			
8.2 Notificando fragilidades de segurança da informação;			x		
8.3 Responsabilidades e procedimentos;			x		
8.4 Aprendendo com os incidentes de segurança da informação;				x	
8.5 Coleta de evidências;			x		

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
8.6 Grau de participação das áreas envolvidos nos processos de geração de informações.			x		
9 - Gestão da continuidade do negócio ISO 27002 – Página 103	0	1	4	0	0
9.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio;			x		
9.2 Continuidade de negócios e análise/avaliação de riscos;		x			
9.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação;			x		
9.4 Estrutura do plano de continuidade do negócio;			x		
9.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.			x		
10 - Conformidade ISO 27002 – Página 108	0	3	4	3	0
10.1 Identificação da legislação vigente;				x	
10.2 Direitos de propriedade intelectual;				x	
10.3 Proteção de registros organizacionais;			x		
10.4 Proteção de dados e privacidade de informações pessoais;			x		
10.5 Prevenção de mau uso de recursos de processamento da informação;				x	
10.6 Regulamentação de controles de criptografia;		x			
10.7 Conformidade com as políticas e normas de segurança da informação;		x			
10.8 Verificação da conformidade técnica;			x		
10.9 Controles de auditoria de sistemas de informação;			x		
10.10 Proteção de ferramentas de auditoria de sistemas de informação.		x			

Avaliador: Flori César Peccin
Data: 22/08/2011

O instrumento a seguir tem por objetivo avaliar a adequação aos controles relacionados à segurança da informação considerando a norma ISO/IEC 27002. De acordo com o código de prática à gestão da segurança da informação considerando os seguintes níveis:

Proteção Inadequada: Não existe nenhum esforço para implementação dos controles recomendados. Produtos e equipamentos certificados não tem qualquer influência na classificação das seções neste nível;
Proteção mínima: A organização adota o mínimo de controles recomendados. Produtos e equipamentos certificados não tem qualquer influência na classificação das seções neste nível;
Proteção razoável: A maioria dos controles são implementados e devem satisfazer os requisitos com base em procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso;
Proteção adequada: Implementa todos os controles recomendados pelo domínio. Sempre que possível é obrigatório o uso de produtos e equipamentos certificados;
Não aplicável: Considerando o segmento ou estrutura da empresa, tal controle não se aplica.

Quadro de análise:

Marque com um “x” na coluna que você considera que a respectiva prática de segurança se encontra:

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
1 - Política da Segurança da Informação. ISO 27002 – Página 8	0	1	1	0	0
1.1 - Documento da política de segurança da informação;		x			
1.2 - Análise crítica da política de segurança da informação			x		
2 - Organizando a Segurança Informação. ISO 27002 – Página 10	0	4	8	5	0
2.1 - Comprometimento da direção com a segurança da informação no processo crítico de gestão comercial;			x		
2.2 - Coordenação da segurança da informação em transações relacionadas aos custos comerciais;				x	
2.3 - Processo de autorização para os recursos de processamento da informação em transações comerciais;				x	
2.4 - Acordos de confidencialidade na definição de política de preços;		x			
2.5 - Acordos de confidencialidade na definição de prazos;		x			
2.6 - Acordos de confidencialidade no estabelecimento de descontos;			x		
2.7 - Acordos de confidencialidade em negociações de compra de mercadorias para comercialização;			x		
2.8 - Contato com departamentos de controladoria, contabilidade, cobrança, vendas e marketing;				x	
2.9 - Contato com grupos de vendedores e representantes;		x			
2.10 - Contato com grupos de filiais;			x		
2.11 - Análise crítica independente de segurança da informação envolvendo operações comerciais;				x	
2.12 - Identificação dos riscos de segurança da informação relacionados às filiais nos processos de gestão de estoques;			x		
2.13 - Identificação dos riscos de segurança de informação relacionados às filiais nos processos de gestão de vendas;			x		
2.14 - Identificação dos riscos de segurança da informação relacionados às filiais nos processos de gestão financeira;				x	
2.15 - Identificando a segurança da informação, quando tratando com os fornecedores;		x			
2.16 - Identificando a segurança da informação, quando tratando com clientes;			x		

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
2.17 - Identificando segurança da informação nos acordos com financeiras e escritórios de cobrança;			x		
3 - Gestão de ativos (GA). ISO 27002 – Página 21	0	0	2	2	0
3.1 - Inventário dos ativos: estoques, patrimônio, financeiro.			x		
3.2 - Proprietário dos ativos - Atribuição de Responsáveis.			x		
3.3 - Recomendações para classificação (Confidencialidade, Integridade, Disponibilidade, Efetividade e Eficiência).				x	
3.4 - Rótulos e tratamento da informação;				x	
4 - Segurança em recursos humanos. ISO 27002 – Página 25	3	6	1	0	0
4.1 - Papéis e responsabilidades nos processos de vendas;		x			
4.2 - Papéis e responsabilidades nos processos de compras;		x			
4.3 - Processo de seleção funcional para gestão de sistemas de custos comerciais;	x				
4.4 - Processo de seleção funcional para gestão de sistemas financeiros (Cobrança, Baixa de Títulos);		x			
4.5 - Termos e condições de contratação;	x				
4.6 - Conscientização, educação e treinamento em segurança da informação;	x				
4.7 - Processo disciplinar quanto a acesso a sistemas, utilização de equipamentos fora da empresa, informações privilegiadas e tráfego de informações;			x		
4.8 - Encerramento de atividades do uso do sistema de gestão de custos, formação de preços		x			
4.9 - Encerramento de atividades do uso do sistema de gestão de financeira (Controladoria, Contabilidade, Cobrança e Financeiro)		x			
4.10 - Processo de gestão de direitos de acesso (interno e externo).		x			
5 - Gerenciamento das operações e comunicações. ISO 27002 – Página 40	3	14	7	7	
5.1 - Documentação dos procedimentos de operação de sistemas de custos comerciais em aplicativos Office;		x			
5.2 - Controles internos sobre as operações de custos comerciais e formação de preços;		x			
5.3 - Gestão de mudanças em operações que impactam em custos comerciais;			x		
5.4 - Separação dos recursos de formação de custos, formação de preços e de confirmação de margens de lucro;				x	
5.5 Eficiências na entrega de serviços;		x			
5.6 Monitoramento e análise crítica de serviços terceirizados;		x			
5.7 Gerenciamento de mudanças para serviços terceirizados;			x		

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
5.8 Gestão de capacidade de transporte e armazenamento;				x	
5.9 Controle aceitação de sistemas;			x		
5.10 Controles codificados e de rastreabilidade de mercadorias;		x			
5.11 Cópias de segurança das informações;			x		
5.12 Controles e segurança dos serviços de redes;				x	
5.13 Gerenciamento de mídias removíveis;				x	
5.14 Descarte de mídias;		x			
5.15 Procedimentos para tratamento de informação;			x		
5.16 Segurança da documentação dos sistemas;		x			
5.17 Políticas e procedimentos para troca de informações;	x				
5.18 Acordos para a troca de informações;	x				
5.19 Mensagens eletrônicas;				x	
5.20 Transações on-line;				x	
5.21 Registros de auditoria;	x				
5.22 Monitoramento do uso do sistema;				x	
5.23 Proteção das informações dos registros (log);		x			
5.24 Registros (log) de administrador e operador;		x			
5.25 Registros (log) de falhas;		x			
5.26 Controles internos sobre as operações de compras e controles de estoques;		x			
5.27 Gestão de mudanças em operações que impactam em compras e controles de estoques;		x			
5.28 Gestão de mudanças em operações que impactam em controles financeiros;		x			
5.29 Controles internos sobre as operações financeiras;		x			
5.30 Gestão de mudanças em operações que impactam nos processos de elaboração de informações estratégicas da Controladoria;			x		
5.31 Controles internos sobre processos de elaboração de informações estratégicas da Controladoria;			x		
6 - Controle de acessos. ISO 27002 – Página 65	1	5	7	10	0
6.1 Política de controle de acesso;		x			
6.2 Registro de usuário;			x		
6.3 Gerenciamento de privilégios;				x	
6.4 Análise crítica dos direitos de acesso de usuário;			x		
6.5 Uso de senhas;		x			
6.6 Equipamento de usuário sem monitoração;	x				
6.7 Política de mesa limpa e tela limpa;		x			
6.8 Política de uso dos serviços de rede;				x	
6.9 Autenticação para conexão externa do usuário;				x	

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
6.10 Identificação de equipamento em redes;				x	
6.11 Proteção e configuração de portas de diagnóstico remotas;				x	
6.12 Segregação de redes;				x	
6.13 Controle de conexão de rede;				x	
6.14 Controle de roteamento de redes;				x	
6.15 Procedimentos seguros de entrada no sistema (log-on);				x	
6.16 Sistema de gerenciamento de senha;			x		
6.17 Uso de utilitários de sistema;		x			
6.18 Desconexão de terminal por inatividade;			x		
6.19 Limitação de horário de conexão;				x	
6.20 Restrição de acesso à informação;			x		
6.21 Isolamento de sistemas sensíveis;		x			
6.22 Computação e comunicação móvel;			x		
6.23 Trabalho remoto.			x		
7 - Aquisição, desenvolvimento e manutenção de sistemas de informação. ISO 27002 – Página 84	3	4	8	1	0
7.1 Análise e especificação dos requisitos de segurança;			x		
7.2 Validação dos dados de entrada;			x		
7.3 Controle do processamento interno;			x		
7.4 Treinamento usuários com a participação das áreas envolvidas;		x			
7.5 Validação de informações de saída;			x		
7.6 Política para o uso de controles criptográficos;		x			
7.7 Gerenciamento de chaves;			x		
7.8 Controle de software operacional;			x		
7.9 Proteção dos dados para teste de sistema;			x		
7.10 Controle de acesso ao código-fonte de programa;		x			
7.11 Procedimentos para controle de mudanças;				x	
7.12 Análise crítica técnica das aplicações após mudanças no sistema operacional;	x				
7.13 Restrições sobre mudanças em pacotes de software;	x				
7.14 Vazamento de informações;	x				
7.15 Desenvolvimento terceirizado de software;		x			
7.16 Controle de vulnerabilidades técnicas.			x		
8 - Gestão de incidentes de segurança da informação. ISO 27002 – Página 98	1	1	3	1	0
8.1 Notificação de eventos de segurança da informação;	x				
8.2 Notificando fragilidades de segurança da informação;		x			
8.3 Responsabilidades e procedimentos;			x		
8.4 Aprendendo com os incidentes de segurança da informação;			x		

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
8.5 Coleta de evidências;				x	
8.6 Grau de participação das áreas envolvidos nos processos de geração de informações.			x		
9 - Gestão da continuidade do negócio ISO 27002 – Página 103	0	1	3	1	0
9.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio;			x		
9.2 Continuidade de negócios e análise/avaliação de riscos;			x		
9.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação;				x	
9.4 Estrutura do plano de continuidade do negócio;			x		
9.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.		x			
10 - Conformidade ISO 27002 – Página 108	0	2	4	4	0
10.1 Identificação da legislação vigente;				x	
10.2 Direitos de propriedade intelectual;				x	
10.3 Proteção de registros organizacionais;				x	
10.4 Proteção de dados e privacidade de informações pessoais;			x		
10.5 Prevenção de mau uso de recursos de processamento da informação;			x		
10.6 Regulamentação de controles de criptografia;				x	
10.7 Conformidade com as políticas e normas de segurança da informação;		x			
10.8 Verificação da conformidade técnica;		x			
10.9 Controles de auditoria de sistemas de informação;			x		
10.10 Proteção de ferramentas de auditoria de sistemas de informação.			x		

Avaliador: Jacson Moacir Demétrio
Data: 23/08/2011

O instrumento a seguir tem por objetivo avaliar a adequação aos controles relacionados à segurança da informação considerando a norma ISO/IEC 27002. De acordo com o código de prática à gestão da segurança da informação considerando os seguintes níveis:

Proteção Inadequada: Não existe nenhum esforço para implementação dos controles recomendados. Produtos e equipamentos certificados não tem qualquer influência na classificação das seções neste nível;
Proteção mínima: A organização adota o mínimo de controles recomendados. Produtos e equipamentos certificados não tem qualquer influência na classificação das seções neste nível;
Proteção razoável: A maioria dos controles são implementados e devem satisfazer os requisitos com base em procedimentos escritos e processos sendo executados em um nível razoável. Produtos e equipamentos certificados têm preferência de uso;
Proteção adequada: Implementa todos os controles recomendados pelo domínio. Sempre que possível é obrigatório o uso de produtos e equipamentos certificados;
Não aplicável: Considerando o segmento ou estrutura da empresa, tal controle não se aplica.

Quadro de análise:

Marque com um “x” na coluna que você considera que a respectiva prática de segurança se encontra:

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
1 - Política da Segurança da Informação. ISO 27002 – Página 8	0	2	0	0	0
1.1 - Documento da política de segurança da informação;		x			
1.2 - Análise crítica da política de segurança da informação		x			
2 - Organizando a Segurança Informação. ISO 27002 – Página 10	6	7	3	1	0
2.1 - Comprometimento da direção com a segurança da informação no processo crítico de gestão comercial;		x			
2.2 - Coordenação da segurança da informação em transações relacionadas aos custos comerciais;		x			
2.3 - Processo de autorização para os recursos de processamento da informação em transações comerciais;		x			
2.4 - Acordos de confidencialidade na definição de política de preços;			x		
2.5 - Acordos de confidencialidade na definição de prazos;			x		
2.6 - Acordos de confidencialidade no estabelecimento de descontos;		x			
2.7 - Acordos de confidencialidade em negociações de compra de mercadorias para comercialização;			x		
2.8 - Contato com departamentos de controladoria, contabilidade, cobrança, vendas e marketing;				x	
2.9 - Contato com grupos de vendedores e representantes;	x				
2.10 - Contato com grupos de filiais;	x				
2.11 - Análise crítica independente de segurança da informação envolvendo operações comerciais;	x				
2.12 - Identificação dos riscos de segurança da informação relacionados às filiais nos processos de gestão de estoques;	x				
2.13 - Identificação dos riscos de segurança de informação relacionados às filiais nos processos de gestão de vendas;	x				
2.14 - Identificação dos riscos de segurança da informação relacionados às filiais nos processos de gestão financeira;	x				
2.15 - Identificando a segurança da informação, quando tratando com os fornecedores;		x			
2.16 - Identificando a segurança da informação, quando tratando com clientes;		x			

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
2.17 - Identificando segurança da informação nos acordos com financeiras e escritórios de cobrança;		x			
3 - Gestão de ativos (GA). ISO 27002 – Página 21	2	2	0	0	0
3.1 - Inventário dos ativos: estoques, patrimônio, financeiro.		x			
3.2 - Proprietário dos ativos - Atribuição de Responsáveis.		x			
3.3 - Recomendações para classificação (Confidencialidade, Integridade, Disponibilidade, Efetividade e Eficiência).	x				
3.4 - Rótulos e tratamento da informação;	x				
4 - Segurança em recursos humanos. ISO 27002 – Página 25	2	6	2	0	0
4.1 - Papéis e responsabilidades nos processos de vendas;		x			
4.2 - Papéis e responsabilidades nos processos de compras;		x			
4.3 - Processo de seleção funcional para gestão de sistemas de custos comerciais;			x		
4.4 - Processo de seleção funcional para gestão de sistemas financeiros (Cobrança, Baixa de Títulos);			x		
4.5 - Termos e condições de contratação;		x			
4.6 - Conscientização, educação e treinamento em segurança da informação;		x			
4.7 - Processo disciplinar quanto a acesso a sistemas, utilização de equipamentos fora da empresa, informações privilegiadas e tráfego de informações;		x			
4.8 - Encerramento de atividades do uso do sistema de gestão de custos, formação de preços	x				
4.9 - Encerramento de atividades do uso do sistema de gestão de financeira (Controladoria, Contabilidade, Cobrança e Financeiro)	x				
4.10 - Processo de gestão de direitos de acesso (interno e externo).		x			
5 - Gerenciamento das operações e comunicações. ISO 27002 – Página 40	8	12	11	0	0
5.1 - Documentação dos procedimentos de operação de sistemas de custos comerciais em aplicativos Office;	x				
5.2 - Controles internos sobre as operações de custos comerciais e formação de preços;		x			
5.3 - Gestão de mudanças em operações que impactam em custos comerciais;	x				
5.4 - Separação dos recursos de formação de custos, formação de preços e de confirmação de margens de lucro;	x				
5.5 Eficiências na entrega de serviços;		x			
5.6 Monitoramento e análise crítica de serviços terceirizados;	x				
5.7 Gerenciamento de mudanças para serviços terceirizados;		x			

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
5.8 Gestão de capacidade de transporte e armazenamento;			x		
5.9 Controle aceitação de sistemas;		x			
5.10 Controles codificados e de rastreabilidade de mercadorias;		x			
5.11 Cópias de segurança das informações;			x		
5.12 Controles e segurança dos serviços de redes;			x		
5.13 Gerenciamento de mídias removíveis;			x		
5.14 Descarte de mídias;	x				
5.15 Procedimentos para tratamento de informação;	x				
5.16 Segurança da documentação dos sistemas;			x		
5.17 Políticas e procedimentos para troca de informações;		x			
5.18 Acordos para a troca de informações;		x			
5.19 Mensagens eletrônicas;		x			
5.20Transações on-line;		x			
5.21 Registros de auditoria;		x			
5.22 Monitoramento do uso do sistema;			x		
5.23 Proteção das informações dos registros (log);	x				
5.24 Registros (log) de administrador e operador;	x				
5.25 Registros (log) de falhas;		x			
5.26 Controles internos sobre as operações de compras e controles de estoques;			x		
5.27 Gestão de mudanças em operações que impactam em compras e controles de estoques;			x		
5.28 Gestão de mudanças em operações que impactam em controles financeiros;			x		
5.29 Controles internos sobre as operações financeiras;		x			
5.30 Gestão de mudanças em operações que impactam nos processos de elaboração de informações estratégicas da Controladoria;			x		
5.31 Controles internos sobre processos de elaboração de informações estratégicas da Controladoria;			x		
6 - Controle de acessos. ISO 27002 – Página 65	3	4	9	7	0
6.1 Política de controle de acesso;			x		
6.2 Registro de usuário;			x		
6.3 Gerenciamento de privilégios;			x		
6.4 Análise crítica dos direitos de acesso de usuário;			x		
6.5 Uso de senhas;			x		
6.6 Equipamento de usuário sem monitoração;			x		
6.7 Política de mesa limpa e tela limpa;	x				
6.8 Política de uso dos serviços de rede;			x		
6.9 Autenticação para conexão externa do usuário;				x	
6.10 Identificação de equipamento em redes;			x		

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
6.11 Proteção e configuração de portas de diagnóstico remotas;		x			
6.12 Segregação de redes;				x	
6.13 Controle de conexão de rede;				x	
6.14 Controle de roteamento de redes;				x	
6.15 Procedimentos seguros de entrada no sistema (log-on);				x	
6.16 Sistema de gerenciamento de senha;				x	
6.17 Uso de utilitários de sistema;		x			
6.18 Desconexão de terminal por inatividade;	x				
6.19 Limitação de horário de conexão;		x			
6.20 Restrição de acesso à informação;				x	
6.21 Isolamento de sistemas sensíveis;	x				
6.22 Computação e comunicação móvel;		x			
6.23 Trabalho remoto.			x		
7 - Aquisição, desenvolvimento e manutenção de sistemas de informação. ISO 27002 – Página 84	0	10	3	0	3
7.1 Análise e especificação dos requisitos de segurança;		x			
7.2 Validação dos dados de entrada;		x			
7.3 Controle do processamento interno;			x		
7.4 Treinamento usuários com a participação das áreas envolvidas;					x
7.5 Validação de informações de saída;		x			
7.6 Política para o uso de controles criptográficos;		x			
7.7 Gerenciamento de chaves;					x
7.8 Controle de software operacional;		x			
7.9 Proteção dos dados para teste de sistema;		x			
7.10 Controle de acesso ao código-fonte de programa;					x
7.11 Procedimentos para controle de mudanças;		x			
7.12 Análise crítica técnica das aplicações após mudanças no sistema operacional;		x			
7.13 Restrições sobre mudanças em pacotes de software;		x			
7.14 Vazamento de informações;		x			
7.15 Desenvolvimento terceirizado de software;			x		
7.16 Controle de vulnerabilidades técnicas.			x		
8 - Gestão de incidentes de segurança da informação. ISO 27002 – Página 98	2	4	0	0	0
8.1 Notificação de eventos de segurança da informação;		x			
8.2 Notificando fragilidades de segurança da informação;		x			
8.3 Responsabilidades e procedimentos;		x			
8.4 Aprendendo com os incidentes de segurança da informação;		x			
8.5 Coleta de evidências;	x				

	1 - Inadequada	2 - Mínima	3 - Razoável	4 - Adequada	Não Aplicável
8.6 Grau de participação das áreas envolvidos nos processos de geração de informações.	x				
9 - Gestão da continuidade do negócio ISO 27002 – Página 103	5	0	0	0	0
9.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio;	x				
9.2 Continuidade de negócios e análise/avaliação de riscos;	x				
9.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação;	x				
9.4 Estrutura do plano de continuidade do negócio;	x				
9.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio.	x				
10 - Conformidade ISO 27002 – Página 108	1	6	3	0	0
10.1 Identificação da legislação vigente;	x				
10.2 Direitos de propriedade intelectual;		x			
10.3 Proteção de registros organizacionais;			x		
10.4 Proteção de dados e privacidade de informações pessoais;			x		
10.5 Prevenção de mau uso de recursos de processamento da informação;			x		
10.6 Regulamentação de controles de criptografia;		x			
10.7 Conformidade com as políticas e normas de segurança da informação;		x			
10.8 Verificação da conformidade técnica;		x			
10.9 Controles de auditoria de sistemas de informação;		x			
10.10 Proteção de ferramentas de auditoria de sistemas de informação.		x			

ANEXO B – ROTEIRO DE ENTREVISTA COM OS GESTORES

1 Nome do respondente

2 Cargo

3 Tempo no Cargo

4 Tempo de empresa

5 Formação acadêmica

6 Idade

7 Principais responsabilidades

SEÇÃO I – INFORMAÕES GERAIS DO GESTORE ENTREVISTADO SOBRE PROCESSOS DE INTEGRAÇÃO ENTRE AS ÁREAS DE CONTROLADORIA E TI

1) De maneira geral, cite quais os fatores limitadores nos processos de integração entre as áreas de Controladoria e TI nas alterações de sistemas/softwares que afetam o ambiente da informação?

2) Quais seriam os processos que possibilitam a aproximação das áreas de Controladoria e TI?

3) Como a Controladoria poderia atuar para evitar possíveis vulnerabilidades no sistema de informações advindos das alterações de sistemas/softwares?

4) Como a TI poderia atuar para evitar possíveis retrabalhos advindos de erros nas alterações de sistemas/softwares que impactam nas atividades operacionais da Controladoria?

SEÇÃO II – POLÍTICAS E CONTROLES RELACIONADOS À SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO NA PERCEPÇÃO DA CONTROLADORIA E TI

5) De maneira geral, quais os riscos possíveis que a empresa pode incorrer ao não estabelecer os papéis e responsabilidades dos usuários envolvidos nos processos de vendas ou de compras? (incluído como

resultado da aplicação do primeiro instrumento metodológico – Domínio n° 4 da norma ISO 27002 – Segurança em RH).

6) 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 este processo? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 4 da norma ISO 27002 – Se gurança em RH).

7) A implementação de procedimentos de controles codificados e de sistema para a rastreabilidade de mercadorias pode contribuir com o processo de gestão de estoques e de atendimento aos clientes? Quais riscos seriam mitigados com esta implementação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Gerenciamento das operações e comunicações).

8) Na percepção da Controladoria de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma IS O 27002 – Gerenciamento das operações e comunicações).

9) Na percepção da TI de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Ge renciamento das operações e comunicações).

10) A definição de políticas e procedimentos para troca de informações entre empresa e entidades externas é relevante para evitar riscos contábeis, fiscais e financeiros? Cite de acordo com seu entendimento quais os principais riscos para a empresa? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Gerenciamento das operações e comunicações).

11) De maneira geral, qual o entendimento sobre a participação das áreas de Controladoria e de TI na elaboração de treinamentos para usuários a fim de garantir a segurança de informações? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma

ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).

12) Quais procedimentos de análise critica técnica das aplicações após mudanças no sistema operacional? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).

13) Como se daria a participação das áreas de Controladoria e de TI nas restrições sobre mudanças em pacotes de software? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).

14) Quais os procedimentos adequados para evitar o risco de vazamento de informações relevantes? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).

15) Após as alterações no sistema operacional, entende-se que deve-se efetuar testes envolvendo usuários responsáveis pela gestão da informações para validar tais alterações? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).

16) De maneira geral, como deve ser o procedimento de notificação de eventos de segurança da informação para conhecimento e tomada de ação corretiva em tempo hábil? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 8 da norma ISO 27002 - Gestão de incidentes de segurança da informação).

17) De maneira geral, considera-se importante o envolvimento das áreas de Controladoria e de TI nas análises e avaliações de riscos de continuidade do negócio no que se refere ao processamento, geração e segurança da informação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 9 da norma ISO 27002 - Gestão da continuidade do negócio).

18) De maneira geral, é entendimento que a participação e envolvimento dos usuários com as políticas e normas de segurança da informação

contribuem com os requisitos de segurança da informação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 10 da norma ISO 27002 - Conformidade).

SEÇÃO III – ATUAÇÃO DAS ÁREAS DE CONTROLADORIA E DE TI NA ORGNIZAÇÃO EM: (I) PROCESSOS DE ALTERAÇÕES DE SOFTWARE; (II) POLITICAS DE SEGURANÇA; (III) INSERÇÃO DOS USUÁRIOS; E, (IV) RISCOS OPERACIONAIS RELACIONADOS

19) Qual a visão da Controladoria em relação ao envolvimento da área nos processos de decisões sobre alterações de sistemas operacionais na empresa? (Corina e Corina, 2009).

20) Quais os requisitos/atributos considerados pelas áreas de Controladoria e de TI quanto a informação disponibilizada aos seus diversos usuários? (CPC, 2008; Cobit, 2007).

21) Qual a percepção das áreas de Controladoria e de TI em relação ao tema segurança da informação e sua importância estratégica para a empresa? (KAYWORTH; WHITTEN, 2010).

22) Quais as principais funções desempenhadas pela área de Controladoria na empresa? (BORINELLI, 2006).

23) De maneira geral, como a área de Controladoria promove ações junto as demais áreas da empresa para direcionar as pessoas aos objetivos da organização? (Corina e Corina, 2009).

24) 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? (OLIVEIRA, 2009).

25) De maneira geral, de que forma a Controladoria atua nos processos de segurança da informação para garantir que o sistema de informações da empresa atenda às necessidades estratégicas e operacionais da empresa? (ATKINSON et. al., 2008).

26) As áreas de Controladoria e de TI consideram relevante adotar uma gestão holística para tornar as implementações de segurança da informação mais eficaz? (YOUNG; WINDSOR, 2010; ELOFF; ELOFF, 2003).

27) De maneira geral entende-se que a inserção dos usuários possa contribuir com a eficácia nas políticas que visam prevenir, detectar ou minimizar eventuais riscos decorrentes de falhas de segurança de informações na empresa? (SPEARS; BARKI, 2010).

28) De que maneira as áreas de TI e de Controladoria podem atuar em conjunto na inserção dos usuários a fim de conscientizá-los com as políticas de segurança de informações? (SPEARS; BARKI, 2010).

29) Que riscos relacionados à segurança da informação podem ser minimizados tendo os usuários como principais aliados da empresa? (BULGURCU; CAVUSOGLU; BENBASAT, 2010).

30) Como as áreas de Controladoria e de TI abordam as necessidades de adequação dos softwares utilizados na empresa com relação as necessidades de geração de informações de apoio a tomada e decisão dos gestores? (WILKIN; CHENHALL, 2010).

ANEXO C – ENTREVISTAS REALIZADAS COM OS GERENTES DE TI, CONTROLADORIA E CONTABILIDADE/FISCAL

NOME DO RESPONDENTE: Luis Carlos Alberti
CARGO: Gerente de TI
TEMPO NO CARGO: 6 anos
TEMPO DE EMPRESA: 25 anos
FORMÇÃO ACADÊMICA: Bacharel em Ciências Contábeis com MBA em Gerenciamento de Projetos e em Gestão Empresarial.
IDADE: 44 anos
PRINCIPAIS RESPONSABILIDADES: Direcionar, desenvolver e conduzir as ações relacionadas ao Planejamento Estratégico de TI. Definir a arquitetura lógica e física da infraestrutura, com sistemas operacionais adequados e gerenciamento da implantação, gerenciando as questões relacionadas a treinamento/capacitação, gestão da performance, seleção de pessoas, remuneração e carreira, bem como pelos indicadores de resultados da equipe de TI. Além disto, estudo e proponho processos para adequação dos sistemas de informação aos objetivos de negócio da empresa, fomentando perante a equipe a realização de pesquisa, geração, desenvolvimento e implantação de novas soluções de tecnologia.
SEÇÃO I – INFORMAÕES GERAIS DO GESTOR ENTREVISTADO SOBRE PROCESSOS DE INTEGRAÇÃO ENTRE AS ÁREAS DE CONTROLADORIA E TI
De maneira geral, cite quais os fatores limitadores nos processos de integração entre as áreas de Controladoria e TI nas alterações de sistemas/softwares que afetam o ambiente da informação? Um dos principais fatores que limitam a integração das áreas de Controladoria e TI, seria o alinhamento quanto ao entendimento do negócio. A TI tem visão técnica e pouco sistêmica do negócio, por outro lado, a Controladoria por possuir uma linguagem contábil e financeira, muitas vezes dificulta a compreensão das demais áreas e da própria TI, gerando uma limitação ao processo de integração destas áreas. Outro fator limitador é a falta de planejamento sistêmico das áreas da empresa quanto às solicitações de customizações dos softwares, onde o senso de urgência prevalece, não diagnosticando o que é necessário e relevante para o negócio. Criando procedimentos adequados para estes fatores limitadores entende-se que possamos aproximar e integrar as áreas.
Quais seriam os processos que possibilitam a aproximação das áreas de Controladoria e TI? Entende-se que o alinhamento da linguagem entre as áreas de Controladoria e de TI seria um processo que possibilitaria a aproximação das áreas. Este processo tende a gerar o entendimento do negócio. Para a realização deste alinhamento, poderíamos criar uma linha ou canal de comunicação, onde a TI juntamente com a Controladoria através de um comitê, passaria a analisar as mudanças de software que afetam o negócio. Contemplando alterações relevantes que afetam o negócio, haveria um processo de homologação. Após, efetuar-se-ia a alteração de software.

Como a Controladoria poderia atuar para evitar possíveis vulnerabilidades no sistema de informações advindos das alterações de sistemas/softwares?

Através de um processo de aprendizado contínuo junto às demais áreas da empresa. Por ter uma linguagem contábil e financeira que não é de domínio de todas as pessoas e áreas da empresa, deve-se disseminar através de um processo educativo que determinadas ações podem afetar as regras de negócio e consequentemente o resultado da empresa. É importante as áreas conhecerem a DRE – Demonstração de Resultado, Margem de Contribuição e que, alterações de sistemas com um processo de análise insuficiente e sem o envolvimento adequado das áreas pode disseminar informações erradas a partir do sistema de informações da empresa para a direção, conselho de administração gerando tomada de decisões equivocadas. Este processo poderia contribuir com a minimização das vulnerabilidades do sistema de informações da empresa.

Como a TI poderia atuar para evitar possíveis retrabalhos advindos de erros nas alterações de sistemas/softwares que impactam nas atividades operacionais da Controladoria?

Um ciclo normal, num processo de alteração de software, consiste inicialmente pela solicitação de alteração de software pelo usuário. A TI procede o entendimento técnico e aprova com o usuário solicitante. Após aprovação, inicia-se a fase do desenvolvimento e de testes que se julga necessário. Posteriormente vai para uma área de homologação. Na etapa de homologação existem as principais dificuldades, pois gerar um ambiente fidedigno de testes e envolver as áreas ou usuários chaves é o grande desafio antes de colocar em operação. Portanto, proporcionar um ambiente fidedigno, envolvendo os usuários chaves espera-se qualificar o processo de entrega de TI minimizando retrabalhos e por conseguinte resultando em ganhos financeiro.

SEÇÃO II – POLÍTICAS E CONTROLES RELACIONADOS À SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO NA PERCEPÇÃO DA CONTROLADORIA E TI

De maneira geral, quais os riscos possíveis que a empresa pode incorrer ao não estabelecer os papéis e responsabilidades dos usuários envolvidos nos processos de vendas ou de compras? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 4 da norma ISO 27002 – Segurança em RH).

Qualquer processo deve ter documentado papéis e responsabilidades quanto a segurança da informação visando não comprometer o negócio. Por exemplo, podemos citar os processos de compras e vendas. No processo de compras, pode se incorrer em negociação privilegiada junto a um fornecedor que tem maior preço, com produtos de qualidade inferior, gerando prejuízos financeiros e de imagem da empresa. No processo de vendas, a definição de papéis e responsabilidades permite alinhamento de prática de preços entre as diversas lojas da empresa, evitando praticas de preços diferentes, descontos a maior para determinados produtos que não caberia a aplicação de desconto, o que resultaria em comprometimento das margens da empresa. Desta forma, estabelecer papéis e responsabilidades quanto a segurança da informação evita possíveis riscos financeiros e intangíveis junto a clientes e fornecedores.

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 este processo? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 4 da norma ISO 27002 – Segurança em RH). A implementação deveria se dar através de treinamentos contínuos. Estes processos devem ser liderados pelas áreas de Controladoria e de TI, aos quais devem elaborar o material técnico para o treinamento. A organização, calendário, recursos para apresentação e envolvimento das pessoas deve ser liderado pela área de RH. Nestes treinamentos seriam abordados aspectos técnicos da segurança da informação por parte da TI e as questões de negócio quanto a informação para tomada de decisão por parte da Controladoria. Desta forma, entende-se que a conscientização dos usuários faria parte da cultura da organização, se tornando fator chave nos processos de segurança e disponibilidade de informações dentro dos critérios necessários para a tomada de decisão dos gestores da empresa. Entende-se que, a segurança da informação somente através da parametrização de softwares quanto a acesso, usos de programas é limitante. A inserção dos usuários e sua responsabilidade no contexto global da empresa seria um fator primordial nas políticas de segurança da informação para as empresas.
A implementação de procedimentos de controles codificados e de sistema para a rastreabilidade de mercadorias pode contribuir com o processo de gestão de estoques e de atendimento aos clientes? Quais riscos seriam mitigados com esta implementação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Gerenciamento das operações e comunicações). Sim. A empresa possui um processo de codificação, mas não temos um processo de rastreabilidade. Atualmente é possível implementar um processo de rastreabilidade, pois o custo está mais acessível para as empresas. Desta forma, pode gerar benefícios principalmente logísticos, de localização dos produtos dentro de um Centro de Distribuição – CD e nas lojas. Permite verificar a qualidade dos estoques e direcionar possíveis promoções de vendas para produtos com saída de linha, e que se não for vendido será substituído no mercado por outro com mais tecnologia, com um preço inferior podendo afetar a lucratividade do negócio. Para o cliente, a rastreabilidade propicia segurança, principalmente porque são processos desassociados, ou seja, quem faz a venda de um produto é o consultor de negócios que utiliza muitas vezes catálogos, quem entrega o produto é o CD, que esta fisicamente localizado distante das lojas, com a rastreabilidade você tem o código do produto e a certeza que o produto que o cliente comprou está sendo entregue. Para fins de auditoria, devido ao volume de itens (6 a 7 mil itens) hoje uma contagem física de 100% levaria 2 dias para se realizar com o CD parado. Com a rastreabilidade permite um processo de auditoria continua, ágil e selecionável. Assim a rastreabilidade permite mitigar riscos financeiros por estoques obsoletos, saldos incorretos levando a tomada de decisões de compras e vendas equivocadas e intangíveis quanto a satisfação da cadeia de valor desde processo inicial da compra até a entrega final do produto ao cliente.

Na percepção da Controladoria de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Ge renciamento das operações e comunicações). Para a Controladoria o log de auditoria permite rastrear o que aconteceu em níveis de implementação no software. A auditoria externa tem como uma das atividades iniciais nos processos de auditoria na empresa, a consulta dos log de auditoria. O log permite identificar usuários e versões de programas modificados que podem ter origem eventuais problemas. Ou seja, pode contribuir operacionalmente em agilizar a identificação do erro, usuários solicitante das alterações e do programador de TI envolvido neste processo.
Na percepção da TI de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Ge renciamento das operações e comunicações). Sim, contribuem. O fluxo de uma alteração passa pelo controle sobre as versões de softwares, para identificar a área solicitante, analisar juntamente com o usuário solicitante as alterações solicitadas. Após desenvolve-se as alterações, faz-se os testes. Porém, o ambiente de testes pode não refletir adequadamente o ambiente oficial gerando falhas ao quais somente serão percebidas após entrada no ambiente oficial. Com os registros (log) de auditoria, permite identificar qual era a versão anterior do programa e imediatamente substituir a versão do programa com erro. A área de TI consegue através do log, identificar qual usuário e área solicitou a alteração, qual o programador que fez a alteração, ou seja, contribui com a gestão da área de TI.
A definição de políticas e procedimentos para troca de informações entre empresa e entidades externas é relevante para evitar riscos contábeis, fiscais e financeiros? Cite de acordo com seu entendimento quais os principais riscos para a empresa? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Gerenciamento das operações e comunicações). É extremamente importante. As normas relativas à troca de informações fazem parte da política de segurança da informação. A empresa também se utiliza de ferramentas de suporte que auxiliam na liberação da troca de informações. Por exemplo, podemos analisar a troca de emails de determinados usuários e identificar qual é a curva normal parar troca de emails, pode-se avaliar, por exemplo, a área de compras e seus contatos com fornecedores, quais são os funcionários acima da curva de troca de informações e dar subsídios aos gestores para agir com base nestas informações. A troca de informações pode comprometer as margens da empresa. Se circular junto ao concorrente uma tabela de preços de determinada promoção, este pode antecipar-se e vir a comprometer um final de semana de vendas. Da mesma forma, riscos fiscais e contábeis com o compartilhamento de senhas para envio de declarações federais ou informações ao SPED. Assim, a estruturação de uma política e procedimentos de troca de informações promove um ambiente que minimize riscos contábeis, fiscais e de negócio.

De maneira geral, qual o entendimento sobre a participação das áreas de Controladoria e de TI na elaboração de treinamentos para usuários a fim de garantir a segurança de informações? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). As áreas de TI, Controladoria e RH, são áreas que tem uma atuação corporativa e devem estar alinhadas na elaboração de treinamentos para usuários a fim de garantir a segurança de informações. Na empresa, estamos implantando um novo ERP e iniciamos um processo através da identificação de usuários chaves para a implantação de treinamentos para que tenham uma visão sistêmica do negócio. Entende-se que a empresa terá pessoas qualificadas e que podem assumir funções no futuro nas mais diversas áreas de atuação. Este programa de treinamento, busca a visão sistêmica da empresa e busca ser uma ação visando a perpetuidade da empresa, uma garantia de sustentabilidade ao negócio.
Quais procedimentos de análise critica técnica das aplicações após mudanças no sistema operacional? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). São procedimentos que envolvem a TI e o cliente solicitante da alteração, no qual a TI contata o seu cliente para verificar se as alterações atenderam suas expectativas. Este procedimento faz parte de um escopo de atuação vinculado ao planejamento da área de TI. Importante é que se deve considerar a participação da área de Controladoria neste processo para avaliar alterações que afetam os pilares do negócio da empresa que são: (i) Clientes; (ii) Produtos e (iii) Margem de Lucro. Alterações solicitadas e documentadas que possam afetar clientes, produtos ou margem de lucro, recebe uma análise preliminar para avaliar possíveis efeitos que podem afetar tomadas de decisão e evitar riscos ao negócio. Citamos por exemplo, alterações que afetem a qualidade dos estoques, as margens dos produtos, a imagem da empresa perante a nossa cadeia de valor.
Como se daria a participação das áreas de Controladoria e de TI nas restrições sobre mudanças em pacotes de software? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). A participação da Controladoria e da TI para ser efetiva nos processos de restrições sobre mudanças em sistemas passa por ter uma atuação pró-ativa. A TI por possuir uma formação mais técnica necessita de uma preparação de visão de negócio que pode ser propiciada pela Controladoria. Com a atuação integrada, alterações solicitadas devem ser analisadas quanto ao seu impacto para o negócio. Desta forma, tem-se um follow-up de todas as alterações demandadas para a área de TI, segregadas por prioridades, as relevantes que afetam os pilares do negócio da empresa das demais que podem ser tratadas de acordo com os recursos disponíveis. Acredita-se que muitos retrabalhos podem ser evitados gerando economias para a empresa.

Quais os procedimentos adequados para evitar o risco de vazamento de informações relevantes? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).

A informação é um ativo importante para a empresa. Para evitar riscos de vazamento de informações devem-se ter políticas e procedimentos claros sobre acesso e trabalhar continuamente a conscientização dos usuários. Muitas informações são valiosas para o mercado, por exemplo, uma base de 5 milhões de clientes, quanto vale no mercado? Se eventualmente, um usuário com acesso indevido à base de informações pode gerar um risco intangível para a empresa. Informações relevantes devem ser identificadas pela empresa e determinar seu acesso a um número de usuários restrito, conscientizá-los. Desta forma, mantêm-se um controle sobre informações relevantes e usuários com acesso as mesmas. Também a utilização de softwares, é um meio eficaz para evitar riscos de vazamento de informações, como a criptografia de dados, que permite a inclusão de senhas que evitam acesso às informações constantes, por exemplo, um notebook que eventualmente foi objeto de furto ou roubo.

Com relação aos técnicos da área de TI que tem acesso à base de dados, pode-se utilizar softwares que mescle as informações, pode trazer dados da base oficial para o ambiente de testes, mesclar, truncar ou distorcer informações que sejam relevantes evitando que determinadas pessoas possam ter acesso. A revisão de perfis de acesso é outro procedimento importante e bastante usual para evitar, por exemplo, que usuários que trocaram de função mantenham o mesmo perfil de acesso anterior e assim acumular acessos aos quais não são necessários.

Após as alterações no sistema operacional, entende-se que deve-se efetuar testes envolvendo usuários responsáveis pela gestão da informações para validar tais alterações? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).

Sim. É entendimento que a responsabilidade da homologação é do usuário final, pois, a TI faz o processo de desenvolvimento do software a partir da solicitação do usuário, analisa, aprova juntamente com o usuário, faz os testes, denominados de “testes unitários”. Quando a TI entende que está adequado, disponibiliza para o ambiente de homologação onde o usuário chave solicitante analisa se os objetivos foram atingidos pelas alterações solicitadas. Importante que a Controladoria participe deste processo principalmente em alterações que afetem os pilares do negócio da empresa quais sejam clientes, produtos e margens de lucro.

De maneira geral, como deve ser o procedimento de notificação de eventos de segurança da informação para conhecimento e tomada de ação corretiva em tempo hábil? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 8 da norma ISO 27002 - Gestão de incidentes de segurança da informação).

O momento adequado para a ação corretiva é no ambiente de homologação de qualquer alteração de software. Existindo um ambiente de homologação estruturado, com testes e envolvimento dos usuários chaves minimiza sensivelmente os riscos de ações corretivas no ambiente oficial de sistemas. O planejamento de alocação de tempo adequado dos testes para homologar antes

de ir para a base oficial, a comunicação e envolvimento das áreas de usuários permitirá que eventuais problemas com segurança da informação que afetam o negócio da empresa seja evitado. Porém ocorrendo eventos, deve-se adotar uma comunicação direcionada aos gestores notificando a informação incorreta e o tempo necessário para correção. Pode também ocorrer notificações de erro por perfil de acesso indevido, uma liberação indevida e o mau uso por parte do usuário. Nesta situação, comunica-se aos gestores envolvidos, o tempo que isto permaneceu na base oficial, quais as possíveis informações que possam ter impacto e que o acesso foi imediatamente restringido. Assim permite uma atuação com maior foco e agilidade para identificar possíveis erros ocasionados.
De maneira geral, considera-se importante o envolvimento das áreas de Controladoria e de TI nas análises e avaliações de riscos de continuidade do negócio no que se refere ao processamento, geração e segurança da informação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 9 da norma ISO 27002 - Gestão da continuidade do negócio). Agregar os conhecimentos de áreas que trabalham com a informação, a TI pensando na estrutura física, nas políticas e procedimentos de um processo da segurança da informação eficiente, e a Controladoria visando formatar informações para tomada de decisão permite que se analise e avalie riscos de continuidade de negócio de uma forma mais holística, contribuindo para mitigar estes riscos. Como exemplo, avaliar o processamento e geração de informações de forma contínua sobre a qualidade dos estoques permitindo um cenário de alinhamento de registros de informações idênticos aos saldos físicos dos estoques da empresa. Do contrário, podem-se tomar decisões de compras que podem gerar estoques obsoletos ou de vendas de algum produto que fisicamente não existe nos estoques da empresa e que gera desconforto junto ao cliente. Numa negociação em volumes maiores, pode-se colocar em risco a continuidade da empresa. Na área Financeira podemos citar ambientes que possibilitem desvios financeiros, perdas por fraudes. Desta forma, as áreas de TI e Controladoria podem contribuir através de análises e de indicadores que permitam monitorar as principais operações da empresa no que tange ao processamento, geração e segurança da informação para mitigar riscos para a empresa. Também agindo pró-ativamente com análises comparativas por exemplo, das receitas, margens, giro de estoques entre lojas de mesmo perfil e porque existem resultados diferentes, é o mercado, o gestor, ou algo relacionado a geração ou segurança da informação que afetam a tomada de decisão.
De maneira geral, é entendimento que a participação e envolvimento dos usuários com as políticas e normas de segurança da informação contribuem com os requisitos de segurança da informação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 10 da norma ISO 27002 - Conformidade). O envolvimento e a participação de usuários nas políticas de segurança da informação contribuem de forma decisiva para a sua eficácia. A comunicação clara com estes usuários, conscientizar sobre a importância de cada um no processo fazendo com que se sintam para integrante, responsáveis e corresponsáveis pelo sistema de informações da empresa. Os processos que permeiam a empresa tem verticalidade, eles nascem numa área e interligam-se

com as demais áreas da empresa. Para ter este envolvimento e participação se faz necessário treinamento de forma sistemática com uma comunicação clara do que realmente é importante. Disseminar a importância de gerar informações com qualidade para o publico certo, e que isto refletirá em decisões acertadas que vão beneficiar a empresa. O usuário é uma das peças chaves para o sucesso de uma política de segurança da informação.

SEÇÃO III – ATUAÇÃO DAS ÁREAS DE CONTROLADORIA E DE TI NA ORGNIZAÇÃO EM: (I) PROCESSOS DE ALTERAÇÕES DE SOFTWARE; (II) POLITICAS DE SEGURANÇA; (III) INSERÇÃO DOS USUÁRIOS; E, (IV) RISCOS OPERACIONAIS RELACIONADOS

Qual a visão da Controladoria em relação ao envolvimento da área nos processos de decisões sobre alterações de sistemas operacionais na empresa? (Corina e Corina, 2009).

A Controladoria por ser responsável pelos sistemas de informações na empresa e ter uma visão sistêmica do negócio, deve envolver-se nos processos que visam alterar os softwares na empresa, analisando o que está sendo solicitado. Deve ter uma atuação pró ativa, contribuindo quando entender tratar-se de uma alteração pertinente, subsidiando com informações que justifiquem tais alterações. Percebe-se que a área de TI efetua muitas alterações em softwares, ou customizações de relatórios que muitas vezes não geram valor para o negócio, alterações são entregues ao solicitante e estas ficam de 1 ano a 2 anos sem ser utilizadas, portanto, existem oportunidades de economia financeira envolvida neste processo. Alterações que impactam positivamente nos pilares de negócio da empresa, ou por questões legais devem ser priorizadas, as que não trazem este contexto passam por um questionamento se realmente cabe tal solicitação.

Quais os requisitos/atributos considerados pelas áreas de Controladoria e de TI quanto a informação disponibilizada aos seus diversos usuários? (CPC, 2008; Cobit, 2007).

A informação deve atender os requisitos de tempestividade, confiabilidade e confidencialidade e direcionada ao público certo. Uma das questões relevantes da entrega da informação ao público certo e no tempo certo, é entender a necessidade do usuário, muitas vezes a precisão da informação pode ter custo elevado de obtenção e comprometer o prazo de entrega, esta percepção as áreas de Controladoria e TI devem possuir e exercitar. Os públicos requerem informações diferentes, como o vendedor, por exemplo, que necessita ter a informação sobre produtos, características, preço, quais são as promoções que a companhia está divulgando, que tipo de cliente é o cliente alvo para aquele tipo de produto. A diretoria necessita de informações sintéticas dos grandes números da companhia, vendas totais, investimentos, fluxo de caixa, ou seja, cada público requer uma gama de informações dentro dos requisitos necessários para que possibilite ações adequadas para a melhoria de performance da empresa como um todo.

Qual a percepção das áreas de Controladoria e de TI em relação ao tema segurança da informação e sua importância estratégica para a empresa? (KAYWORTH; WHITTEN, 2010) A importância estratégica da segurança da informação é considerada um requisito básico. A segurança física é de responsabilidade da área de TI com apoio de uma auditoria para analisar de forma sistemática se estão sendo adotadas as melhores práticas de segurança da informação como, por exemplo, acessos adequados, realização de backups das informações, etc. A Controladoria por municiar com informações a tomada de decisões dos gestores, em especial as decisões estratégicas do conselho de administração e diretoria, atua para que o ambiente da informação seja seguro e estável. Os resultados obtidos pela empresa nestes seus 52 anos de existência, reforçam a importância estratégica da segurança das informações, pois num ambiente de extrema concorrência, margens apertadas, onde os produtos vendidos possuem práticas de preços muito semelhantes o suporte de um ambiente informacional seguro e com os principais requisitos possibilitam o apoio às melhores decisões.
Quais as principais funções desempenhadas pela área de Controladoria na empresa? (BORINELLI, 2006) A Controladoria tem como função modelar os sistemas de informações que permitam de forma ágil tomar decisões. Além disto, atua na gestão dos estoques, elaboração dos preços de venda, apoia as diversas áreas de empresa com informações sobre o negócio, como por exemplo, decisões de compras. Atua junto às diversas áreas da empresa orientado sobre as melhores práticas de gerar informação, demonstrando possíveis reflexos de gerar informações com erro, objetivando ao final do processo informações de qualidade.
De maneira geral, como a área de Controladoria promove ações junto as demais áreas da empresa para direcionar as pessoas aos objetivos da organização? (Corina e Corina, 2009). A Controladoria carece ainda de ações sistêmicas que disseminem e direcionem as pessoas aos objetivos da organização. A tarefa não é simples, pois a empresa é grande, possui diversas lojas, mas ações realizadas como no passado onde todas as lojas foram visitadas e reuniões realizadas com os principais gestores para disseminar conceitos de formação da margem de contribuição, os componentes da margem (despesas, recursos), o DRE que geraram bons resultados. Estas informações estão publicadas na *internet,* porém pela rotatividade das equipes, se faz necessário sistematizar este processo.
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? (OLIVEIRA, 2009) A Controladoria atua tendo como suporte a ferramenta *Business Intelligence - BI*, onde foi construído um modelo de negócio, que contempla orçamento, previsto x realizado e gerações de informações, ao qual permitem agilidade ao processo decisório. Estas informações estão disseminadas junto aos diversos gestores através da publicação na *intranet* da empresa.

De maneira geral, de que forma a Controladoria atua nos processos de segurança da informação para garantir que o sistema de informações da empresa atenda às necessidades estratégicas e operacionais da empresa? (ATKINSON et al., 2008)
A atuação da Controladoria nos processos de segurança da informação está sendo demandando atualmente pela implantação de um novo *ERP*, ao qual possibilita cenários de integração e visão sistêmica dos processos da empresa. Porém, existem oportunidades para que ações possam ser realizadas de forma mais sistemática e não em eventos originados por alterações legais, como por exemplo, substituição tributária do ICMS que não foi tratada adequadamente em determinado estado da federação a qual afetou margens. A atenção aos processos que podem afetar os pilares do negócio e a atuação integrada com a TI criam oportunidades de otimizar operações, minimizar eventuais riscos e garantir um ambiente de segurança das informações.
As áreas de Controladoria e de TI consideram relevante adotar uma gestão holística para tornar as implementações de segurança da informação mais eficaz? (YOUNG; WINDSOR, 2010; ELOFF; ELOFF, 2003)
A gestão holística é extremamente relevante para as áreas de Controladoria e de TI. Nos processos atuais essa prática é incipiente, devido à falta de treinamentos, a rotatividade e disseminação da conscientização dos usuários. Uma política de segurança da informação para ser eficaz tem nos usuários seu principal aliado, e atualmente o cenário é de que estes usuários atuam operacionalmente de forma muito pontual, devido à falta de treinamentos. Com o advento da implantação do novo *ERP,* estamos adotando ações de integração dos usuários, criamos uma célula, onde as pessoas de diferentes áreas aos quais denominados de usuários chaves visualizam todo processo de negócio, desde seu inicio, no cadastro de produto, a importância de uma conta contábil, processo de compra, estocagem, vendas, ou seja, de forma verticalizada todos visualizam os processos nas mais diferentes áreas da empresa, uma visão do todo, uma gestão holística. Este experimento pode propiciar pessoas capacitadas para multi funções, e cria uma oportunidade de se ter multiplicadores que possam qualificar futuras implementações de segurança da informação.
De maneira geral entende-se que a inserção dos usuários possa contribuir com a eficácia nas políticas que visam prevenir, detectar ou minimizar eventuais riscos decorrentes de falhas de segurança de informações na empresa? (SPEARS; BARKI, 2010)
A inserção do usuário é fator primordial para a obtenção de uma política de segurança da informação visando mitigar riscos. Inserindo os usuários permite que surjam contribuições para melhoria nos processos de segurança da informação, e temos na empresa este objetivo. Temos por objetivo aprimorar os processos de treinamentos, reforçar sua importância como corresponsável nos projetos de segurança física da informação, aliado a qualidade da informação, esta junção dá suporte ao sistema informacional da empresa. Isto contribuirá para dar suporte quando ocorrer substituições de funções na empresa, ou seja, este usuário deve passar por um processo de treinamento e conscientização visando evitar riscos decorrentes de falhas de segurança da informação na empresa. Este processo é um investimento para a empresa pois, criando uma equipe de treinamento qualificada, atuando de forma sistemática em cada evento

relacionado a segurança da informação, gera benefícios intangíveis para a empresa. Muitas empresas entendem que estas políticas de inserção de usuários tem um custo elevado, e que num primeiro momento até pode ser, porém, a médio e longo prazo cria-se uma cultura organizacional de proteção aos sistemas informacionais da empresa que minimizam riscos ao negócio. Aliado ao fator usuário, pode-se citar a utilização de softwares que restringem e fazem a gestão de eventos relacionados a segurança da informação, ou seja, temos tecnologias e pessoas contribuindo integradamente aos processos de segurança da informação.
De que maneira as áreas de TI e de Controladoria podem atuar em conjunto na inserção dos usuários a fim de conscientizá-los com as políticas de segurança de informações? (SPEARS; BARKI, 2010) A conscientização dos usuários passa por um processo sistêmico de treinamentos e comunicação das políticas de segurança da informação. As áreas de TI e Controladoria podem atuar em conjunto na elaboração de um portal ou canal de comunicação em *web,* onde todas as informações estariam disponibilizadas de forma clara e na linguagem adequada ao público que se pretende atingir. Este processo seria antecedido de um treinamento para disseminação das políticas e normas de segurança de informações estabelecido pela direção da empresa, bem como, da importância da informação para a Controladoria e gestores que se utilizam dela para tomada de decisão. De uma forma clara treinar e comunicar a todos sobre sua importância nos processos que envolvem o item “informação”. Ao final, divulga-se o portal ou canal de comunicação *web*. Este processo de clarificar os usuários sobre as políticas e normas de segurança da informação seria um movimento integrado das áreas de Controladoria e de TI que pode propiciar a participação dos usuários com suas contribuições, ou seja, gerar um ambiente de melhoria continua.
Que riscos relacionados à segurança da informação podem ser minimizados tendo os usuários como principais aliados da empresa? (BULGURCU; CAVUSOGLU; BENBASAT, 2010) Podem ser minimizados riscos financeiros e intangíveis. Como por exemplo, a informação indevida prestada a um cliente que compromete vendas, que pode desencadear uma publicidade negativa gerando perdas de mais clientes. Muitas vezes perdemos clientes que não voltam mais sem saber o real motivo. A origem pode estar numa informação indevida, mal comunicada que frustrou sua expectativa como consumidor. Podia ser a compra mais importante da vida dele, ou que iria presentear alguém, enfim uma decepção com riscos incalculáveis. No processo de compras, um usuário não estando consciente e aliado as políticas e normas de segurança da informação, pode fornecer informações estratégicas que podem afetar negociações com fornecedores, promoções de vendas, enfim, gerando riscos financeiros que muitas vezes comprometem os resultados de um período.
Como as áreas de Controladoria e de TI abordam as necessidades de adequação dos softwares utilizados na empresa com relação as necessidades de geração de informações de apoio a tomada e decisão dos gestores? (WILKIN; CHENHALL, 2010) A abordagem inicial é a definição de uma política baseada nos pilares do negócio da empresa, ou seja, compras, vendas e margens. Estabelecer o que pode e o que não afetar estes pilares. A partir disto, a Controladoria e TI podem

compartilhar os requisitos de alterações de *software* através da elaboração de um *frame,* onde esses requisitos vão definir premissas a serem seguidas nas propostas das áreas em relação a alterações de *software*. A área solicitante de alteração de *software* deve avaliar os requisitos estabelecidos, e analisar o impacto da alteração. Como exemplo, pode-se citar, alterações que afetam o pilar vendas/clientes em decorrência de uma mudança na política de crédito onde a Controladoria atuaria para analisar seus reflexos para o negócio, efeitos nas margens de contribuição e elencar possíveis riscos, ganhos ou perdas, ou seja, juntamente com o usuário solicitante e a área de TI efetuar uma avaliação de seus impactos para o negócio. Este *frame* seria um filtro para segregar alterações significativas para o negócio, das menos importantes. Seria um canal de comunicação com as áreas que solicitam alterações, gerando questionamentos quanto aos impactos nos pilares de negócio da empresa, direcionando ações da área de TI no que se refere aos desenvolvimentos de alterações pertinentes e relevantes para a empresa. Para a Controladoria, possibilita atuar nos aspectos que merecem atenção quanto a informação para tomada de decisão, direcionado para uma postura pró ativa. Atualmente esta abordagem não está sistematizada na empresa, muito do que se faz nesta linha de atuação se dá pela parceria entre as áreas de Controladoria e de TI, pelo envolvimento e entendimento de alguns requisitos que entende-se poderão afetar as informações disponibilizadas para a Controladoria. A ideia de elaboração de um *frame* é um avanço que pode gerar bons resultados, inclusive de economias financeiras em alterações que muitas vezes prevalece o senso de “urgência” e não o que é relevante e tem impacto para o negócio. Isto ficariam mais claro com a implementação deste processo.

NOME DO RESPONDENTE: Agostinho Luiz Peroni
CARGO: Gerente de Controladoria
TEMPO NO CARGO: 6 anos
TEMPO DE EMPRESA: 18,5 anos
FORMAÇÃO ACADÊMICA: Bacharel em Ciências Contábeis com especialização em Controladoria, MBAs em Finanças Corporativas e Logística e Operações.
IDADE: 38 anos
PRINCIPAIS RESPONSABILIDADES: Gerenciar o processo orçamentário anual e submeter para avaliação da alta administração, acompanhando para que os valores orçamentários sejam executados a fim de garantir a rentabilidade prevista. Apresentar os resultados para direção e gestores de área, demonstrando as variações entre o previsto e realizado, desenvolver estudos de viabilidade, aquisição e venda (imobilizados, produtos, bens etc.) conforme demanda da alta administração da Companhia auxiliando na tomada de decisões.
SEÇÃO I – INFORMAÕES GERAIS DO GESTOR ENTREVISTADO SOBRE PROCESSOS DE INTEGRAÇÃO ENTRE AS ÁREAS DE CONTROLADORIA E TI
De maneira geral, cite quais os fatores limitadores nos processos de integração entre as áreas de Controladoria e TI nas alterações de sistemas/softwares que afetam o ambiente da informação? Um dos principais fatores limitadores nos processos de integração entre as áreas de Controladoria e TI está na visão muito técnica das equipes de TI. É necessário conhecer o negócio da empresa, pois somente o conhecimento em linguagens de programação limita a integração, podendo ser um fator de retrabalhos em decorrência do fator comunicação entre usuário solicitante de alterações, técnico de TI e a linguagem de negócio da Controladoria. Existindo este alinhamento entende-se que pode-se restringir o número de alterações nos sistemas, porque muitas delas, constata-se que não ajudam na melhoria da atividade da empresa. A Controladoria pode e deve contribuir no entendimento do negócio da empresa.
Quais seriam os processos que possibilitam a aproximação das áreas de Controladoria e TI? Todos os processos ligados ao negócio principal da empresa possibilitam a aproximação das áreas de Controladoria e de TI, quais sejam: (i) comprar; (ii) estocar; (iii) vender e (iv) distribuir. São processos estratégicos para o negócio, ao qual se faz necessário um controle aprimorado e próximo, onde as áreas de TI e Controladoria devem focar suas ações.
Como a Controladoria poderia atuar para evitar possíveis vulnerabilidades no sistema de informações advindos das alterações de sistemas/softwares? Através de uma atuação de validação junto ao usuário chave solicitante da alteração e a equipe da TI. Muitas alterações são demandas para a TI e que não passam por um filtro de validar se estão claras suas contribuições para o negócio da empresa. Se este processo existir sistematicamente, muitas alterações não serão feitas, pois não contribuem com os principais processos ligados ao negócio da

empresa e pode-se evitar possíveis vulnerabilidades nos sistemas de informações da empresa. Além disto, permite identificar e classificar as solicitações ligadas ao negócio, as menos relevantes e por área solicitante, gerando indicadores que possibilitam uma gestão sobre estas demandas de alterações de softwares.
Como a TI poderia atuar para evitar possíveis retrabalhos advindos de erros nas alterações de sistemas/softwares que impactam nas atividades operacionais da Controladoria? Validando as alterações antes de serem implementadas. Na empresa, utilizamos a *intranet* como um sistema de divulgação de informações corporativo, onde usuários solicitam alterações dentro de sua visão específica, de sua área de atuação. Com a adoção de um processo de validação, envolvendo a área solicitante e analisando seus impactos com base nas principais áreas de negócio da empresa com o apoio da Controladoria, pode-se suprimir muitas demandas e retrabalhos nas atividades operacionais.
SEÇÃO II – POLÍTICAS E CONTROLES RELACIONADOS À SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO NA PERCEPÇÃO DA CONTROLADORIA E TI
De maneira geral, quais os riscos possíveis que a empresa pode incorrer ao não estabelecer os papéis e responsabilidades dos usuários envolvidos nos processos de vendas ou de compras? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 4 da norma ISO 27002 – Segurança em RH). Ao não estabelecer papéis e responsabilidades dos usuários, pode gerar operacionalmente nas equipes a falta de foco, atividades estratégicas não sendo atendidas na prioridade necessária como, por exemplo, formação de preços fora de mercado gerando perda de rentabilidade. Outros fatores são a falta de alinhamento entre as equipes e de assumir erros de negócio, pois quando os resultados são satisfatórios todos são parte integrante, quando são deficitários ou ocorrem ineficiências em determinadas operações, ninguém pode ser responsabilizado. Desta forma, a empresa deve estabelecer papéis e responsabilidades para evitar riscos financeiros, riscos de ter equipes desalinhadas e até sem qualificação para cada processo da empresa.
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 este processo? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 4 da norma ISO 27002 – Segurança em RH). A implementação deveria se dar através de treinamentos contínuos. As áreas envolvidas devem ser o RH, que na empresa concentra todas as políticas treinamento, ou seja, atuaria como coordenador dos treinamentos. A área de T.I, como gestora das políticas e normas de segurança da informação, a Controladoria em temas relacionados a importância da informação para tomada de decisão, e as demais áreas da empresa para auxiliar nas definições de acesso, seleção de usuários chaves e de programas.

A implementação de procedimentos de controles codificados e de sistema para a rastreabilidade de mercadorias pode contribuir com o processo de gestão de estoques e de atendimento aos clientes? Quais riscos seriam mitigados com esta implementação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Gerenciamento das operações e comunicações).
Sim, contribui muito, principalmente para os itens que são sensíveis as atualizações de tecnologia, como os de informática, áudio e vídeo. Ao adotar controles codificados e de sistema para a rastreabilidade destas mercadorias, por exemplo, mitigaria os riscos de perda de estoques, perdas de margens, pois permitiria controlar estoques e vender dentro do conceito primeiro que entra é o primeiro que sai. Para isto, o sistema de codificação e rastreabilidade devem contemplar todas as informações pertinentes para uma eficiente gestão no centro de distribuição (CD) para facilitar ao gestor do CD, prateleiras, boxes, permitindo que fisicamente a gestão possa realmente controlar e evitar obsolescência de estoques.
Na percepção da Controladoria de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Ge renciamento das operações e comunicações).
Ajuda a identificar nas alterações de sistema, quem as solicitou, que período e técnico da TI que desenvolveu tais alterações. Muitas vezes isso vai ajudar a entender o objetivo da alteração ou o que se esperava dela confrontando como o operacionalmente ela gerou. Ocorre eventualmente a identificação de um programa escrito há muito tempo atrás, que gera uma problema operacional, com os registros log possibilita uma rastreabilidade para entender os efeitos desta solicitação, porque foi feita e se fazia sentido. É um suporte para evitar discussões que geram perda de energia e gera foco para atuação.
Na percepção da TI de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Ge renciamento das operações e comunicações).
Contribuem como suporte na gestão da TI quanto as alterações de sistema, na identificação do usuários solicitantes, do técnico responsável pelo desenvolvimento da melhoria e na homologação final.
A definição de políticas e procedimentos para troca de informações entre empresa e entidades externas é relevante para evitar riscos contábeis, fiscais e financeiros? Cite de acordo com seu entendimento quais os principais riscos para a empresa? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Gerenciamento das operações e comunicações).
Estabelecer políticas e procedimentos de troca de informações define responsabilidades e controles sobre este processo. O apoio da tecnologia através de um software, também é importante para gerar informações e gráficos de acompanhamento de determinadas trocas de informações consideradas estratégicas e previamente mapeadas, possibilitando seu monitoramento.

Quanto aos riscos, podemos citar o não cumprimento de prazos legais por envio em atraso, gerando penalidades fiscais e tributárias. Também riscos financeiros e de imagem para a empresa, em decorrência de negociações de fornecimento de mercadorias negociadas a preços exclusivos ao qual o concorrente teve acesso.
De maneira geral, qual o entendimento sobre a participação das áreas de Controladoria e de TI na elaboração de treinamentos para usuários a fim de garantir a segurança de informações? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). As áreas de TI e Controladoria devem atuar junto com o RH para definir os procedimentos de treinamentos, abordando os pontos mais críticos dos processos de segurança das informações. O processo de conscientizar os usuários de que as informações geradas por eles são extremamente importantes para as decisões tomadas na empresa, fazendo-se sentir como parte integrante do processo, gera comprometimento e maior zelo e deve estar contemplado nos treinamentos e na forma de comunicar isto a nível corporativo. Assim, entende-se que estas ações contribuem para solidificar as políticas de segurança da informação.
Quais procedimentos de análise critica técnica das aplicações após mudanças no sistema operacional? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). Preliminarmente têm que analisar as alterações e seus impactos sobre a linha mestra da empresa, ou seja, comprar, vender, estocar, entregar e efeitos sobre as margens. Se a respostas são afirmativas deve-se adotar um procedimento de análise critica e técnica das áreas de negócio TI e Controladoria com o usuário solicitante para garantir a continuidade da performance das operações após as alterações no sistema operacional. Alterações sem efeitos sobre a linha mestra da empresa não devem ser priorizadas e assim atendidas de acordo com os recursos disponíveis.
Como se daria a participação das áreas de Controladoria e de TI nas restrições sobre mudanças em pacotes de software? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). A Controladoria tem preocupação com relação aos impactos das alterações nos softwares que podem afetar a lucratividade da empresa. Se estas alterações tem influência nos custos das mercadorias, nos controles dos estoques, afetam margens de contribuição deve ter atuação da Controladoria. A Controladoria deve apoiar a TI para filtrar e aprofundar as análises sobre alterações de software, através da formação de um comitê multidisciplinar destas áreas, criando restrições ou filtros que qualifiquem e questionem solicitações de alterações. Este processo entende-se educativo, e pode gerar economias para a empresa com a redução de solicitações e minimizar retrabalhos operacionais.

Quais os procedimentos adequados para evitar o risco de vazamento de informações relevantes? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).
Adotando uma política de controle sobre o fluxo de informações estratégicas da empresa que contemple responsabilidades. Na política, contemplar a segmentação de controle de acesso por usuário atrelado ao perfil de usuário vinculado a função ou cargo. Disseminar a conscientização corporativa e comunicar os parceiros externos sobre tal política, pois muitas negociações estratégicas que tem impacto no negócio são sigilosas. Como exemplo, a política de preços é uma informação estratégica, apesar de sensível a cópia, mas que tem um espaço de tempo, onde a empresa consegue trabalhar melhor o preço, políticas de promoções, publicidade. Se por ventura vazar uma informação desta natureza, terá impacto direto na lucratividade daquele mês ou quem sabe comprometendo o desempenho do exercício. Desta forma, a informação é um ativo relevante e que deve ser preservado.
Após as alterações no sistema operacional, entende-se que deve-se efetuar testes envolvendo usuários responsáveis pela gestão da informações para validar tais alterações? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.).
Sim. É entendimento que a responsabilidade da homologação é do usuário final. A TI desenvolve tecnicamente a alteração demandada, contudo, o usuário solicitante deve verificar se as alterações surtiram seus efeitos diante do que se propunha a alteração.
De maneira geral, como deve ser o procedimento de notificação de eventos de segurança da informação para conhecimento e tomada de ação corretiva em tempo hábil? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 8 da norma ISO 27002 - Gestão de incidentes de segurança da informação).
Os procedimentos de notificação de eventos de segurança da informação para ações de correção devem ser realizados antes das alterações entrarem no ambiente oficial. Este processo deve contemplar auditorias para verificar perfis de acesso dos usuários, verificações em ambiente de teste para validar alterações efetuadas para evitar que erros contaminem o ambiente oficial de informações da empresa. Ocorrem muitos problemas advindos de alterações na legislação, onde na empresa por trabalhar na comercialização de 4 a 5 mil itens, em 5 estados, com legislação de ICMS específicas, eventual alteração em que impacte na classificação de alguns itens e que é específica para determinado estado, eventualmente ocorre de impactar em outro estado gerando divergências tributárias que imediatamente são corrigidas. Com a adoção de auditorias e testes antes da homologação pode-se minimizar erros em eventos de segurança da informação.

De maneira geral, considera-se importante o envolvimento das áreas de Controladoria e de TI nas análises e avaliações de riscos de continuidade do negócio no que se refere ao processamento, geração e segurança da informação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 9 da norma IS O 27002 - Gestão da continuidade do negócio).
Sim, porque em última estância, é a área de Controladoria a responsável pelas informações que permeiam e dá suporte a tomada de decisões dos gestores. Desta forma, a Controladoria deve validar junto a T.I as informações destinadas aos usuários, estabelecer um alinhamento na comunicação das informações estratégicas e que podem impactar em riscos de negócio. Por exemplo, quando a empresa estiver falando de venda líquida deve ser uniforme para todas as áreas, não pode ter confusão, uns utilizando venda bruta. Toda e qualquer informação contida em relatórios deve estar alinhada com as diretrizes da empresa e quem traduz e comunica estas, é a Controladoria, desta forma é relevante manter um alinhamento com a área da TI, evitando possíveis impactos nas decisões dos gestores.
De maneira geral, é entendimento que a participação e envolvimento dos usuários com as políticas e normas de segurança da informação contribuem com os requisitos de segurança da informação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 10 da norma ISO 27002 - Conformidade).
Sim. O envolvimento dos usuários com as políticas e normas de segurança da informação propicia um ambiente de maior segurança. Ao transmitir aos usuários o entendimento da complexidade de um ambiente de informação na empresa e que ele deve contribuir com sugestões para a melhoria deste ambiente, propicia a sua integração com as políticas e normas de segurança da informação ao qual irá gerar um alinhamento aos requisitos de segurança da informação.
SEÇÃO III – ATUAÇÃO DAS ÁREAS DE CONTROLADORIA E DE TI NA ORGNIZAÇÃO EM: (I) PROCESSOS DE ALTERAÇÕES DE SOFTWARE; (II) POLITICAS DE SEGURANÇA; (III) INSERÇÃO DOS USUÁRIOS; E, (IV) RISCOS OPERACIONAIS RELACIONADOS
Qual a visão da Controladoria em relação ao envolvimento da área nos processos de decisões sobre alterações de sistemas operacionais na empresa? (Corina e Corina, 2009).
Primeiramente temos que avaliar que tipo de alteração, a demandada por obrigatoriedade de normatização ou legal, esta deve ser implementada de forma ágil evitando riscos para a empresa. As alterações em decorrência de demandas pelos usuários chaves devem passar por uma avaliação em relação aos seus efeitos nos pilares estratégicos do negócio. O envolvimento da Controladoria deve ser na definição das diretrizes políticas e operacionais da empresa, que envolvam processos de venda, compras, estocagem, enfim participar e comunicar claramente as demais áreas da empresa qualquer alteração nas diretrizes que impactam no resultado da empresa. Deve participar efetuando testes e avaliações, porque enfim, são de sua responsabilidade as informações fornecidas para a gestão da empresa. A uniformização de conceitos entre as áreas também é de suma importância, pois ao analisar resultados individuais por loja, analise de margens de lucro por linha de produtos deve sempre, direcionar ao resultado e diretrizes estabelecidas pela empresa. Portanto, a Controladoria

deve participar para possibilitar um alinhamento aos processos que envolvem alterações de sistema da empresa.
Quais os requisitos/atributos considerados pelas áreas de Controladoria e de TI quanto a informação disponibilizada aos seus diversos usuários? (CPC, 2008; Cobit, 2007). Relevância, tempestividade e confiabilidade. A informação disponibilizada deve estar correta para o usuário. Quando a Controladoria fornece uma informação, esta deve prever estes requisitos, não adianta fornecer a informação e dizer "opa, espera um pouquinho que temos que analisar melhor, espera pode estar errado!". Neste momento a Controladoria perde sua credibilidade, daí por diante, cria-se um ambiente de desconfiança que fica difícil superar com o usuário da informação.
Qual a percepção das áreas de Controladoria e de TI em relação ao tema segurança da informação e sua importância estratégica para a empresa? (KAYWORTH; WHITTEN, 2010) As decisões estratégicas da empresa são tomadas com base nas informações fornecidas pela Controladoria. A segurança da informação é um tema considerado estratégico para a empresa. A empresa já vivenciou casos, por alterações de parametrizações em cargos de funcionários que gerou questionamentos por parte do conselho de administração, pois como os cargos concentram todas as informações, gerou distorções nas análises. Desta forma, o ambiente da informação, a segurança da informação, está interligado com a credibilidade das áreas de TI e Controladoria que são as gestoras do ambiente informacional na empresa.
Quais as principais funções desempenhadas pela área de Controladoria na empresa? (BORINELLI, 2006) A principal função da Controladoria é de modelar o sistema de informações da empresa, onde se destaca o orçamento, o acompanhamento do previsto com o realizado. Controles de custos e despesas fixas. A Controladoria é responsável também, pelas informações prestadas ao conselho de administração e diretoria. Realiza análises de investimentos, de resultados, ponto de equilíbrio das lojas, definições das principais premissas na formação de preços, como percentual de comissão, carga tributária e de estabelecer a margem mínima que a empresa está disposta a trabalhar neste ambiente de extrema concorrência.
De maneira geral, como a área de Controladoria promove ações junto as demais áreas da empresa para direcionar as pessoas aos objetivos da organização? (Corina e Corina, 2009). A partir do planejamento, do processo de orçamento, onde a direção e gerentes são envolvidos. Nestes processos é que a área de Controladoria atua para direcionar as pessoas aos objetivos da organização. A Controladoria atua para que os objetivos traçados sejam atingidos pela empresa, para isto, fornece informações sobre o andamento dos resultados realizados confrontando com o orçado, sinalizando possíveis desvios. Informações de margens, custos, são disponibilizadas diariamente através de publicação na *intranet* da empresa, isto possibilita ações ágeis para corrigir eventuais desvios da meta, inclusive com simulador ao qual demonstra o resultado da loja ao final do mês se a loja continuar com a performance atual. Outra ação importante é o alinhamento conceitual entre todas as áreas quanto aos termos que medem os resultados das

lojas, como o nosso conceito de resultado atrelado à margem mercantil.
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? (OLIVEIRA, 2009) A Controladoria atua a partir das diretrizes estabelecidas pela direção da empresa, modelando o sistema de informações da empresa para que esteja conectado a estas diretrizes. Este processo é disseminado junto aos nossos analistas para que tenham foco nas manutenções necessárias para que o sistema de informações apresente sempre resultados atualizados da performance do negócio. Existem demandas solicitadas pela direção relacionadas à prestação de novas informações e que, em conjunto com a TI efetua-se a modelagem, validação e disponibilização. É um processo contínuo de evolução.
De maneira geral, de que forma a Controladoria atua nos processos de segurança da informação para garantir que o sistema de informações da empresa atenda às necessidades estratégicas e operacionais da empresa? (ATKINSON et al., 2008) A Controladoria atua nas decisões para implementação de alterações em software que impactam nos pilares do negócio da empresa. Orienta e sugere melhorias no sistema para dar maior segurança e confiabilidade, com acompanhamento constante. Atualmente com o volume de informações gerados diariamente se faz necessário a Controladoria atuar pró ativamente para que o sistema de informações da empresa esteja sempre alinhado aos objetivos de negócio.
As áreas de Controladoria e de TI consideram relevante adotar uma gestão holística para tornar as implementações de segurança da informação mais eficaz? (YOUNG; WINDSOR, 2010; ELOFF; ELOFF, 2003) Sim. A gestão holística está vinculada as ações que possibilitam integrar as áreas aos objetivos da empresa, conectando as implementações de segurança da informação. Permite visualizar e analisar o *status* atual da empresa, projetando o que se pretende implementar para buscar a eficácia em qualquer implementação que envolva a segurança da informação. Ainda temos um cenário de departamentalização muito forte, que muitas vezes se preocupam somente com seu universo, com suas informações. A implantação do novo *ERP* tem nos demonstrado tratar-se de um evento que gera a integração das áreas, exige-se uma visão mais sistêmica de todo o processo, e do próprio negócio da empresa de forma verticalizada. Ele traz muito forte a gestão holística.
De maneira geral entende-se que a inserção dos usuários possa contribuir com a eficácia nas políticas que visam prevenir, detectar ou minimizar eventuais riscos decorrentes de falhas de segurança de informações na empresa? (SPEARS; BARKI, 2010) Os usuários são peças chaves na identificação de riscos decorrentes de falhas de segurança da informação. Usuários conscientes dão sustentação às políticas e procedimentos da segurança de informação. A prática de treinamentos contínuos permite uma estabilidade ao ambiente da informação, pois evita ineficiências por rotatividade, pois no nosso setor este fator é relevante girando em torno de 4% ou 5% ao mês. Para um quadro de 6 mil funcionários, 300 acabam entrando e saindo por mês, se não tiver uma atuação contínua de

conscientização temos um custo intangível e riscos que podem advir de falhas de segurança da informação na empresa. Este processo deve estar conectado as atividades de integração de cada novo funcionário.
De que maneira as áreas de TI e de Controladoria podem atuar em conjunto na inserção dos usuários a fim de conscientizá-los com as políticas de segurança de informações? (SPEARS; BARKI, 2010) As áreas de TI e de Controladoria podem atuar através do monitoramento, acompanhamento, orientação e com treinamentos. De nada adianta implementar um treinamento se este não for sistêmico e fizer parte das rotinas operacionais das áreas. Entende-se que este processo gera a inserção e a conscientização dos usuários de sua importância nas políticas de segurança da informação. Porém, este processo requer alocação de recursos iniciais para sua completa implementação e atualmente na empresa, verificamos que a Controladoria poderia atuar de outra forma se isto fosse disponibilizado. Nossa equipe é composta de 4 pessoas com uma gama enorme de atividades focadas em gerar informações aos gestores das 300 lojas que hoje compõem o negócio da empresa. De qualquer forma, trata-se de um assunto pertinente para ambas as áreas, Controladoria e de TI, ao qual cabe planejar e identificar o melhor formato para tornar este processo mais intenso e não somente eventual.
Que riscos relacionados à segurança da informação podem ser minimizados tendo os usuários como principais aliados da empresa? (BULGURCU; CAVUSOGLU; BENBASAT, 2010) A minimização de erros no sistema de informações da empresa. Com a inserção dos usuários ás políticas de segurança da informação, qualquer alteração necessária no software da empresa, que por questões de legislação, ou advindas por necessidades do negócio, existe um ambiente de maior atenção, de controle. Desta forma, minimiza-se riscos financeiros e intangíveis relacionados à imagem da empresa diante de sua cadeia de valor.
Como as áreas de Controladoria e de TI abordam as necessidades de adequação dos softwares utilizados na empresa com relação as necessidades de geração de informações de apoio a tomada e decisão dos gestores? (WILKIN; CHENHALL, 2010) A abordagem se dá basicamente sobre os principais pilares do negócio da empresa, ou seja, comprar, estocar, vender, entregar. Se as adequações no software da empresa tiverem relação com estes pilares, deve-se dar total atenção e prioridade, pois estão relacionadas diretamente aos processos que impactam no resultado da empresa. O processo de compras é extremamente relevante na empresa, pois ao realizar uma compra errada, quer por questões de valor, volumes ou de logística, irá comprometer as vendas, afetará a competitividade da empresa. Por exemplo, ao estimar a venda de 1.000 unidades de determinada mercadoria e ao realizar 500 unidades, restarão 500 unidades no estoque, que demandará uma ação de realocação em outras lojas e por fim, promoções. A questão logística também é relevante, pois a empresa possui 3 centros de distribuição (CD) e a alocação de volumes e itens devem estar adequadas ao consumo daquelas praças de vendas. Desta forma, os softwares devem contemplar informações do histórico das negociações da empresa, e estas devem ser validadas com informações atuais de mercado, ao qual embasa muitas decisões sobre os processos de comprar, vender e estocar. O processo de tomada de decisão em negociações requer a integração das

áreas de negócio, Vendas, Compras e o suporte da Controladoria com informações que possibilitem as melhores decisões alinhadas ao planejamento da empresa. A área de TI deve garantir um ambiente de informação seguro.

NOME DO RESPONDENTE: Flori Cesar Peccin
CARGO: Gerente de Contabilidade/Fiscal
TEMPO NO CARGO: 6 anos
TEMPO DE EMPRESA: 19 anos
FORMAÇÃO ACADÊMICA: Bacharel em Ciências Contábeis e Administração Comércio Exterior com especialização em Planejamento Tributário e MBA em Finanças Corporativas.
IDADE: 36 anos
PRINCIPAIS RESPONSABILIDADES: Gerir os processos de apuração dos balancetes/resultados mensais e balanços anuais, apuração de impostos e tributos mensais e anuais de acordo com a legislação, normas e práticas contábeis. Planejar os registros e controles dos atuais e novos processos/operações da Companhia, em conformidade com as práticas contábeis, desenvolvendo estudos e novos cenários para tomada de decisão da Empresa. Acompanhar fiscalizações tributárias, auditorias externas, bem como desenvolver as demonstrações financeiras e contábeis da Companhia. Gerir o processo de planejamento tributário, em conformidade com as diretrizes da gestão e avaliação da legislação vigente.
SEÇÃO I – INFORMAÕES GERAIS DO GESTOR ENTREVISTADO SOBRE PROCESSOS DE INTEGRAÇÃO ENTRE AS ÁREAS DE CONTROLADORIA E TI
De maneira geral, cite quais os fatores limitadores nos processos de integração entre as áreas de Controladoria e TI nas alterações de sistemas/softwares que afetam o ambiente da informação? Os principais fatores limitadores nos processos de integração entre as áreas de Controladoria e TI estão na falta de alinhamento quanto à visão de negócio, de priorizar os objetivos gerais e estratégicos da empresa em detrimento das necessidades específicas das áreas. Isto reflete na distância entre o conhecimento das necessidades da gestão e a sua aplicação de forma técnica e operacional. Ao estabelecer este alinhamento, a junção do conhecimento específico das duas áreas, com foco comum, pode-se gerar uma sinergia que tenha por objetivo a melhora de performance operacional de cada área dentro do seu foco de atuação, refletindo na qualificação do ambiente da informação da empresa como um todo.
Quais seriam os processos que possibilitam a aproximação das áreas de Controladoria e TI? O processo que possibilita a aproximação das áreas de Controladoria e de TI é o planejamento estratégico, ao qual contempla as prioridades da empresa. Isto possibilita análises conjuntas entre as áreas de TI e Controladoria sobre os principais processos que tem efeito no resultado da empresa e permite um alinhamento das ações de cada área de forma integrada. A Controladoria, por possuir uma visão sistêmica do negócio, pode contribuir com a área de TI a priorizar o desenvolvimento ou alterações nos softwares alinhados com as prioridades estabelecidas no planejamento estratégico, aumentando a assertividade e a qualidade dos dados, transformando a informação útil e precisa para o processo decisório da empresa (diretoria e áreas de gestão). A questão do desenvolvimento das equipes com profissionais capacitados com

conhecimento nas mais diversas áreas também permite um alinhamento da linguagem facilitando a comunicação entre as áreas.
Como a Controladoria poderia atuar para evitar possíveis vulnerabilidades no sistema de informações advindos das alterações de sistemas/softwares? Primeiramente deve participar dos desenvolvimentos dos softwares, junto à área de TI de forma consultiva, utilizando-se de seu conhecimento sistêmico, com o objetivo de que, as alterações de softwares estejam alinhadas as premissas de integridade de dados e aos objetivos de negócio da empresa. Posteriormente, desenvolver testes pontuais e específicos sobre os processos ligados as principais operações da empresa, com avaliações sobre as regras de negócio, efetuando testes aleatórios, procurando garantir o máximo de segurança sobre o ambiente da informação com visão sistêmica dos processos. 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.
Como a TI poderia atuar para evitar possíveis retrabalhos advindos de erros nas alterações de sistemas/softwares que impactam nas atividades operacionais da Controladoria? Capacitar a equipe de TI para ter conhecimentos sobre os processos principais da empresa. Envolver os usuários chaves para validar alterações de software, estabelecer uma cultura de arquitetura de processos na empresa, onde especifique as fases a serem cumpridas como, por exemplo, avaliação econômica e financeira do projeto de alteração demandado e se o mesmo está alinhado com o negócio da empresa. Implementar solicitações de alterações através de um formulário ou documento que seja descrito de forma detalhada qual a necessidades e objetivos das alterações, a partir disto, criar procedimentos de alinhamento com o usuário solicitante das questões estruturais de software; mensuração adequada do tamanho do desenvolvimento; definição de plano de execução; acompanhamento do desenvolvimento da TI apresentando ao usuário solicitante. Após, estabelecer um ambiente de homologação com todas as características de aprovação para que o usuário efetue os testes, que a TI efetue um acompanhamento em conjunto com o usuário antes de ser disponibilizado oficialmente, desta forma, entende-se que se minimizaria retrabalhos que impactam nas informações geradas pela Controladoria.
SEÇÃO II – POLÍTICAS E CONTROLES RELACIONADOS À SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO NA PERCEPÇÃO DA CONTROLADORIA E TI
De maneira geral, quais os riscos possíveis que a empresa pode incorrer ao não estabelecer os papéis e responsabilidades dos usuários envolvidos nos processos de vendas ou de compras? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 4 da norma ISO 27002 – Segurança em RH) Ao não estabelecer papéis e responsabilidades dos usuários pode gerar desequilíbrio no negócio privilegiando metas individuais; ao invés de haver alinhamento com os objetivos da empresa. Outros fatores são a falta de foco das áreas podendo gerar desequilíbrio na gestão da empresa, influência nas

responsabilidades das outras áreas, falta de definição dos papéis claros de cada pessoa. Todas estas situações podem gerar riscos dentro das atividades e processos operacionais de comprar, vender e entregar. Desta forma, se faz necessário estabelecer papéis e responsabilidades dos usuários visando atingir o objetivo comum da empresa, para que os processos estejam alinhados funcionando como uma engrenagem, evitando assim, riscos de continuidade da empresa.

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 este processo? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 4 da norma ISO 27002 – Segurança em RH).

A implementação deveria se dar, primeiramente a partir da direção da empresa. Dirigentes que acreditam na segurança da informação através de estudos ou opiniões sobre o tema, podem influenciar de forma efetiva as áreas de gestão e criar um ambiente propicio para a disseminação deste processo como sendo parte da cultura da empresa.

O processo de implementação deve ser desenvolvido da seguinte forma: (i) Controladoria estabeleceria o formato e os pontos de foco de segurança da informação alinhados com a diretoria; (ii) TI auxiliaria na estruturação de dados e acompanhamento da implementação; (ii) RH na formatação, estruturação e metodologia de aplicação, divulgação do projeto às áreas. 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.

A implementação de procedimentos de controles codificados e de sistema para a rastreabilidade de mercadorias pode contribuir com o processo de gestão de estoques e de atendimento aos clientes? Quais riscos seriam mitigados com esta implementação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Gerenciamento das operações e comunicações).

O desenvolvimento de controles operacionais claros e estruturados possibilita uma melhor gestão de estoques. As variáveis pessoas e volume de operações são relevantes na influencia de gerar informações imprecisas em função da característica especifica da empresa. A implementação de controles codificados e um sistema de com rastreabilidade de dados, é uma ferramenta de auxilio no controle e gestão de estoques, onde limita a influência das pessoas em função das informações claras e estruturadas. Isto pode reduzir custos operacionais, possibilidade de atuação em produtos com giro lento, custos com perdas de estoques. Pode contribuir no processo de atendimento ao cliente externo, segurança das informações internas tanto para auditoria e por consequência a gestão da empresa.

Na percepção da Controladoria de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Ge renciamento das operações e comunicações). Os registros de auditoria nas alterações de sistema possibilitam a rastreabilidade das alterações, que o processo foi acompanhado e discutido em todas as suas fases de aplicação. No caso de identificação de inconsistência nos processos, facilita a busca retroativa dos responsáveis e os pontos específicos que devem ser trabalhados, revistos.
Na percepção da TI de que forma os registros (log) de auditoria em alterações de sistema contribuem para a melhoria operacional da área? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Ge renciamento das operações e comunicações). Especificamente sobre a TI, os registros log permite a rastreabilidade das informações centrada no formato em que as solicitações foram realizadas, facilidade de identificação dos erros de programação, possibilitando maior agilidade e segurança na identificação dos erros. Na gestão contribui também para identificar eventuais fragilidades da equipe técnica para ações de treinamento.
A definição de políticas e procedimentos para troca de informações entre empresa e entidades externas é relevante para evitar riscos contábeis, fiscais e financeiros? Cite de acordo com seu entendimento quais os principais riscos para a empresa? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 5 da norma ISO 27002 – Gerenciamento das operações e comunicações). A comparabilidade com dados externos pode ser entendida como uma forma de gestão importante para as empresas, entretanto, deve ser feita de forma segura e eficiente. Entende-se que a direção deve investir continuamente na disseminação e conscientização da política de procedimentos para troca de informações entre empresa e entidades externas. Estabelecer perfil de responsabilidade de acessos e envio de dados estruturado com senhas, limitações de acesso de dados por usuários externos, restrições e avaliação contínua do envio de informações para usuários externos mitigam riscos financeiros, intangíveis de imagem e de desgastes entre os gestores da empresa.
De maneira geral, qual o entendimento sobre a participação das áreas de Controladoria e de TI na elaboração de treinamentos para usuários a fim de garantir a segurança de informações? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). As áreas de Controladoria e de TI podem disseminar seus conhecimentos através de treinamentos, explorando e valorizando os pontos críticos específicos ou comuns que afetam a segurança da informação nas mais diferentes áreas da empresa. Em conjunto com o RH, desenvolvem-se métodos e focos de atuação prioritários para a gestão da empresa a fim de conscientizar quanto ao

entendimento do tema e sua importância. Desta forma, cria-se um ambiente de valorização pela responsabilidade e de disseminação de se ter atenção aos processos críticos da empresa aos quais foram definidos no planejamento deste processo educativo.
Quais procedimentos de análise critica técnica das aplicações após mudanças no sistema operacional? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). Após a entrada em produção das alterações de software, deve existir um acompanhamento se a mesma está produzindo os resultados esperados quando da sua solicitação e se não causou nenhum efeito colateral nos processos da empresa. Isso deve ser feito num ambiente de homologação. Para solicitar uma alteração de software, deve ser listado os efeitos desejados e também os possíveis efeitos indesejados. Assim, possibilita um acompanhamento após a entrada em produção, dos resultados, confirmando se estão corretos ou corrigindo imediatamente se não o estão. Entende-se que, este processo é de extrema importância para as empresas. Atualmente nos deparamos com cenários de empresas, onde ocorrem solicitações ou desenvolvimentos unilaterais, excluindo áreas de negócio do processo, gerando até possíveis riscos fiscais, financeiros e de integridade de informações. Assim, percebe-se a importância do envolvimento das áreas de Controladoria e de TI junto aos usuários para dar ênfase e foco nos pilares principais do negócio, com o objetivo de gerar informações qualitativas, quantitativas e dar clareza ao processo decisório.
Como se daria a participação das áreas de Controladoria e de TI nas restrições sobre mudanças em pacotes de software? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). Considerando que a Controladoria tem a visão sistêmica dos processos da empresa, esta deve desenvolver um processo sistêmico que contemple: (i) questionamento da aderência aos principais processos estratégicos da empresa com relação as alterações propostas; (ii) avaliação econômica e financeira das alterações e; (iii) avaliação do impactos das alterações e sua aplicabilidade operacional. Este processo deveria permear toda a empresa, passando a ser parte de sua cultura administrativa. A área de TI participa com a sistematização e atua em conjunto com a Controladoria apoiando nas análises técnicas. Naturamente este processo pode contribuir nas restrições às alterações que não estiverem conectadas a melhoria de performance das áreas ou ao aumento da lucratividade da empresa, gerando resultados de economia financeira para a empresa.
Quais os procedimentos adequados para evitar o risco de vazamento de informações relevantes? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). Estabelecer políticas claras de uso de informações; utilizar-se de softwares que possibilitam criptografar informações, criar senhas e política de uso restringindo o acesso conforme a relevância da informação. Implementar auditorias sobre os log de acesso e envio, revisar perfis de acesso e criar procedimentos de

monitoramento continuo no que se refere a informações estratégicas e relevantes para a empresa. Estas ações devem estar conectadas com o envolvimento dos usuários, de todas as áreas da empresa, de forma estrutural, e comunicar de forma clara eventuais punições ás informações cometidas quanto ao vazamento de informações. Após disseminar este processo corporativamente, existindo infrações nas políticas de uso da informação deve-se punir.
Após as alterações no sistema operacional, entende-se que deve-se efetuar testes envolvendo usuários responsáveis pela gestão da informações para validar tais alterações? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 7 da norma ISO 27002 - Aquisição, desenvolvimento e manutenção de sistemas de informação.). Os usuários responsáveis devem participar desde o início do processo de alterações no sistema operacional. Devem realizar as definições de escopo das alterações, estabelecer possíveis efeitos estruturais não planejados. Participar dos testes necessários para identificar possíveis falhas no desenvolvimento efetuado pela equipe técnica da TI até o processo de homologação das alterações.
De maneira geral, como deve ser o procedimento de notificação de eventos de segurança da informação para conhecimento e tomada de ação corretiva em tempo hábil? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 8 da norma ISO 27002 - Gestão de incidentes de segurança da informação). A notificação de eventos de erro deve ocorrer no processo de homologação, com a participação dos usuários chaves, juntamente com as áreas de Controladoria e de TI. A ideia é de se estabelecer usuários chaves e disseminar a visão sistêmica do negócio propiciada pelo conhecimento das áreas de Controladoria e de TI, permitindo um alinhamento e antecipando eventuais problemas no desenvolvimento ou no escopo de qualquer alteração que impacte no software da empresa. Desta forma, as notificações de erro precedem a entrada das alterações no ambiente oficial da empresa. Este processo poderia ser construído a partir da construção de comitês de discussão e analise sobre alterações de software.
De maneira geral, considera-se importante o envolvimento das áreas de Controladoria e de TI nas análises e avaliações de riscos de continuidade do negócio no que se refere ao processamento, geração e segurança da informação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 9 da norma ISO 27002 - Gestão da continuidade do negócio). O envolvimento das áreas de Controladoria e de TI é extremamente importante. A Controladoria através de seu conhecimento técnico e teórico, com ferramentas e métodos, e visão sistêmica, tem condições de contribuir no acompanhamento e orientação quanto aos riscos de continuidade dos negócios. Processamento, geração e segurança da informação que impactem na avaliação de rentabilidade por linha, segmento de produtos, valorização e realização de ativos, mensuração de passivos contingentes e principalmente na analise da geração de caixa são alguns dos pontos de atenção das áreas de Controladoria e de TI que podem colaborar nas avaliações de risco da empresa. A TI também atua na integridade dos dados operacionais, de vendas, estoques, clientes e impostos fornecendo o ambiente de informação seguro para a Controladoria realizar suas atividades de

acordo com sua missão e função.
De maneira geral, é entendimento que a participação e envolvimento dos usuários com as políticas e normas de segurança da informação contribuem com os requisitos de segurança da informação? (incluído como resultado da aplicação do primeiro instrumento metodológico – Domínio n° 10 da norma ISO 27002 - Conformidade). A segurança da informação deve ser um projeto corporativo, partindo da direção da empresa, passando pelas áreas estratégicas de negócios para que se tenha uma adequada implementação. Dentre as áreas chaves, cito a TI e a Controladoria, que devem instrumentalizar os usuários chaves quanto à importância dos requisitos de segurança da informação. A criação de uma cultura de gestão da informação, com a divulgação das políticas e normas de segurança da informação, a importância de cada área para o processo sistêmico, seus reflexos no contexto da empresa vinculado a uma avaliação continua através do estabelecimento de regras e treinamentos, inserem os usuários, transformando-os como corresponsáveis e comprometidos com os processos que envolvem a segurança da informação.
SEÇÃO III – ATUAÇÃO DAS ÁREAS DE CONTROLADORIA E DE TI NA ORGNIZAÇÃO EM: (I) PROCESSOS DE ALTERAÇÕES DE SOFTWARE; (II) POLITICAS DE SEGURANÇA; (III) INSERÇÃO DOS USUÁRIOS; E, (IV) RISCOS OPERACIONAIS RELACIONADOS
Qual a visão da Controladoria em relação ao envolvimento da área nos processos de decisões sobre alterações de sistemas operacionais na empresa? (Corina e Corina, 2009). A participação da Controladoria deve estar focada na relação custo x benefício, ou seja, nas alterações que possam afetar os resultados a serem apresentados na última linha do demonstrativo de resultado da empresa, ou seja, o lucro líquido. Como exemplos, podemos citar a participação no processo de mudança de pessoas entre áreas que acrescentam ou podem acrescentar informações mais alinhadas ao negócio; orientar, acompanhar e treinar os usuários para um maior entendimento das alterações que possam impactar as principais operações da empresa. Filtrar as que não são importantes e por fim, gerar um ambiente corporativo de maior aderência e de reflexões quanto as solicitações de alterações de sistema, questionando: É importante para o negócio esta alteração?
Quais os requisitos/atributos considerados pelas áreas de Controladoria e de TI quanto a informação disponibilizada aos seus diversos usuários? (CPC, 2008; Cobit, 2007). A norma contábil estabelece algumas premissas como compreensibilidade, relevância, confiabilidade e comparabilidade. A compreensibilidade de uma informação é que a mesma deve ser prontamente entendida pelos usuários tendo em vista sua relevância para a tomada de decisões. Neste sentido, o usuário deve ser conhecedor das informações, sendo um assunto técnico deve-se referenciar de forma detalhada para o usuário, adotar uma comunicação clara. A relevância de uma informação que dizer que estas devem ser relevantes às necessidades dos usuários na tomada de decisões. A confiabilidade da informação, para ser útil, a informação deve ser confiável, ou seja, deve estar livre de erros ou vieses relevantes e representar adequadamente aquilo que se

propõe a representar. A comparabilidade da informação, os usuários devem poder comparar as informações fornecidas, como exemplo, as demonstrações contábeis de uma entidade ao longo do tempo, a fim de identificar tendências na sua posição patrimonial, financeira e de desempenho. A Controladoria deve se preocupar em tratar informações muitas vezes técnica traduzindo para uma linguagem que permita maior entendimento e gere resultados objetivos nas ações tomadas a partir delas. Deve procurar evitar o excesso de informações.
Qual a percepção das áreas de Controladoria e de TI em relação ao tema segurança da informação e sua importância estratégica para a empresa? (KAYWORTH; WHITTEN, 2010) O processo de tomada de decisões dentro de uma empresa deve estar centrado em informações seguras. A importância que é dada para a segurança da informação pode ser determinante no resultado das decisões tomadas pela diretoria ou conselho de administração. A administração sobre informações estruturadas e seguras, é de responsabilidade das áreas de TI e de Controladoria e é considerado tema estratégico na empresa.
Quais as principais funções desempenhadas pela área de Controladoria na empresa? (BORINELLI, 2006) A Controladoria tem diversas funções na empresa, dentre elas citamos a de subsidiar o processo de tomada de decisão dos gestores, com informações confiáveis relacionadas aos principais processos de negócio da empresa. O sistema de informações deve contemplar ocorrências externas e internas. Pode-se citar ainda, outras funções da Controladoria como: (i) implantar os sistemas de informações contábeis e financeiras da empresa; (ii) motivação, que refere-se aos efeitos dos sistemas de controle sobre o comportamento das pessoas diretamente vinculadas; (iii) coordenação, que contempla assessoria e proposta de soluções prestadas à direção da empresa; (iv) avaliação e interpretação dos resultados; (v) planejamento, ao qual determina se os planos são consistentes e viáveis e se podem servir de base para avaliação posterior; e; (vi) acompanhamento ao qual consiste em verificar e monitorar os planos traçados pela gestão da empresa.
De maneira geral, como a área de Controladoria promove ações junto as demais áreas da empresa para direcionar as pessoas aos objetivos da organização? (Corina e Corina, 2009). A partir da implementação do planejamento orçamentário, enviando as premissas para as áreas da empresa e desenvolvendo cenários que apoiam a tomada de decisão a Controladoria direciona as áreas aos objetivos da organização. O orçamento é peça chave ao qual a empresa controla as metas de resultados estabelecidos *versus* sua realização dentro do exercício, orientando e acompanhando as áreas envolvidas. Funciona como balizador na tomada de decisões quanto à formação de preço, onde a política de vendas deve passar por uma aprovação econômica da Controladoria. Este processo é suportado por informações qualitativas e quantitativas, com ações junto a área de TI, buscando o alinhamento. Processos que podem gerar riscos são efetuados avaliações em conjunto com a TI para que os objetivos da organização não sejam atingidos.

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? (OLIVEIRA, 2009)
A Controladoria atua a partir do orçamento estabelecido pela companhia, onde se estruturou informações de acompanhamento de resultado, considerando os principais *drivers* da companhia. A estruturação está formatada na ferramenta de *BI* onde as informações são obtidas de forma on-line no transacional da empresa. Esse *drivers* são definidos com base na visão sistêmica da empresa conduzindo as áreas operacionais (vendas e compras) aos objetivos estabelecidos pela direção da empresa definidos no seu planejamento macro. A Controladoria cabe manter atualizada esta plataforma de informações, sinalizar eventuais desvios, direcionando aos resultados previamente estabelecidos em conjunto quando da realização do orçamento.
De maneira geral, de que forma a Controladoria atua nos processos de segurança da informação para garantir que o sistema de informações da empresa atenda às necessidades estratégicas e operacionais da empresa? (ATKINSON et al., 2008)
A Controladoria atua em processos operacionais da empresa através da análise de rentabilidade por linha de produtos, resultado por lojas, contribuição das áreas e seu alinhamento com o orçamento ou premissas de negócio da empresa. Também atua de forma pró ativa nos assuntos tributários tendo em vista as grandes alterações impostas pela prática da substituição tributária e das obrigações fiscais exigidas atualmente, como por exemplo, o Sped – Sistema Público de Escrituração Digital. A área de TI contribui com seu conhecimento, ela se envolve dentro da questão conceitual e fiscal também, existindo uma sinergia entre as áreas. Qualquer processo alterado é discutido em conjunto com a TI, ela desenvolve e acaba definindo o escopo das alterações, efetua os acompanhamentos, as alterações e os riscos que poderão estar envolvidos nesses processos.
As áreas de Controladoria e de TI consideram relevante adotar uma gestão holística para tornar as implementações de segurança da informação mais eficaz? (YOUNG; WINDSOR, 2010; ELOFF; ELOFF, 2003)
As áreas acreditam que uma visão holística possa solucionar uma série de problemas de integridade de dados e foco em informações não alinhadas com o todo. Um sistema integrado onde as decisões específicas são fundamentadas e tem alinhamento com o todo da corporação são mais eficientes no processo decisório e possibilitam uma maior segurança e assertividade no resultado a ser atingido. Esse é o cenário que a empresa está buscando com a implementação de um novo *ERP*, trabalhar com a visão de processo único e compartilhado (entrada, processo e saída) de forma integrada, on-line.
De maneira geral entende-se que a inserção dos usuários possa contribuir com a eficácia nas políticas que visam prevenir, detectar ou minimizar eventuais riscos decorrentes de falhas de segurança de informações na empresa? (SPEARS; BARKI, 2010)
O processo de gestão da informação depende da integração mútua entre as áreas da empresa. A sistematização da informação com todas as áreas, alinhadas aos objetivos da empresa contribuem para minimizar eventuais riscos em decorrência de falhas de segurança da informação. Este processo parte das

diretrizes estabelecidas, a forma de estruturação, forma de controle e de operacionalização. Se os usuários não estiverem integrados, inseridos no processo e treinados para desenvolverem o que foi planejado, o resultado ficará prejudicado. Portanto, a sua inserção é determinante para que o que foi planejado seja executado, através do seu comprometimento as ações de prevenção, e identificação podem ser trabalhadas na sua origem e serem desenvolvidas de forma adequada. Outro efeito importante é de se ampliar a base de conhecimento, como o sistema se operacionaliza, quais suas fragilidades e os usuários como aliados nestes processos.
De que maneira as áreas de TI e de Controladoria podem atuar em conjunto na inserção dos usuários a fim de conscientizá-los com as políticas de segurança de informações? (SPEARS; BARKI, 2010) As áreas de TI e de Controladoria devem desenvolver as políticas de segurança da informação, comunicar suas premissas, objetivos e ações junto ao público de usuários de forma corporativa. Estabelecer os perfis de todos os usuários e seus acessos aos sistemas da empresa. Após disseminar através de treinamentos operacionais e de conscientização quanto ao tema segurança da informação, estes processos integrados propiciam a inserção dos usuários.
Que riscos relacionados à segurança da informação podem ser minimizados tendo os usuários como principais aliados da empresa? (BULGURCU; CAVUSOGLU; BENBASAT, 2010) O não comprometimento dos usuários poderá gerar uma série de informações imprecisas. Quando o usuário tem a percepção de não ser parte integrante de um ambiente de segurança da informação, não adequadamente treinado este, pode ocasionar entrada de informações erradas no sistema da empresa, incompletas ou não relacionadas com o objetivo da empresa, poluindo, criando barreiras e riscos ao negócio. Sobre riscos, podemos citar os advindos de informações relacionadas a clientes (possibilidade de pós venda com base nas informações documentadas/solicitadas), tratamento fiscal das operações, gestão de estoques, enfim, processos relevantes para o negócio que tendo os usuários como principais aliados serão relevantemente minimizados.
Como as áreas de Controladoria e de TI abordam as necessidades de adequação dos softwares utilizados na empresa com relação as necessidades de geração de informações de apoio a tomada e decisão dos gestores? (WILKIN; CHENHALL, 2010) Primeiramente, as adequações dos softwares devem estar alinhadas com a estratégia da empresa, salvo se as alterações forem de caráter normativo ou fiscal, ao qual tem tratamento especifico com relação a sua priorização. A Controladoria e a TI desenvolvem a metodologia e disponibilizam a ferramenta de publicação das modificações a serem implementadas, detalhando seus efeitos e a sua importância em cada processo. Abordam junto a cada responsável, suas solicitações de adequação dos softwares e quais resultados se pretende atingir. Definir claramente as premissas que afetam o cliente e o resultado da companhia dando priorização e foco nesses itens para que os processos se convertam neste sentido. Planejar, treinar e testar continuamente para que seja garantida a qualidade da informação para o processo decisório da empresa.

ANEXO D – COBIT 4.1 – AHP - QUESTIONÁRIOS

Avaliador: Luis Carlos Alberti

Data: 03/11/2011

Para responder o questionário, leve em consideração a seguinte tabela do grau de maturidade do processo.

GRAU DE MATURIDADE	DESCRIÇÃO
0 – Inexistente	Neste nível há uma absoluta falta do processo. A organização não tem conhecimento sobre as implicações que a falta do processo pode gerar.
1 – Inicial	Neste nível os processos são esporádicos e desorganizados, não existe documentação e controle alguma.
2 – Repetitivo, mas intuitivo	Neste nível os processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos.
3 – Definido	Neste nível os procedimentos estão estabelecidos e são cumpridos. Inicio do uso de indicadores para controle.
4 – Gerenciado	Neste nível os processos estão integrados e alinhados. As metas e planos são baseados em dados e indicadores consistentes.
5 – Otimizado	Boas práticas são seguidas e automatizadas, com base em resultados de melhoria contínua.

Quanto ao **Nível de Importância**, deve ser considerado o grau de importância que o processo representa dentro de sua organização.

Questionário

Processos COBIT		Nível de maturidade							Nível de Importância		
		0 - Inexistente	1 - Inicial	2 - Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado		1 - Baixa	2 - Média	3 - Alta
PO - Organização e planejamento											
PO1	**Define o planejamento estratégico de TI** A empresa dispõem de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio					X				X	

PO2	**Define a arquitetura da informação** A empresa documenta a estrutura de TI e sistemas de informação com modelos e dicionário de dados.			X							X
PO3	**Determina as Diretrizes da Tecnologia** A empresa define e implementa um plano de infraestrutura, arquitetura e padrões de tecnologia com boa relação custo-benefício, que atendam os requisitos atuais e futuros do negócio.			X							X
PO4	**Define a organização de TI e seus relacionamentos** A empresa estabelece a estrutura de RH de TI com cargos, suas responsabilidades e os relacionamentos com as demais áreas da organização.				X				X		
PO5	**Gerencia o Investimento de TI** A empresa busca melhorar continuamente a relação custo-benefício da TI e sua contribuição para a lucratividade do negócio com serviços integrados que atendam às expectativas do usuário final.				X						X
PO6	**Comunica as metas e diretrizes gerenciais** A empresa estabelece e comunica as metas de TI para a equipe e as políticas de TI para a organização.				X						X
PO7	**Gerencia os recursos humanos de TI** Gerencia o RH de TI com um plano de capacitação e desenvolvimento de pessoal e plano de carreira considerando as necessidades do negócio e as tecnologias utilizadas na empresa. Desenvolve mecanismos de motivação para a equipe de TI.		X								X

PO8	**Gerencia a qualidade** Mantém de um sistema de gestão da qualidade com documentação dos processos, seleção de fornecedores e melhoria contínua de TI, integrado ao sistema de qualidade da empresa.			X							X
PO9	**Avalia e gerencia os riscos** Mantém um quadro de gestão de riscos, analisa ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência.				X						X
PO10	**Gerencia os projetos** Coordena projetos através de um plano mestre com níveis de qualidade, recursos necessários e prazos observando modelos e melhores práticas de mercado.					X				X	
AI - Aquisição e Implementação											
AI1	**Identifica soluções de automação** Para compra ou desenvolvimento de novas aplicações é realizada uma análise de requisitos, considerando fontes alternativas, análise de viabilidade econômica e tecnológica, análise de risco, custo benefício.				X						X
AI2	**Adquiri e Mantém Software Aplicativo** A empresa torna disponíveis as aplicações em alinhamento com os requisitos do negócio, no prazo desejado e com um custo razoável.					X					X

AI3	**Adquire e mantém a arquitetura tecnológica** Mantém um plano de manutenção, aquisição e implementação de melhoria da infra-estrutura tecnológica com o objetivo de dar sustentação as aplicações da empresa.				X						X
AI4	**Desenvolve e mantém procedimentos de TI** Disponibiliza documentação e treinamento os usuários e profissionais de TI para correta utilização dos sistemas e infra - estrutura de TI.			X							X
AI5	**Obtém recursos de TI** Dispõe de um procedimento para aquisição de recursos necessários de TI, incluindo hardware, software, serviços, pessoas e fornecedores.						X				X
AI6	**Gerenciar mudanças** Avalia e aprova mudanças no ambiente, tanto em equipamentos e arquitetura quanto em sistemas e processos.					X					X
AI7	**Instala e certifica soluções e mudanças** Antes da entrega de novas soluções de TI (Software, Hardware e Sistemas) são realizados testes apropriados e um acompanhamento pós-implantação.					X					X
DS - Entrega e suporte											
ES1	**Define níveis e mantém os acordos de níveis de serviços** Formaliza os níveis de atendimento e internos e externos das soluções TI.						X				X

ES2	**Gerencia os serviços de terceiros** Acompanha e avalia os serviços contratados.					X					X
ES3	**Gerenciar desempenho e capacidade da TI** A empresa define e revisa periodicamente os recursos computacionais e garante que não haja escassez de recursos, evitando problemas de desempenho nas aplicações ou desperdício de investimentos.					X				X	
ES4	**Garante a continuidade dos serviços** Assegura a continuidade dos serviços, incluindo sistemas de Backup, manutenção de equipamentos, testes e plano de contingência de hardware e serviços críticos.					X					X
ES5	**Garante a segurança dos sistemas** A empresa dispõe de políticas de segurança, visa a preservação da confidencialidade, da integridade e da disponibilidade da informação.				X					X	
ES6	**Identifica e Aloca Custos** A empresa coleta de forma completa os custos de TI, e faz sua alocação de maneira justa e aceita pelos usuários do negócio.					X					X
ES7	**Educa e treina os usuários** A empresa mantém um plano de treinamento de usuários e profissionais de TI para uso eficaz e eficiente dos sistemas de informação.		X								X
ES8	**Gerencia a central de serviços e incidentes** Existe o registro e controle das solicitações e incidências de TI.						X				X

ES9	**Gerencia a configuração** A empresa dispõe de um repositório/registro das configurações de hardware e software com o objetivo de minimizar e resolver problemas com mais agilidade.				X						X
ES10	**Gerencia os problemas** Existe uma metodologia de ações corretivas e preventivas para os problemas de TI.					X					X
ES11	**Gerencia os dados** Define o ciclo de vida da informação, com definição de prazos para disponibilidade, arquivo morto e descarte de acordo com os requisitos do negócio e da legislação.				X						X
ES12	**Gerencia a infra-estrutura** Existe uma definição dos requisitos físicos e controle do ambiente físico para os equipamentos de TI, incluindo fatores ambientais, de acesso, instalações entre outros.				X					X	
ES13	**Gerenciar operações** Administra o funcionamento das operações de TI					X					X
ME - Medição e monitoramento											
MO1	**Monitora e avalia a desempenho de TI** Utiliza indicadores para monitorar e gerenciar o desempenho dos processos de TI.					X				X	
MO2	**Monitora e avalia o controle interno** Estabelece mecanismos de controle interno dos requisitos da área e monitora a sua execução.				X					X	
MO3	**Assegura a conformidade aos requisitos externos** Estabelece processo de revisão dos requisitos de legislação, contratuais e de negócio.			X							X

MO4	**Fornecer governança de TI** Estabelece um efetivo modelo de governança, que inclui definição da estrutura organizacional, processos, liderança, perfis e responsabilidades, a fim de garantir que os investimentos estejam alinhados às estratégias da organização.				X					X	

Avaliador: Cipriano Arrosi

Data: 04/11/2011

Para responder o questionário, leve em consideração a seguinte tabela do grau de maturidade do processo.

GRAU DE MATURIDADE	DESCRIÇÃO
0 – Inexistente	Neste nível há uma absoluta falta do processo. A organização não tem conhecimento sobre as implicações que a falta do processo pode gerar.
1 – Inicial	Neste nível os processos são esporádicos e desorganizados, não existe documentação e controle alguma.
2 – Repetitivo, mas intuitivo	Neste nível os processos seguem um padrão de regularidade, com alta dependência do conhecimento dos indivíduos.
3 – Definido	Neste nível os procedimentos estão estabelecidos e são cumpridos. Inicio do uso de indicadores para controle.
4 – Gerenciado	Neste nível os processos estão integrados e alinhados. As metas e planos são baseados em dados e indicadores consistentes.
5 – Otimizado	Boas práticas são seguidas e automatizadas, com base em resultados de melhoria contínua.

Quanto ao **Nível de Importância**, deve ser considerado o grau de importância que o processo representa dentro de sua organização.

Processos COBIT		Nível de maturidade							Nível de Importância		
		0 - Inexistente	1 - Inicial	2 - Repetitivo	3 - Definido	4 - Gerenciado	5- Otimizado		1 - Baixa	2 - Média	3 - Alta
PO - Organização e planejamento											
PO1	**Define o planejamento estratégico de TI** A empresa dispõem de um Plano de TI com base em um plano estratégico de negócio, vinculando as diretrizes de TI às necessidades do negócio				X						X
PO2	**Define a arquitetura da informação** A empresa documenta a estrutura de TI e sistemas de informação com modelos e dicionário de dados.			X							X
PO 3	**Determina as Diretrizes da**			X							X

	Tecnologia A empresa define e implementa um plano de infraestrutura, arquitetura e padrões de tecnologia com boa relação custo-benefício, que atendam os requisitos atuais e futuros do negócio.										
PO4	**Define a organização de TI e seus relacionamentos** A empresa estabelece a estrutura de RH de TI com cargos, suas responsabilidades e os relacionamentos com as demais áreas da organização.			X						X	
PO5	**Gerencia o Investimento de TI** A empresa busca melhorar continuamente a relação custo-benefício da TI e sua contribuição para a lucratividade do negócio com serviços integrados que atendam às expectativas do usuário final.		X							X	
PO6	**Comunica as metas e diretrizes gerenciais** A empresa estabelece e comunica as metas de TI para a equipe e as políticas de TI para a organização.				X						X
PO7	**Gerencia os recursos humanos de TI** Gerencia o RH de TI com um plano de capacitação e desenvolvimento de pessoal e plano de carreira considerando as necessidades do negócio e as tecnologias utilizadas na empresa. Desenvolve mecanismos de motivação para a equipe de TI.		X								X
PO8	**Gerencia a qualidade** Mantém de um sistema de gestão da qualidade com documentação dos processos, seleção de fornecedores e melhoria contínua de TI, integrado ao sistema de qualidade da empresa.			X							X
PO9	**Avalia e gerencia os riscos** Mantém um quadro de gestão de riscos, analisa ameaças, impactos no negócio e vulnerabilidades da informação e instalações, bem como a probabilidade de ocorrência com um plano de contingência.			X							X
C 1	**Gerencia os projetos**				X						X

	Coordena projetos através de um plano mestre com níveis de qualidade, recursos necessários e prazos observando modelos e melhores práticas de mercado.										
AI - Aquisição e Implementação											
AI1	**Identifica soluções de automação** Para compra ou desenvolvimento de novas aplicações é realizada uma análise de requisitos, considerando fontes alternativas, análise de viabilidade econômica e tecnológica, análise de risco, custo benefício.					X				X	
AI2	**Adquiri e Mantem Software Aplicativo** A empresa torna disponíveis as aplicações em alinhamento com os requisitos do negócio, no prazo desejado e com um custo razoável.				X					X	
AI3	**Adquire e mantém a arquitetura tecnológica** Mantém um plano de manutenção, aquisição e implementação de melhoria da infra - estrutura tecnológica com o objetivo de dar sustentação as aplicações da empresa.			X					X		
AI4	**Desenvolve e mantém procedimentos de TI** Disponibiliza documentação e treinamento os usuários e profissionais de TI para correta utilização dos sistemas e infra-estrutura de TI.				X					X	
AI5	**Obtém recursos de TI** Dispõe de um procedimento para aquisição de recursos necessários de TI, incluindo hardware, software, serviços, pessoas e fornecedores.					X			X		
AI6	**Gerenciar mudanças** Avalia e aprova mudanças no ambiente, tanto em equipamentos e arquitetura quanto em sistemas e processos.					X				X	
AI7	**Instala e certifica soluções e mudanças** Antes da entrega de novas soluções de TI (Software, Hardware e Sistemas) são realizados testes apropriados e um acompanhamento pós-implantação.					X				X	

DS - Entrega e suporte		

ES1	**Define níveis e mantém os acordos de níveis de serviços** Formaliza os níveis de atendimento e internos e externos das soluções TI.				X						X
ES2	**Gerencia os serviços de terceiros** Acompanha e avalia os serviços contratados.				X						X
ES3	**Gerenciar desempenho e capacidade da TI** A empresa define e revisa periodicamente os recursos computacionais e garante que não haja escassez de recursos, evitando problemas de desempenho nas aplicações ou desperdício de investimentos.			X						X	
ES4	**Garante a continuidade dos serviços** Assegura a continuidade dos serviços, incluindo sistemas de Backup, manutenção de equipamentos, testes e plano de contingência de hardware e serviços críticos.			X							X
ES5	**Garante a segurança dos sistemas** A empresa dispõe de políticas de segurança, visa a preservação da confidencialidade, da integridade e da disponibilidade da informação.			X							X
ES6	**Identifica e Aloca Custos** A empresa coleta de forma completa os custos de TI, e faz sua alocação de maneira justa e aceita pelos usuários do negócio.				X						X
ES7	**Educa e treina os usuários** A empresa mantém um plano de treinamento de usuários e profissionais de TI para uso eficaz e eficiente dos sistemas de informação.		X								X
ES8	**Gerencia a central de serviços e incidentes** Existe o registro e controle das solicitações e incidências de TI.				X						X
ES9	**Gerencia a configuração** A empresa dispõe de um repositório/registro das configurações de hardware e software com o objetivo de minimizar e resolver problemas com mais agilidade.			X							X
S 1	**Gerencia os**			X							X

	problemas Existe uma metodologia de ações corretivas e preventivas para os problemas de TI.										
ES11	**Gerencia os dados** Define o ciclo de vida da informação, com definição de prazos para disponibilidade, arquivo morto e descarte de acordo com os requisitos do negócio e da legislação.			X							X
ES12	**Gerencia a infra-estrutura** Existe uma definição dos requisitos físicos e controle do ambiente físico para os equipamentos de TI, incluindo fatores ambientais, de acesso, instalações entre outros.				X						X
ES13	**Gerenciar operações** Administra o funcionamento das operações de TI					X					X
ME - Medição e monitoramento											
MO1	**Monitora e avalia a desempenho de TI** Utiliza indicadores para monitorar e gerenciar o desempenho dos processos de TI.				X						X
MO2	**Monitora e avalia o controle interno** Estabelece mecanismos de controle interno dos requisitos da área e monitora a sua execução.			X						X	
MO3	**Assegura a conformidade aos requisitos externos** Estabelece processo de revisão dos requisitos de legislação, contratuais e de negócio.		X								X
MO4	**Fornecer governança de TI** Estabelece um efetivo modelo de governança, que inclui definição da estrutura organizacional, processos, liderança, perfis e responsabilidades, a fim de garantir que os investimentos estejam alinhados às estratégias da organização.			X							X

ANEXO E – ANÁLISE DE CONTEÚDO PARA SELEÇÃO CATEGORIAS ENTREVISTAS

	TEMAS / QUESTÕES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	Fatores limitadores da integração das áreas de Controladoria e TI	■										■						■	■	■		■	■	■		■	■	■	■		■
2	Áreas com formação / competências diferentes - Controladoria e TI	■	■									■		■							■	■	■	■					■		
3	Falta de planejamento das customizações de software	■			■								■	■				■												■	■
4	Não priorização de alterações de software relevantes para o negócio em detrimento necessidades específicas das áreas	■		■	■								■	■															■	■	■
5	Restrições sobre alterações em softwares	■		■	■								■	■	■		■				■			■					■		
6	Falta de alinhamento da comunicação entre usuários, áreas de Controladoria e TI	■	■	■								■	■	■		■		■	■	■		■	■	■			■	■	■	■	■
7	Criar um Comitê composto pelas áreas de Controladoria e TI para analisar mudanças de software que afetam o negócio		■	■	■		■		■			■	■	■		■	■		■	■		■	■	■		■	■	■	■		■
8	Processos ligados aos pilares do negócio - (i) comprar; (ii) estocar; (iii) vender; (iv) distribuir; (v) pós-venda e (vi) tributação		■	■	■	■		■			■		■	■		■	■	■	■	■	■	■	■		■	■	■	■	■	■	■
9	Processos que integram as áreas de Contorladoria e TI		■	■	■		■							■			■	■	■	■			■			■					■
10	Planejamento Estratégico	■	■	■		■	■	■												■		■	■	■	■		■				
11	Profissionais com conhecimento nas mais diversas áreas da empresa		■		■							■				■		■				■					■	■	■		
12	Vulnerabilidade no sistema de informações advindo das alterações de software			■					■				■		■	■						■							■	■	

	TEMAS / QUESTÕES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
13	Treinamentos contínuos e de conscientização junto aos usuários chaves das demais áreas da empresa (SI / Controladoria)	■	■	■	■		■		■			■		■	■		■	■	■	■		■	■	■		■	■	■	■	■	■
14	Homologação sistêmica das alterações de software junto ao usuário solicitante			■	■		■		■			■	■	■	■	■	■	■	■	■	■							■	■	■	■
15	Indicadores para identificar alterações de software que impactam ao negócio, das menos relevantes			■			■						■	■	■			■				■	■				■	■	■	■	
16	Controladoria e TI atuando de forma integrada nas alterações de software	■		■	■				■			■	■	■	■		■	■		■		■	■	■		■	■		■	■	
17	Alterações de software alinhadas as premissas de integridade de dados e aos objetivos de negócio			■	■				■				■	■	■	■	■	■	■		■									■	■
18	Retrabalhos advindos de erros nas alterações de software				■				■				■	■		■	■		■									■		■	
19	Riscos (Ganhos ou perdas) econômicos e financeiros				■	■		■			■		■		■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
20	Criar um ambiente fidedigno para a realização dos testes após alteração de software				■				■	■			■	■		■	■	■	■		■	■						■	■		■
21	Arquitetura de processos de alterações de software com especificações de necessidades, objetivos e retornos esperados	■		■	■		■		■	■		■	■	■		■	■	■	■			■	■					■	■		■
22	Documentar papéis e responsabilidades de usuários envolvidos em processos de compras e vendas					■		■			■							■											■		
23	Documentar papéis e responsabilidades de usuários quanto a segurança da informação					■	■			■	■			■	■	■	■	■	■			■						■	■		
24	Riscos de imagem da empresa (clientes, fornecedores, acionistas, funcionários)					■		■							■		■	■		■	■	■	■	■	■	■	■	■	■	■	■
25	Falta de foco aos objetivos da empresa privilegiando metas individuais					■												■											■	■	■

	TEMAS / QUESTÕES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
26	Treinamentos integrados realizados pela Controladoria e TI abordando segurança da informação e a informação para tomada de decisão						■					■		■	■					■	■	■	■	■	■	■	■	■		■
27	Participação dos usuários nos processos de segurança da informação e disponibilidade de informações para tomada de decisão						■		■			■		■	■	■	■		■	■	■	■	■	■	■	■	■	■		■
28	Através da Direção da empresa influenciando as áreas de gestão, em especial as relacionadas aos pilares do negócio - Projeto corporativo	■					■					■		■	■					■		■	■	■	■	■	■				
29	Gestão de estoques e atendimento a clientes							■										■		■			■								
30	Controles codificados e de rastreabilidade de mercadorias							■										■													
31	Afetar margens de lucratividade				■	■		■			■						■	■		■	■		■	■	■	■	■	■	■	■	■
32	Rastreabilidade das alterações de sistema/software (log) - gestão equipes								■	■					■		■	■		■	■					■		■	■		■
33	Controles das versões dos softwares									■			■	■	■	■	■	■											■		■
34	Políticas e procedimentos de troca de informações com entidades externas										■				■			■			■	■	■	■		■	■	■		■	
35	Riscos contábeis, fiscais e tributários				■	■		■			■						■	■		■	■	■	■	■	■	■	■	■	■	■	■
36	Políticas e normas de segurança da informação (Controle de acesso, perfis usuários, etc...)	■	■		■		■				■	■	■	■	■	■	■	■	■		■	■		■	■			■	■	■	■
37	Relacionamentos comerciais com fornecedores e clientes					■		■			■						■	■									■			■	
38	Comparabilidade com informações externas - benchmarking										■										■		■	■			■				
39	Riscos de integridade das informações			■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■
40	Gestão holística (Sistema aberto em contínua interação com o ambiente)	■	■	■	■		■				■	■	■			■	■	■	■	■		■	■	■	■	■	■	■	■		■

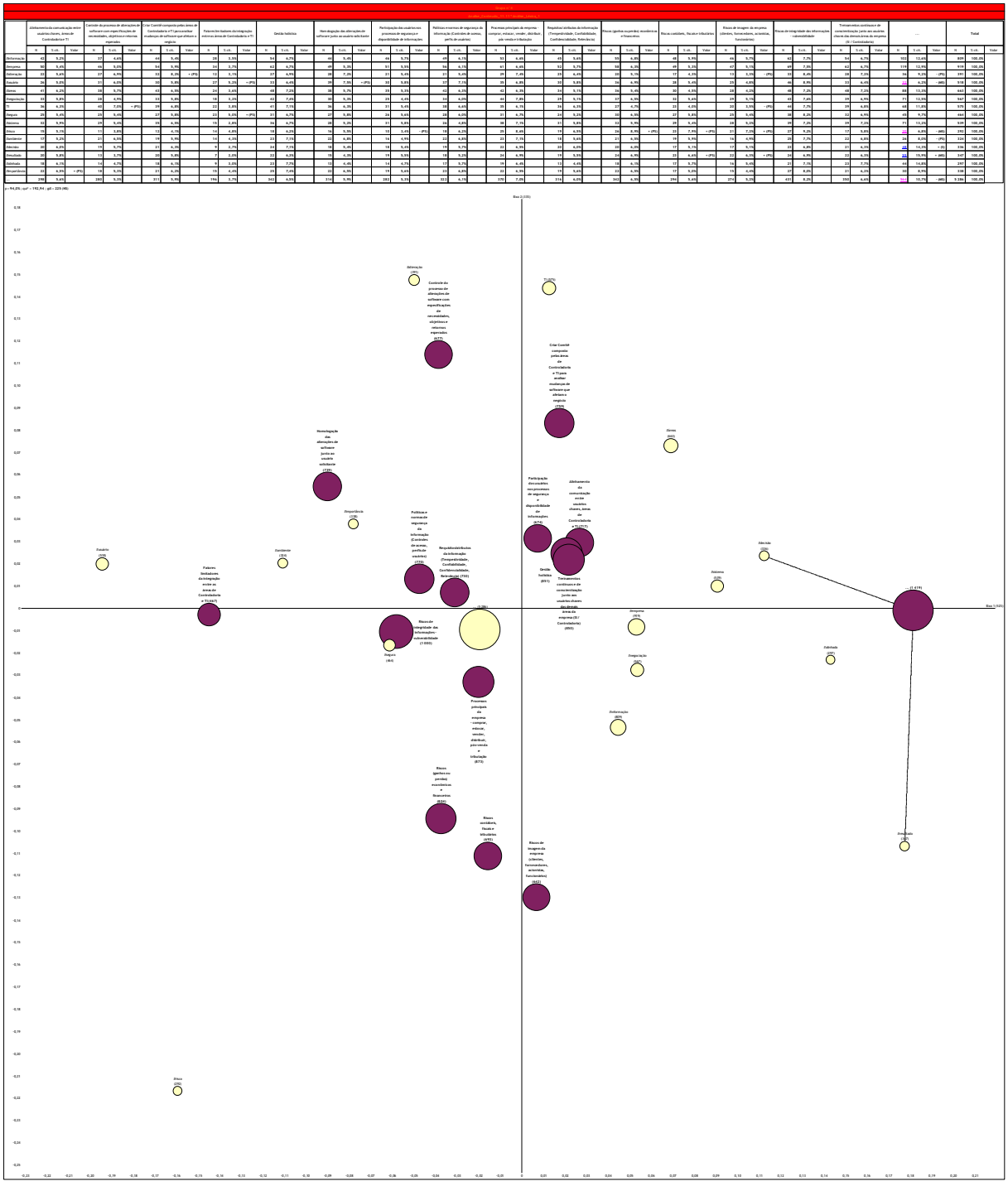
	TEMAS / QUESTÕES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
41	Requisitos/atributos da informação (Tempestividade, Confiabilidade, Confidencialidade, Relevância, etc.)																														
42	Modelar o sistema informacional da empresa																														
43	Direcionar as áreas aos objetivos da organização																														
44	Ferramenta *Business Intelligence - BI*																														

Análise de Conteúdo para classificação das categorias as respostas dos gestores

	CLASSIFICAÇÃO DAS CATEGORIAS / QUESTÕES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	**Alinhamento da comunicação entre usuários chaves, áreas de Controladoria e TI**	■	■	■								■	■	■		■		■	■	■		■	■	■			■	■	■	■	■
2	***Business Intelligence - BI* (Sistemas de informações para tomada de decisão)**																								■	■	■				
3	**Controle do processo de alterações de software com especificações de necessidades, objetivos e retornos esperados**	■		■	■		■		■	■		■	■	■		■	■	■	■			■	■					■	■		■
4	**Criar Comitê composto pelas áreas de Controladoria e TI para analisar mudanças de software que afetam o negócio**		■	■	■		■		■			■	■	■		■	■		■	■		■	■	■		■	■	■	■		■
5	Direção da empresa influenciando as áreas de gestão com foco nos pilares do negócio - Projeto corporativo	■					■					■		■	■					■		■	■	■	■	■	■				
6	**Fatores limitadores da integração entre as áreas de Controladoria e TI**					■	■			■	■			■	■	■	■	■	■			■						■	■		
7	**Gestão holística em Segurança da Informação**	■	■	■	■		■				■	■	■			■	■	■	■	■		■	■	■	■	■	■	■	■		■
8	**Homologação das alterações de software junto ao usuário solicitante**			■	■		■		■			■	■	■	■	■	■	■	■	■	■	■						■	■	■	■
9	Modelagem do sistema informacional da empresa																						■	■	■	■					■
10	**Participação dos usuários nos processos de segurança e disponibilidade de informações**						■		■			■		■	■	■	■		■	■	■	■	■	■	■	■	■	■	■		■
11	**Políticas e normas de segurança da informação (Controle de acesso, perfis usuários, etc...)**	■	■		■		■				■	■	■	■	■	■	■	■	■		■	■		■	■			■	■	■	■
12	**Processos principais da empresa - comprar, estocar, vender, distribuir, pós-venda e tributação**		■	■	■	■		■			■		■	■		■	■	■	■	■	■	■	■		■	■	■	■	■	■	■

	CLASSIFICAÇÃO DAS CATEGORIAS / QUESTÕES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
13	**Requisitos/atributos da informação (Tempestividade, Confiabilidade, Confidencialidade, Relevância, etc.)**																														
14	**Riscos (Ganhos ou perdas) econômicos e financeiros**																														
15	**Riscos de integridade das informações - vulnerabilidade**																														
16	**Treinamentos contínuos e de conscientização junto aos usuários chaves das demais áreas da empresa (SI / Controladoria)**																														

ANEXO F – MAPAS ANÁLISES QUALITATIVAS DAS ENTREVISTAS – *SOFTWARE SPHINX*

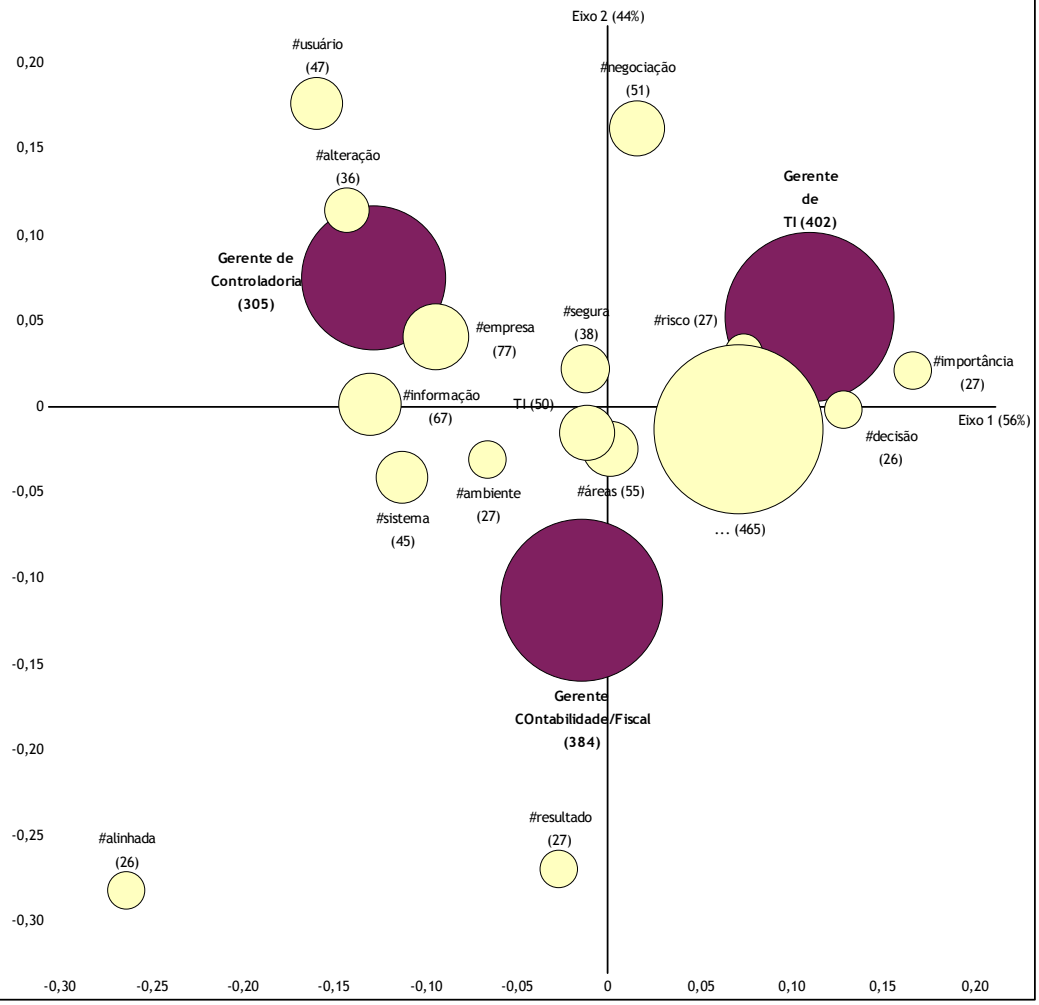


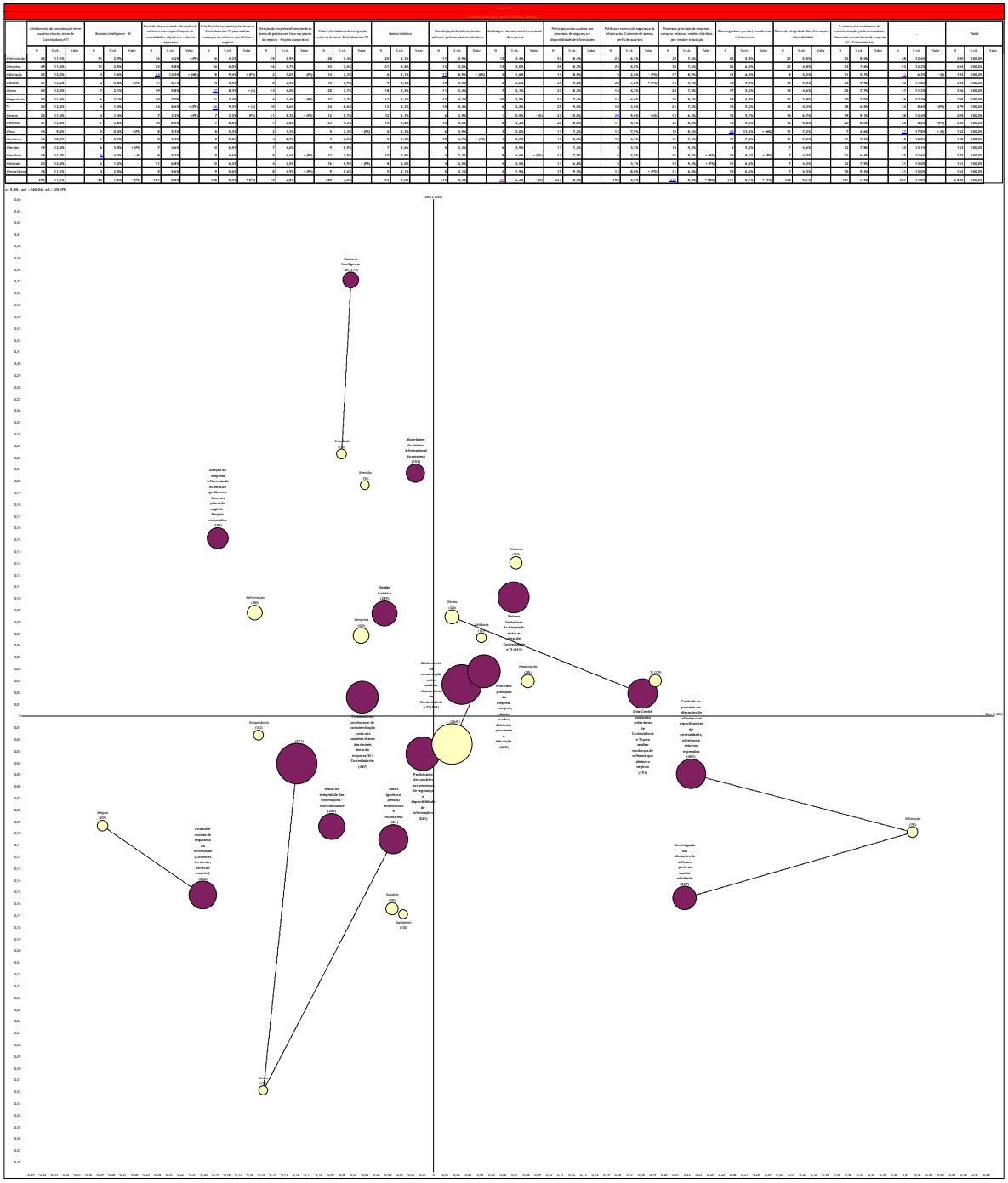
Grupo n°5

Cargo * Análise_Léxica_1

	Gerente COntabilidade/Fiscal			Gerente de Controladoria			Gerente de TI			**Total**		
	N	% cit.	Valor	N	% cit.	Valor	N	% cit.	Valor	N	% cit.	Valor
#informação	**24**	**35,8%**		**22**	**32,8%**		**21**	**31,3%**		**67**	**100,0%**	
#empresa	**26**	**33,8%**		**25**	**32,5%**		**26**	**33,8%**		**77**	**100,0%**	
#alteração	**11**	**30,6%**		**13**	**36,1%**		**12**	**33,3%**		**36**	**100,0%**	
#usuário	**13**	**27,7%**		**18**	**38,3%**		**16**	**34,0%**		**47**	**100,0%**	
#áreas	**20**	**36,4%**		**15**	**27,3%**		**20**	**36,4%**		**55**	**100,0%**	
#negociação	**14**	**27,5%**		**16**	**31,4%**		**21**	**41,2%**		**51**	**100,0%**	
TI	**18**	**36,0%**		**14**	**28,0%**		**18**	**36,0%**		**50**	**100,0%**	
#segura	**13**	**34,2%**		**11**	**28,9%**		**14**	**36,8%**		**38**	**100,0%**	
#sistema	**17**	**37,8%**		**14**	**31,1%**		**14**	**31,1%**		**45**	**100,0%**	
#risco	**9**	**33,3%**		**7**	**25,9%**		**11**	**40,7%**		**27**	**100,0%**	
#ambiente	**10**	**37,0%**		**8**	**29,6%**		**9**	**33,3%**		**27**	**100,0%**	
#decisão	**9**	**34,6%**		**6**	**23,1%**		**11**	**42,3%**		**26**	**100,0%**	
#resultado	**13**	**48,1%**		**6**	**22,2%**		**8**	**29,6%**		**27**	**100,0%**	
#alinhada	**13**	**50,0%**	**+ (PS)**	**8**	**30,8%**		**5**	**19,2%**		**26**	**100,0%**	
#importância	**9**	**33,3%**		**6**	**22,2%**		**12**	**44,4%**		**27**	**100,0%**	
...	**165**	**35,5%**		**116**	**24,9%**	**- (MS)**	**184**	**39,6%**	**+ (S)**	**465**	**100,0%**	

p = **36,0%** ; qui² = **32,17** ; gdl = **30** (NS)



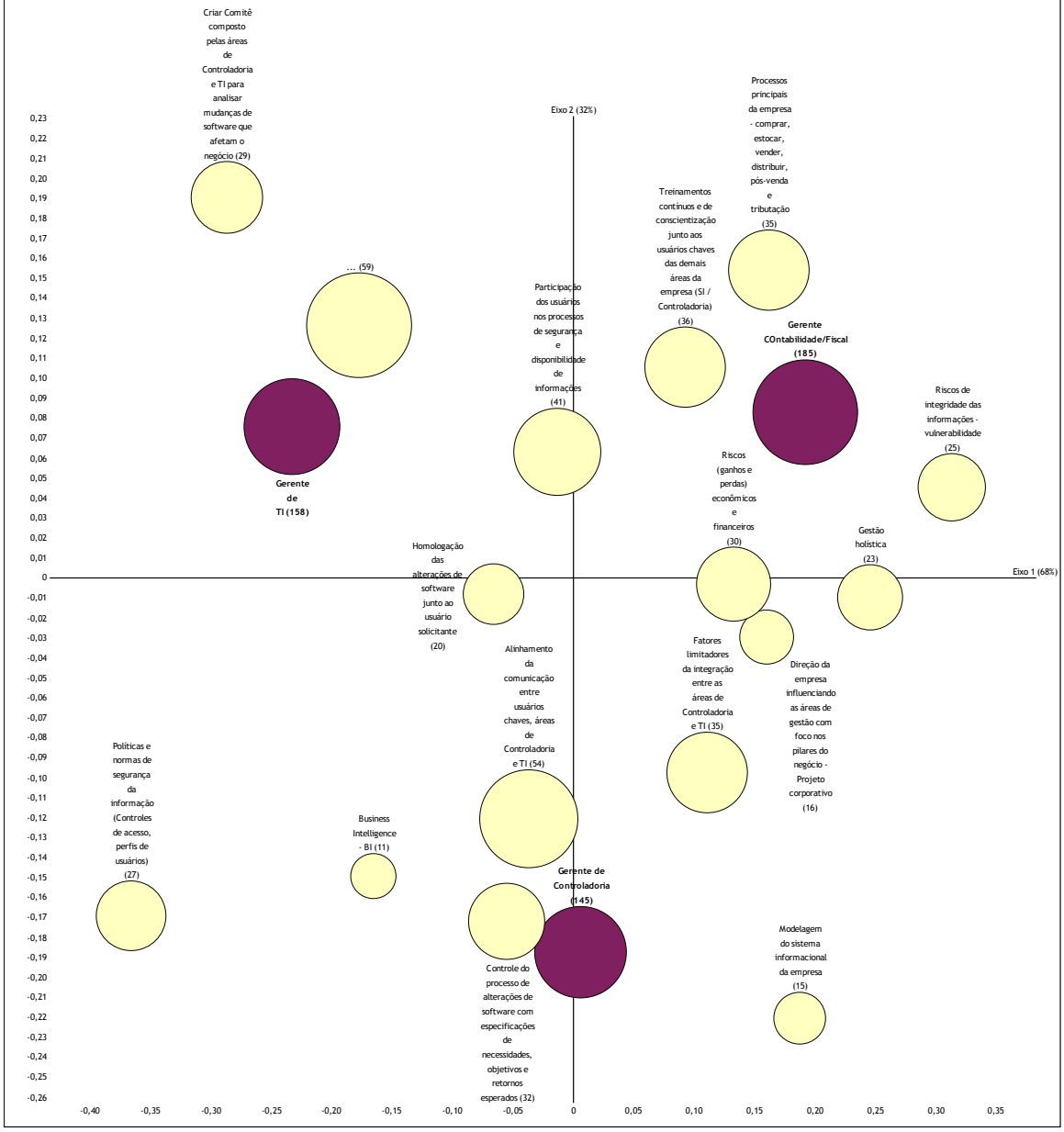


Grupo n° 8

Cargo * Analise_Cont_por_gestor

	Gerente COntabilidade/Fiscal			Gerente de Controladoria			Gerente de TI			Total		
	N	% cit.	Valor	N	% cit.	Valor	N	% cit.	Valor	N	% cit.	Valor
Alinhamento da comunicação entre usuários chaves, áreas de Controladoria e TI	18	33,3%		19	35,2%		17	31,5%		54	100,0%	
Business Intelligence - BI	3	27,3%		4	36,4%		4	36,4%		11	100,0%	
Controle do processo de alterações de software com especificações de necessidades, objetivos e retornos esperados	10	31,3%		12	37,5%		10	31,3%		32	100,0%	
Criar Comitê composto pelas áreas de Controladoria e TI para analisar mudanças de software que afetam o negócio	9	31,0%		6	20,7%		14	48,3%		29	100,0%	
Direção da empresa influenciando as áreas de gestão com foco nos pilares do negócio - Projeto corporativo	7	43,8%		5	31,3%		4	25,0%		16	100,0%	
Fatores limitadores da integração entre as áreas de Controladoria e TI	14	40,0%		12	34,3%		9	25,7%		35	100,0%	
Gestão holística	11	47,8%		7	30,4%		5	21,7%		23	100,0%	
Homologação das alterações de software junto ao usuário solicitante	7	35,0%		6	30,0%		7	35,0%		20	100,0%	
Modelagem do sistema informacional da empresa	6	40,0%		6	40,0%		3	20,0%		15	100,0%	
Participação dos usuários nos processos de segurança e disponibilidade de informações	16	39,0%		11	26,8%		14	34,1%		41	100,0%	
Políticas e normas de segurança da informação (Controles de acesso, perfis de usuários)	5	18,5%		10	37,0%		12	44,4%		27	100,0%	
Processos principais da empresa - comprar, estocar, vender, distribuir, pós-venda e tributação	17	48,6%	+ (PS)	8	22,9%		10	28,6%		35	100,0%	
Riscos (ganhos e perdas) econômicos e financeiros	13	43,3%		9	30,0%		8	26,7%		30	100,0%	
Riscos de integridade das informações - vulnerabilidade	13	52,0%	+ (PS)	7	28,0%		5	20,0%		25	100,0%	
Treinamentos contínuos e de conscientização junto aos usuários chaves das demais áreas da empresa (SI / Controladoria)	16	44,4%		9	25,0%		11	30,6%		36	100,0%	
...	20	33,9%		14	23,7%		25	42,4%		59	100,0%	

p = **56,7%** ; qui² = **28,07** ; gdl = **30 (NS)**



UNIVERSIDADE DO VALE DO RIO DOS SINOS

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS

NÍVEL MESTRADO

AUTORIZAÇÃO

Eu, Luiz Carlos Schneider, CPF 429.255.920-15 autorizo o Programa de Mestrado em Ciências Contábeis da UNISINOS a disponibilizar a Dissertação de minha autoria sob o título **"AVALIAÇÃO DE PROCESSOS DE SEGURANÇA DA INFORMAÇÃO NA INTEGRAÇÃO DAS ÁREAS DE CONTROLADORIA E DE TECNOLOGIA DA INFORMAÇÃO"**, orientada pelo professor doutor Adolfo Aberto Vanti, para:

Consulta (X) Sim ( ) Não
Empréstimo (X) Sim ( ) Não
Reprodução:

Parcial (X) Sim ( ) Não
Total (X) Sim ( ) Não

Divulgar e disponibilizar na Internet gratuitamente, sem ressarcimento dos direitos autorais, o texto integral da minha Dissertação citada acima, no *site* do Programa, para fins de leitura e/ou impressão pela Internet

Parcial (X) Sim ( ) Não
Total (X) Sim ( ) Não

Em caso afirmativo, especifique:
Sumário: (X) Sim ( ) Não
Resumo: (X) Sim ( ) Não
Capítulos:(X)Sim ( ) Não Quais_____
Bibliografia: (X) Sim ( ) Não
Anexos: (X) Sim ( ) Não

São Leopoldo, 22 de Junho de 2012.

Assinatura do(a) Autor(a)

Visto do(a) Orientador(a)

Programa de Pós-Graduação - Mestrado

Ciências Contábeis

Curso recomendado pela CAPES

Conceito 4

CAPES

TERMO DE INSERÇÃO DE DISSERTAÇÕES E TESES NA BIBLIOTECA DIGITAL

Dados

Nome/Autor: LUIZ CARLOS SCHNEIDER RG: 5032337734 CPF: 429.255.920-15 Email: schneider.luizc@gmail.com Fone: (54) 9903-3567

Endereço: Rua Silveira Martins, n° 386 Município/UF: Farroupilha/RS

Programa/Curso de Pós-Graduação: Programa de Pós Graduação em Ciências Contábeis – Nível Mestrado

Nome do Orientador: Prof. Dr. Adolfo Aberto Vanti

Nome do Co-orientador: _____

Membros da Banca: Prof. Dr. Angel Cobo – Univ. Cantabria; Prof. Dr. Carlos Alberto Diehl – UNISINOS e Prof. Dr. Clóvis Antônio Kronbauer – UNISINOS.

Data da Defesa: 24/04/2012 Número de páginas: 199

Título do Trabalho Acadêmico: **"AVALIAÇÃO DE PROCESSOS DE SEGURANÇA DA INFORMAÇÃO NA INTEGRAÇÃO DAS ÁREAS DE CONTROLADORIA E DE TECNOLOGIA DA INFORMAÇÃO"**

Instituição de Defesa: UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS

Instituição de Fomento: _____

Objeto

Nos termos da Portaria CAPES n.º 13, de 15 de fevereiro de 2006, disponibilizo (em caráter gratuito, por tempo indeterminado e sem ressarcimento dos direitos autorais), bem como me responsabilizo pelo conteúdo do trabalho acadêmico acima indicado para inserção no Banco de Dados e *Sites* aos quais esteja vinculada a Biblioteca da Universidade do Vale do Rio dos Sinos – UNISINOS, para fins de leitura pela internet.
Autorizo, ainda, a UNISINOS, em caráter gratuito e independente de prévia notificação, a ceder o meu Trabalho Acadêmico para Bibliotecas Digitais de outras instituições de ensino, cultura e pesquisa.

DECLARO QUE LI E CONCORDO COM TODAS AS CONDIÇÕES E TERMOS DO PRESENTE DOCUMENTO.

São Leopoldo, 22 de Junho de 2012.

_____

Luiz Carlos Schneider