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

MARCOS CREPALDI

DEFINIÇÃO DE CRITÉRIOS PARA AVALIAÇÃO DE PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO (TI) CONSIDERANDO *ACCOUNTABILITY* NO GERENCIAMENTO DE RISCOS: UM ESTUDO EM INSTITUIÇÕES FINANCEIRAS BANCÁRIAS NO BRASIL

SÃO LEOPOLDO
2013

Marcos Crepaldi

DEFINIÇÃO DE CRITÉRIOS PARA AVALIAÇÃO DE PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO (TI) CONSIDERANDO *ACCOUNTABILITY* NO GERENCIAMENTO DE RISCOS: UM ESTUDO EM INSTITUIÇÕES FINANCEIRAS BANCÁRIAS NO BRASIL

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre, pelo Programa de Pós-Graduação em Ciências Contábeis da Universidade do Vale do Rio dos Sinos – UNISINOS.
Área de concentração: Controladoria e Finanças

Orientador: Prof. Dr. Adolfo Alberto Vanti

São Leopoldo

2013

C93 Crepaldi, Marcos, 1973-
Definição de critérios para avaliação de processos de tecnologia da informação (TI) considerando accountability no gerenciamento de riscos : um estudo em instituições financeiras bancárias no Brasil / Marcos Crepaldi ; Orientador: Adolfo Alberto Vanti. – 2013.
110 f. ; il. ; 30 cm

Dissertação (mestrado)–Universidade do Vale do Rio dos Sinos, São Leopoldo, RS, 2013

Inclui bibliografias

1. Tecnologia da Informação. 2. Governança de TI. 3. Accountability. 4. Gerenciamento de riscos. 5. COBIT®. I. Vanti, Adolfo Alberto. II. Universidade do Vale do Rio dos Sinos - Programa de Pós-Graduação em Ciências Contábeis. III. Título.

CDD – 303.4833

Ficha catalográfica elaborada pela Bibliotecária Élia da Silva, CRB-14/1250

Marcos Crepaldi

DEFINIÇÃO DE CRITÉRIOS PARA AVALIAÇÃO DE PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO (TI) CONSIDERANDO *ACCOUNTABILITY* NO GERENCIAMENTO DE RISCOS: UM ESTUDO EM INSTITUIÇÕES FINANCEIRAS BANCÁRIAS NO BRASIL

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

Aprovada em 24 de Abril de 2013

BANCA EXAMINADORA

Prof. Dr. Wilson Toshiro Nakamura – MACKENZIE

Profa. Dra. Clea Beatriz Macagnan – UNISINOS

Prof. Dr. Miguel Afonso Sellitto – UNISINOS

AGRADECIMENTOS

O trabalho do pesquisador é árduo. Exige dedicação, persistência e superação. Um turbilhão de sentimentos envolve um processo de profundas transformações.

Expresso meu agradecimento especial ao Prof. Dr. Adolpho Alberto Vanti e aos professores do PPG em Ciências Contábeis da Unisinos pelo compartilhamento de experiências, atenção dispensada e rigor exigido.

Agradeço meus familiares e amigos que compreenderam os longos períodos de ausência, apoiando e incentivando incondicionalmente.

RESUMO

Definir critérios para avaliação de processos de TI considerando *accountability* no gerenciamento de riscos nas maiores instituições financeiras bancárias com operação no Brasil constitui-se o objetivo da presente pesquisa, classificada como descritiva. Analisar critérios de modelo estabelecido, evidenciar formas de mensuração de desempenho à luz da GTI e investigar evidências do gerenciamento de riscos, responsabilização, prestação de contas e transparência em Relatórios de Gerenciamento de Riscos, constituíram-se meios para a definição de critérios proposta. Técnicas de Análise de Conteúdo, Análise Lexical, Estatística Descritiva e construção de Mapas Fatoriais, auxiliaram na evidenciação dos resultados. A Análise de Conteúdo permitiu a identificação de frequência dos critérios. Aliada à Análise Lexical permitiu a verificação de influências entre as variáveis categóricas e as variáveis léxicas. A Análise Lexical viabilizou o estabelecimento de relações de influência entre os conceitos (risco, estratégia, desempenho, tecnologia da informação, segurança, responsabilidade, prestação de contas e transparência) e as categorias (critérios para avaliação). Os resultados mostraram que há relação significante entre os critérios analisados e os elementos de gerenciamento de riscos e *accountability*.

Palavras-chave: Tecnologia da Informação. Governança de TI. *Accountability*. Gerenciamento de Riscos. COBIT®.

ABSTRACT

This descriptive study aims at define criteria which are used to evaluate IT processes considering accountability in risk management within the largest bank financial institutions which operate in Brazil. Analyzing established model criteria, spotting performance measurement procedures in light of GTI and investigating risk management evidences, responsibilities, accounting and transparency within Risk Management Reports were the means used for the definition of criteria. Content Analysis Techniques, Lexical Analysis, Descriptive Statistics and Factorial Maps development supported the results corroboration. Content Analysis allowed the criteria frequency to be identified and together with Lexical Analysis permitted the influences among categorical and lexical variables to be verified. Lexical Analysis provided the establishment of influence relations among concepts (risk, strategy, performance, information technology, security, responsibility, accounting and transparency) and categories (evaluation patterns). The results demonstrated that there is a meaningful relation among the analyzed criteria, risk management elements and accountability.

Keywords: Information Technology. IT Governance. Accountability. Risk Management. COBIT®.

LISTA DE QUADROS

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A globalização da economia, o fluxo de capital, a remoção de barreiras comerciais e o desaparecimento do papel público versus privado em algumas iniciativas aumentaram o impacto de fracassos para além das fronteiras empresariais. Desencadearam a necessidade de gerenciamento dos riscos associados à tecnologia da informação (TI) (PINTO, 2008; MARTIN e HALACHMI, 2012). Esforços são necessários para que as organizações se mantenham competitivas. Pressões exercidas pela economia global requerem que sistemas de informações sejam implantados (ITGI, 2006).

O surgimento de casos de fraudes com implicações de abrangência internacional tem provocado um processo de melhoria nas normas e práticas organizacionais, bem como o estabelecimento de padrões de comportamento por órgãos reguladores (APREDA, 2011) e de governança corporativa, diminuindo os conflitos da teoria de agência. O problema de agência impulsionou a evolução da governança corporativa, segregando propriedade e gerenciamento. A legislação societária limita-se às relações básicas entre proprietários e gestores, não compreendendo garantias para o sucesso do negócio (DUBE, 2011), almejadas pela governança corporativa.

Também os casos de falências afetam amplas regiões geográficas e casos de divulgação de irregularidades financeiras afetam muitos negócios em diversos países. Riscos associados à tecnologia da informação apresentam-se como ameaças iminentes ao desempenho dos objetivos organizacionais, pois os processos tecnológicos é que sustentam os processos empresariais (DUBE, 2011).

Crises em países desenvolvidos ameaçam os sistemas financeiros globais. Ações governamentais com o intuito de regular o setor bancário quanto a transparência são imprescindíveis. Há relações entre a redução da flexibilização de regras de supervisão e estados de estabilidade nos mercados financeiros (MENDONÇA, GALVÃO e LOURDES, 2011). Sugere-se que vulnerabilidades do setor financeiro podem ser minimizadas com ações dos órgãos reguladores.

Situações de má conduta corporativa acontecidas nas últimas décadas têm prejudicado o crescimento, a geração de valor e a reputação de empresas. Costa (2011) identifica as principais condutas que afetam a credibilidade e o desempenho de instituições financeiras: simulação de operações lucrativas; desvio de recursos e

evasão de divisas; lavagem de dinheiro; emissão irregular de debêntures; uso indevido de recursos; fraudes contábeis e conluio com terceiros. Essas situações ameaçam a sobrevivência dos negócios e expõem as instituições a riscos, que podem ser evitados com a adoção de padrões de comportamento empresarial voltado para práticas mais confiáveis. Os sistemas de tecnologia da informação são apontados por Bart e Turel (2010) como necessários às organizações por auxiliarem a reduzir os riscos de perdas, erros, fraudes ou não conformidades.

Riscos estão relacionados à probabilidade futura de resultados insatisfatórios (BARKI, RIVARD e TALBOT, 2001). Tem-se no conceito três componentes: o evento negativo, a chance de ocorrência e o tempo futuro. O primeiro componente expressa a possibilidade iminente da ocorrência de circunstâncias diversas às esperadas para o alcance do desempenho almejado. Circunstâncias estas que independem da percepção dos responsáveis, pois os riscos podem existir sem seu conhecimento. Além disso, sua identificação não elimina a probabilidade de ocorrência (segundo componente). O tempo futuro (terceiro componente) dá ao risco a qualidade de potencialidade, já que o risco é uma possibilidade por definição. Ao ocorrer o evento provável deixa de ser risco, tornando-se um fato (SILVA, 2011).

Riscos relacionados a fraudes, perdas, má conduta, erros, reputação, desempenho inadequado, falências, interesses divergentes entre principal e agente, imagem, desvios de recursos e não conformidade, dentre outros, podem ser acompanhados, controlados, reduzidos ou mitigados utilizando-se recursos da TI. Sistemas de TI são utilizados no gerenciamento das ameaças que os riscos apresentam aos negócios, possibilitando a prevenção de indesejáveis eventos futuros ou a reparação de danos ao patrimônio provocados pela efetivação da predição do risco.

Tecnologia da informação auxilia o gerenciamento das questões de negócios, incluindo planejamento, estratégia, recursos, investimentos, decisões, métodos, estruturas e formas de avaliação (SIDOROVA et al., 2008). Algumas organizações dependem substancialmente dos processos de TI, dentre elas estão as instituições financeiras bancárias. Nelas, os processos de TI são necessários para a operacionalização de suas atividades nos níveis estratégico, tático e operacional. Impulsionadas pela necessidade de integração de sistemas e processos de TI para disponibilizar com agilidade e comodidade volumes necessários de produtos e serviços financeiros aos usuários de serviços bancários, as instituições financeiras

intensificaram nos últimos anos o uso da TI como diferenciação competitiva (PIRES, 2011).

A dependência das empresas aos sistemas de informação traz proporcionalmente vulnerabilidades e exposição a novos riscos. Garantias de segurança da informação são desafios para a gestão. Leis e regulamentos acerca de conformidade e responsabilização auxiliam no gerenciamento dos processos de TI e confiam maior grau de proteção às informações (ITGI, 2006; PEREIRA e SILVA, 2012). Responsabilização, prestação de contas e transparência são conceitos que possibilitam eficiência e segurança aos processos de TI e às informações disponíveis para a manutenção do negócio.

Responsabilização dos envolvidos, transparência e a prestação de contas das ações executadas ou decisões tomadas no âmbito dos processos de TI fazem parte dos conceitos relacionados à *accountability*. Esta se traduz como o reconhecimento da responsabilização e atitudes transparentes sobre as ações, tomadas de decisões, definição de políticas e desenvolvimento de serviços e produto. Envolve todos os aspectos que impactam sobre a performance organizacional (ACCOUNTABILITY, 2008).

Proteger informações e responsabilizar os principais gestores são exigências inegociáveis no âmbito empresarial. Atribuem-se aos líderes o estabelecimento e reforço de níveis adequados de segurança, pois possuem autoridade, *accountability* e recursos para agir e garantir conformidade (WESTBY e ALLEN, 2007). Segurança de dados e integridade das informações são preocupações constantes para a gestão organizacional. O'Connor e Martinsons (2006) atribuem à governança de tecnologia da informação (GTI) as soluções técnicas para a mitigação dos riscos.

Câmaras de comércio, instituições, bancos centrais e bolsas de valores do mundo todo têm sido mais ativos nos domínios da governança de tecnologia da informação. Buscam a mitigação de riscos contra a reputação, o aumento da capacidade de operação e a continuidade do empreendimento (APREDA, 2011).

A abordagem de Weill e Ross (2005) apresenta relações entre o modelo de governança de tecnologia da informação, o processo de tomada de decisão e as escolhas estratégicas. Vasarhelyi e Alles (2008) afirmam que informações precisas e oportunas são essências nos negócios, exigindo um sistema capaz de produzi-las e integridade dos controles que gerenciam esse sistema. A finalidade da governança da tecnologia da informação é apresentada como harmonização entre as estratégias

e as necessidades de informações geradas para tomadas de decisões estratégicas.

Garantir a utilização eficaz da tecnologia da informação é o intuído da governança de TI. Acrescenta-se também a necessidade do alinhamento estratégico, gerenciamento de riscos, geração de valor e medição de desempenho (WILKIN e CHENHALL, 2010). Analogamente, a governança corporativa abrange as relações entre a gestão e o gestor, entre proprietários e interessados. Fornece estrutura para a definição dos objetivos gerais, descreve o método pelo qual os objetivos serão atingidos e a maneira pela qual o desempenho será monitorado (ITGI, 2006).

O uso em escala de sistemas de informação, a necessidade de alinhamento entre o papel da tecnologia da informação e o planejamento estratégico, e as mudanças nos processos empresariais e no ambiente tecnológico da informação, desencadearam urgência na adoção de modelos de governança de tecnologia da informação (KNORST, 2010). Além da adoção de modelos é imperativa sua constante revisão e evolução. Neste trabalho analisa-se o modelo COBIT®, direcionando-se para definição de critérios para avaliação.

O COBIT® é um modelo de governança de TI que envolve as áreas focais da governança: alinhamento estratégico, entrega de valor, gestão de recursos, gestão de risco e mensuração de desempenho (ITGI, 2007). O presente trabalho observa também os conceitos relacionados à *accountability*. Assegurar o alinhamento das estratégias voltadas a TI com os objetivos do negócio, promover o uso adequado e responsável dos recursos de TI com vistas à maximização dos benefícios produzidos, gerenciar os riscos (diminuindo, mitigando ou externalizando) compõe a abrangência do COBIT® (BUTLER e BUTLER, 2010), além dos enfoques de responsabilização, prestação de contas e transparência, compreendidas neste trabalho.

O modelo COBIT® compreende os processos das funções de TI e estabelece controles, proporcionando relação entre os requisitos de governança de TI, processos de TI e controles de TI (ITGI, 2007).

1.1 PROBLEMA DA PESQUISA

Sendo os processos de TI responsáveis pela geração de informações, que são elementos essenciais para as operações empresariais, aliadas aos riscos que

estão sujeitas, à diversidade de sistemas tecnológicos utilizados e aos diferentes níveis de utilização desses sistemas, evidenciou-se o seguinte problema: Como definir critérios para avaliação de processos de TI considerando *accountability* no gerenciamento de riscos nas maiores instituições financeiras bancárias com operação no Brasil?

1.2 OBJETIVOS

Os objetivos estão segregados em geral e específicos. O objetivo geral está relacionado com a pretensão do resultado da pesquisa. Já os objetivos específicos possuem caráter mais instrumental, específico, atendendo a questões ou fases da pesquisa.

1.2.1 Objetivo Geral

O objetivo geral da pesquisa é definir critérios para avaliação de processos de TI considerando *accountability* no gerenciamento de riscos nas maiores instituições financeiras bancárias com operação no Brasil.

1.2.2 Objetivos Específicos

- Avaliar os critérios para avaliação de processos de TI no modelo COBIT® relacionados ao gerenciamento de riscos e conceitos da *accountability*.
- Identificar formas de mensuração do desempenho quanto ao gerenciamento de riscos à luz da governança de TI.
- Apresentar evidências da gestão de riscos, responsabilização, prestação de contas e transparência a partir da Análise Lexical e Análise de Conteúdo dos Relatórios de Gerenciamento de Riscos de instituições financeiras.

1.3 DELIMITAÇÃO DO TEMA

Inicialmente a pesquisa investiga os riscos de TI à luz da governança de TI

utilizando-se de critérios do modelo COBIT® acrescidos os conceitos relacionados à *accountability*. Em um segundo momento definem-se os critérios para avaliação do gerenciamento de riscos dos processos de TI, observando-se os conceitos de responsabilização, prestação de contas e transparência. Não se constituem alvos da pesquisa: a análise dos diferentes modelos de governança de tecnologia da informação; a verificação de adequação dos procedimentos utilizados; ou mensuração de níveis de maturidade dos processos de TI.

Utilizando-se do método de pesquisa *survey*, o estudo define critérios para avaliação de processos de TI considerando accountability no gerenciamento de riscos nas maiores instituições financeiras bancárias que desenvolvem atividades no Brasil. As instituições financeiras pesquisadas compõem-se dos maiores conglomerados ou instituições independentes com operação no Brasil no terceiro trimestre do ano de 2012. Todas possuem cadastro regular junto ao Banco Central do Brasil (BACEN), divulgaram Relatórios de Gerenciamento de Riscos referentes à Setembro de 2012 e constam nos relatórios do BACEN emitidos à mesma época. Foram descartas as organizações não financeiras.

1.4 JUSTIFICATIVA E RELEVÂNCIA DO ESTUDO

Informações precisas, tempestivas e em volumes cada vez maiores estão sendo demandadas pelas organizações. Essa necessidade ampliou a utilização de recursos tecnológicos gerando significativa dependência aos recursos de TI. Facilidade no acesso e disponibilização contínua de informações são características reais buscadas na TI, assim como segurança, qualidade (tanto em nível de conteúdo como de suporte), conformidade e consistência (TAROUCO e GRAEML, 2011).

Investimentos em recursos de TI desencadearam investimentos em gerenciamento de riscos. Maior volume de dados requer maior nível de proteção (PELANDA, 2006). Há certa proporcionalidade entre o aumento da necessidade de investimentos em segurança da informação (mitigação de riscos) e o crescimento da dependência técnica e operacional das empresas quanto aos processos de TI (FLORES et al., 2011).

Gastos com segurança e riscos com falha na segurança (roubo de dados, fraudes e perda de informações de clientes, por exemplo) têm aumentado proporcionalmente. A presença de ativos intangíveis nas organizações demanda

recursos e atenção. Empresas que não fornecem proteção adequada a suas informações essenciais estão se tornando mais visíveis e menos aceitáveis no mercado (ITGI, 2006). Além dos gastos aplicados aos sistemas de tecnologia da informação, o mau funcionamento desses sistemas provocam expressivas perdas financeiras (BART e TUREL, 2010).

É crescente o número de incidentes de segurança observados nos últimos anos. Esses incidentes acompanham o aumento na utilização das ferramentas da internet (KNORST, 2010). Entre 1999 e 2012 o número de incidentes no Brasil aumentou substancialmente. Em 1999 foram notificados 3.107 casos de incidentes e em 2011 o total de casos informados somaram 399.515 (crescimento aproximado de 12.860%). No ano de 2012 o período de janeiro a setembro acumulou 356.946 incidentes relatados. No terceiro trimestre de 2012 houve um aumento de 36% nas notificações em relação ao trimestre anterior e de 54% em comparação com o mesmo período de 2011 (CERT.BR, 2012).

Fraudes financeiras corporativas em empresas americanas foram determinantes para a promulgação da Lei *Sarbanes-Oxley* (2002) nos Estados Unidos. A partir dela o conceito de governança corporativa tornou-se amplamente discutido. Os processos de TI foram readequados com a finalidade de criar mecanismos confiáveis de auditoria e de segurança. A lei americana estabelece transparência nos relatórios financeiros das empresas, mitigação de riscos, procedimento para impedir a ocorrência de fraudes e responsabilização (PELANDA, 2006; MORRIS, GRIPPO e BARSKY, 2012).

Controlar o fluxo de informações e proteger as ameaças de riscos empresariais são necessidades que requerem o surgimento de práticas recomendadas, expressas em contratos e regulamentos (TAROUCO e GRAEML, 2011). Constata-se o desenvolvimento de normas de segurança da informação e sistemas de segurança, como ABNT NBR ISO/IEC 27001 (ABNT, 2006) e ISO/IEC 27002 (2005) e de modelos de governança de TI, como COBIT® (ITGI, 2006).

Projetos de pesquisas desenvolvidos no meio acadêmico estão direcionados à análise e à gestão de riscos no contexto da GTI. Buscam, por exemplo, identificar as vulnerabilidades no âmbito organizacional, avaliando os impactos e as probabilidades de ocorrência de riscos; criar mecanismos de avaliação dos controles de segurança dos sistemas organizacionais; determinar mecanismos de

identificação, avaliação e monitoramento dos riscos; revisar e criar modelos que possibilitem a avaliação de riscos e da segurança da informação.

Ao serem combinados os conceitos pautados na *accountability* (responsabilização, prestação de contas e transparência) e os critérios dos processos de TI do modelo COBIT®, ampliam o enfoque tradicional e permitem a definição de critérios para avaliação de processos de TI para o gerenciamento de riscos.

O presente trabalho é original ao ambicionar investigar e propor definição de critérios para avaliação de processos de TI, com o intuito de gerar conhecimento interdisciplinar, envolvendo governança de TI, *accountability* e gerenciamento de riscos. Os três focos tem sido discutidos pela comunidade acadêmica nos últimos anos, porém se desconhece seu estudo simultâneo.

Salienta-se que este trabalho contempla os critérios para avaliação dos processos de TI do COBIT® (ITGI, 2006), segurança, qualidade, conformidade e consistência (TAROUCO e GRAEML, 2011), perdas financeiras, solidez e integridade de informações (BART e TUREL, 2010), falhas na segurança e fraudes (ITGI, 2006; SPEARS e BARKI, 2010), transparência, mitigação de riscos e fraudes (SARBANES-OXLEY, 2002), no atendimento aos princípios da governança de Ti.

1.5 ESTRUTURA DO TRABALHO

A estrutura do presente trabalho apresenta seis capítulos. No primeiro destacam-se a contextualização do tema, a apresentação do problema da pesquisa e seus objetivos (geral e específicos), a delimitação do tema e a evidenciação da relevância do estudo.

No Capítulo 2 encontra-se revisão de literatura sobre gerenciamento de riscos, compreendendo: conceituação, caracterização, finalidade e abrangência da tecnologia da informação. Destaca-se a necessidade de integração da TI aos objetivos organizacionais, suas vantagens e o uso de processos de TI na mitigação de riscos. Relacionam-se conceitos de segurança e riscos no processo de gerenciamento de riscos. Apresentam-se e discutem-se os conceitos frequentemente citados na produção técnica e acadêmica acerca da *accountability* (responsabilidade, responsabilização, prestação de contas e transparência).

Governança de TI é tratada no âmbito de sua conceituação e de seus

objetivos (criação de valor para empresa, moderação de riscos, garantia da conformidade legal e jurídica, identificação de responsáveis, gerenciamento de recursos, monitoração de desempenho e alinhamento estratégico). *Framework* teórico das relações entre informação, TI e governança de TI está apresentado na Figura 1. Interações entre estrutura organizacional, áreas foco da GTI e *accountability* estão ilustradas na Figura 3.

Sendo nesta pesquisa o COBIT® o modelo escolhido para fornecer os critérios para avaliação de riscos de processos de TI, apresentam-se suas melhores práticas e seus processos de TI (34 critérios), divididos em quatro domínios (planejamento e organização; aquisição e implementação; entrega e suporte; e monitoramento).

Ao final do Capítulo 2 evidencia-se quadro resumo (Quadro 2) com os principais conceitos utilizados nesta pesquisa (risco, estratégia, desempenho, tecnologia da informação, segurança, responsabilidade, transparência e prestação de contas) à luz da gestão de riscos, GTI, COBIT® e *accountability*. Estes conceitos foram utilizados como norteadores na revisão dos critérios para avaliação de processos de TI de modelo de GTI.

Os procedimentos metodológicos usados no estudo estão apresentados no Capítulo 3. Nele os instrumentos de coleta (critérios da amostra e fonte de dados) e os instrumentos de análise dos dados (Estatística Descritiva, Análise de Conteúdo, Análise Lexical, teste Qui-Quadrado e Mapas Fatoriais) são apresentados. Neste mesmo capítulo expõem-se as etapas da presente pesquisa.

No Capítulo 4 encontram-se a análise dos resultados. Contempla a caracterização do setor bancário brasileiro, o perfil da amostra estudada, a análise de critérios para avaliação de processos de TI considerando *accountability* no gerenciamento de riscos, e a análise dos Relatórios de Gerenciamento de Riscos. Finaliza-se o presente trabalho com a Conclusão (Capítulo 5), onde são expostos os principais resultados obtidos com a pesquisa, as contribuições do estudo, suas limitações e recomendações para trabalhos futuros.

2 REVISÃO DE LITERATURA

Neste capítulo desenvolve-se a revisão de literatura acerca dos seguintes conteúdos: governança de tecnologia da informação, *accountability,* gerenciamento de riscos e o modelo COBIT® de GTI.

2.1 GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO (GTI)

Governança de TI responde pela coordenação das estruturas da organização e de seus processos de TI no alcance da estratégia, dos objetivos e das metas definidas (ITGI, 2008a, p. 12). Implantar a estratégia e manter as operações empresariais proporcionando melhores condições de competição no momento atual e no futuro são funções atribuídas a TI. Para Chun (2005), GTI consiste em estabelecer direitos e poderes de decisão e na apresentação de responsabilidades quanto à utilização adequada dos recursos de TI.

Historicamente a tecnologia da informação está orientada para o ambiente organizacional interno e focada no presente. Já a governança de tecnologia da informação direciona-se ao futuro do negócio, alinhada os objetivos estratégicos de TI e à estratégia organizacional (MENEZES, 2005). Apesar da aproximação dos conceitos de gerenciamento de tecnologia da informação e governança de tecnologia da informação, há clara distinção. Enquanto que a gestão de TI é responsável pelo fornecimento e gestão de eficazes serviços e produtos de TI, a GTI centra-se na utilização e transformação dos recursos de TI para atender às demandas do negócio e dos clientes da empresa (GHEORGHE, 2010). As ações da GTI são influenciadas pelas perspectivas do negócio, pela infraestrutura de pessoas e de operações (TAROUCO e GRAEML, 2011).

Assegurar a proteção dos ativos de informação é um dos objetivos centrais da governança de TI (CALDER e WATKINS, 2008). Tendo a segurança da informação ligação estreita com a governança de TI, os investimentos em TI geram benefícios para a segurança da informação de forma imediata ou futura. O montante dos investimentos nem sempre correspondem aos benefícios imediatos, tornando difíceis as decisões de investimentos pelos gestores (FLORES et al., 2011).

A GTI não deve ser considerada de maneira isolada, porque está ligada com outros ativos da empresa, como: ativos financeiros, humanos, propriedade

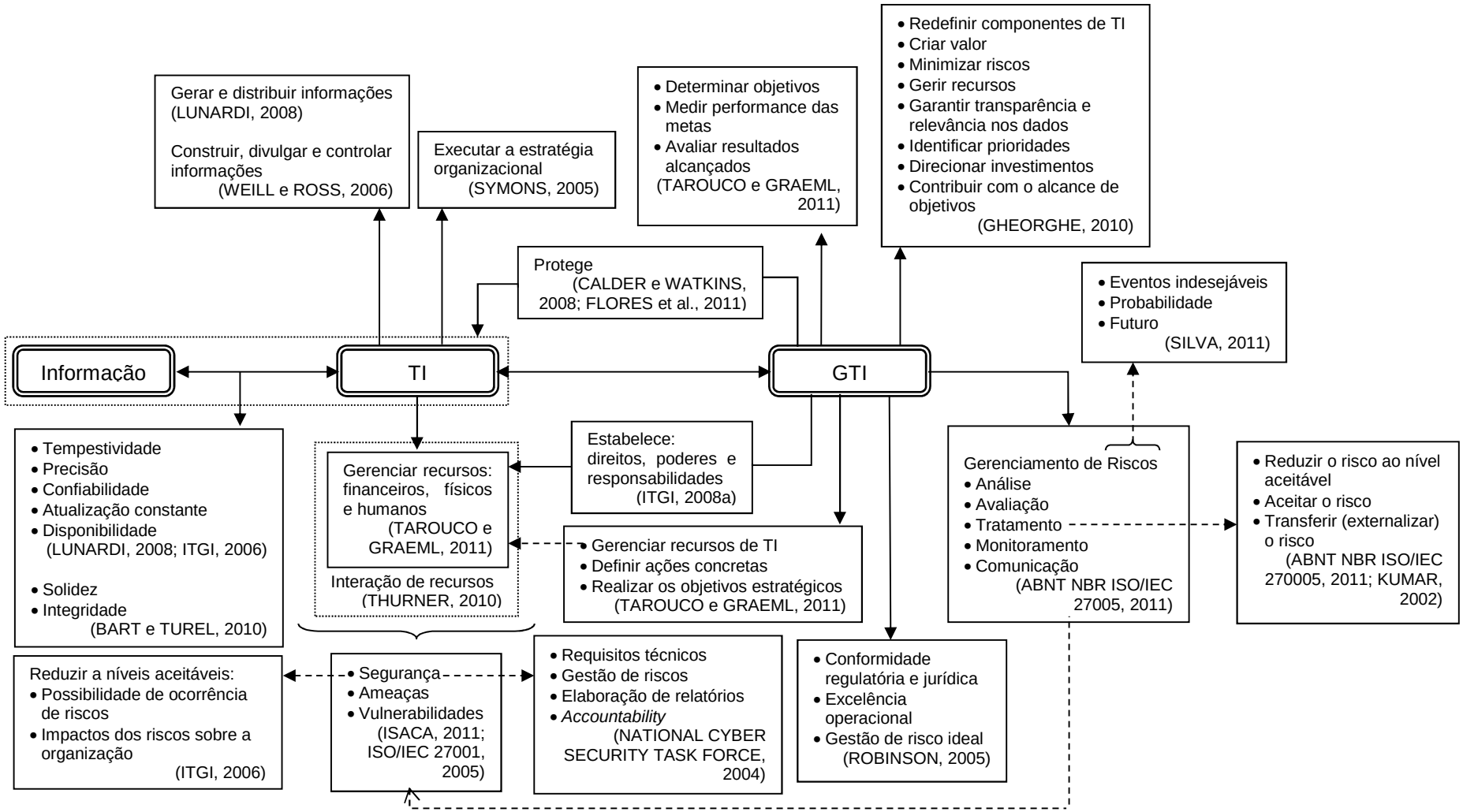
intelectual, dentre outros. Desta forma, compartilhando mecanismos de gestão e processos empresariais, a GTI deve coordenar os processos de forma ampla, para a tomada de decisão empresarial (GHEORGHE, 2010).

Da mesma maneira que a governança corporativa tem como um dos seus focos gerenciar as operações das empresas da forma mais eficaz; de acordo com as expectativas dos acionistas, a prudência financeira, reputação, vantagem competitiva e gestão de riscos; a governança de tecnologia da informação procura atingir resultados semelhantes (WILKIN e CHENHALL, 2010).

Novas quotas de mercado, criação de vantagem competitiva e adaptação para desafios em novos ambientes empresariais, são abordagens da GTI sob a perspectiva estratégica (HARISON e BOONSTRA, 2009). A necessidade de gerir as ferramentas de TI para atingir as estratégias organizacionais, impulsionou o surgimento da governança de TI (BUTLER e BUTLER, 2010). A interação entre os recursos de TI e os objetivos estratégicos exige da GTI assegurar as estratégias e políticas organizacionais, bem como os benefícios, custos e serviços de segurança sejam compreendidos (ITGI, 2006).

Na Figura 1 podem ser observadas as relações conceituais entre informação, tecnologia da informação e governança de TI. Destacam-se a necessidade do atendimento aos objetivos estratégicos e a interdependência entre os recursos de TI, a necessidade de segurança e mitigação de riscos e o próprio gerenciamento dos riscos. Os relacionamentos entre os principais conceitos e a abrangência dos próprios conceitos são expressos na figura. A inter-relação conceitual fica evidente observando-se também os componentes e os termos utilizados nas definições levantadas na revisão da literatura.

Figura 1 – *Framework* teórico das relações entre: informação, tecnologia da informação e governança de tecnologia da informação



Fonte: Elaborada pelo Autor.

Para Tarouco e Graeml (2011) as estratégias organizacionais devem ser o ponto de partida para o desenvolvimento e implantação de estratégias de TI. O alcance da vantagem competitiva depende proporcionalmente ao nível de interação entre elas. A adoção da GTI no cenário de competitividade é ampliada, buscando-se mecanismos que possibilitem o estabelecimento de objetivos, avaliação de resultados e o nível de desempenho de metas estabelecidas.

A governança de TI (ITGI, 2006) tem dois objetivos principais: garantir a criação de valor para o negócio e moderar os riscos associados aos sistemas de informação a partir de investimentos em recursos de TI. Neste sentido, a tecnologia da informação integra as operações de gestão, tornando-se essencial para a manutenção e crescimento da empresa. As principais dificuldades enfrentadas são: alinhar a estratégia de TI com a estratégia e as metas empresariais; fornecer estruturas organizacionais que facilitem a implementação de estratégias e metas; incentivar a adoção e implementação de sistemas de controle de TI; e medir o desempenho. O objetivo da governança de TI dentro de uma organização é para enfrentar esses desafios de forma eficaz e eficiente, a fim de aperfeiçoar a estratégia de negócios.

Conformidade regulatória e jurídica, excelência operacional e gestão de risco ideal são áreas de atuação da GTI. A conformidade legal abrange os atos e declarações da empresa e de seus executivos. Weill e Ross (2005) destaca que empresas com governança de TI geram 20% mais lucros que outras empresas com má governança, mesmo quando estratégias semelhantes são empregadas.

A governança de TI define a estrutura de TI, as medidas de controle interno, o acompanhamento dos processos, a otimização da gestão de riscos e os sistemas de informações globais. Melhorias significativas podem ser alcanças a partir da GTI (VERHOEF, 2007). A boa governança de TI está associada à compreensão dos objetivos de TI (por consequência com objetivos estratégicos da organização) e ao envolvimento de todas as áreas do negócio, tendo como resultado aumento da probabilidade de alcance das metas (BOWEN, CHEUNG e ROHDE, 2007).

Neste sentido, a boa governança tem ação em focos causais de riscos em tecnologia da informação (KUMAR, 2002). Visa o alinhamento estratégico e a criação de valor de negócio, o alcance da missão, visão e objetivos estratégicos (FERNANDES e ABREU, 2008). A boa governança é expressa por princípios que dão origem a códigos de melhores práticas e condutas. Os princípios expressam

direções e envolvem políticas, estratégias e planos. Desenvolve cultura voltada a segurança empresarial. Diversos são os princípios da boa governança. Dentre as principais áreas, tem-se: *accountability*, adequação, conformidade, ética, capacidade de resposta e gestão de riscos (ALLEN, 2005, p. 32).

Accountability estabelece responsabilidades e dá autoridade para agir. Confere aos *stakeholders* com acesso a redes corporativas, necessidade do entendimento das suas responsabilidades quanto à segurança da empresa. A *accountability* é um dos princípios da governança corporativa ligado à identificação de responsabilidades e responsáveis. Envolve a promoção da transparência quanto a informações adequadas para todos os *stakeholders* (IBGC, 2010; BUTLER e BUTLER, 2010).

Adequação envolve políticas, procedimento, processos e controles compatíveis com riscos assumidos. Vincula o volume dos investimentos aos níveis de riscos (probabilidade, frequência e gravidade das possíveis ocorrências). Compara o custo da reconstrução do ativo com o custo de sua proteção (GEER, 2004).

Conformidade garante a conformidade legal e regulamentar com todos os requisitos do negócio e os estabelecidos por agentes externos. Vale-se da auditoria interna e externa como fonte de fiscalização, avaliação e documentação (ALLEN, 2005). Protege o investimento, defende os investidores e garante a segurança dos dados do negócio (LAGZDINS e SLOKA, 2012). Conformidade é um requisito da boa governança corporativa capaz de restabelecer confiança, integridade e responsabilidade nas instituições após períodos de crise (LAGZDINS, 2012).

Ética permite a inexistência de conflitos entre o uso de informações e o comportamento adequado dos *stakeholders*. Relaciona-se à privacidade da informação e preservação dos interesses de todos os envolvidos (ALLEN, 2005). Envolve os princípios de honestidade, integridade, *fairness* e preocupação com o outro (BELLO, 2012, p. 228).

Capacidade de Resposta diz respeito à habilidade dos responsáveis em agir coordenadamente para impedir ou controlar ameaças e vulnerabilidades. A capacidade de resposta abarca o exercício regular de continuidade da empresa, efeitos de eventos indesejáveis, gerenciamento de crises e formulação de planos de gestão de incidentes (ITGI, 2006; ALLEN, 2005).

Gestão de riscos abrange definição, supervisão e monitoramento da eficácia

das estratégias de proteção das informações. Respostas aos riscos potenciais, identificação de possíveis danos, mensuração de custos de perdas, danos, divulgação, falhas no acesso, reconstrução de informações e desenvolvimento de controles, também são ações atribuídas ao gerenciamento de riscos (ALLEN, 2005; MORRIS, GRIPPO e BARSKY, 2012; SPEARS e BARKI, 2010).

A governança de TI é um sistema pela qual o uso atual e futuro da tecnologia da informação são direcionados e controlados. Esse sistema tem o objetivo de avaliar e orientar a utilização da TI no apoio e acompanhamento da organização no alcance dos seus planos, incluindo a estratégia e a política de uso dos recursos de TI. Proporciona entendimento, exige cumprimento das obrigações legais, regimentais e éticas relativas às atividades e responsabilidades dos envolvidos na gestão organizacional (ISO/IEC 38500, 2008). Atribui-se à GTI, cinco áreas foco, representadas na Figura 2.

Figura 2 – Áreas foco de atuação da governança de tecnologia da informação

Fonte: Baseado em ITGI (2008b, p. 6).

Enquanto que o alinhamento estratégico e entrega de valor são resultados da governança de tecnologia da informação, medida de desempenho, gestão de recursos e gestão de riscos são condicionantes da governança de TI (ROSA, 2008). Matitz e Bulgacov (2011) identificaram o desempenho como capacidade de geração

de resultados operacionais mensuráveis a partir de processos internos e da utilização regrada de recursos. É medido através da verificação do grau de realização das metas estabelecidas. Desempenho organizacional está diretamente relacionado ao alcance de resultados em um determinado período. Fernandes, Fleury e Mills (2006) lembram a existência de diferentes áreas de resultados, com distintos interesses e até mesmo conflitantes. Relacionam as áreas de resultado ao número de *stakeholders*.

Diversos autores discorrem sobre as áreas focos da GTI, conforme segue:

a) alinhamento estratégico – esse domínio tem seu início na concepção de uma estratégia de TI de acordo com a estratégia global da organização (GHEORGHE, 2010). A separação entre GTI e os objetivos estratégicos é algo difícil, já que a missão global da empresa está expressa na estratégia (CALLAHAN; BASTOS e KEYES, 2004). Valente (2006) salienta que um dos objetivos da governança de TI é o alinhamento entre as várias áreas de negócio que compõem uma organização. O alinhamento estratégico resulta da integração das estratégias definidas pela organização com recursos de TI e seu adequado uso. Também regula os investimentos em TI de acordo com as estratégias globais (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008);
b) gerenciamento de recursos – os aspectos operacionais da TI e a capacidade de implementação efetiva das políticas de gestão dos recursos ligados a TI são abrangidos pela GTI (ROSS, 2003). Os regulamentos e padrões de gerenciamento dos recursos de TI são definidos pela própria empresa de acordo com sua experiência, exigências particulares ou de acordo com as melhores práticas padronizadas por órgãos relacionados à governança de TI (VERHOEF, 2007). O gerenciamento dos recursos de TI permite a correta aplicação dos investimentos (humanos e equipamentos) para atender as demandas de maneira eficiente e eficaz (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008). Essa dimensão tem como objetivo direcionar o uso dos recursos de TI, supervisionar o financiamento, garantir capacidade suficiente de TI, infraestrutura que suporte os requisitos futuros e atuais do negócio (HARDY, 2003) e o

gerenciamento das interdependências encontradas entre os próprios recursos (THURNER, 2010);

c) gerenciamento de riscos – interrupções, fraudes ou falhas relacionadas a tecnologia da informação apresentam ameaças para os negócios. Assim, o gerenciamento dos riscos está relacionado às operações da TI. A implementação de controles que identificam possíveis futuros problemas ou suas causas e o modo de mitigar esses acontecimentos cabem a GTI (ROSA, 2008). Eventos não previsíveis (característica intrínseca de alguns negócios), incompreensão dos objetivos organizacionais (em qualquer nível), má especificação dos objetivos, falhas em estimativas orçamentárias (custos e tempos), frequentes mudanças tecnológicas, desempenhos insuficientes e baixos níveis de conformidade dos produtos ou serviços, são para Kumar (2002) causas de riscos que envolvem tecnologia da informação. A gestão de riscos assegura a avaliação da ameaça a qual a organização está suscetível no âmbito da TI, identificando o nível do impacto para o negócio (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008). É o processo em que se identificam as vulnerabilidades e as ameaças à estrutura da organização, como também os procedimentos utilizados para minimizar o impacto nos recursos de TI (GHEORGHE, 2010);
d) entrega de valor – as relações entre os investimentos em TI, menor riscos, maior retorno, aumento da vantagem competitividade, oferta de dados úteis e tempestivos, maior qualidade dos serviços e diminuição dos custos são elementos da GTI. Também integra a forma de mensurar os resultados provenientes dos investimentos em TI. Entrega de valor corresponde à maximização dos usos da TI (VAN GREMBERGEN, DE HAES e GULDENTOPS, 2004; GHEORGHE, 2010). Ela confronta os investimentos em TI e a agregação de valor para a organização, mede os benefícios trazidos pelos recursos aplicados (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008). Acompanha o prazo de entrega, os gastos realizados dentro dos parâmetros orçamentários, os benefícios prometidos. Traduz-se em vantagem competitiva, satisfação do cliente, produtividade e rentabilidade (ITGI, 2006);
e) mensuração do desempenho – a GTI possibilita com o estabelecimento de

> indicadores de mensuração do desempenho da TI, demonstrando a performance dos investimentos. O acompanhamento e monitoração da implementação da estratégia organizacional, compreendendo: implantação de projetos, usos de recursos e desempenho de processos (ITGI, 2007). Informações sobre os resultados alcançados de forma oportunas, precisas e relevantes são indispensáveis para a gestão organizacional, bem como a comparação com medidas de desempenho projetadas (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008). A medição do desempenho identifica se os sistemas atingiram as metas definidas (GHEORGHE, 2010).

Autores como Van Grembergen, De Haes e Guldentops (2004), Weil e Ross (2005), Lunardi (2008), Lunardi, Becker e Maçada (2010) analisam, além das áreas focais, a responsabilidade pelas decisões em TI (*accountability*), descrita na Seção 2.2 deste estudo.

Alto grau de desempenho nas áreas focais da GTI, com consequente elevação no retorno do capital investido, é característica da boa governança. A avaliação de cada área foco identifica o nível de gerenciamento dos recursos disponíveis de TI e o potencial de geração de resultados a partir dos mecanismos de gerenciamento da TI (LUNARDI, BECKER e MAÇADA, 2010).

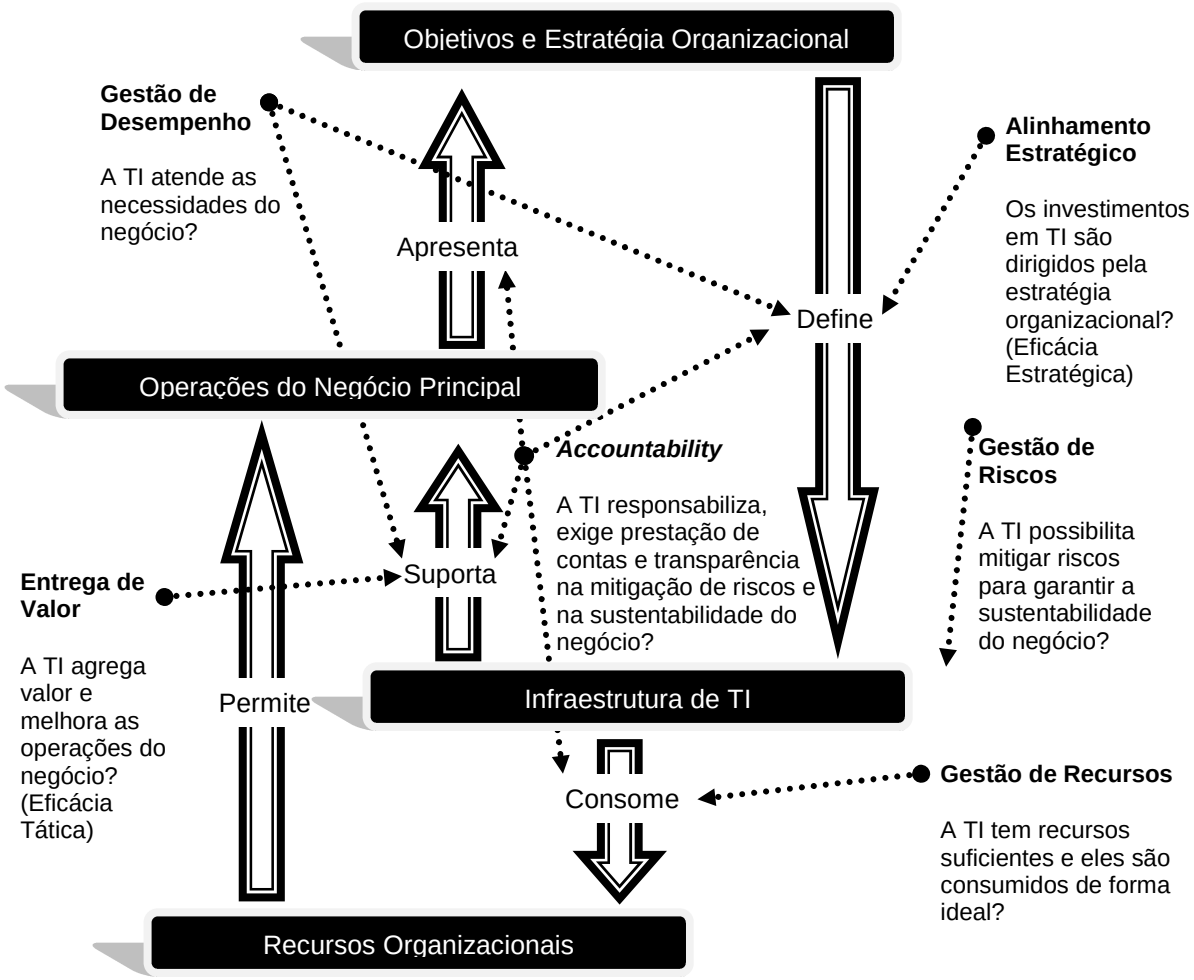
A Implantação de uma estrutura de GTI deve levar em conta fatores relevantes (GHEORGHE, 2010), como: o desenvolvimento tecnológico (as decisões relacionadas a TI devem ser tomadas em tempo hábil, com entendimento de todos os riscos associados a TI), o controle financeiro (grandes projetos de TI necessitam de grandes investimentos, necessitando da identificação do responsável por eventuais desperdícios financeiros); inovação e controle sobre a TI (casos em que a inovação é inerente a TI, podem conflitar com o objetivo de exercer controle sobre o ambiente de TI); e infraestrutura de dados (a obrigação pela manutenção de dados é de todos os departamentos).

Os objetivos principais da governança em tecnologia da informação podem ser resumidos da seguinte forma: garantir o alinhamento da estratégia da tecnologia da informação com a estratégia da empresa; possibilitar que a tecnologia da informação atenda às necessidades do negócio e maximize a entrega de valores;

garantir a utilização racional de todos os recursos disponíveis de TI; e gerenciar os riscos de TI (ROSA, 2008).

Relações entre os elementos da governança de TI e a estrutura organizacional, observados os recursos de TI, podem ser observados na Figura 3.

Figura 3 – Estrutura organizacional, áreas foco da governança de tecnologia da informação e *accountability*



Fonte: Baseado em Butler e Butler (2010, p. 37).

As práticas de GTI associadas aos cinco domínios apresentam-se como fatores expressivos para a tomada de decisão. A realização dos objetivos da GTI atinge o alinhamento dos investimentos em TI com os objetivos do negocio, assegura a utilização responsável dos recursos de TI, dentro dos limites orçamentários, e garante que o desempenho corresponde ao plano estratégico. Seguir os princípios da GTI significa diminuir a possibilidade de riscos de TI, o

permanente controle de ameaças e fraquezas do sistema, a melhora do desempenho organizacional, conformidade e desenvolvimento organizacional (GHEORGHE, 2010). A relação entre as áreas focos da GTI possuem diferentes níveis de gestão e funções. Apesar de que em alguns aspectos a contribuição apresenta-se em nível micro, a GTI precisa estabelecer um nível macro, abrangendo a organização, suas estratégias, seus processos e seus recursos aplicados.

Os objetivos principais da governança em tecnologia da informação podem ser resumidos da seguinte forma:

a) assegurar o alinhamento da estratégia da empresa com a estratégia da TI;
b) possibilitar que a TI atenda às necessidades do negócio e maximize a entrega de valores;
c) garantir a utilização racional de todos os recursos de TI disponíveis;
d) gerenciar os riscos de TI;
e) monitorar o desempenho dos recursos de TI (ROSA, 2008; ITGI, 2008b).

Ao construir a estrutura para a GTI, três elementos são considerados essenciais: estrutura da governança corporativa (quem toma as decisões e quem é o responsável), os processos de governança (como as decisões são tomadas) e a governança da comunicação (monitoramento, medição e comunicação das decisões tomadas e dos resultados atingidos). Na estrutura da governança corporativa são definidos os papéis, as funções e as responsabilidades sobre os investimentos nos processos de TI, bem como a hierarquia dos cargos. Os processos de governança incluem todos os processos aplicados nas tomadas de decisão, de acordo com a estrutura definida. A comunicação das informações sobre os resultados é base para a manutenção, avaliação e adaptação dos processos e da estrutura de GTI (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008; LARSEN, PEDERSON e ANDERSON, 2006; BUTLER e BUTLER, 2010).

Recentemente, ao analisar-se o desempenho das áreas foco, outros conceitos estão sendo incorporados à GTI. Responsabilização, transparência e prestação e contas são dimensões da *accountability* que fazem parte da abrangência da GTI.

A responsabilidade pode ser entendida como capacidade (competência) ou como direito, enquanto que a prestação de contas significa uma obrigação ou uma

autoridade (*know-how*). Ao responsabilizar as ações e decisões adotadas pelos envolvidos nos processos de TI, exigindo-se a prestação de contas sobre os resultados alcançados para o sucesso da atividade chave, o COBIT® incorpora o conceito de *accountability* (FELTUS, PETIT e DUBOIS, 2009).

O COBIT® é uma ferramenta de suporte gerencial usada com o propósito de resolver falhas de controle, técnicas, riscos e de comunicação. Incentiva a adoção de boas práticas de GTI, permitindo atualização e harmonização com outros padrões. Alinha os processos com a estratégia empresarial, demarca as funções de TI, permite a responsabilização por processos, possui linguagem comum, abrange os requisitos legais e dos órgãos reguladores (ITGI, 2007, p 10). Percebe-se que os critérios do COBIT® não repudiam os conceitos da *accountability*. Pelo contrário, visualiza-se uma ampliação necessária desses critérios clássicos com o enfoque dado pela *accountability*. A responsabilização de todos os envolvidos nos processos de TI compreende as áreas focais da GTI e da governança corporativa, as quais o COBIT® está vinculado (FELTUS, PETIT e DUBOIS, 2009).

2.2 *ACCOUNTABILITY*

Exigências de sustentabilidade (maximização dos resultados econômicos positivos ou minimização dos impactos sociais e ambientais negativos) por parte dos que detém interesses sobre o negócio têm provocado esforços para ações organizacionais responsáveis. Como resposta, as empresas buscam atuar com maior transparência e responsabilidade estabelecendo por consequência eficientes formas de prestação de contas (LANDRUM e DAILY, 2012; PEREIRA e SILVA, 2012). Maior responsabilização nas ações corporativas estão proporcionalmente relacionadas com melhores desempenhos, salvo casos em que a falta de recursos ou a complexidade da atividade afetam negativamente a performance (KING, DAVIS e MINTCHIK, 2012).

Responsabilidade por transparência nas decisões, equidade no tratamento, democracia nas tomadas de decisões, eficiência dos processos e integridade das informações são tomados como sinônimos de *accountability* (ABDULLAHI, ENYINNA e STELLA, 2012). Responsabilidade vincula-se a um objeto, tornando o sujeito ativo responsável pelas ações em que envolvam o objeto e o coloca sob a ameaça de sanções. Prestação de contas descreve a estrutura necessária para que

a responsabilidade ocorra. A relação entre responsabilidade e prestação de contas se dá sobre as causas das ações e eventos que interferem nas decisões sobre o objeto. Enquanto a responsabilidade tem o intuito de identificar o responsável, a prestação de contas exige deste a divulgação das informações atinentes (FELTUS, PETIT e DUBOIS, 2009).

Há estreita correlação entre *accountability* e transparência (*disclosure*) (ABDULLAHI, ENYINNA e STELLA, 2012). A transparência é condição necessária para a responsabilização, embora não seja seu determinante. O pressuposto de que transparência gera responsabilidade pode ser questionado, uma vez em que os dois termos não são definidos precisamente e são utilizados para significar perspectivas distintas (FOX, 2007; LANDRUM e DAILY, 2012).

Responsabilidade tem duas dimensões:

a) capacidade (para realizar ações ou tomar decisões) ou direito de exigir respostas;
b) capacidade de impor sanções.

A primeira está voltada para a execução e a segunda para o controle. A *accountability* compreende os dois enfoques (FOX, 2007). Responsabilização concentra-se nas relações de agência, no desempenho administrativo e nas relações profissionais. A má conduta tem relação direta com o nível de disponibilização de informações (*disclosure*) sobre as ações ou decisões. Havendo falta de transparência, a tendência é que haja menor responsabilidade (ABDULLAHI, ENYINNA e STELLA, 2012).

A *accountability* incita o comprometimento das pessoas na realização de suas funções organizacionais, evidencia responsabilidades e exige prestação de contas no que se referem a prazos, custos e resultados (LUNARDI, BECKER e MAÇADA, 2010). Weill e Ross (2005) pautam os direitos decisórios e as responsabilidades no tocante a GTI. A boa GTI define as incumbências e as responsabilidades por decisões sobre tecnologia da informação (VAN GREMBERGEN, DE HAES e GULDENTOPS, 2004). Definir, comunicar e fazer compreender papéis e responsabilidades são tarefas da organização (ITGI, 2006). Todas as atividades que demandam recursos de TI necessitam da identificação de pessoas responsáveis pela utilização dos recursos, pela execução da atividade pela prestação de contas. A

GTI assegura a execução, a adequada utilização de recursos e a responsabilização. Define, informa e aplica sansões na ocorrência de não conformidades (MAIZLISH e HANDLER, 2005).

São princípios da *accountability*: a inclusão, a relevância e a capacidade de resposta (ACCOUNTABILITY, 2008, p. 9). A inclusão refere-se ao estabelecimento de estratégias de TI abrangentes, capazes de gerar informações que atendam às necessidades de todo o grupo de interessados na organização. A relevância abrange a definição de objetivos e determinação de padrões de gerenciamento e avaliação das estratégias de TI e do próprio desempenho dos recursos de TI. Responsabilização dos envolvidos nos processos também faz parte do princípio da relevância. As estratégias, os objetivos e os padrões voltados para o gerenciamento e para o desempenho devem ser comunicados ao grupo. As informações devem auxiliar as decisões e as ações às quais as pessoas do grupo são responsáveis. A capacidade de resposta da *accountability* diz respeito ao suprimento de necessidades ligadas à informação.

Duas condições são necessárias para que os impactos da *accountability* sejam positivos: os sujeitos devem agir de acordo com os interesses ao quais representa (responsabilização) e devem justificar suas decisões (prestação de contas) (KING, DAVIS e MINTCHIK, 2012). Para a governança corporativa a *accountability* não se limita a simples responsabilidade (senso moral). Abarca a legitimidade que a organização tem em atribuir, ao grupo ou pessoas do grupo interessados, responsabilização por ações (decisões) ou elementos regulatórios (políticas ou estratégias), frente ao desempenho almejado (ACCOUNTABILITY, 2008; BUTLER e BUTLER, 2010).

Autores como Ezzine e Olivero (2013), Hall (2012), Comite (2012), Raban (2012), Sorensen (2012) e Lawrence e Nezhad (2009) utilizam responsabilidade, responsabilização, prestação de contas e transparência ao mencionarem o termo *accountability*. Ezzine e Olivero (2013) constatam convergência dos termos responsabilidade e transparência em estudos comparativos de códigos de governança corporativa. Hall (2012) relaciona responsabilidade, prestação de contas e transparência ao analisar a administração pública norte americana em tempos de crise. Comite (2012) evidencia a responsabilidade, a responsabilização e a transparência nas ações da administração pública italiana. A responsabilidade abrange a obrigação do adequado uso de recursos, enquanto que responsabilização

acrescenta o dever de atingir e relatar o nível de desempenho alcançado. Raban (2012) elenca responsabilização, prestação de contas e transparência ao estudar modelo de privacidade e proteção no processamento de dados. Para Sorensen (2012) a prestação de contas e a responsabilização são elementos que compõem os processos de inovação pública. Lawrence e Nezhad (2009) mencionam a importância da responsabilização, da prestação de contas e da transparência. A transparência é compreendida como um meio para reforçar a prestação de contas. A responsabilização abrange a veracidade das informações e autoridade em gerir recursos e tomar decisões.

Apesar de que as decisões organizacionais são tomadas em níveis de gestão mais elevados dos negócios, as atividades voltadas a GTI normalmente ultrapassam até mesmo os limites do gerenciamento (DAMIANIDES, 2005). A governança de TI surgiu com a finalidade de descrever a forma como o responsável pela governança conduziria a supervisão, monitoramento, controle e gestão da entidade. Com o passar do tempo, a GTI alcançou papel estratégico e funcional da tecnologia da informação. Questões relacionadas com direitos de decisão e ações táticas ampliaram a sua concepção. A GTI consiste na definição e implementação de processos, estruturas e mecanismos relacionados com a execução de responsabilidades, guiadas e sustentadas pelas estratégias e objetivos organizacionais (ITGI, 2007; VAN GREMBERGEN e DE HAES, 2009). Responsabilidade, prestação de contas e transparência foram incorporadas à GTI.

2.3 GERENCIAMENTO DE RISCOS EM TI

A informação é um recurso crítico utilizado na gestão empresarial. Ela deve possuir dimensões que permitam o acesso a todos os *stakeholders*, respeitando as características da formação do capital da organização. Também deve ser capaz de cumprir sua finalidade ou propósito, satisfazendo as necessidades que demandaram sua evidenciação. A informação é considerada uma ponte entre os dados observados e o conhecimento necessário para a realização dos objetivos organizacionais (ISACA, 2010).

A TI é o principal instrumento de geração e distribuição de informações relacionadas a aspectos operacionais ou financeiros das organizações. Incumbe-se a TI a responsabilidade em dar garantias de precisão, confiabilidade,

tempestividade, atualização constante e disponibilidade às informações que circulam dentro ou entre organizações (LUNARDI, 2008, p. 33). Abrange as formas de investimentos em recursos tecnológicos empregados na geração de valor para o negócio. Esses investimentos englobam, dentre outras aplicações: automatização de processos gerenciais ou produtivos, desenvolvimento de vantagem competitiva, atendimento de normas e regulamentos internos ou externos (WEILL e ROSS, 2006).

Além de sua estreita relação com os controles internos organizacionais e o sucesso dos negócios, a importância da TI foi destacada a partir de obrigações expressas em Lei, como a aprovação da Lei Sarbanes-Oxley SOX (KAARST-BROWN; KELLY, 2005). Garantias em relação à solidez e à integridade das informações e dos controles internos das organizações é o que se espera dos sistemas de tecnologia da informação.

Para executarem suas funções de forma eficaz os conselhos de administração e gestores necessitam de segurança quanto às informações relacionadas ao planejamento estratégico, relatórios financeiros, remuneração de executivos, conformidade legais e regulamentares (BART e TUREL, 2010).

Para os negócios, a TI superou sua função inicial de facilitar a geração de informações, assumindo a responsabilidade de executar a estratégia empresarial (SYMONS, 2005). Centra-se na construção, divulgação e controle de informação necessária para: o registro, controle e gerenciamento das operações (WEILL e ROSS, 2006).

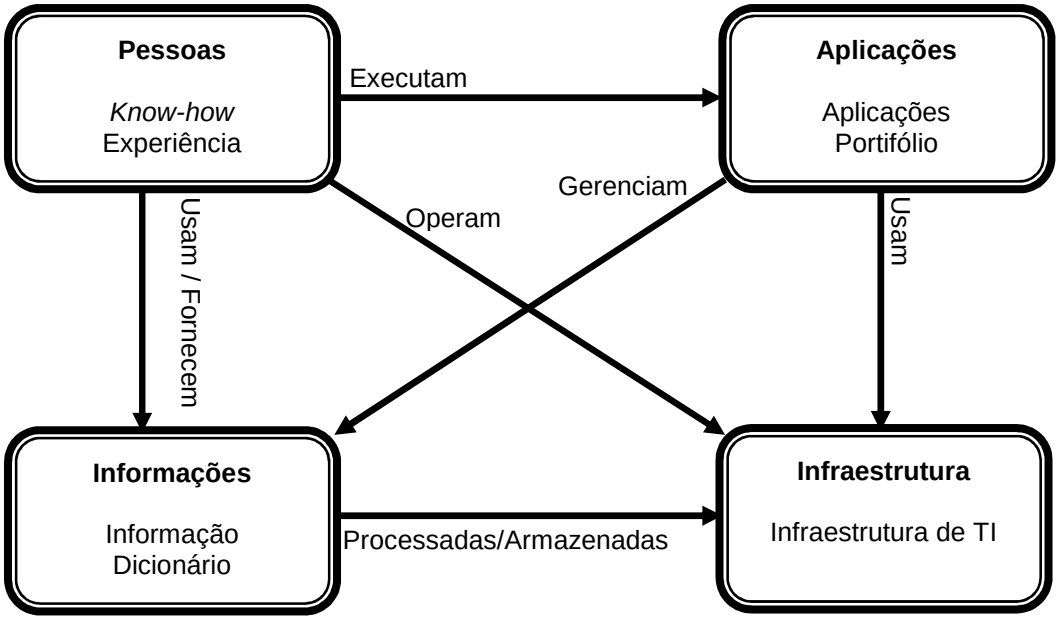
Esse aumento de importância também elevou o nível de dependência das entidades, o que tornou necessário maior atenção voltada aos processos de TI (DE HAES e VAN GREMBERGEN, 2008). Empresas contemporâneas dependem consideravelmente da TI, uma vez que ela fomenta aspectos relevantes do negócio (como a definição de objetivos estratégicos) e funções administrativas (FLORES et al., 2011).

A estratégia organizacional deve ser o ponto de partida para o desenvolvimento e para a implantação de estratégias de TI. O alcance da vantagem competitiva depende proporcionalmente ao nível de interação entre elas. A adoção da GTI em ambientes competitivos torna-se relevante. Ela auxilia na escolha ou no desenvolvimento de mecanismos que possibilitem a determinação de objetivos, a medição da performance quanto as metas estabelecidas e a avaliação de resultados

alcançados. Permite o gerenciamento adequado dos recursos disponíveis na área de TI (financeiros, físicos e humanos) e a definição de ações concretas para a realização dos objetivos estratégicos (TAROUCO e GRAEML, 2011).

Na definição da infraestrutura de TI deve-se considerar o conhecimento dos componentes humanos. Estes são responsáveis pela manutenção de aplicações existentes e o desenvolvimento de novas. As aplicações, além de determinarem uma estrutura mínima de suporte, também são responsáveis por determinados componentes de processamento e armazenamento de informações. Diferentes componentes do sistema utilizam, gerenciam, determinam, influenciam e recebem interferências de outros recursos (THURNER, 2010, p. 13), conforme pode ser observado na Figura 4. Ações desencadeadas pela contínua evolução tecnológica necessitam assegurar a coordenação de todos os recursos de TI.

Figura 4 – Interdependência dos recursos de tecnologia da informação



Fonte: Baseado em Thurner (2010, p. 13).

O desempenho global dos recursos de TI depende do nível de interação entre eles. Ao usar a infraestrutura e executar aplicações as pessoas geram informações, armazenadas na própria infraestrutura de TI. As aplicações gerenciam as informações, permitindo o acesso às pessoas interessadas e autorizadas.

De acordo com os níveis de utilização dos recursos de TI, variam também os

níveis de segurança, ameaças e vulnerabilidades (ISACA, 2011). Com o contínuo desenvolvimento da tecnologia, a TI passa a ser um requisito essencial para o desenvolvimento estratégico e para aumentar o desempenho de qualquer organização. As constantes mudanças tecnológicas exigem tomadas de decisões para os componentes de TI, a partir da compreensão dos riscos e das oportunidades associadas (GHEORGHE, 2010).

Considerando-se a informação um ativo com importância semelhante a qualquer outro ativo considerado essencial aos negócios, é imperativa sua proteção. Esse é o entendimento da norma ISO/IEC 27002 (2005). Atualmente, complexidade na interconectividade entre as empresas (organizadas em cadeias de produção) expõe a informação está a ameaças e vulnerabilidades. Desse modo, a segurança da informação é alcançada com conjunto de controles (estabelecidos, implementados, monitorados, analisados e melhorados continuamente) que incluem: políticas, processos, procedimentos, estruturas organizacionais, softwares e hardwares. Spears e Barki (2010) evidenciam a participação do usuário (componente humano) na eficácia da gestão de riscos de segurança de sistemas. Constatam o papel do usuário no aprimoramento dos controles de segurança e na proteção de informações confidenciais nos processos do negócio.

Novos desafios se apresentam para as organizações: redefinir a estrutura dos componentes de TI com o objetivo de criar valor e minimizar riscos através da gestão eficaz de todos os recursos; integrar todas as ferramentas para garantir a transparência e dados relevantes; identificar as prioridades em projetos de TI; e direcionar investimentos para contribuir com o alcance dos objetivos e a criação de valor (GHEORGHE, 2010).

A segurança da informação não se limita a requisitos técnicos. Constitui-se desafio organizacional, envolve gestão eficiente de riscos, elaboração de relatórios constantes e *accountability*. Demanda o envolvimento de todos interessados na organização e requer avaliação de ameaças e planos de respostas (NATIONAL CYBER SECURITY SUMMIT TASK FORCE, 2004).

Um dos objetivos da segurança da informação é reduzir para um nível aceitável a possibilidade de ocorrência ou os impactos dos riscos sobre a organização (ITGI, 2006, p. 14).

Neste sentido, a segurança da informação oferece proteção contra risco de perdas, descontinuidade operacional, usos indevidos, divulgação não autorizada e

danos, além de identificar civil e legalmente as responsabilidades. Abrangem os processos físicos e eletrônicos, pessoas, tecnologia e as relações entre parceiros, clientes e terceiros. Assegura os quesitos de confidencialidade, disponibilidade e integridade para as informações (ITGI, 2006, p. 14).

Os domínios da segurança da informação absorveram conceitos como utilidade e posse de informações. A posse está relacionada com os riscos de roubo, engano ou de fraude. Confiança e responsabilidade nas transações eletrônicas são exigências da economia mundial. A segurança da informação é alcançada quando: o sistema de informação disponibiliza tempestivamente as informações, resistindo a ataques e demonstrando capacidade de recuperação frente a possíveis ataques (disponibilidade); a informação é acessada somente por usuários autorizados (confidencialidade); há proteção contra modificações nos relatórios disponibilizados (integridade); e quando o trânsito de informações, interno ou externo, está protegido e direcionado aos usuários específicos (autenticação no acesso). Esses requisitos têm diferentes níveis de importância, dependendo do contexto. A integridade, por exemplo, é qualidade crítica para decisões estratégicas (ITGI, 2006, p. 20).

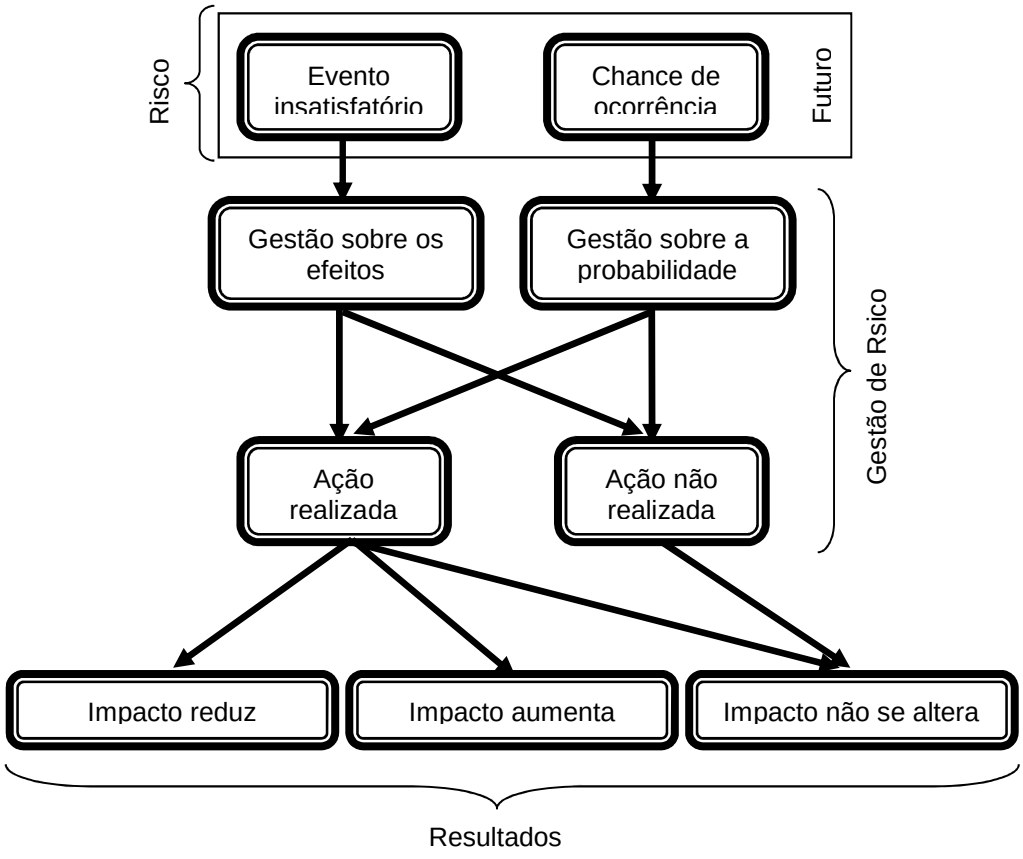
O processo de gerenciamento de riscos da informação envolve as atividades de definição de contexto, análise, avaliação, tratamento e aceitação do risco. É iniciado pela identificação de contexto ou cenário, tendo a presença da comunicação, do monitoramento e da análise crítica de riscos em todo o processo. Análise, avaliação e tratamento do risco são destinados a reduzir os riscos a níveis aceitáveis (ABNT NBR ISO/IEC 27005, 2011). Proteger as informações da organização pressupõe: compreender a importância da própria informação e do seu sistema de segurança; assegurar que os investimentos destinados à segurança concordam com as estratégias (global e de riscos); desenvolver sistema de segurança; e gerar relatórios periódicos de acompanhamento (ITGI, 2006).

A transferência dos riscos para terceiros também se apresenta como uma forma de tratamento de riscos. A transferência de risco para terceiros reduzir o risco para a organização original, porém não diminui a probabilidade de ocorrência de outros riscos. A empresa que externaliza o risco, assume a possibilidade da empresa destinatária não o gerenciar adequadamente. Com o tratamento (redução ou transferência) os riscos residuais são assumidos pela empresa e planos de gerenciamento das consequências (incluindo a identificação de meios de financiamento) são traçados. Controle de risco, entendido como redução da

consequência ou da probabilidade de ocorrência, envolve determinar o benefício relativo de novos controles (grau de eficiência, novos procedimentos e alterações físicas) comparados com a eficácia dos controles existentes (ABNT NBR ISO/IEC 27005, 2011).

Estratégias de gerenciamento de riscos devem ter como escopo: identificar, classificar e estimar a probabilidade dos riscos; avaliar a importância e abrangência dos riscos nas atividades do negócio; e implementar ações destinadas à redução do risco a níveis aceitáveis (KUMAR, 2002). A relação entre os elementos conceituais do risco, o gerenciamento de riscos e os resultados esperados, estão postos na Figura 5.

Figura 5 – Relações entre elementos conceituais do risco e gestão de risco



Fonte: Baseado em Silva (2011, p. 79).

A gestão de riscos concentra-se na possibilidade de ocorrência futura de um evento desfavorável, não incorporando a ocorrência desses eventos, pois a ocorrência os torna fatos. A gestão de riscos é uma atividade complexa, já que seu objeto é uma presunção futura a qual não se tem controle sobre sua efetivação, nem

sobre a eficácia das ações envolvidas. Elementos ambientais e fatores humanos dão às variáveis, maior grau de incerteza e dificultam o planejamento e a implementação de ações que almejam gerar o resultado esperado. Por vezes, aumentam o impacto e a probabilidade de ocorrência do risco (SILVA, 2011).

A atividade de tratamento do risco envolve evidenciar e avaliar opções para o tratamento dos riscos identificados, elaborar planos e implementar o tratamento propriamente dito. Pode-se evitar o risco com a não execução da atividade suscetível a ele. Porém, a atitude de aversão ao risco ou posicionamento sem o domínio de todas as informações disponíveis, podem aumentar a importância de outros riscos, os custos incorridos no tratamento e as falhas nas decisões. Podem provocar escolhas que representam menor risco potencial sem levar em conta os benefícios correlacionados (ABNT NBR ISO/IEC 27005, 2011).

A dependência das empresas contemporâneas a TI é potencialmente equivalente ao crescimento das ameaças aos seus ativos de informação. Com isso, as empresas são obrigadas a realizar investimentos em segurança da informação destinados a mitigar ameaças, ao gerenciamento de incidentes e a evitar consequências negativas aos objetivos do negócio (FLORES et al., 2011). O tipo de tecnologia adotada, o desempenho dessa tecnologia, sua harmonização com os objetivos estratégicos, a definição de políticas e responsabilidades são questões que interferem em maior ou menor escala o desempenho organizacional. Hardy (2006) salienta que o potencial efeito negativo ligado a consideráveis prejuízos financeiros ou expressiva perda de credibilidade (reputação e imagem), pode ser desencadeado por eventos simples de quebra de segurança, erro operacional ou ataque de vírus.

Gerenciamento de riscos, responsabilização, transparência e prestação de contas são termos utilizados simultaneamente ao se tratar de processos de TI. Gerenciamento de riscos de TI envolve segurança das informações, gestão de recursos, mitigação de ameaças e vulnerabilidades. Envolve também a responsabilização, a transparência e a prestação de conta por ações e decisões tomadas. Esses conceitos estão relacionados à *accountability*.

2.4 *CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY* (COBIT®)

Existem diversos modelos de GTI, não havendo padrão único, porém, todos

utilizam as melhores práticas (GHEORGHE, 2010). Dentre eles há o COBIT®, um modelo de governança de tecnologia da informação mantido pela *Information Systems Audit and Control Association*. Permite que as deficiências relativas aos quesitos: de controle, técnicos, riscos de negócio e comunicação sejam supridas. Assegura que a área de TI esteja alinhada com os objetivos do negócio, suportando assim, a GTI. São objetivos do COBIT®: habilitar a área de TI para a maximização dos resultados; garantir o adequado uso dos recursos de TI; e gerenciar os riscos de TI de forma apropriada (ITGI, 2008a).

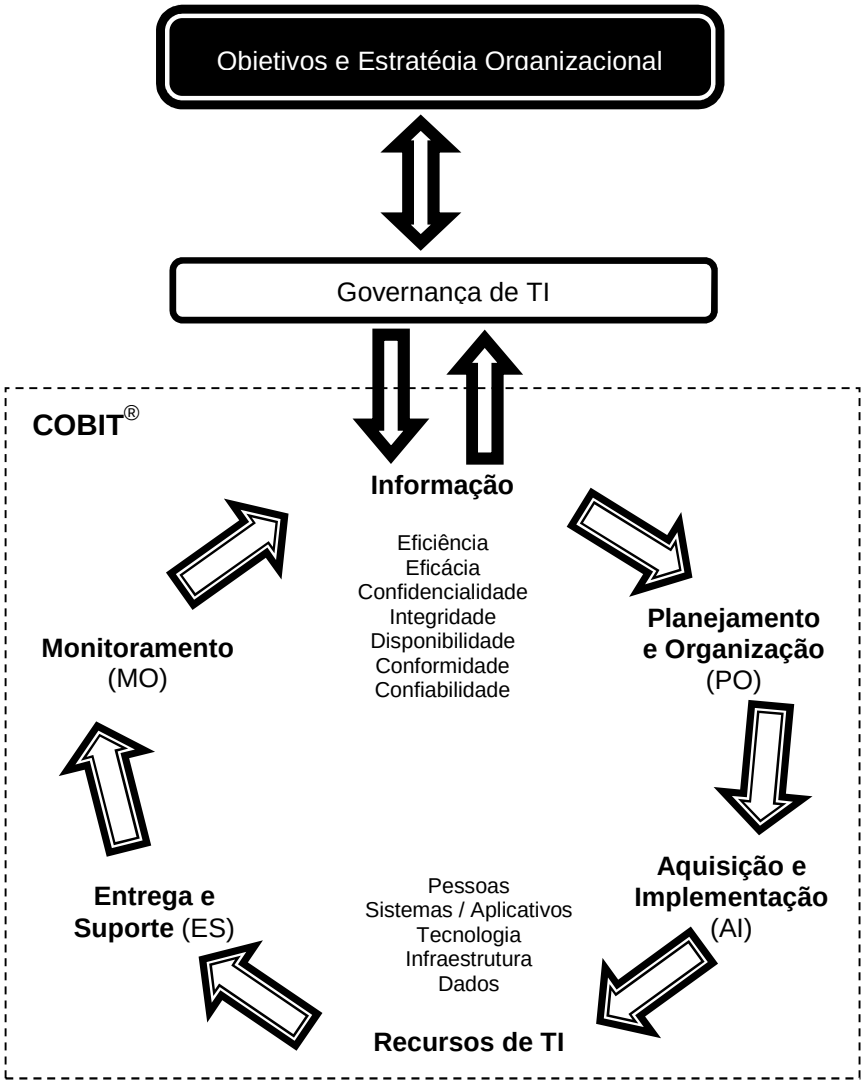
O modelo apresenta um conjunto de melhores práticas e processos de negócio ligados a domínios (Figura 6) voltados à tecnologia da informação. Divide as funções de TI em 34 processos, descritos nos quatro domínios (ITGI, 2008b):

a) Planejamento e Organização (PO) – esse domínio fornece direção para entrega de soluções e prestação de serviços, abrangendo os níveis estratégico e tático. Diz respeito à identificação da maneira que melhor para a consecução dos objetivos do negócio;
b) Aquisição e Implementação (AI) – esse domínio fornece as soluções. Para realizar as estratégias de TI, soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, bem como implementadas e integradas aos processos do negócio. As alterações e a manutenção dos sistemas existentes estão abrangidas por esse domínio para garantir que as soluções continuam gerando resultados para a organização;
c) Entrega e Suporte (ES) – esse domínio recebe as soluções e os torna utilizáveis para o usuário final. Preocupa-se também com a entrega efetiva dos serviços necessários (gestão da entrega, segurança e continuidade, suporte de serviços para usuários, e gestão de dados e facilidades operacionais). Todos os processos de TI precisam ser periodicamente avaliados ao longo do tempo para assegurar sua qualidade e o cumprimento dos requisitos de controle;
d) Monitoramento (MO) – esse domínio tem a finalidade de monitorar todos os processos a fim de assegurar o cumprimento dos objetivos definidos. Engloba também a gestão do desse desempenho, monitoramento do controle interno, a conformidade regulamentar e a governança.

Cada domínio é composto por uma série de processos, divididos em atividades e dispostos em uma estrutura lógica e gerenciável. Executar corretamente as atividades permite a execução do processo e o alcance da necessidade do domínio a que faz parte (KNORST, 2010).

Como pode ser observado na Figura 6, o COBIT® é um modelo de GTI orientado pela estratégia global do negócio. As informações geradas pelos recursos de TI (físicos, virtuais e humanos) abrangem os quatro domínios.

Figura 6 – *Framework* COBIT®



Fonte: Baseado em ITGI (2008b, p. 26).

O domínio Planejamento e Organização engloba o processo de gerenciamento de riscos de TI. Os potenciais impactos negativos aos objetivos da

organização provocados por situações não previamente planejadas devem ser identificados, analisados e avaliados. Para isso, a estrutura de gestão de riscos de TI deve estar alinhada com a estrutura de gestão de riscos da organização; o contexto, o objetivo e os critérios da avaliação de riscos devem ser estabelecidos; os eventos com potencial impacto negativo devem ter sua natureza determinada, sua ocorrência registrada e seu histórico mantido; a probabilidade e o impacto de todos os riscos identificados devem ser regularmente avaliados qualitativamente (abrangência do impacto) e quantitativamente (impacto financeiro), de forma individual, por categoria ou de maneira agrupada; estratégias de resposta ao risco (evitar, reduzir, compartilhar ou aceitar) devem ser identificadas, assim, como a determinação de responsabilidades e definição dos níveis de tolerância; as atividades de respostas aos riscos devem ser priorizadas e planejadas, com monitoramento dos planos que estão sendo executados e comunicação de desvios à alta administração (ITGI, 2008a).

Algumas vantagens do modelo COBIT® são destacadas por Cantón (2008): preocupar-se com o alcance dos objetivos estratégicos, compreender a amplitude da TI, identificar domínios e responsabilidades a partir de processos, ser aceito pelos órgãos reguladores (pelo BACEN, por exemplo, regulador das instituições financeiras no Brasil) no que tange aos controles de TI e possuir linguagem de fácil entendimento. O conjunto de boas práticas apresentado pelo COBIT® está mais concentrado em controle e menos em execução. Isso ajuda a otimizar os investimentos em tecnologia da informação e a garantir a prestação de serviços (ITGI, 2008b). Os códigos de boas práticas ou regras de comportamento derivam de princípios da governança corporativa, assim como das normas internas da organização que regulam a execução das rotinas diárias. Adoção das melhores práticas permite a realização das atividades e processos de TI de forma confiável, observável, criticável e corrigível (APREDA, 2011).

O COBIT® comporta as áreas focais da governança corporativa e da governança de TI. Para cada área foco, o COBIT® relaciona processos voltados a TI.

Quadro 1 – COBIT® e as áreas focais da governança de tecnologia da informação

Áreas foco da GTI	**COBIT®**
Alinhamento Estratégico	Ligar os planos de negócios e os de TI. Alinhar as operações de TI com as operações da organização. Definir, manter e validar a proposta de valor de TI. Processos do estágio "Planejar e Organizar (PO)" estão fortemente relacionados com o alinhamento estratégico.
Entrega de Valor	Executar a proposta de valor de TI. Garantir que a TI entregue os benefícios prometidos previstos na estratégia da organização. Otimizar custos e prever o valor intrínseco de TI. Os estágios "Adquirir e Implementar (AI)" e "Entregar e Suportar (ES)" têm maior foco na entrega de valor. Gerenciar incidentes e gerenciar mudanças são processos que mostram o valor da TI aos usuários/clientes, pelo contato direto.
Gestão de Risco	Preocupar-se com riscos e requerimentos de conformidade. Ser transparente sobre riscos significantes e gerenciamento dos riscos. "Adquirir e Implementar (AI)" e "Entregar e Suportar (ES)" focam também a gestão de riscos, principalmente nos processos de gestão da continuidade de serviços de TI, segurança de sistemas e gestão de serviços terceirizados.
Gestão de Recursos	Utilizar os recursos e aplicar investimentos da melhor forma possível. Gerir apropriadamente os recursos críticos de TI: aplicativos, informações, infraestrutura e pessoas. Gestão de capacidade, gestão de pessoas e fornecedores procuram atender o foco.
Mensuração de Desempenho	Acompanhar e monitorar a implementação da estratégia, a execução de um projeto, o uso de recursos, o desempenho dos processos e atividades. Juntamente com a descrição dos processos, o COBIT® sugere indicadores baseados nos níveis: operacional, tático e estratégico.

Fonte: ITGI (2008b, p. 13).

Os elementos das áreas focos devem estar coordenados. A infraestrutura e o *know-how* das pessoas, por exemplo, devem ser compatíveis. A gestão de recursos requer o gerenciamento das interdependências dos próprios recursos (THURNER, 2010).

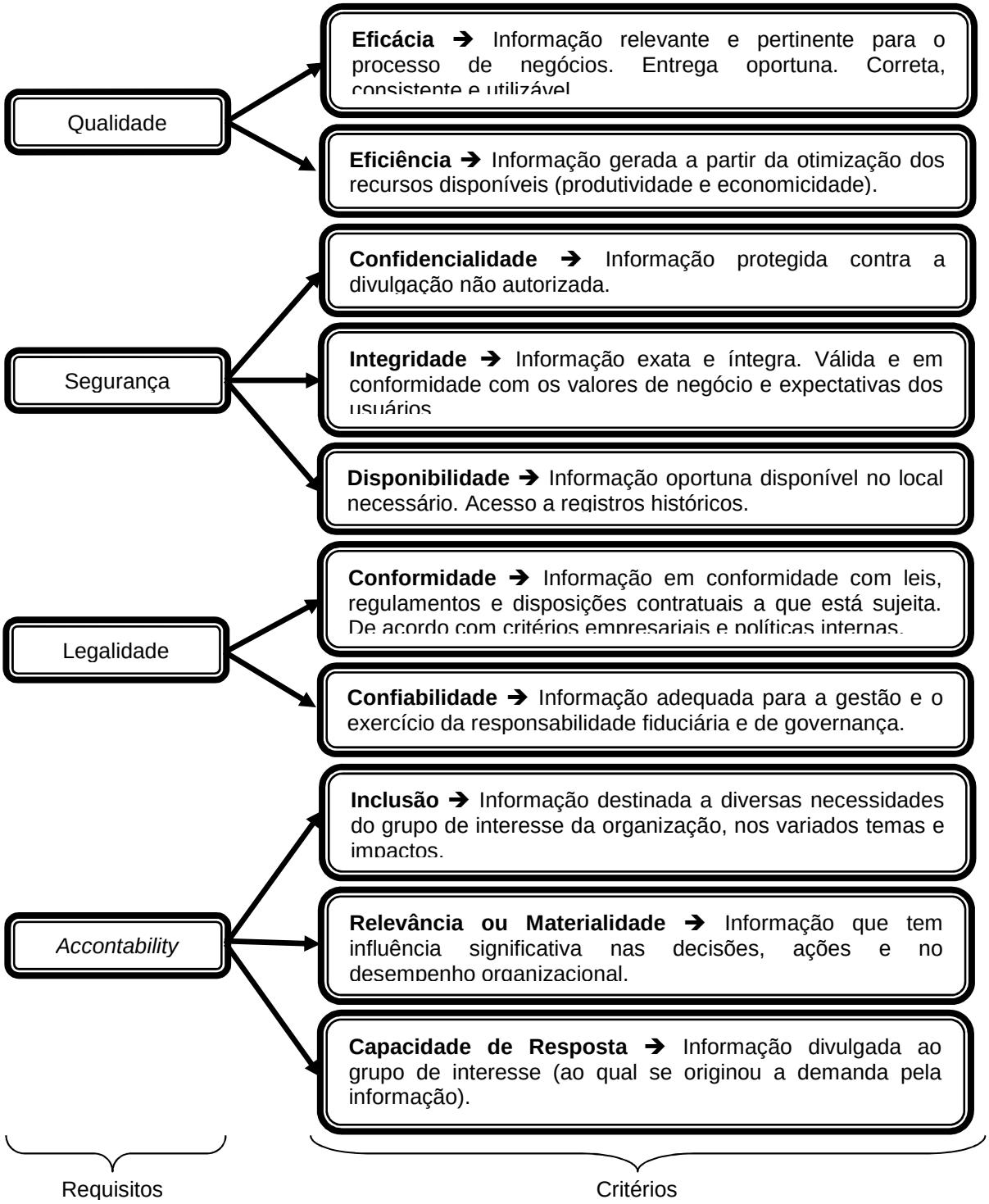
A gestão de riscos identifica potenciais problemas antes de sua ocorrência, possibilitando que as ações de tratamento do risco sejam planejadas e executadas com a percepção de mitigar os impactos negativos. Divide-se em três partes: definição da estratégia de gestão de riscos (determinação de origens, categorias e definição de parâmetros de análise de riscos, estabelecimento de estratégias as serem utilizadas); identificação e análise de riscos (identificação e documentação da avaliação de riscos e sua categorização); e tratamento dos riscos identificados

(plano para mitigação dos impactos negativos provocados pelos riscos e monitoramento periódico da situação do risco) (SOFTWARE ENGINEERING INSTITUTE, 2010).

Considerando-se a informação como a base para o processo de gestão organizacional, o COBIT® destaca critérios para as informações que devem ser observados na aplicação ou uso dos recursos de TI. As informações necessitam estar de acordo com determinados critérios de controle, que segundo modelo COBIT® referem-se aos requisitos de negócio para obter informações (ITGI, 2008b).

O modelo COBIT® compreende quatro níveis de usuários, sendo eles: direção executiva, administração, gestores de TI e auditores (ITGI, 2008b). Em nível de diretoria executiva, auxilia na definição de valores de investimentos de TI, equilibrando riscos e controlando os investimentos em ambientes de TI. A gestão do negócio efetua, com auxílio do COBIT®, o gerenciamento e o controle de todos os serviços prestados pela TI, sejam eles de origem interna ou externalizados. Cabe à administração de TI disponibilizar, controlar e gerenciar os serviços de TI necessários à realização dos objetivos estratégicos. Para os auditores (internos ou independentes) o COBIT® fornece informações para a emissão de pareceres e formulação de recomendações sobre os controles internos. Os processos e atividades elencados pelo modelo constituem-se de ferramental para uso na auditoria, controle e na área de segurança.

Figura 7 – Critérios de informações (COBIT® e *accountability*)



Fonte: Baseado em ITGI (2008b, p. 10-11) e Accountability (2008, p. 9-16).

É fato que os conceitos que envolvem a governança de TI e a *accountability* são apresentados de forma diversa pelos autores. O Quadro 2 apresenta resumo das descrições dos principais conceitos utilizados no presente trabalho sob a ótica

da GTI, do modelo COBIT® e da *accountability*. Estas descrições fundamentam teoricamente os critérios para avaliação de processos de TI.

Quadro 2 – Resumo descritivo dos principais conceitos abordados

(Continua)

Governança de Tecnologia da Informação	
Conceito	**Descrição**
Risco	Probabilidade de insatisfatório resultado futuro (BARKI, RIVARD e TALBOT, 2001; SILVA, 2011).
Estratégia	Ponto de partida para desenvolvimento e implantação de estratégias de TI. Permite a busca de mecanismos par estabelecer objetivos, avaliar resultados e níveis de desempenho de metas (TAROUCO e GRAEML, 2011).
Desempenho	Capacidade de geração de resultados operacionais mensuráveis a partir de processos internos e da utilização regrada de recursos (MATITZ e BULGACOV, 2011). Atendimento às necessidades do negócio, maximização da entrega de valor, uso racional de recursos de TI e gerenciamento adequado dos riscos (ROSA, 2008).
TI	Recursos tecnológicos destinados a construir, divulgar e controlar informações aos interessados atuais e futuros (WEILL e ROSS, 2006; ISO/IEC 38500, 2008).
Segurança (Risco Operacional)	Proteção permanente dos dados em informações organizacionais (O'CONNOR e MARTINSONS, 2006). Diminuição da possibilidade de riscos e o permanente controle de ameaças e fraquezas do sistema (GHEORGHE, 2010). Assegurar a proteção dos ativos de informação é um dos objetivos centrais da governança de TI (CALDER e WATKINS, 2008).
Responsabilidade	Identificação de quem toma as decisões e quem é o responsável. Definição de papéis, funções e hierarquia dos cargos (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008; LARSEN, PEDERSON e ANDERSON, 2006; BUTLER e BUTLER, 2010). Autoridade para agir (BUTLER e BUTLER, 2010).
Transparência	Comunicação das decisões tomadas, como são tomadas e dos resultados atingidos (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008; LARSEN, PEDERSON e ANDERSON, 2006; BUTLER e BUTLER, 2010).
Prestação de Contas	A comunicação das informações sobre resultados é base para a manutenção, avaliação e adaptação dos processos e da estrutura de GTI (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008; LARSEN, PEDERSON e ANDERSON, 2006; BUTLER e BUTLER, 2010).
Accountability	
Conceito	**Descrição**
Risco	Impacto social e ambiental negativo (LANDRUM e DAILY, 2012; PEREIRA e SILVA, 2012).
Estratégia	Elemento regulatório de orientação para a responsabilização e prestação de contas e transparência frente a objetivos almejados (LAWRENCE e NEZHAD, 2009; ACCOUNTABILITY, 2008; BUTLER e BUTLER, 2010).
Desempenho	Sucesso nos resultados da atividade chave (FELTUS, PETIT e DUBOIS, 2009).
TI	Recursos utilizados para a geração de informações ao grupo interessado, definição de objetivos, padrões de gerenciamento e avaliação, e comunicação (ACCOUNTABILITY, 2012).
Segurança (Risco Operacional)	Maior responsabilização nas ações corporativas está proporcionalmente relacionada a melhores desempenhos (KING, DAVIS e MINTCHIK, 2012).
Responsabilidade	Direito delegado e a obrigação atribuída (FELTUS, PETIT e DUBOIS, 2009). Legitimidade em atribuir responsabilização por ações (decisões) ou elementos regulatórios (políticas ou estratégias), frente ao desempenho almejado (ACCOUNTABILITY, 2008; BUTLER e BUTLER, 2010; COMITE, 2012).

(Conclusão)

Accountability	
Conceito	**Descrição**
Transparência	Condição necessária para a responsabilização, embora não seja seu determinante (FOX, 2007; LANDRUM e DAILY, 2012). Na falta de transparência, a tendência é que haja menor responsabilidade (ABDULLAHI, ENYINNA e STELLA, 2012).
Prestação de Contas	Os sujeitos devem justificar suas decisões (KING, DAVIS e MINTCHIK, 2012). Significa uma obrigação ou uma autoridade (know-how) (FELTUS, PETIT e DUBOIS, 2009).
COBIT®	
Conceito	**Descrição**
Risco	Evento ou problema com potencial impacto negativo que devem ser identificado antes de sua ocorrência (ITGI, 2006; SOFTWARE ENGINEERING INSTITUTE, 2010).
Estratégia	Orientação para identificar riscos e avaliar sua importância para os negócios (KUMAR, 2002).
Desempenho	Diminuir, mitigar ou externarlizar riscos (BUTLER e BUTLER, 2010).
TI	Soluções adquiridas ou desenvolvidas, integradas aos processos do negócio na geração de resultados (ITGI, 2008b).
Segurança (Risco Operacional)	Supressão das deficiências relativas aos requisitos de controle, técnicos, riscos e comunicação (ITGI, 2008a).
Responsabilidade	Demarcação das funções de TI e identificação pessoal do responsável pelos processos de TI (ITGI, 2007; FELTUS, PETIT e DUBOIS, 2009).
Transparência	Comunicação do desempenho em linguagem de fácil entendimento (ITGI, 2008b). A adoção das melhores práticas nas atividades e processos de TI dá confiabilidade e permite a observação, crítica e correção (APREDA, 2011).
Prestação de Contas	Informar sobre os resultados alcançados provenientes das ações e decisões adotadas (FELTUS, PETIT e DUBOIS, 2009).
Gestão de Riscos	
Conceito	**Descrição**
Risco	Ameaça a qual a organização está suscetível no âmbito da TI (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008).
Estratégia	Escopo ou orientação organizacional para a área de TI (ITGI, 2008a, ITGI, 2008b).
Desempenho	Maximização dos resultados, uso adequado dos recursos de TI e mitigação de riscos (ITGI, 2008a).
TI	Componentes utilizados para minimizar riscos (GHEORGHE, 2010), gerenciar incidentes (FLORES et al., 2011) e garantir a segurança das informações (ITGI, 2006).
Segurança (Risco Operacional)	Proteção contra riscos de perdas, descontinuidade operacional, usos indevidos, divulgação não autorizada e danos (ITGI, 2006). Não se limita a recursos técnicos. Demanda o envolvimento de todos os interessados na organização e requer avaliação de ameaças e planos de respostas (NATIONAL CYBER SECURITY SUMMIT TASK FORCE, 2004)
Responsabilidade	Identificação civil e legal pela proteção contra riscos (ITGI, 2006).
Transparência	Condição para criar valor e minimizar riscos (GHEORGHE, 2010).
Prestação de Contas	Elaboração de relatórios de segurança (NATIONAL CYBER SECURITY SUMMIT TASK FORCE, 2004). Comunicação de desvios identificados aos responsáveis (ITGI, 2008a).

Fonte: Elaborado pelo Autor.

Ameaça, probabilidade de resultado insatisfatório, evento com impacto negativo e problema potencial são expressões que descrevem conceitualmente o risco. Sob as quatro óticas (gestão de riscos, GTI, COBIT® e *accountability*) o risco

apresenta-se como uma situação possível ainda não concretizada, que oferece probabilidade de dificuldade futura à organização.

Orientação, ponto de partida, escopo e elemento regulatório definem a estratégia. Na gestão de riscos está voltada para identificação e avaliação dos riscos. Para a GTI, estabelece objetivos, metas, avaliação e níveis de desempenho. A estratégia, para o COBIT®, orienta a área de TI e para a *accountability*, regula a responsabilização, prestação de contas e transparência.

GTI, COBIT® e *accountability* utilizam termos semelhantes para conceituar desempenho. Focam na capacidade de geração e maximização de resultados. Gestão de riscos concentra-se no risco, evento que interfere no alcance dos resultados esperados.

TI é entendida como conjunto de componentes, recursos ou soluções tecnológicas utilizadas na geração, proteção, segurança, avaliação, controle e comunicação de informações. À segurança relaciona-se a incumbência de salvaguardar dados e informações.

Responsabilidade trata da identificação pessoal por ações e decisões relacionadas a cargos, funções, papéis e interessados dos negócios. Está ligada à necessidade ou obrigatoriedade pelo cumprimento de determinadas tarefas ou atividades. Responsabilização dá maior amplitude ao espaço de atuação, incluindo o uso de recursos para o alcance de metas ou objetivos.

Transparência e prestação de contas estão conceitualmente ligadas. Ambos os termos voltam-se para a comunicação de decisões e ações. Estão diretamente relacionados com a responsabilidade, aparecendo algumas vezes como condição necessária daquela.

A abrangência dos conceitos expressos no Quadro 2 delimitam o enfoque que o presente trabalho assume, não havendo pretensão de confrontá-los com entendimentos diversos aos destacados.

3 PROCEDIMENTOS METODOLÓGICOS

Apresentam-se neste capítulo os procedimentos metodológicos utilizados na pesquisa, caracterizada como descritiva e do tipo levantamento.

3.1 CARACTERIZAÇÃO DA POPULAÇÃO E AMOSTRA DA PESQUISA

A população da presente pesquisa, entendida como o conjunto de indivíduos ou objetos que possuem determinadas características em comum (MARTINS; THEÓPHILO, 2009), compõe-se das maiores instituições financeiras cadastradas no Banco Central do Brasil (BACEN) nas formas de instituições independentes ou conglomerados e que publicaram na internet o Relatório de Gerenciamento de Riscos referente ao terceiro trimestre de 2012. A relação das instituições foi obtida mediante relatório emitido pela Divisão de Sistemas Cadastrais (DISIC), Departamento de Monitoramento do Sistema Financeiro (DESIG), do Banco Central do Brasil (BACEN). Refere-se ao terceiro trimestre de 2012, sendo publicadas com data base de Setembro de 2012.

Escolheu-se instituição financeira bancária pelo nível de utilização de recursos físicos, humanos e financeiros relacionados à tecnologia da informação. Pereira e Silva (2012), Flores et al. (2011) e ITGI (2006) evidenciaram a proporcionalidade entre a dependência ou a utilização de recursos de TI e o grau de exposição a riscos.

Inicialmente a relação de instituições financeiras obtida junto ao Banco Central do Brasil foi estratificada segundo quatro critérios: ativo total, depósitos totais, número de funcionários e número de agências. Com isso identificaram-se as 50 maiores instituições do setor em cada um dos quatro critérios.

Esses critérios foram selecionados a partir dos elementos de classificação divulgados pelo BACEN. Destacam as instituições com maior volume de recursos geradores de operações financeiras, com maior exposição a riscos que envolvem os recursos humanos e transferência de dados. Sendo possível a existência de organizações não financeiras nos conglomerados financeiros (BB, BIC e CITIBANK, por exemplo), manteve-se ativo total e depósitos totais como requisitos.

O ranking das 50 maiores instituições/conglomerados em cada critério possibilitou, combinado à disponibilização do Relatório de Gerenciamento de Riscos,

possibilitou a definição da população da pesquisa, que compôs-se com as maiores organizações. Elas foram relacionadas em pelo menos três dos quatro critérios determinados e possuem publicação do relatório mencionado anteriormente.

Com esse procedimento, determinou-se a população a ser pesquisada. A composição abrange as 34 maiores instituições/conglomerados financeiros com operação de atividades no Brasil no terceiro trimestres de 2012.

A amostra compôs-se a partir da relação das maiores instituições financeiras bancárias com operação no Brasil, sendo definida como um recorte ou um subconjunto da população (MARTINS e THEÓPHILO, 2009). Das 34 instituições/conglomerados que compuseram a população, quatro (ABCBRASIL, BNB, BRB e BRDE) não foram incluídas na pesquisa por apresentarem Relatório de Gerenciamento de Riscos exclusivamente quantitativo. Requerendo, a pesquisa, informações acerca da existência ou não de procedimentos, processos e práticas, o relatório exclusivamente quantitativo impossibilita a extração dos dados necessários. Após esse processo de busca e análise da qualidade das fontes dos dados, compôs-se uma amostra com 30 instituições/conglomerados financeiros.

Quadro 3 – Relação de instituições/conglomerados da amostra

(Continua)

Instituição ou Conglomerado	Ativo Total	Depósito Total	Funcionários	Agências
ALFA	X	X	X	X
BANCOGMAC	X	X	X	
BANCOOB	X	X	X	X
BANESE		X	X	X
BANESTES	X	X	X	X
BANPARA		X	X	X
BANRISUL	X	X	X	X
BB	X	X	X	X
BIC	X	X	X	X
BMG	X	X	X	X
BNDES	X	X	X	
BNPPARIBAS	X	X	X	X
BRADESCO	X	X	X	X
BTGPACTUAL	X	X	X	X
CEF	X	X	X	X
CITIBANK	X	X	X	X
DAYCOVAL	X	X	X	X
DEUTSCHE	X	X	X	X
FIBRA	X	X	X	X
INDUSVAL	X	X	X	X
ITAU	X	X	X	X
JPMORGANCHASE	X	X	X	X
MERCANTILDOBRASIL	X	X	X	X

(Conclusão)

Instituição ou Conglomerado	Ativo Total	Depósito Total	Funcionários	Agências
PINE	X	X	X	X
RABOBANK	X	X	X	X
RURAL	X	X	X	X
SAFRA	X	X	X	X
SANTANDER	X	X	X	X
VOLKSWAGEN	X	X	X	
VOTORANTIM	X	X	X	X

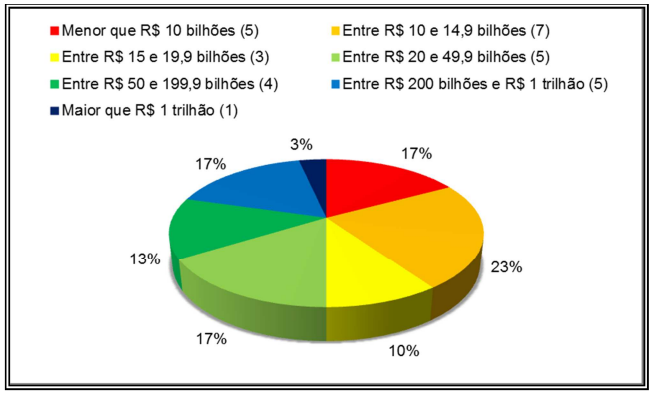
Fonte: Elaborado pelo autor.

A amostra representa 99% da soma de todos os ativos totais das maiores instituições/conglomerados financeiros com operação no Brasil em Setembro de 2012. A expressividade também pode ser constatada por: 99% do total de depósitos totais; 97% do número total de funcionários; e 99% do número total de agências em operação. Percebe-se que um dos maiores conglomerados bancários com operação no Brasil, o HSBC, não compõe a amostra por não haver sido encontrado fonte de divulgação do relatório do referido período de análise.

O controle acionário das organizações pesquisadas possui três formatações: controle público (23%), controle privado nacional (50%) e controle privado estrangeiro (27%). Quanto à composição, 22 organizações são conglomerados financeiros (73%) e oito instituições independentes (27%). Entre os conglomerados estão o BB, ITAÚ, BRADESCO e SANTANDER. CEF e BNDES integram com outras organizações a parcela da amostra classificada como instituição independente.

As instituições/conglomerados, quanto ao valor do “ativo total”, foram distribuídas conforme representação da Figura 8.

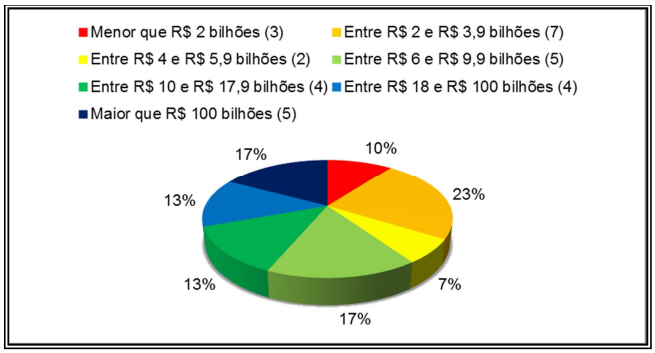
Figura 8 – Composição da amostra quanto ao “ativo total”



Fonte: Elaborado pelo autor.

BB, ITAÚ, BRADESCO, CEF, BNDES e SANTANDER são as organizações com “ativo total” superior a R$ 450 bilhões. Todas as outras não excedem R$ 120 bilhões. Observando-se os montantes de “depósitos totais”, as organizações enquadram-se nas faixas apresentadas na Figura 9.

Figura 9 – Composição da amostra quanto aos “depósitos totais”

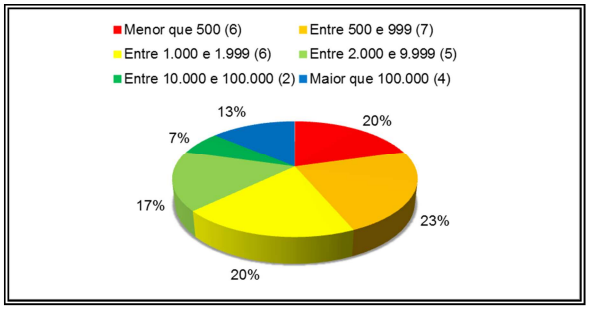


Fonte: Elaborado pelo autor.

SANTANDER, BRADESCO, ITAÚ, CEF e BB excedem o montante de R$ 120 bilhões em “depósitos totais”. As demais estão na faixa inferior a R$ 30 bilhões. Os “depósitos totais” acumulam os valores dos depósitos: à vista, em poupança, interfinanceiros, a prazo e outras modalidades de depósitos.

Há certa variação do número de funcionários, oscilando entre 300 e 130 mil.

Figura 10 – Composição da amostra quanto ao “número de funcionários”

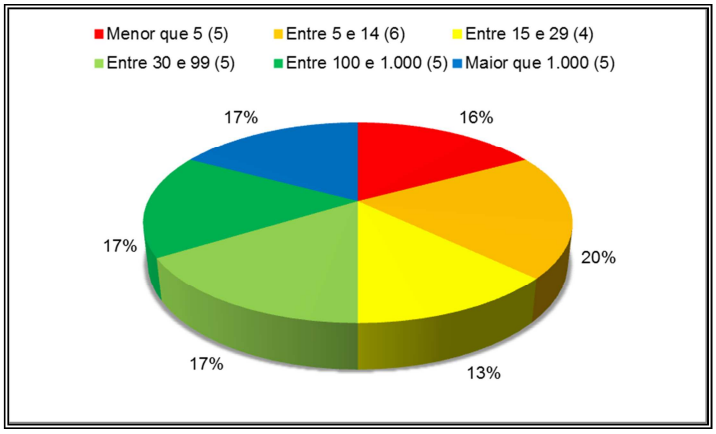


Fonte: Elaborado pelo autor.

Apenas BRADESCO, CEF, ITAÚ e BB possui número de funcionários superior a 100.000. SANTANDER tem em torno de 55.000, enquanto todas as outras instituições/conglomerados possuem menos que 12.000 funcionários cada. O

número de agência varia de uma até 5.340. Na Figura 11 apresenta-se uma estratificação das faixas de número de agências por instituições/conglomerado.

Figura 11 – Composição da amostra quanto ao “número de agências”



Fonte: Elaborado pelo autor.

As instituições com maior número de agências são: BB, BRADESCO, ITAÚ, CEF e SANTANDER, todas com mais de 2.550 funcionários. Todas as outras possuem menos que 500 funcionários. Reforça aqui a expressividade da amostra selecionada por representar, nos critérios de composição da amostra, em torno de 90% do total geral de instituições financeiras cadastradas no BACEN, além de abranger entre 97% e 99% da população de estudo. Caracterizada a amostra, apresentam-se as três fases de investigação: análise de critérios para avaliação de processos de TI, Análise de Conteúdo e Análise Lexical.

3.2 FONTE DE DADOS

A coleta de dados observou os quesitos da seleção de amostra (Quadro 3). Os dados para a pesquisa foram coletados em documentos obtidos junto às organizações que compõem a amostra. A fonte de dados constitui-se de relatórios que abordam o assunto em estudo. Esses relatórios possuem obrigatoriedade na divulgação periódica, com acesso irrestrito, inclusive na internet, sendo exigência do órgão regulador do setor. Desses documentos foram extraídos os textos que possibilitaram a Análise de Conteúdo e a Análise Lexical, observando-se o método de pesquisa *survey*.

Os dados extraídos dos relatórios investigados quanto aos critérios para avaliação de processos de TI, foram revisados a partir da produção científica (artigos, dissertações e teses coletadas em bancos de dados online, como EbscoHost, Capes, IBBA e bancos de dissertações e teses, dentre outros) e da produção técnica (legislação, normas técnicas, resoluções e instruções normativas emitidas por órgãos reguladores do setor). Tanto a produção científica como a técnica foi utilizada na construção do instrumento.

3.3 TÉCNICA DE ANÁLISE DE DADOS

Sobre os dados coletados foram aplicadas algumas técnicas de análise. Para a organização sistemática dos dados (MARTINS e THEÓPHILO, 2009) utilizou-se a Estatística Descritiva. Quadros e gráficos auxiliaram no aparelhamento e análise dos dados, bem como na apresentação de resultados encontrados.

A investigação baseou-se na revisão da literatura da produção científica e técnica para efetuar a análise e atualização de critérios para avaliação de processos de TI. O resultado dessa etapa foi utilizado na análise dos relatórios, utilizando-se a Análise de Conteúdo. A Análise de Conteúdo é definida como um conjunto de procedimentos metodológicos empíricos aplicados em discursos, que permite a classificação ou categorização de componentes de significação do texto (BARDIN, 2011).

O objetivo da Análise de Conteúdo é evidenciar dados, informações e conhecimentos que estão inseridos na representação textual (ROCHA e DEUSDARÁ, 2005). Propõe-se a investigar a mensagem que está expressa ou oculta no texto. A presença ou ausência de unidades de registro (palavras) podem possuir semelhante importância. Ausência pode traduzir a necessidade ou o objetivo da não apresentação (BARDIN, 2011). Os principais passos para a realização da Análise de Conteúdo estão descritos na sequência:

a) preparação dos dados – leitura completa dos documentos a serem analisados com objetivo de garantir que os mesmos contemplam os requisitos da pesquisa; catalogação para rápida identificação; verificação de formatos;
b) identificação das unidades do texto ou balizamento – releitura dos

documentos com objetivo de evidenciar unidades de classificação; o balizamento permite que unidades de análise possam ser futuramente confrontadas com a categorização, por exemplo;

c) categorização ou classificação do texto – consiste em um procedimento onde são reconhecidos elementos que caracterizam o objetivo e o problema da pesquisa; são rubricas de identificação entre as unidades de análise e os critérios da pesquisa; depende fundamentalmente da percepção do pesquisador;
d) descrição – refere-se a comunicação dos resultado; no caso de uma pesquisa quantitativa, a descrição envolve a elaboração de ilustrações para demonstrar frequências e percentuais, por exemplo; sendo pesquisa qualitativa, elaboram-se textos sintetizados ou mapas;
e) interpretação dos resultados – os resultados da pesquisa são expressos com a análise das categorias teóricas; numa outra direção, a partir das informações e categorias constrói-se elementos teóricos (BARDIN, 2011).

Encontram-se na literatura, diversidade de passos para a realização da Análise de Conteúdos. Outra análise que objetiva a investigação de discursos é a Análise Lexical. Esse tipo de análise visa proporcionar a compreensão do texto através de seu léxico, do conjunto de palavras utilizadas para a formação do texto ou de expressões (SPHINX BRASIL, 2007).

Os resultados das análises de conteúdo e lexical podem ser apresentados através de Mapas Fatoriais. Para sua elaboração utiliza-se o teste Qui-Quadrado. É um teste não paramétrico utilizado para testar o tipo de relação entre as variáveis: independência ou dependência. Efetua, portanto, um estudo relacional (MOTTA, 2006). Os Mapas Fatoriais são elaborados também a partir das tabelas de contingências das variáveis. Efetuando-se o cruzamento das variáveis, identificam-se influências, causalidades ou coincidências (SPHINX BRASIL, 2007).

O valor Qui-Quadrado de cada célula foi obtido a partir da identificação dos valores esperados: (Total de Observações da Linha / Total Geral de Observações) * Total de Observações da Coluna = Valor Esperado. O total de léxicos observados em um critério (total da linha) foi dividido pelo total de léxicos observados (total geral de todas as linhas), sendo o resultado multiplicado pelo número total de observações de um léxico no texto (total de observações de uma coluna).

Com o Valor Esperado para cada célula, subtraindo-se do Valor Observado para a mesma célula, pode-se achar Diferença, sendo, Diferença = Valor Esperado – Valor Observado. Finalmente o Qui-Quadrado é encontrado elevando-se a Diferença de cada célula ao Quadrado e dividindo-se o resultado pelo Valor Esperado para cada célula.

Numa tabela de contingência onde as linhas representam os critérios e as colunas os léxicos, o Qui-Quadrado de cada célula é encontrado com a equação (1):

$$\text{Qui-Quadrado} = \frac{\{[(\Sigma \text{ Linha} / \Sigma \text{ Léxicos Observados na Amostra}) * \Sigma \text{ coluna}] - \text{Valor Observado na Célula}\}^2}{\text{Valor Esperado}} \quad (1)$$

Com o uso do teste Qui-Quadrado, verifica-se que quanto maior o desvio maior é a existência de relação significativa entre as variáveis testadas. No Mapa, a incidência da variável é representada proporcionalmente ao tamanho da superfície. As ligações entre as variáveis representam o nível de significância, ou seja, de relação entre elas (SPHINX BRASIL, 2007). As faixas de significância utilizada na pesquisa são:

Quadro 4 – Níveis de significância utilizados na pesquisa

Faixa de Significância	Indicação Abreviada	Nível de Significância
Muito Significante	MS	p<1%
Significante	S	1%<p<5%
Pouco Significante	PS	5%<p<15%”;
Não Significante	NS	p>15

Fonte: Elaborado pelo Autor.

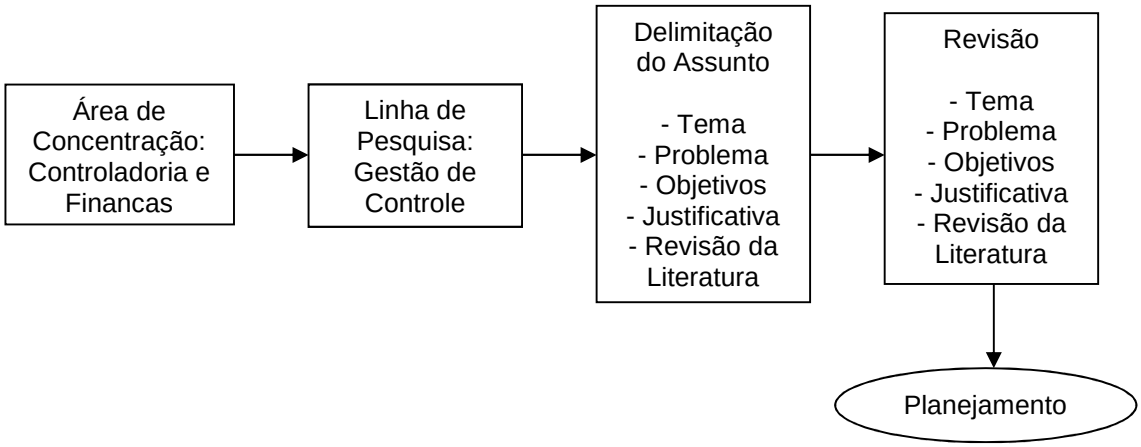
O valor-p representa a probabilidade estatística de rejeição da hipótese nula, que no caso seria a inexistência de dependência envolvendo as variáveis estudadas. As análises foram efetuadas sobre os resultados do teste Qui-Quadrado e os dados das tabelas de contingência.

3.4 ETAPAS DA PESQUISA

A realização da pesquisa compôs-se de quatro etapas: estruturação, planejamento, execução e finalização. Para melhor entendimento, apresenta-se um

fluxo ilustrativo para cada fase. A pesquisa foi estruturada a partir da área de concentração e linha de pesquisa do mestrado.

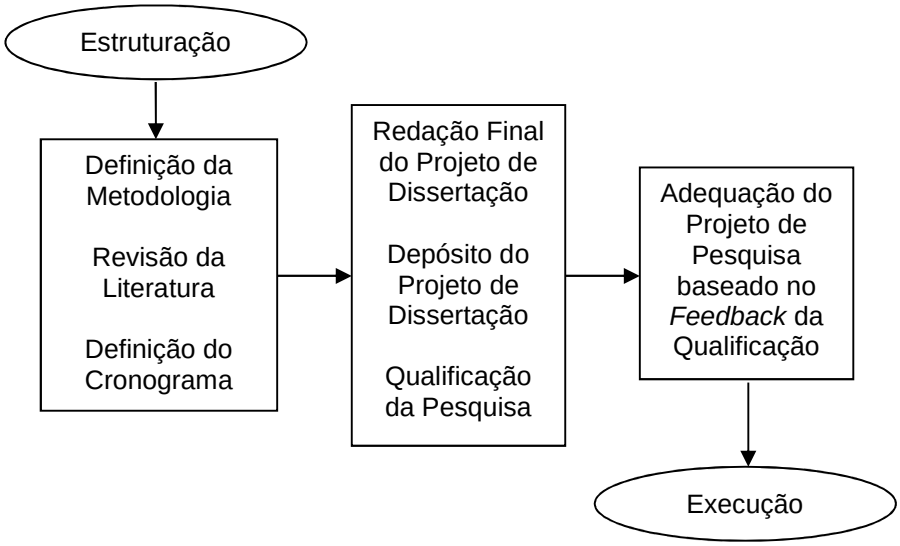
Figura 12 – Estruturação da pesquisa



Fonte: Elaborado pelo autor.

Definidos o tema (definição de critérios para avaliação de processos de TI considerando responsabilização, prestação de contas e transparência no gerenciamento de riscos) e a abrangência do estudo (maiores instituições financeira bancárias independentes ou conglomerados, que operam no Brasil), efetuou-se levantamento acerca da produção técnica e científica, expressa na revisão da literatura (Figura 13). Organizações do ramo financeiro foram escolhidas como alvo da pesquisa pelo expressivo nível de dependência destas aos processos de TI, bem como a utilização de modelos de governança de TI (como o COBIT®). Definiu-se a metodologia a ser empregada na pesquisa e elaborou-se cronograma de atividades. Submeteu-se o projeto para qualificação.

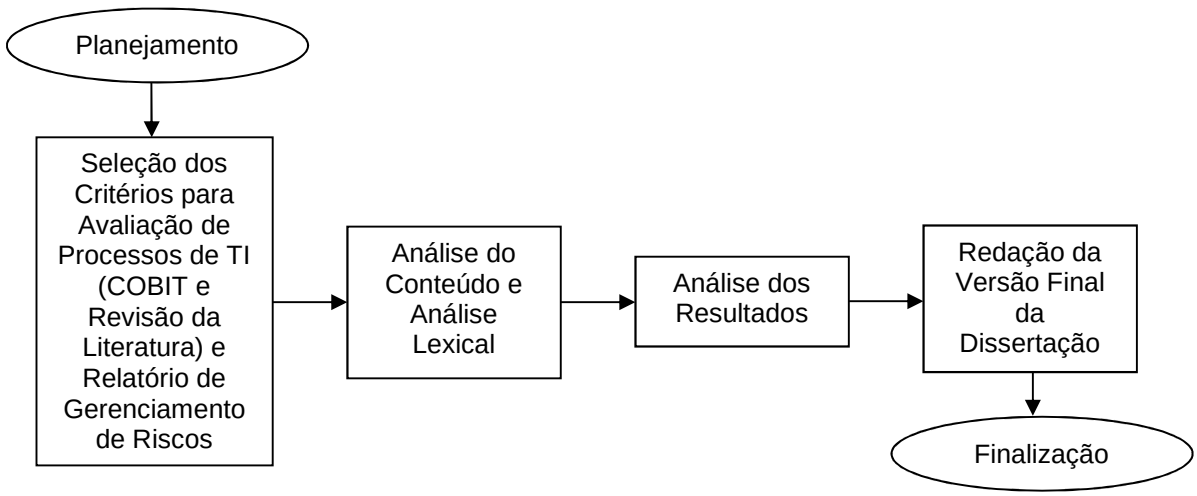
Figura 13 – Planejamento da pesquisa



Fonte: Elaborado pelo autor.

Obtendo-se a qualificação do projeto de pesquisa em banca examinadora e realizadas as adequações sugeridas, investigou-se empiricamente o objetivo proposto deste trabalho. A etapa de execução caracteriza-se pelo uso de meios e técnicas metodológicas e estatísticas na coleta e processamento dos dados e na apresentação dos resultados encontrados, bem como os testes estatísticos que dão confiabilidade a esses resultados.

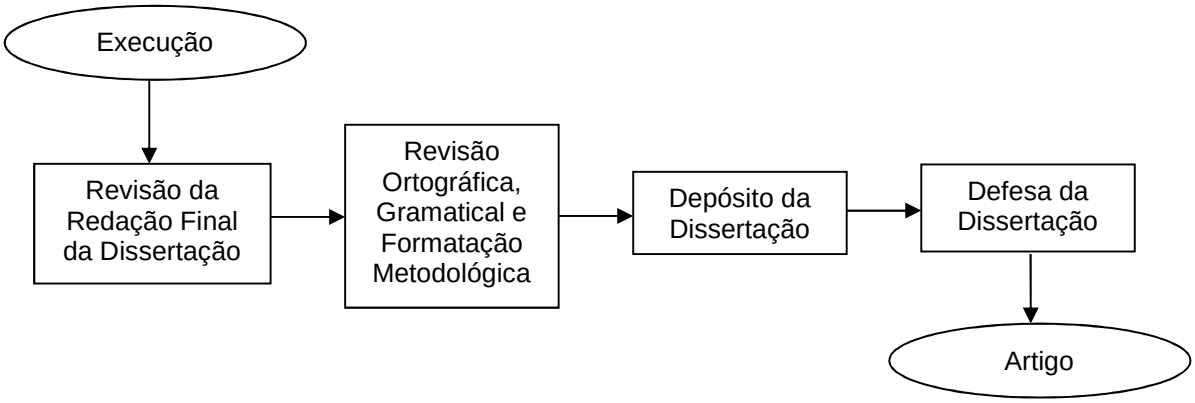
Figura 14 – Execução da pesquisa



Fonte: Elaborado pelo autor.

Com base na revisão da literatura e nos critérios do modelo COBIT® 4.1, sintetizou-se os critérios para avaliação de processos de TI, que foram utilizados para categorizar os Relatórios de Gerenciamento de Riscos e realizar Análise de Conteúdo (Quadro 8). Efetuou a Análise Lexical dos relatórios. Os resultados das duas análises foram confrontados. Os dois últimos procedimentos utilizaram o software *Sphinx Survey* – Edição Léxica.

Figura 15 – Finalização da pesquisa



Fonte: Elaborado pelo autor.

Considera-se a defesa da dissertação em banca examinadora o seu estágio final, porém, a produção acadêmica e científica tem como característica a continuidade de estudos. Desta forma, a produção de artigos se apresenta como etapa posterior a finalização da dissertação.

4 ANÁLISE DOS RESULTADOS ENCONTRADOS

Em termos gerais, a análise dos resultados apresenta duas fases. A primeira refere-se à investigação teórica concernente aos critérios para avalição dos processos de TI. Os 34 critérios do modelo COBIT®, distribuídos nos seus cinco domínios, foram confrontados com a revisão bibliográfica efetuada a partir da produção técnica e científica voltada ao gerenciamento de riscos, responsabilização, prestação de contas e transparência. Esta ação resultou na identificação de mais 34 critérios teóricos, adicionais ao modelo COBIT®. Posteriormente os 68 critérios foram analisados e sintetizados em 32 critérios (Quadro 8), conforme procedimentos descrito na Seção 4.2, constituindo-se no instrumento de investigação posterior.

Na segunda fase da pesquisa, selecionou-se 30 Relatórios de Gerenciamento de Riscos das maiores instituições financeiras bancárias (independentes ou conglomerados) que operam no Brasil. A escolha seguiu o procedimento de seleção de amostra descrito na Seção 3.1. Os relatórios foram encontrados em websites oficiais de cada integrante da amostra no período que compreende o quarto trimestre de 2012 e o mês de janeiro de 2013.

Procedeu-se a categorização dos relatórios a partir dos 32 critérios selecionados na primeira etapa. Paralelamente efetuou-se a Análise Lexical, com o uso do software *Sphinx Survey* – Edição Léxica (v. 5.1.0.8). Os referidos relatórios têm publicação trimestral, conforme orientação do Banco Central do Brasil (CIRCULAR BACEN n. 3.477/2009). As análises da categorização e lexical dos relatórios auxiliaram na definição dos critérios para avaliação de processos de TI considerando-se a *accountability* no gerenciamento de riscos.

A produção científica (artigos publicados em periódicos, dissertações e teses) e a produção técnica (legislação e normas técnicas) foram utilizadas para revisar o instrumento de coleta de dados. O instrumento de coleta foi aplicado sobre os Relatórios de Gerenciamento de Riscos emitidos no terceiro trimestre de 2012 pelas maiores instituições/conglomerados financeiros bancários que operam no Brasil (Pesquisa Documental). Por serem os relatórios desse período os mais recentemente publicados e constatando-se que não há um padrão de comportamento das instituições financeiras bancárias quanto à manutenção da disponibilidade de todos os relatórios emitidos, o estudo limitou-se aos documentos do período citado.

4.1 SETOR BANCÁRIO BRASILEIRO

O setor bancário brasileiro caracteriza-se por transformações ocorridas nas últimas décadas. Evidenciam-se dois aspectos: adoção crescente de recursos tecnológicos (acompanhando o desenvolvimento da tecnologia) e as alterações no ambiente regulatório (STEFFANELLO, 2010).

Grandes investimentos em tecnologia da informação são aplicados para garantir o fornecimento, a qualidade e a segurança dos serviços bancários. A disponibilização de ferramentas e aplicativos para uso remoto são necessidades frequentes. Ameaça de crises e necessidade de novos serviços tornou a TI um componente indispensável ao setor bancário brasileiro. O desenvolvimento de soluções tecnológicas bancárias no Brasil colocou o país em posição de referência mundial, quando se trata de inovação e qualidade de serviços aos clientes (FEBRABAN, 2012). O desenvolvimento e o nível crescente de utilização de recursos tecnológicos da informação podem ser justificados com a constatação de alguns comportamento observados no setor.

Quadro 5 – Comportamento bancário: atendimento, produtos e serviços

Dado	Referência	Comportamento
Agências e Postos de Atendimento	2002 - 2011	↑ 26%
Contas Correntes	2002 - 2011	↑ 64%
Contas Poupança	2002 - 2011	↑ 69%
População Bancarizada	2002 - 2011	↑ 93%
Correspondentes Bancários	2002 - 2011	↑ 389%
Pontos de Autoatendimento	2002 - 2011	↑ 47%
Contas com Internet Banking	2002 - 2011	↑ 367%
Volume de Transações Bancárias	2007 - 2011	↑ 54%
Volume de Cheques Emitidos	2001 - 2011	↓ 62%

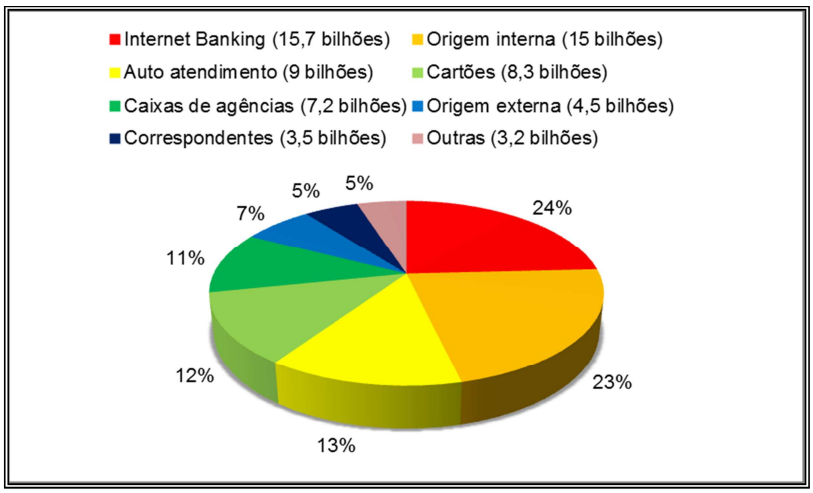
Fonte: Baseado em FEBRABAN (2012).

Na última década houve um aumento significativo da população que utiliza os serviços e produtos bancários. O acesso remoto cresceu exponencialmente. De 2010 para 2011 o número de contas correntes com acesso ao Internet Banking cresceu 11%. Em 2011, 46% do total de contas correntes possuíam acesso remoto, sendo 24% de todas as operações bancárias realizadas no ano, efetuadas neste canal de atendimento. Espera-se que em 2018 aproximadamente 75 bilhões de contas correntes terão acesso via internet (FEBRABAN, 2012).

O número médio de contas correntes por agência bancária, no Brasil em 2011 foi de 4.315, similar a média da Austrália e Estados Unidos. Ferramentas que possibilitam a acessibilidade aos portadores de deficiência têm sido empregadas. Em 2011, 67% dos terminais de autoatendimento estavam adaptados (FEBRABAN, 2012). A redução no volume de cheques emitidos representa a preferência dos usuários por serviços eletrônicos.

O emprego da TI permite ao usuário diversas opções de acesso aos serviços e produtos bancários. As transações podem ser operadas pelo próprio usuário, bem como por um operador. O setor bancário disponibiliza ferramentas tecnológicas que permitem o atendimento das necessidades dos clientes de forma diferenciada.

Figura 16 – Transações bancárias por origem em 2011



Fonte: Baseado em FEBRABEN (2012).

Cabe ressaltar que “origem interna” refere-se às transações relativas a tarifação e impostos, enquanto que “origem externa” corresponde a serviços de débito automático, crédito de salários, proventos de aposentadorias e serviços de cobrança, dentre outros. Estabelecimentos comerciais, correios e casas lotéricas são exemplos de “correspondentes”.

Percebe-se que a maior parte das transações realizadas em 2011 ocorreu fora das agências bancárias. O volume de transações via internet banking e nos postos de autoatendimento, individualmente, superam em duas vezes o número de transações realizadas com a utilização dos caixas das agências. Em 2009, a FEBRABAN (2009) previu mudança no comportamento dos clientes bancários

decorrente dos investimentos realizados na área da TI.

O aumento do número de clientes, serviços, produtos e a diversificação de canais de atendimento, obrigam as instituições financeiras bancárias a realizarem investimentos em TI para garantir a eficiência operacional (prestação dos serviços bancários), a continuidade e a segurança das operações. Entre 2009 e 2011, segundo dados da FEBRARAN (2012), o crescimento dos investimentos em TI pelo setor bancário brasileiro foi de 27% (cerca de R$ 14 bilhões em 2009 e R$ 18 bilhões em 2011).

Os investimentos dos últimos anos foram aplicados em: hardware, telecomunicações e, principalmente, em software (30% do volume investido em 2011). O montante de recursos financeiros direcionados ao desenvolvimento de software tem aumentado a importância do mercado brasileiro no cenário internacional de tecnologia voltada a instituições bancárias. Projeções da FEBRABAN (2012) apontam para um crescimento nos investimentos bancários em tecnologia em 42% até 2015.

Quanto ao ambiente regulatório, o Banco Central do Brasil tem importante papel para o setor. Preocupa-se com a integridade das instituições financeiras brasileiras e acompanha o desenvolvimento de normas internacionais. Várias ações são exigidas às instituições financeiras. Dentre eles está adoção das regras do Comitê de Basileia.

4.2 ANÁLISE DE CRITÉRIOS

O instrumento de coleta de dados utilizado para a análise de critérios para avaliação de riscos partiu da identificação de aspectos relacionados ao:

a) gerenciamento de riscos;
b) responsabilização, prestação de contas e transparência, conceitos ligados ao termo *accountability*.

A revisão da literatura da produção científica e técnica com o enfoque de analisar critérios para avaliação de processos de TI, observando o gerenciamento de riscos e a *accountability*, possibilitou o estabelecimento de relações conceituais de todos os 34 critérios originais do modelo COBIT®. Nesse procedimento de

atualização teórica, outros 34 critérios para avaliação de processos de TI foram levantados, também observados o gerenciamento de riscos e a *accountability*.

Apresentam-se no Quadro 6 todos os 68 critérios, individualmente identificados com aspectos conceituais obtidos com a revisão bibliográfica.

Quadro 6 – Análise de critérios para avaliação de processos de tecnologia da informação

(Continua)

PO – Organização e Planejamento	
PO1	Define o planejamento estratégico de TI (HARISON; BOONSTRA, 2009) e (BUTLER; BUTLER, 2010; CALLAHAN, BASTOS e KEYES, 2004). Harmoniza com a estratégia global (WIKIN e CHENHALL, 2010).
PO2	Define a arquitetura da informação (ALLEN, 2005; SOFTWARE ENGINEERING INSTITUTE, 2010).
PO3	Determina diretrizes da tecnologia (LUNARDI, BECKER e MAÇADA, 2010; ITGI, 2006; GEER, 2004; ALLEN, 2005; MORRIS, GRIPPO E BARSKY, 2012, KUMAR, 2002).
PO4	Define a estrutura de RH de TI e seus relacionamentos (TAROUCO e GRAEML, 2011; THURNER, 2010; DE HAES e VAN GREMBERGEN, 2008).
PO5	Gerencia investimento de TI (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008, PELANDA, 2006; FLORES et al., 2011). Direciona-os à criação de valor (GHEORGE, 2010).
PO6	Comunica as metas e diretrizes gerenciais (ISACA, 2010; SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008; LARSEN, PEDERSON e ANDERSON, 2006; BUTLER e BUTLER, 2010).
PO7	Gerencia os recursos humanos de TI (GHEORGHE, 2010; THURNER, 2010; TAROUCO e GRAEML, 2011; BUTLER e BUTLER, 2010; LUNARDI, BECKER e MAÇADA, 2010). Compromete as pessoas, evidencia responsabilidades e exige prestação e contas (LUNARDI, BECKER e MAÇADA, 2010).
PO8	Gerencia a qualidade dos serviços de TI (ITGI, 2008b; TAROUCO e GRAEML, 2011; GHEORGHE, 2010; VAN GREMBERGEN, DE HAES e GULDENTOPS, 2004.).
PO9	Avalia e gerencia os riscos (SILVA, 2011; WILKIN e CHENHALL, 2010; VERHOEF, 2007; MORRIS, GRIPPO e BARSKY, 2012; ROSA, 2008; SOFTWARE ENGINEERING INSTITUTE, 2010).
PO10	Gerencia os projetos com planos de níveis de qualidade, utilização de recursos e prazos (ITGI, 2007; GHEORGHE, 2010; SILVA, 2011).
AI – Aquisição e Implementação	
AI1	Identifica soluções de automação (ITGI, 2006; WEILL e ROSS, 2006).
AI2	Adquire e mantém software aplicativo (THURNER, 2010; ITGI, 2008b).
AI3	Adquire e mantém a arquitetura tecnológica (THURNER, 2010; HARDY, 2003).
AI4	Desenvolve e mantém procedimentos de TI (GHEORGHE, 2010; ABNT NBR ISO/IEC 27005, 2011).
AI5	Obtém recursos de TI a partir de procedimentos de aquisição (TAROUCO e GRAEML, 2011).
AI6	Gerencia mudanças em equipamentos, arquitetura, sistemas e processos (KNORST, 2010; GHEORGHE, 2010).
AI7	Instala e certifica soluções e mudanças (ITGI, 2006).
ES – Entrega e Suporte	
ES1	Define níveis e mantém os acordos de níveis de serviços com usuários internos e externos (PIRES, 2011; ITGI, 2006).
ES2	Gerencia os serviços de terceiros (BUTLER e BUTLER, 2010; ABNT NBR ISO/IEC 27005, 2011).
ES3	Gerencia desempenho e capacidade da TI (APREDA, 2011; ITGI, 2006; ALLEN, 2005; MATITZ e BULGACOV, 2011; HARDY, 2003; ACCOUNTABILITY, 2008).
ES4	Garante a continuidade dos serviços (ITGI, 2006).
ES5	Garante a segurança dos sistemas (CALDER e WATKINZ, 2008; GEER, 2004; LAGZDINS e SLOKA, 2012; BART e TUREL, 2010; ISACA, 2011).
ES6	Identifica e aloca custos (BOWEN, CHEUNG e ROHDE, 2007; MORRIS, GRIPPO e BARSKY, 2012; GEER, 2004).
ES7	Educa e treina os usuários e equipe de TI (ITGI, 2006).
ES8	Gerencia a central de serviços e incidentes de TI (WEIL e ROSS, 2006; ITGI, 2008b).
ES9	Gerencia a configuração de software e hardware (ISO/IEC 27002, 2005).
ES10	Gerencia os problemas tecnológicos e respectivos incidentes (FLORES et al., 2011).
ES11	Gerencia os dados quanto à disponibilização, ao arquivamento e ao descarte (GHEORGHE, 2010; VAN GREMBERGEN, DE HAES e GULDENTOPS, 2004; LAGZDINS e SLOKA, 2012).
ES12	Gerencia a infraestrutura de TI (ITGI, 2008a; VERHOEF, 2007; TAROUCO e GRAEML, 2011; GHEORGE, 2010).
ES13	Gerencia operações de TI (WEIL e ROSS, 2006; ITGI 2008a; WILKIN e CHENHALL, 2010).

(Continuação)

MO – Monitoramento		
MO1	Monitora e avalia a desempenho dos processos de TI (SYMONS, 2005; DE HAES e VAN GREMBERGEN, 2008; GHEORGHE, 2010).	
MO2	Monitora e avalia o controle interno (ABNT NBR ISO/IEC 27005, 2011, ITGI, 2007; MORRIS, GRIPPO e BARSKI, 2012).	
MO3	Assegura a conformidade aos requisitos externos (ROBINSON, 2005; KUMAR, 2002; ITGI, 2006; PEREIRA e SILVA, 2012; TAROUCO e GRAEML, 2011). Atribui sanções ao identificar ocorrências de não conformidade (MAIZLISH e HANDLER, 2005). Responsabiliza ações frente a elementos regulatórios (políticas e estratégias) (ACCOUNTABILITY, 2008; BUTLER e BUTLER, 2010).	
MO4	Fornece modelo de governança de TI (WILKIN e CHENHALL, 2010; CALDES e WATKINS, 2008; LAGZDINS, 2012; BUTLER e BUTLER, 2010; GHEORGHE, 2010).	
GTI – Governança de TI		
Adequação	GTIA1	Segue políticas, procedimento, processos e controles da estratégia de proteção e segurança (GEER, 2004).
	GTIA2	Adequa os custos dos investimentos em segurança aos níveis de riscos assumidos (probabilidade, frequência e gravidade das possíveis ocorrências) (GEER, 2004).
	GTIA3	Compara o custo da reconstrução do ativo com o custo de sua proteção (GEER, 2004).
Conformidade	GTIC1	Garante conformidade legal e regulamentar com requisitos internos e externos (ALLEN, 2005).
	GTIC2	Protege o investimento e os interesses dos investidores (LAGZDINS e SLOKA, 2012).
	GTIC3	Garante a segurança dos dados do negócio (LAGZDINS e SLOKA, 2012).
	GTIC4	Reestabelece confiança, integridade e responsabilidade após períodos de crise (LAGZDINS, 2012).
Ética	GTIE1	Permite a inexistência de conflitos entre principal e agente (ALLEN, 2005).
	GTIE2	Envolve princípios de honestidade, integridade, fairness e preocupação com o outro (BELLO, 2012).
Capacidade de Resposta	GTICR1	Coordena ações para impedir ou controlar ameaças à segurança (ITGI, 2007; ALLEN, 2005).
	GTICR2	Guia as ações para a continuidade do negócio (ITGI, 2007; ALLEN, 2005).
	GTICR3	Recupera efeitos negativos de situações indesejáveis (ITGI, 2007; ALLEN, 2005).
	GTICR4	Gerencia crises e formula planos de gestão de incidentes (ITGI, 2007; ALLEN, 2005).
Gestão de Riscos	GTIGR1	Define, supervisiona e monitora a eficácia estratégica na proteção das informações (ALLEN, 2005; MORRIS, GRIPPO e BARSKY, 2012).
	GTIGR2	Assegura resposta aos riscos potenciais (ALLEN, 2005; MORRIS, GRIPPO e BARSKY, 2012).
	GTIGR3	Identifica danos, ameaças e vulnerabilidades (ALLEN, 2005; MORRIS, GRIPPO e BARSKY, 2012; FLORES et al., 2011).
	GTIGR4	Mensura custos de perdas, danos ou falhas no acesso de informações (ALLEN, 2005; MORRIS, GRIPPO e BARSKY, 2012).
	GTIGR5	Mensura custos de reconstrução de informações (ALLEN, 2005; MORRIS, GRIPPO e BARSKY, 2012).
	GTIGR6	Mensura custos de desenvolvimento de controles (ALLEN, 2005; MORRIS, GRIPPO e BARSKY, 2012).
	GTIGR7	Garante redução de riscos de perdas, erros, fraudes, não conformidade, reputação ou perdas financeiras (COSTA, 2011; PELANDA, 2006; BART e TUREL, 2010; FLORES et al., 2011).
	GTIGR8	Inibe uso indevido ou desvios de recursos (COSTA, 2011; ITGI, 2006).
	GTIGR9	Inibe fraudes contábeis (COSTA, 2011; ITGI, 2006).
	GTIGR10	Reduz falhas e riscos de segurança (PELANDA, 2006; ITGI, 2006; SPEARS e BARKI, 2010).
	GTIGR11	Controla ameaças e vulnerabilidades com políticas, processos, procedimentos e equipamentos (ABNT NBR ISO/IEC 27002, 2005; FLORES et al., 2011).
ACC – *Accountability*		
Responsabilização	ACCR1	Responsabiliza ações e tomadas de decisão quanto à supervisão, monitoramento, controle e gestão da TI (ITGI, 2006; ITGI, 2007; VAN GREMBERGEN, DE HAES, 2009; COMITE, 2012).
	ACCR2	Acompanha o processo de melhoria das normas e práticas organizacionais internacionais (APREDA, 2011).
	ACCR3	Responsabiliza os envolvidos na geração de informações (ACCOUNTABILITY, 2008).
	ACCR4	Garante qualidade, confiabilidade e segurança às informações geradas (VASARHELYI e ALLES, 2008; O'CONNOR e MARTINSONS, 2006; ITGI, 2006; TAROUCO e GRAEML, 2011; BART e TUREL, 2010; LUNARDI, 2008; GHEORGHE, 2010).

(Conclusão)

ACC – *Accountability*		
Prestação de Contas	ACCP1	Gera informações significantes para o cumprimento dos objetivos, estratégias e padrões de desempenho (ACCOUNTABILITY, 2008).
	ACCP2	Gera informações precisas, tempestivas e relevantes (VASARHELYI e ALLES, 2008; O'CONNOR e MARTINSONS, 2006; ITGI, 2006; TAROUCO e GRAEML, 2011; BART e TUREL, 2010; LUNARDI, 2008; GHEORGHE, 2010).
	ACCP3	Observa a interdependência entre os recursos de TI (pessoas, aplicações, infraestrutura e informações) na gestão dos recursos de TI (THURNER, 2010).
Transparência	ACCT1	Garante acesso aos usuários dos serviços de TI (PIRES, 2010; O'CONNOR e MARTINSONS, 2006).
	ACCT2	Emite relatórios com transparência nas informações para os diversos usuários (PELANDA, 2006).
	ACCT3	Atende as necessidades de todos os usuários dos produtos e serviços da TI (ACCOUNTABILITY, 2008).

Fonte: Adaptado de ITGI (2007).

Os quatro domínios do modelo COBIT® tradicional (Organização e Planejamento – PO, Aquisição e Implementação – AI, Entrega e Suporte – ES e Monitoramento – MO) foram mantidos no processo de revisão dos critérios de processos de TI. Na sequência foram acrescentados dois outros tópicos: Governança de TI – GTI (adequação, conformidade, ética, capacidade de resposta e gestão de riscos) e *Accountability* – ACC (responsabilização, prestação de contas e transparência). O tópico Governança de TI abrangeu os elementos do gerenciamento de riscos e o tópico *Accountability*, por sua vez, envolveu critérios relacionados à responsabilização, à prestação de contas e à transparência.

Individualmente, cada critério foi analisado com o propósito de se identificar e estabelecer relações teóricas. Todos os 68 critérios inicialmente relacionados foram confrontados com a revisão da literatura. Em uma segunda análise, efetuou-se a seleção, união e/ou desmembramento de critérios listados. Verificaram-se relações significativas entre alguns critérios, o que possibilitou a ação de junção. Em outros casos percebeu-se a necessidade de segregação (em dois ou mais critérios) para compreender os quesitos conceituais. Gerenciamento de risco e *accountability* também foram utilizados como balizadores dessa análise.

Procedeu-se o descarte dos critérios: PO1, PO2, PO3, PO8, AI1, AI2, AI6, ES6 e ES9. Fundamentando-se da revisão da literatura, o descarte baseou-se na classificação destes critérios como secundários para a área focal de gerenciamento de riscos (ITGI, 2007, p. 177).

Além da seleção, unificaram-se alguns critérios, observando as semelhanças entre eles. Esta ação possibilitou estabelecer paridades e permitiu o agrupamento de diversos critérios, relacionados a seguir.

Quadro 7 – Agrupamento de critérios por paridade

Critérios Agrupadores	Enfoque	Critérios Incorporados
PO4	Define e capacitada estrutura de RH para documentação, atendimento de demandas e incidentes.	PO7 e ES7
PO5	Gerencia investimentos em recursos para infraestrutura, segurança, proteção de ativos e desenvolvimento de controles (mensurando e alocando custos, inibindo desvios e usos indevidos).	AI3, AI5, ES12, GTIA2, GTIA3, GTIC2, GTIGR4, GTIGR5, GTIGR6 e GTIGR8
PO6	Comunica metas, políticas e diretrizes à equipe de TI para estabelecer responsabilidades e exigir prestação de contas.	ACCP2
PO9	Gerencia ameaças, incidentes e vulnerabilidades, corretiva e preventivamente.	ES8, ES10, GTICR1, GTICR3, GTIGR3, GTIGR7, GTIGR9, GTIGR10 e GTIGR11
ES3	Monitora e avalia operações, processos, procedimentos, capacidade e desempenho da TI.	AI4, ES13 e MO1
ES5	Garante qualidade, confiabilidade e segurança dos sistemas e das informações.	GTIC3 e ACCR4
ES11	Gerencia acesso, arquivamento e descarte de dados, fornecendo produtos e serviços com transparência nas informações para atender às necessidades dos usuários.	ACCT2, ACCR3 e ACCT3
GTICR2	Guia as ações para a continuidade do negócio.	ES4

Fonte: Elaborado pelo autor.

A redução de critérios por similaridade pode ser exemplificada com a união dos critérios PO4, PO7 e ES7. Originalmente, PO4 compreende a estrutura de RH e as relações com as demais áreas. PO7 volta-se para o gerenciamento da equipe de RH, enquanto que ES7 trata do treinamento de usuários e da equipe de TI. A união de todos esses critérios gerou nova redação, mantendo-se o primeiro código PO4: Define e capacita a estrutura de RH para documentação, atendimento de demandas e incidentes. Os demais critérios (Quadro 7) sofreram tratamento semelhante.

O processo de junção, alinhado com a revisão da literatura, identificou a necessidade de desmembramento de três quesitos (ES1, ES2 e MO3). ES1 foca a entrega e suporte de serviços internos, ES2 está relacionado aos serviços externalizados e o MO3 abrange aspectos de conformidade aos requisitos externos. Para abranger a *accountability*, esses critérios ganharam enfoques distintos, ligados à responsabilização, à prestação de contas e à transparência.

Partindo de uma revisão teórica acerca de critérios para avaliação de

processos de TI, voltados para o gerenciamento de riscos e *accountability*, após realização de análise descrita nesta seção, elaborou-se um quadro contendo os 32 critérios utilizados para categorizar os Relatórios de Gerenciamento de Riscos, na fase da investigação.

Quadro 8 – Critérios para avaliação de processos de tecnologia da informação revisados

(Continua)

Código	Descrição
PO4	Define e capacita estrutura de RH para documentação, atendimento de demandas e incidentes.
PO5	Gerencia investimentos em recursos para infraestrutura, segurança, proteção de ativos e desenvolvimento de controles (mensurando e alocando custos, inibindo desvios e usos indevidos).
PO6	Comunica metas, políticas e diretrizes à equipe de TI para estabelecer responsabilidades e exigir prestação de contas.
PO9	Gerencia ameaças, incidentes e vulnerabilidades, corretiva e preventivamente.
PO10	Usa plano: de nível de qualidade, utilização de recursos e prazos para gerenciar projetos de TI.
AI7	Instala e certifica novas soluções e mudanças.
ES1A	Define responsabilização pela entrega e suporte dos serviços de TI.
ES1B	Define transparência na entrega e suporte dos serviços de TI.
ES1C	Define prestação de contas pela entrega e suporte dos serviços de TI.
ES2A	Gerencia (responsabiliza) os serviços de TI realizados por terceiros.
ES2B	Gerencia (exige transparência) nos serviços de TI realizados por terceiros.
ES2C	Gerencia (exige prestação de contas) dos serviços de TI realizados por terceiros.
ES3	Monitora e avalia operações, processos, capacidade e desempenho da TI.
ES5	Garante qualidade, confiabilidade e segurança dos sistemas e das informações.
ES11	Gerencia acesso, arquivamento e descarte de dados, fornecendo produtos e serviços com transparência nas informações para atender às necessidades dos usuários.
MO2	Monitora e avalia o controle interno.
MO3A	Responsabiliza e indica sanções quanto à conformidade aos requisitos externos.
MO3B	Exige transparência quanto à conformidade aos requisitos externos.
MO3C	Exige prestação de conta das ações e decisões quanto à conformidade aos requisitos externos.
MO4	Fornece modelo de governança de TI.
GTIA1	Segue políticas, procedimento, processos e controles da estratégia de proteção e segurança.
GTIC1	Garante conformidade legal e regulamentar com requisitos internos e externos.
GTIC4	Reestabelece confiança, integridade e responsabilidade após períodos de crise.
GTIE1	Permite a inexistência de conflitos entre o principal e o agente.
GTIE2	Envolve princípios de honestidade, integridade, fairness e preocupação com o outro.
GTICR2	Guia as ações para a continuidade do negócio.

(Conclusão)

Código	Descrição
GTICR4	Formula plano para gestão de crises e incidentes.
GTIGR1	Define, supervisiona e monitora a eficácia estratégica na proteção das informações.
ACCR1	Responsabiliza ações e tomadas de decisão quanto à supervisão, monitoramento, controle e gestão da TI.
ACCR2	Acompanha o processo de melhoria das normas e práticas internacionais.
ACCP1	Gera informações significantes para o cumprimento dos objetivos, estratégias e padrões de desempenho.
ACCP3	Observa a interdependência entre os recursos de TI (pessoas, aplicações, infraestrutura e informações) na gestão dos recursos de TI.

Fonte: Adaptado de ITGI (2007).

Enquanto que PO4, PO5, PO9, PO10, AI7, ES3, ES5, ES11, MO2, MO4, GTIA1, GTIC1, GTICR2, GTICR4, GTIGR1, ACCR2, ACCP1 e ACCP3 estão mais voltados para o gerenciamento de riscos, PO6, ES1A, ES1B, ES1C, ES2A, ES2B, ES2C, MO3A, MO3B, MO3C, GTIC4, GTIE1, GTIE2 e ACCR1 estão mais voltados para a *accountability*.

Dessa forma, para atender aos conceitos relacionados à *accountability* e gerenciamento de riscos, evidenciados na revisão da literatura, atualizou-se a lista de critérios tradicionais do COBIT® 4.1, reelaborando o rol de critérios. Tanto a união quanto a segregação de critérios visou a atender quesitos específicos de avaliação: o gerenciamento de riscos, a transparência, a responsabilização e a prestação de contas. Essa atualização contribuiu com a Análise de Conteúdos dos relatórios analisados descrita na seção seguinte.

4.3 ANÁLISE DE CONTEÚDO

A Análise de Conteúdo dos Relatórios de Gerenciamento de Riscos compreendeu a segunda fase da análise dos dados. Os documentos selecionados, conforme descritos na Seção 3.1, foram investigados a partir da lista de critérios (Quadro 8). Identificou-se a ocorrência desses critérios nos documentos analisados. Na sequência aplicou-se a Análise Lexical, percebendo-se as relações entre os elementos textuais dos relatórios.

Observando-se a obrigatoriedade da divulgação de informações relativas ao gerenciamento de riscos por todas as instituições financeiras bancárias que desenvolvem atividades no Brasil, constituem-se fonte de dados os Relatórios de

Gerenciamento de Riscos publicados pela amostra desta pesquisa referentes ao terceiro trimestre de 2012. De acordo com a Circular BACEN n. 3.477 (2009) as instituições financeiras devem apresentar detalhamento acerca dos sistemas, processos e controles internos utilizados no gerenciamento de riscos: operacional, crédito, mercado e liquidez.

Devem descrever os objetivos, políticas e estratégias de gerenciamento, bem como formas de avaliação, mensuração e mitigação dos riscos. A periodicidade mínima de atualização dos relatórios deve ser:

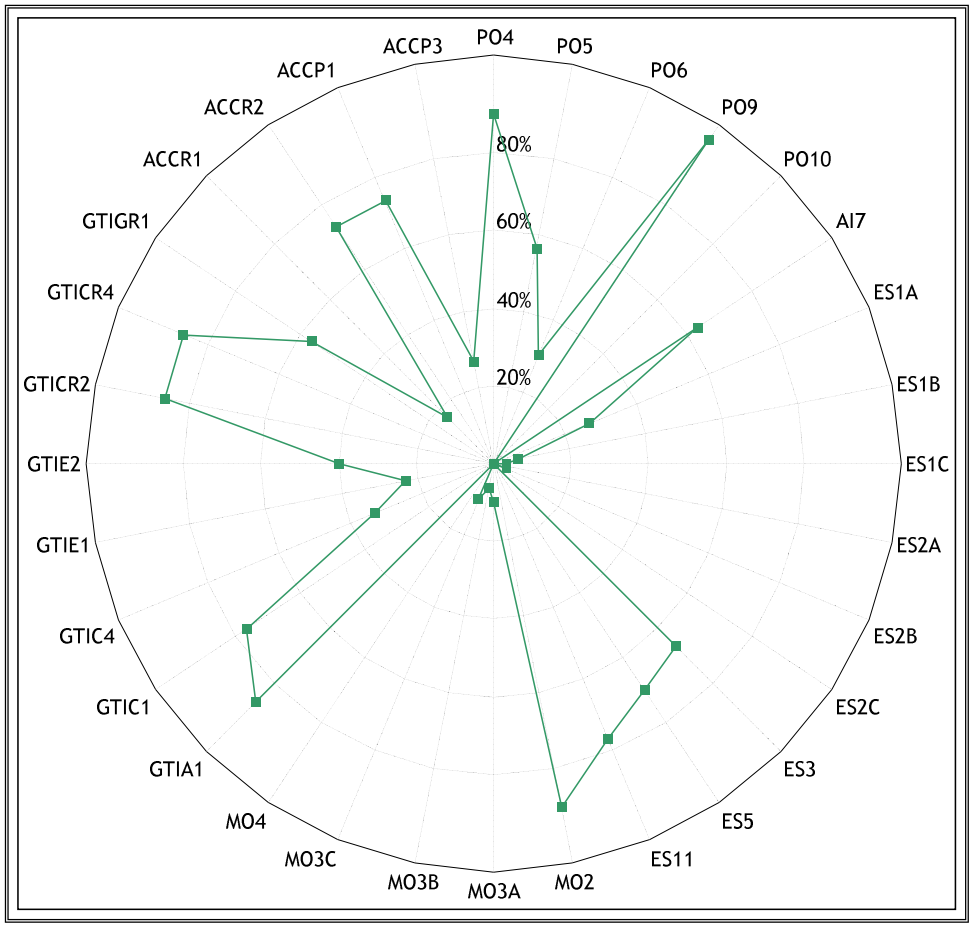
a) anual para informações qualitativas;
b) trimestral para informações de natureza quantitativa.

Constata-se que é prática comum às maiores instituições/conglomerados financeiros que operam no Brasil, a publicação trimestral também das informações qualitativas. Os relatórios utilizados nesta análise foram buscados nos websites oficiais de cada organização integrante da amostra.

Como já mencionado anteriormente, foram selecionados os relatórios referentes ao terceiro trimestre de 2012 por este ser o período mais recente de divulgação. Como pode ser evidenciado, não é prática comum a todas as instituições/conglomerados disponibilizar os relatórios de períodos anteriores, delimitando-se a investigação nos relatórios desse período.

Os relatórios selecionados possuem redação na língua portuguesa e são disponibilizados em arquivos no formato PDF. Todos foram integralmente lidos e categorizados pelos critérios de avaliação de processos de TI, apresentados no Quadro 8. Após leitura, para aumentar a segurança na identificação dos critérios, buscou-se por palavras ou expressões no texto com auxilio da ferramenta de busca do software *Adobe® Reader® X – Versão 10.1.6*. O mapa da categorização dos relatórios segundo os critérios pode ser consultado no Apêndice A. A incidência de cada critério encontrado nos documentos analisados possibilitou a construção da Figura 17.

Figura 17 – Frequência de critérios nos Relatórios de Gerenciamento de Riscos



Fonte: Elaborado pelo autor.

Os critérios com maior incidência foram: PO4, PO9, MO2, GTIA1, GTICR2 e GTICR4. Esses critérios estão relacionados: à definição e capacitação de estrutura de RH; gerenciamento de ameaças, incidentes e vulnerabilidades de forma preventiva e corretiva; monitoramento e avaliação dos controles internos; observância das políticas, procedimentos, processos e controles da estratégia de proteção e segurança; direcionamento de ações para a continuidade do negócio; e formulação de planos para gestão de crises e incidentes. Todos estão diretamente relacionados com o gerenciamento de riscos.

PO10, ES1B, ES1C, ES2A, ES2B, ES2C, MO3A, MO3B, MO3C e MO4 são critérios com baixa frequência. Destes, apenas PO10 (utilização de planos para níveis de qualidade, recursos e prazos em projetos de TI) refere-se ao gerenciamento de risco. Os demais estão vinculados aos conceitos de

responsabilização, prestação de contas e transparência. Evidencia-se maior presença de critérios do gerenciamento de riscos, comparada aos ligados a *accountability*.

Ao verificar a frequência dos critérios, levando-se em conta a evidenciação dos critérios por tipo de composição organizacional (conglomerado ou instituição independente), percebe-se que a distribuição relativa é semelhante nas duas composições. O mesmo pode ser verificado no tipo de controle (público, privado nacional ou privado estrangeiro).

4.4 ANÁLISE LEXICAL

Para a realização da Análise Lexical, os Relatórios de Gerenciamento de Riscos, obtidos em arquivos digitais no formato PDF foram individualmente convertidos inicialmente para o formado DOCX. Executou-se a conversão com a ferramenta online disponível no endereço <http://convertonlinefree.com/PDFToWORDEN.aspx>. Escolheu-se essa ferramenta por possibilitar a conversão sem alteração de formatos ou exclusão de dados, mantendo inclusive as ilustrações.

A conversão para o formato DOCX foi necessária para o tratamento uniforme de todos os relatórios. Os conteúdos dos arquivos individuais foram agrupados em um único arquivo, contendo 1.067 páginas de texto, sendo que algumas ações foram executadas:

a) exclusão de todos símbolos “:”, “<” e “>” do texto;
b) exclusão de todos os cabeçalhos e rodapés que continham: nome do relatório, nome da instituição/conglomerado, período de abrangência e paginação;
c) exclusão de sumários e ilustrações;
d) leitura do texto para correção de palavras que foram fragmentadas no processo de conversão dos formatos PDF para DOCX;
e) revisão ortográfica e gramatical;
f) balizamento dos relatórios;
g) conversão do texto para o formato TXT.

A exclusão de símbolos utilizados pelo software *Sphinx Survey* no

balizamento dos textos foi necessária para que o software pudesse reconhecer os comandos. A ferramenta “Localizar e Substituir” do Microsoft Word executou a operação. Dados dos cabeçalhos, rodapés e do sumário podem distorcer a Análise Lexical em função de sua repetição. A exclusão desses elementos é recomendada.

O processo de conversão de formatos pode separar sílabas de uma mesma palavra, formando outras palavras distintas. Com isso procedeu a leitura textual com o objetivo de correção ortográfica. Buscando garantir a integridade do texto, após a leitura, usou-se a ferramenta de verificação ortográfica e gramatical do Microsoft Word.

Encerrou-se a preparação do texto com o balizamento dos relatórios (identificação dos relatórios a partir de codificação específica indicada pelo software, o que permite a análise de dados por variáveis) e conversão para o formato TXT, procedimentos necessários para o processamento dos dados. O balizamento utilizou os seguintes elementos: nome da instituição/conglomerado; tipo de composição; tipo de controle; volume do ativo total; volume de depósitos totais; número de funcionários; número de agências; e conteúdo. Para facilitar a análise, cada um dos 32 critérios também foram colocados como balizadores.

A conversão final para formato TXT foi efetuada pelo Microsoft Word, com a codificação de texto padrão do Windows, que exclui todos os formatos, imagens e objetos do texto. Após a importação dos relatórios no software *Sphinx Survey* – Edição Léxica, os dados foram analisados.

Ao ser importado para o software o texto apresentou as seguintes características: 133.802 palavras no texto; 8.150 léxicos (palavras diferentes); 3.671 palavras únicas. Procedeu-se então, alguns passos para o tratamento do texto para posterior análise do conteúdo:

Passo 1 – verificou-se a existência de palavras longas. Estas foram desmembradas, agrupadas ou excluídas.

Passo 2 – as palavras instrumentais foram ignoradas. Utilizou-se a ferramenta do software “Reduzir”, dentro da funcionalidade “Análise Lexical”. Essa ação efetua limpeza de 582 palavras instrumentais, já cadastradas em um dicionário.

Passo 3 – ainda na ferramenta “Reduzir”, ignorou-se as palavras com menos de três letras. Antes de executar essa operação, analisou-se na relação de palavras do texto, em ordem de quantidade de sílabas, a qualidade das palavras, para assegurar que nenhuma palavra com duas letras contendo conteúdo fosse ignorada.

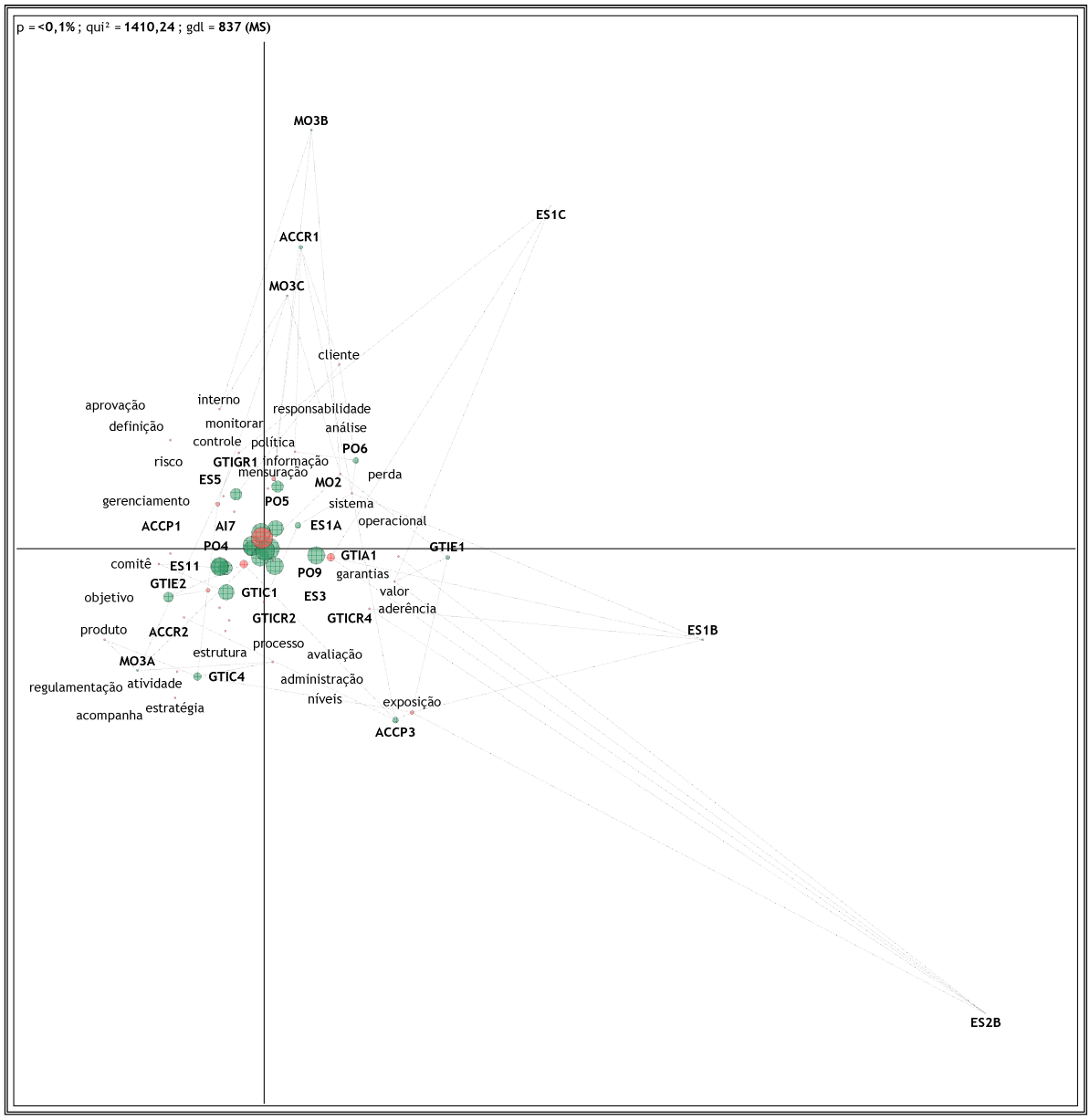
Passo 4 – com auxílio da ferramenta “Reagrupar”, opção “Reagrupar automaticamente por raiz”, as palavras de mesma raiz (seis caracteres) foram agrupas. Essa ação gerou 1.129 agrupamentos, que foram individualmente revisados.

Passo 5 – manualmente foram analisadas as palavras e agrupamentos restantes, chegando-se em um texto com as seguintes características: 37.993 palavras com conteúdo; 54.037 palavras ignoradas (resultantes da redução automática dos passos 2 e 3); 41.772 palavras deletadas (resultantes do processo manual de exclusão de léxicos sem conteúdo dos passos 1 e 5); 586 léxicos reduzidos; e 41 palavras únicas.

Com o objetivo de facilitar a Análise Lexical, foram efetuadas algumas “Recodificações”, que são agrupamentos de determinados léxicos para facilitar a análise. Criou-se: “Léxico_50%” (contendo 50% da incidência dos léxicos mais frequentes), “Léxicos_Risco”, “Léxicos_Estratégia”, “Léxicos_Desempenho”, “Léxicos_TI”, “Léxicos_Segurança”, “Léxicos_Responsabilidade”, “Léxicos_Transparência”, “Léxicos_Prestação_de_Contas” (todos envolvendo os léxicos referentes a cada conceito, presentes no Quadro 1), “Gerenciamento_de_Riscos” e “Accountability” (contendo os léxicos encontrados nos conceitos encontrados na revisão da literatura).

As frequências dos principais léxicos e dos critérios que mais apareceram nos relatórios podem ser observadas na Figura 18. As influências entre as variáveis são representadas pelas ligações. Para melhor visualização efetuou-se recorte em 50% dos léxicos presentes.

Figura 18 – Mapa de significância: critérios e léxicos (50%)



Legenda: Software *Sphinx Survey* – Edição Léxica.

Fonte: Elaborado pelo autor.

Ao realizar o teste Qui-Quadrado encontrou-se “p=<0,001”, o que representa significância nas relações, ou seja, há dependência entre as variáveis. O teste Qui-Quadrado verifica se há ou não independência dos termos da Análise de Conteúdo. Para tornar válido o teste Qui-Quadrado, os critérios que não apresentaram incidência (PO10, ES2A, ES2C e MO4) foram excluídos da análise.

Do total de 586 léxicos encontrados após tratamento aplicado ao texto (reduções e reagrupamentos), optou-se por representar 50% para melhor

visualização. Os léxicos mais frequentes do texto analisado (superior a 500 incidências), em ordem foram: risco, gerenciamento, operacional, controle, exposição, política e processos. No mapa, cada variável está ilustrada com círculos de tamanho proporcional à incidência observada.

Os critérios MO3B, ES1B, ES1C e ES2B foram os critérios que mais exerceram interferências sobre as outras categorias. Eles tratam da responsabilização quanto à conformidade aos requisitos externos; transparência e prestação de contas quanto à entrega e suporte de serviços de TI; e transparência nos serviços de TI externalizados. Quanto mais distanciada a posição de uma categoria do centro do gráfico, maior é a influência exercida sobre as propriedades dos fatoriais. Quanto mais próximas do centro, menor ou nula é a sua influência (SPHINX BRASIL, 2007).

As relações mais significativas entre os critérios e os léxicos são apuradas segundo a verificação das contribuições absolutas. O critério MO3B possui relação significativa com os léxicos: “política” (ocorrência = 39; percentual de citação = 3,3%; contribuição absoluta = 7,31), “perda” (oc. = 44; cit. = 3,8%; c.a. = 15,62) e “interno” (oc. = 39; cit. = 3,3%; c.a. = 7,31). A responsabilização por conformidade aos requisitos externos relaciona-se significativamente com aspectos internos, relacionados à política e a perdas.

ES1B relaciona-se significativamente com: “sistema” (oc. = 35; cit. = 3,4%; c.a. = 16,91), “aderência” (oc. = 32; cit. = 3,1%; c.a. = 25,05), “operacional” (oc. = 102; cit. = 10,0%; c.a. = 5,37) e “exposição” (oc. = 48; cit. = 4,7%; c.a. = 5,96). A transparência na entrega e suporte de serviços de TI possui significância com sistema, com a adesão, com a exposição e aspectos operacionais.

ES1C tem relação destacada com os léxicos: “valor” (oc. = 16; cit. = 3,6%; c.a. = 4,11), “operacional” (oc. = 59; cit. = 13,2%; c.a. = 15,48) e “responsabilidade” (oc. = 15; cit. = 3,4%; c.a. = 4,89). A prestação de contas na entrega e suporte de serviços de TI está significativamente relacionada com responsabilidade, operacional e valor. A estreita ligação entre prestação de contas e responsabilidade apontada por Landrum e Daily (2012), Pereira e Silva (2012) e Feltus, Petit e Dubois (2009) fica evidenciada na análise de significância deste critério.

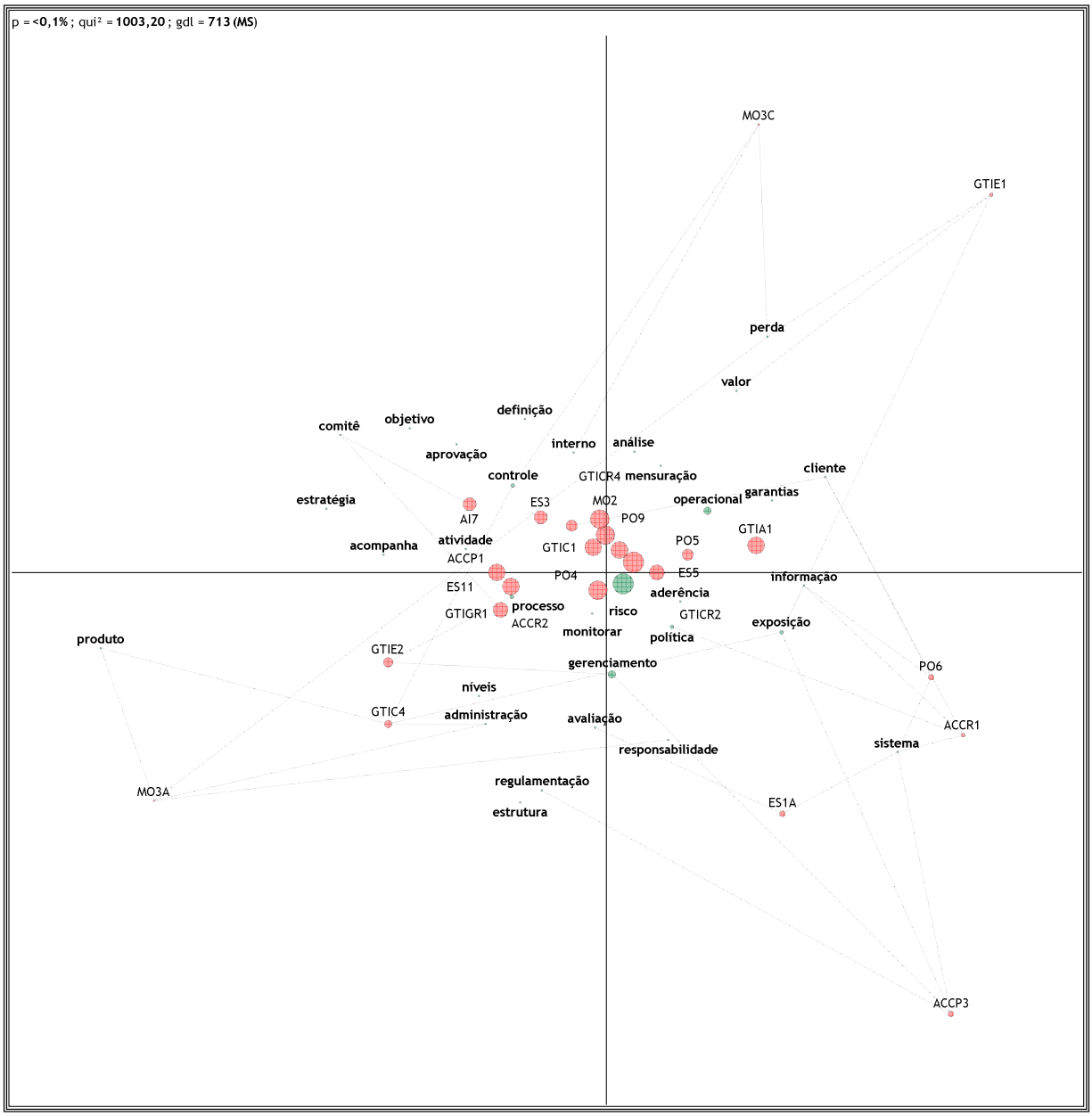
ES2B relaciona-se com: “valor” (oc. = 27; cit. = 5,3%; c.a. = 22,66), “operacional” (oc. = 57; cit. = 11,1%; c.a. = 6,43), “garantia” (oc. = 26; cit. = 5,1%; c.a. = 26,13), “exposição” (oc. = 45; cit. = 8,8%; c.a. = 46,11) e “aderência” (oc. = 13;

cit. = 2,5%; c.a. = 5,59). A transparência nos serviços de TI externalizados relaciona-se ao valor, operacional, garantia, exposição e aderência. Há necessidades de garantias de geração de valor nos serviços operacionais prestados por terceiros, e isso está relacionado com a transparência.

A ocorrência refere-se à frequência absoluta em que o léxico foi encontrado para cada critério analisado. O percentual de citação refere-se à frequência relativa do léxico. Calcula-se com a divisão da frequência absoluta do léxico (por critério) pela soma das frequências absolutas de todos os léxicos do critério. A contribuição absoluta refere-se ao desvio da contribuição absoluta das variáveis.

Com a finalidade de verificar o comportamento das relações entre os critérios e os léxicos (50%), foram excluídos da análise os critérios MO3B, ES1B, ES1C e ES2B, apresentando-se novo Mapa. A exclusão desses critérios evidencia uma nova classe de influências exercidas, mantendo-se a significância das relações (“p<0,001” no teste de independência do Qui-Quadrado).

Figura 19 – Mapa de significância: critérios reduzidos e léxicos (50%)



Legenda: Software *Sphinx Survey* – Edição Léxica.

Fonte: Elaborado pelo autor.

A Figura 19 mostra que com a exclusão das distorções provocadas pelas influências dos quatro critérios anteriormente mencionados, novos critérios passam a exercer maior influência. São eles: MO3A (responsabilização quanto à conformidade aos requisitos externos – relação significante com “produto” (contribuição absoluta 25,82), “perda” (5,37), “administração” (11,23) e responsabilidade (4,69)), MO3C (prestação de contas de ações e tomadas de decisão quanto à conformidade aos

requisitos externos – “controle” (21,31), “interno” (5,15) e “perda” (17,45)), GTIE1 (conflitos entre principal e agente – “exposição” (9,36), “valor” (19,40) e “perda” (16,90)) e ACCP3 (percepção da interdependência entre os recursos de TI – “gerenciamento” (7,95), “regulamentação” (4,64), “exposição” (20,67) e “sistema” (3,94)).

Constatam-se nas duas formas de análise que os critérios associados aos conceitos ligados à *accountability* (responsabilização, prestação de contas e transparência) foram os critérios que mais exercem influência sobre os léxicos nos Relatórios de Gerenciamento de Riscos analisados.

Analisando-se os léxicos de forma segmentada, por tipo de composição (instituição independente ou conglomerado) e por tipo de controle (público, privado nacional ou privado estrangeiro), a incidência relativa dos léxicos nos relatórios não mostrou significativa diferença. Analisando-se individualmente cada um dos 32 critérios inicialmente definidos e os conceitos que nortearam o estudo, observam-se relações significativas. Destacam-se a seguir as principais relações encontradas. Encontram-se nos Apêndices B, C, D, E, F, G, H e I os resultados completos.

Quadro 9 – Níveis de relação entre critérios e conceitos

(Continua)

Critério	Conceitos							
	Risco	**Estratégia**	**Desempenho**	**TI**	**Segurança**	**Responsabilidade**	**Transparência**	**Prestação de contas**
PO9								
PO4	S	S	MS	S	MS	MS	MS	MS
PO5	MS	MS	MS	MS	MS		S	MS
PO6	MS	MS	MS	MS	MS	MS		
PO10								
AI7	MS	MS	MS	MS	MS	MS	MS	MS
ES1A	MS	MS	MS	MS	MS	MS	S	S
ES1B		MS	MS	MS	MS	MS	S	
ES1C		MS	MS	MS	MS	MS	MS	MS
ES2A								
ES2B			MS	MS	MS		MS	
ES2C								
ES3		MS	MS	MS	MS	MS	S	MS

(Conclusão)

Critério	Conceitos							
	Risco	Estratégia	Desempenho	TI	Segurança	Responsabilidade	Transparência	Prestação de contas
ES5	S	MS	MS	MS	MS	MS		
ES11		MS	MS		MS	MS	MS	S
MO2		S	MS	MS		MS		MS
MO3A	MS	MS	MS	MS	MS	MS	MS	MS
MO3B	S				MS	MS		MS
MO3C				MS	MS	S		
MO4								
GTIA1		MS	MS	MS	MS	MS		MS
GTIC1	MS	MS	S	S	MS	MS	MS	MS
GTIC4	MS	S	MS	S	S		S	S
GTIE1	S	MS	MS	MS	MS	MS	MS	MS
GTIE2		MS	MS	MS	MS	MS	MS	MS
GTICR2					S	MS		MS
GTICR4		S		MS	MS	MS	S	MS
GTIGR1		S	S			MS	MS	MS
ACCR1	S	MS	MS	MS	MS	MS		MS
ACCR2	S	S	MS	MS	MS	MS	MS	S
ACCP1			MS	MS	MS	S		
ACCP2	S		MS	MS	MS	MS	S	MS

Fonte: Elaborado pelo autor.

As relações “muito significantes” (MS) são as que obtiveram “p<0,01” ou “p<1%”. Já as relações “significantes” (S) possuem “0,01<p<0,05” ou “1%<p<5%”, no teste Qui-Quadrado. Os critérios foram analisados individualmente com o teste Qui-Quadrado. Os critérios PO4, AI7, ES1A, MO3A, GTIC1, GTIC4, GTIE1 e ACCR2 têm, segundo identificado nos Relatórios de Gerenciamento de Riscos da amostra, significância com todos os conceitos delimitados para a pesquisa. Estes estão relacionados ao gerenciamento de riscos e à *accountability*. Os componentes desses critérios estão relacionados à:

a) estrutura e capacitação de RH;
b) instalação e certificação de novas soluções;
c) responsabilização pela entrega e suporte de serviços e pela conformidade aos requisitos externos;
d) garantia da conformidade legal e regulamentar;

e) reestabelecimento de confiança, integridade e responsabilidade após crises;
f) inexistência de conflitos entre o principal e o agente;
g) acompanhamento de melhorias das normas e práticas internacionais.

A incidência dos léxicos (retirados do quadro conceitual da revisão da literatura) tem relação significava com a evidenciação dos critérios nos Relatórios de Gerenciamento de Riscos. Os conceitos presentes nas relações significativas são: segurança, responsabilidade, desempenho e tecnologia da informação.

Sugere-se que, baseado na evidência os léxicos dos conceitos anteriormente citados, a segurança, a responsabilidade, o desempenho e a tecnologia da informação são elementos que se relacionam ao gerenciamento de riscos e à *accountability* nos Relatórios de Gerenciamento de Risco das instituições/conglomerados pesquisados.

Os critérios também foram testados com relação aos léxicos identificados nos conceitos relacionados, primeiramente, com gerenciamento de riscos e, posteriormente, *accountability*. Nos dois testes os resultados foram semelhantes, sendo que a maioria dos critérios obtiveram no teste Qui-Quadrado “p<0,01”, indicando “muito significante” a relação entre gerenciamento de riscos e os critérios (na primeira análise) e gerenciamento de riscos e *accountability* (segunda análise).

Como pode ser verificado no Apêndice J, somente os critérios PO9, PO10, AI7, ES2A, ES2C e MO4 não possuem relação significativa com elementos do gerenciamento de riscos. Quanto à relação entre os critérios e *accountability* (Apêndice K), apenas PO9, PO10, ES2A, ES2C e MO4 não apresentaram relação significativa.

Verifica-se, entretanto, que esse resultado já era esperado, pois PO9 foi identificado em todos os relatórios analisados, enquanto que P10, ES2A, ES2C e MO4 não foram evidenciados em nenhum dos documentos analisados. Assim, apenas o critério AI7 (Instala e certifica novas soluções e mudanças) não apresentou relação significante com o gerenciamento de riscos para a amostra analisada.

Sugere-se com o resultado dos dois testes, que os critérios revisados e fundamentados (Quadro 8) compreendem os aspectos relacionados à *accountability* no gerenciamento de riscos. Os resultados obtidos sobre a amostra pesquisada demonstram que a definição de critérios observou os elementos propostos.

Critérios para avaliação de processos de TI expressos em modelos necessitam ser constantemente analisados. Neste trabalho escolheu-se efetuar a análise de critérios para avaliação de processos de TI considerando-se *accountability* no gerenciamento de riscos. Envolveram-se os termos: risco, estratégia, desempenho, tecnologia da informação, segurança, responsabilidade, prestação de contas e transparência. Relatórios de Gerenciamento de Riscos foram estudados com Análise de Conteúdo e Análise Lexical.

5 CONCLUSÃO

Pautando-se no objetivo de propor definição de critérios para avaliação de processos de TI considerando *accountability* no gerenciamento de riscos nas maiores instituições financeira bancárias com operação no Brasil, o presente estudo propôs-se investigar o seguinte problema de pesquisa: Como definir critérios para avaliação de processos de TI considerando *accountability* no gerenciamento de riscos nas maiores instituições financeiras bancárias com operação no Brasil?

Delimitou-se estudar as maiores instituições/financeiras bancárias que desenvolveram atividades no terceiro trimestre de 2012, considerando-se as evidências:

a) o acesso remoto aos serviços e produtos bancários na última década cresceu em torno de 370% (FEBRABAN, 2012);
b) os volumes financeiros investidos em tecnologia da informação pelas organizações bancárias no Brasil foram expressivos (cerca de R$ 14 bilhões em 2011) e há previsão de crescimento em 42% nos investimentos até 2015 (FEBRABAN, 2009; FEBRABAN. 2012);
c) quanto maior for o volume de dados que necessita ser processado, transmitido e disponibilizado para acesso com segurança, maiores são os investimentos necessários para sua proteção (PELANDDA, 2006);
d) o aumento da dependência (técnica e operacional) das organizações quanto aos recursos ligados à tecnologia da informação, aumentam proporcionalmente sua exposição ao risco de TI (PEREIRA e SILVA, 2012; TAROUCO e GRAEML, 2011; FLORES et al., 2011; ITGI, 2006).

Essas evidências relacionam o volume de operações com a necessidade ou dependência por investimentos em tecnologia da informação e consequentemente com maior nível de exposição aos riscos. Tendo a definição de critérios para avaliação de processos de TI considerando *accountability* no gerenciamento de riscos como objetivo da pesquisa, as maiores instituições financeiras bancárias satisfizeram os requisitos necessários para o estudo.

Efetuando-se o procedimento de fundamentação teórica dos critérios para avaliação de processos de TI, baseando-se inicialmente no modelo COBIT®, o que

possibilitou a evidenciação de outros critérios presentes na literatura não comportados pelo modelo estudado, e reordenando-os (Seção 4.2), atendeu-se o objetivo específico de avaliar os critérios à luz do gerenciamento de riscos considerando os conceitos relacionados à *accountability*.

As premissas teóricas utilizadas no estudo foram resumidamente expressas em duas ilustrações: a primeira expõe o *framework* teórico acerca das relações entre informação, tecnologia da informação e governança de TI (Figura 1); e a segunda delimita os enfoques teóricos norteadores da investigação (Quadro 1).

Ao traduzir as boas práticas da governança de TI: alinhar estratégias, usar recursos com responsabilidade, reduzir possibilidades de riscos, melhorar o desenvolvimento organizacional, garantir conformidades, executar serviços com eficiência e avaliar o desempenho (GHEORGE, 2010; WILKIN e CHENHALL, 2010), para os critérios utilizados na investigação, cumpriu-se a proposição de identificar formas de mensuração de desempenho no gerenciamento de risco à luz da GTI.

A separação entre propriedade, gestão e controle organizacional (BERLE e MEANS, 1984) ocasionou a possibilidade de divergências de interesses entre o proprietário (principal) e o gestor (agente). Delegar a outrem poder e autoridade para tomar decisões sobre o patrimônio representa um elemento conceitual da teoria de agência (JENSEN e MECKLING, 1976). Ao incluir os preceitos da *accountability*, envolvendo os conceitos de responsabilização, prestação de contas e transparência nos processos de TI, contribui-se para a redução da assimetria de informações (AKERLOF, 1970) e, consequentemente, nos aspectos relacionados ao problema de agência.

A partir da atualização e fundamentação teórica dos critérios de modelo para avaliação de processos de TI pôde-se investigar as evidências do gerenciamento de riscos, responsabilização, prestação de contas e transparência (Quadro 9). Analisou-se o conjunto de Relatórios de Gerenciamento de Riscos das maiores instituições/conglomerados financeiros com operação de atividades no Brasil referentes ao terceiro trimestre de 2012. As técnicas de Análise de Conteúdo e Análise Léxica foram utilizadas para identificação das informações expressas nos referidos relatórios.

Ao investigar os relatórios de gerenciamento de riscos identificou-se um conjunto de critérios, expressos no Quadro 8, capaz de avaliar o desempenho dos processos de tecnologia da informação. Os critérios avaliam o gerenciamento de

riscos incluindo-se os conceitos de transparência, responsabilidade e prestação de contas. Conforme teste de significância realizado e os resultados expressos no Quadro 9 o conjunto de critérios mostraram-se significantes com os conceitos delimitados para a pesquisa.

Uma característica das técnicas de Análise de Conteúdo e Análise Lexical é a dependência da percepção do pesquisador. Mesmo sendo seguidos todos os procedimentos recomendados para o processo de coleta de dados e análise dos resultados é importante considerar a possibilidade da percepção do pesquisador estar expressa nos resultados.

Cabe ressaltar que a amostra representa mais de 90% das instituições/conglomerados com atividades no Brasil, nos quesitos: ativo total, depósitos totais, número de agências e número de funcionários. Foram observadas as regras fundamentais para utilização de Análise de Conteúdo: representatividade e homogeneidade da amostra e pertinência dos documentos analisados (BARDIN, 2011). Os resultados dessa pesquisa estão relacionados a uma população determinada, as maiores organizações do segmento, cabendo cuidado nas generalizações.

Para novas pesquisas, sugerem-se alguns temas: a influência da centralização ou descentralização da decisão no gerenciamento de riscos; o nível de aderência das instituições financeiras ao cronograma de implantação do Acordo de Basileia (I, II e III) e as relações com o gerenciamento de riscos e *accountability*; as diferentes estruturas de gerenciamento de riscos adotadas e o desempenho atingido; e o processo de gerenciamento de riscos relacionados à conformidade legal e regulatória, os níveis de riscos assumidos e as estratégias de gestão de riscos.

REFERÊNCIAS BIBLIOGRÁFICAS

ABDULLAHI, Muraina; ENYINNA, Okpara; STELLA, Ahunanya. Tax payer's perception of transparency and accountability of tax revenue utilization in Lagos Starte of Nigeria. **International Journal of Business, Accounting and Finance**, v. 6, n. 1, p. 63-74, 2012.

ACCOUNTABILITY. **Norma de princípios de acountability AA1000APS**. Madrid: Accountability, 2008.

AKERLOF, George A. The market for "lemons": quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, v. 84, n. 3, p. 488-500, 1970.

ALLEN, Julia H. **Governing for entreprise security**. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.

APREDA, Rodolfo. The statute of governance: a pivotal linkage between principles of governance and corporate practices. **CEMA Working Papers:** Serie Documentos de Trabajo, Universidad del CEMA, n. 442, feb., 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **ABNT NBR ISO IEC 27001**: tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação – requisitos. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **ABNT NBR ISO IEC 27005**: tecnologia da informação – técnicas de segurança – gestão de riscos de segurança da informação. Rio de Janeiro, 2011.

BANCO CENTRAL DO BRASIL – BACEN. **Circular n. 3.477 de 24 de Dezembro de 2009**. Dispõe sobre a divulgação de informações referentes à gestão de riscos, ao Patrimônio de Referência Exigido (PRE), de que trata a Resolução nº 3.490, de 29 de agosto de 2007, e à adequação do Patrimônio de Referência (PR), de que trata a Resolução nº 3.444, de 28 de fevereiro de 2007. Disponível em: <http://www.bcb.gov.br/pre/normativos/circ/2009/pdf/circ_3477_v1_O.pdf>. Acesso em: 17 mar. 2013.

BANCO CENTRAL DO BRASIL – BACEN. **Sedes de instituições bancárias sob a supervisão do BACEN, em funcionamento no país**. Brasília, 30 nov. 2012. Disponível em: <http.www.bcb.gov.br/?RELINST>. Acesso em: 20 dez. 2012. Arquivo postado no link Bancos comerciais, múltiplos e Caixa Econômica.

BARDIN, Laurence. **Análise de Conteúdo**. São Paulo: Edições 70, 2011.

BARKI, Heni; RIVARD, Suzanne; TALBOT, Jean. An integrative contingency model of sotware project risk management. **Journal of Management Information Systems**, v. 17, n. 4, p. 37-69, 2001.

BART, Chris; TUREL, Ofir. IT and the board of directors: an ampirical investigation into the "governance questions" canadian board members ask about IT. **Journal of Information Systems**, v. 24, n. 2, p. 147-172, 2010.

BELLO, Shukurat Moronke. Impact of ethical leadership on employee job performance. International Journal of Business and Social Science, v. 3, n. 11, p. 228-236, 2012.

BERLE, Adolf A.; MEANS, Gardiner C. **A moderna sociedade anônima e a propriedade privada**. São Paulo: Abril Cultural, 1984.

BOWEN, Paul L.; CHEUNG, May-Yin Decca.; ROHDE, Fiona H. Enhancing IT governance practices: a model and case study of an organization's efforts. **International Journal of Accounting Information Systems**, v. 8, n. 3, p. 191-221, 2007.

BUTLER, Rika; BUTLER, Marthinus J. Beyond king III: assigning accountability for IT governance in South African enterprises. **South African of Business Management**, v. 41, n. 3, p. 33-45,. 2010.

CALDER, Alan; WATKINS, Steve. **IT governance**: a manager's guide to data security and ISO 2001/ISO 27002. 4. ed. London and Philadelphia: Kogan Page, 2008.

CALLAHAN, Joanne; BASTOS, Cassio; KEYES, Dwayne. The evolution of IT governance at NB Power. In: VAN GREMBERGEN, Wim. **Strategies for information technology governance**. Hershey, PA: Idea Group Publishing . 2004. p. 343-356.

CANTÓN, Edméa Pujol. **Governança de TI nas instituições financeiras no Brasil**: uma avaliação de tendências. 2008. Dissertação (Mestrado em Tecnologia) – Programa de Mestrado em Tecnologia: Gestão, Desenvolvimento e Formação – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2008.

CERT.BR. **Total de incidentes reportados ao CERT.br por ano**. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 15 nov. 2012.

CHUN, M. W. S. IT matters: the IT governance road map. **Graziadio Business Report**, v. 8, n. 3, 2005.

COMITE, Ubaldo. The italian public administration and the system of accountability in the managerial Perspective. **Business and Management Review**, v. 1, n. 12, p. 84-88, 2012

CONSELHO MONETÁRIO NACIONAL – CMN. **Resolução CMN n. 2.607, de 27 de maio de 1999**. Estabelece limites mínimos de capital realizado e patrimônio líquido das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: <http://www.bcb.gov.br/pre/normativos/res/1999/pdf/res_2607_v3_P.pdf>. Acesso em: 06 maio 2012.

COSTA, Ana Paula Paulino. **Casos de fraudes corporativas financeiras**: antecedentes, recursos substantivos e simbólicos relacionados. 2011. Tese (Doutorado em Administração de Empresas) – Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas, São Paulo, 2011.

DAMIANIDES, Marios. Sarbanes-Oxley and IT governance: new guidance on it control and compliance. **Information Systems Management**, v. 22, n. 1, p 77-85, 2005.

DE HAES, Steven; VAN GREMBERGEN, Wim. An exploratory study into the design of an IT governance minimum baseline through Delphi research. **Communications of the Association for Information Systems**, v. 22, p. 443-458, 2008.

DUBE, Indrajit. Is corporate governance the answer to corporate structural failure? **US-China Law Review**, v. 8, n. 5, p. 413-430, may., 2011.

EZZINE, Hanene; OLIVERO, Bernard. Evolution of corporate governance during the recente financial crises. The International Journal of Business and Finance Research, v. 7, n. 1, p. 85-100, 2013.

FEDERAÇÃO BRASILEIRA DE BANCOS – FEBRABAN. **A sociedade conectada:** setor bancário em números, tendências tecnológicas e agenda atual. São Paulo: FEBRABAN, 2012.

FEDERAÇÃO BRASILEIRA DE BANCOS – FEBRABAN. **Relatório Anual 2009**. São Paulo: FEBRABAN, 2009.

FELTUS Christophe; PETIT, Michaël; DUBOIS, Eric. Strengthening employee's responsibility to enhance governance of IT: COBIT® RACI chart case study. In: PROCEEDINGS OF THE FIRST ACM WORKSHOP ON INFORMATION SECURITY GOVERNANCE, 2009, Chicago. Chicago, **ACM**, p. 23-31, 2009.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Feraz. **Implantando a governança de TI**: da estratégia à gestão dos processos e serviços. Rio de Janeiro: Brasport, 2008.

FLORES, Waldo Rocha; SOMMESTAD, Teodor; HOLM, Hannes; EKSTEDT, Mathias. Assessing future value of investments in security-related IT governance control objectives: surveying IT professionals. **Electronic Journal Information Systems Evaluation**, v. 14, n. 2, p. 216-227, 2011.

FOX, Jonathan A. The uncertain relationship between transparency and accountability. **Development in Practice**, v. 17, n. 4-5, p. 663-671, 2007.

FREITAS, Henrique; OLIVEIRA, Mírian; SACCOL, Amarolinda Zanela; MOSCAROLA, Jean. O método de pesquisa survey. Revista de Administração, v. 35, n. 3, p. 105-112, 2000.

GEER, Daniel E. **Security of information when economics matters**. Waltham, MA: Verdasys Inc., 2004.

GHEORGHE, Mirela. Audit methodology for IT governance. **Informatica Economica**, v. 14, n. 1, p. 32-42, 2010.

HALL, Jeremy L. Performance and accountability in a time of economic crisis. **Public Performance & Management Review**, v. 35, n. 3, p. 485-488, 2012.

HARDY, Gary. Coordinating IT governance: a new role for IT strategy committees, **Information Systems and Control Journal**, v. 4, 2003.

HARDY, Gary. Using IT governance and COBIT® to deliver value with IT and respond to legal, regulatory and compliance challenges. **Information Security Technical Report**, v. 11, n. 1, p. 55-61, 2006.

HARISON, Elad; BOONSTRA, Albert. Essential competencies for technochange management: towards an assessment model. **International Journal of Information Management**. v. 29, n. 4, p. 283–294, 2009.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION – ISACA. **COBIT® 5**: design paper exposure draft. Rolling Meadows: ISACA, 2010.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION – ISACA. **IT control objectives for cloud computing**: controls and assurance in the cloud. Rolling Meadows: ISACA, 2011.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA – IBGC. **Código das melhores práticas de governança corporativa**. 4. ed. São Paulo: IBCG, 2010.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27002**: code of practice for Information security management, Switzerland, 2005.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 38500**: corporate governance of information. Geneva, 2008.

IRANMANESH, H.; SHIRKOUHI, S. Nazari; SKANDARI, M. R. Risk evaluation of information technology projects based on fuzzy analytic hierarchal process. **World Academy of Science, Engineering and Technology**, v. 40, p. 351-357, 2008.

IT GOVERNANCE INSTITUTE – ITGI. **Aligning COBIT® 4.1, ITIL V3 and ISO/IEC 27002 for business benefit**. Rolling Meadows: ITGI, 2008a.

IT GOVERNANCE INSTITUTE – ITGI. **COBIT® 4.1**: excerpt. Rolling Meadows: ITGI, 2008b.

IT GOVERNANCE INSTITUTE – ITGI. **COBIT® 4.1**: modelo, objetivos de controle, diretrizes de gerenciamento, modelo de maturidade. Rolling Meadows: ITGI, 2007.

IT GOVERNANCE INSTITUTE – ITGI. **Information security governance**: guidance for boards of directors and executive management. 2. ed. Rolling Meadows: ITGI, 2006.

JENSEN, Michael C.; MECKLING, William H. Theory of the firm: managerial behaviour, agency costs and ownership structure. **Journal of Financial Economics**, v. 3, n. 4, 1976.

KAARST-BROWN, Michelle; KELLY, Shirley. IT governance and Sarbanes-Oxley: the latest pitch or real challenges for the IT function? In: PROCCEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 38TH, 2005, Kauai. Hawaii, **HICSS**, v. 8, p. 236-245, 2005.

KING, Ronald R.; DAVIS, Shawn M; MINTCHIK, Natalia. Mandatory disclosure of the engagement partner's identity: potential benefits and unintended consequences. **Accounting Horizons**, v. 26, n. 3, p. 533-561, 2012.

KNORST, André Marcelo. **Alinhamento estratégico entre objetivos de negócio e segurança da informação no contexto da governança de tecnologia da informação (TI):** um estudo no setor de automação. 2010. Dissertação (Mestrado em Administração) – Programa de Pós-Graduação em Administração – Universidade do Vale do Rio dos Sinos. São Leopoldo, 2010.

KUMAR, Ram L. Managing risks in IT projects: an options perspective. **Information & Management**, v. 40, n. 1, p. 63-74, 2002.

LAGZDINS, Arnis. Corporate governance, compliance and banking boards in Latvia: the results of a survey. **Journal of Business Management**, n. 5, p. 126-143, 2012.

LAGZDINS, Arnis; SLOKA, Biruta. Compliance program in Latvias' banking sector: the results of a servey. **European Integration Studies**, n. 6, p. 225-232, 2012.

LANDRUM, Nancy E.; DAILY, Cynthia M. Corporate accountability: a path-goal perspective. **International Journal of Business Insights & Transformation**, v. 4, n. 3, p. 50-62, 2012.

LARSEN, Michel Holm; PEDERSEN, Mogens Kühn; ANDERSEN, Kim Viborg. IT governance: reviewing 17 IT governance tools and analysing the case of Novozymes A/S. In: PROCEEDINGS OF THE HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 39th, 2006, Kauai. Hawaii: **HICSS**, v. 8, p. 195-206, 2006.

LAWRENCE, Pareena G.; NEZHAD, Sheila. Accountability, transparency, and government cooption: a case study of four NGOs. **International NGO Journal**, v. 4, n. 3, p. 76-83, 2009.

LUNARDI, Guilherme Lerch. **Um estudo empírico e analítico do impacto da governança de TI no desempenho organizacional**. 2008. Tese (Doutorado em Administração) – Programa de Pós-Graduação em Administração – Universidade Federal do Rio Grande do Sul. Porto Alegre, 2008.

LUNARDI, Guilherme Lerch; BECKER, João Luiz; MAÇADA, Antonio Carlos Gastaud. Governança de TI e suas implicações para a gestão da TI: um estudo acerca da percepção dos executivos. In: ENCONTRO DA ANPAD – EnANPAD, 34., 2010, Rio de Janeiro. **Anais eletrônicos...** Rio de Janeiro: ANPAD, 2010. p. 1-17.

MAIZLISH, Bryan; HANDLER, Robert. 2005. **IT portifolio management step-by-step**: unlocking the business value of technology. New Jersey: John Wiley & Sons, 2005.

MARTIN, Marie H.; HALACHMI, Arie. Public-private partnerships in global health: addressing issues of public accountability, risk management and governance. **Public Administration Quarterly**, v. 36, n. 2, p. 189-237, 2012.

MARTINS, Gilberto de Andrade; THEÓPHILO, Carlos Renato. **Metodologia da investigação científica para ciências sociais aplicadas**. 2. ed. São Paulo: Atlas, 2009.

MATITZ, Queila Regina Souza; BULGACOV, Sergio. O conceito desempenho em estudos organizacionais e estratégia: um modelo de análise multidimensional. **RAC**, Curitiba, v. 15, n. 4, p. 580-607, 2011.

MENDONÇA, Helder Ferreira; GALVÃO, Délio José Cordeiro; LOURDES, Renato Falci Villela. Regulação e transparência: evidências a partir da crise do subprime. **Economia Aplicada**, v. 15, n. 1, p. 23-44, 2011.

MENEZES, Haroldo Nunes. **Avaliação do nível de maturidade da governança de tecnologia da informação**: estudo de caso em indústrias de grande porte. 2005. Dissertação (Mestrado em Informática Aplicada) – Universidade de Fortaleza, Fortaleza, Ceará, Brasil, 2005.

MORRIS, Jan Taylor; GRIPPO, Frank; BARSKY, Noah. **A new era of accountability?** Strategic Finance, v. 93, n. 11, p. 42-45, 2012.

NATIONAL CYBER SECURITY SUMMIT TASK FORCE. **Information security governance**: a call to action. 2004.

O'CONNOR, Neale G.; MARTINSONS, Maris G. Management of information systems: insights from accounting research. **Information & Management**, v. 43, n. 8, p. 1014–1024, 2006.

PELANDA, Maurício Luiz. **Modelos de governança de tecnologia da informação adotados no Brasil**: um estudo de casos múltiplos. 2006. Dissertação (Mestrado em Administração) – Programa de Pós-Graduação em Administração – Universidade Metodista de São Paulo, São Bernardo do Campo, 2006.

PEREIRA, Ruben; SILVA, Miguel Mira. IT governance implementation: the determinant factors. **Communications of the IBIMA**, v. 2012, p. 1-16, 2012.

PINTO, Arthur R. Globalization and the study of comparative corporate governance. **Wisconsin International Law Journal**, v. 23, n. 3, p. 477-504, 2008.

PIRES, Marcel Ginotti. **A integração pós-fusão dos sistemas e da tecnologia da informação nas fusões e aquisições em instituições bancárias**. 2011. Tese (Doutorado em Administração) – Departamento de Administração da Faculdade de Administração, Economia e Contabilidade – Universidade de São Paulo. São Paulo, 2011.

RABAN, Yoel. Privacy accountability model and policy for security organizations. **I-Business**, v. 4, n. 2, p. 168-172, 2012.

ROBINSON, Nick. It excellence starts with governance. **Journal of Investiment Compliance**, v. 6, n. 3, p. 45-49, 2005.

ROCHA, Décio; DEUSDARÁ; Bruno. Análise de Conteúdo e análise do discurso. **ALEA**, v. 7, n. 2, p. 305-322, 2005.

ROSA, Paulo Sérgio. **Risco operacional e governança em processos de tecnologia da informação de organizações de alta** confiabilidade: estudo no Banco Central do Brasil. 2008. Dissertação (Mestrado em Administração) – Centro de Pesquisa e Pós-Graduação em Administração, Universidade Federal do Paraná. Curitiba, 2008.

ROSS, Jeanne W. Creating a strategic IT architecture competency: learning in stages. **MIS Quarterly Executive**, v. 2, n. 1, p. 31-43, 2003.

SAATY, Thomas L. Decision making with the analytic hierarchy process. **Int. J. Services Sciences**, v. 1, n. 1, p. 83-98, 2008.

SARBANES-OXLEY ACT. Congress of the United States of America. Washington: 2002.

SIDOROVA, Anna; EVANGELOPOLOUS, Nicholas; VALACICH, Joseph. S.; RAMAKRISHNAN, Thiagarajan. Uncovering the intellectual core of the information systems discipline. **Management Information Systems Quarterly**, v. 32, n. 3, p. 467-482, 2008.

SILVA, Priscila Coelho. **Análise da gestão de riscos em projetos de sistemas de informação**. 2011. Dissertação (Mestrado em Adminitração) – Programa de Pós-Graduação em Administração – Universidade Federal do Rio Grande do Sul. Porto Alegre, 2011.

SOFTWARE ENGINEERING INSTITUTE. **CMMI for development, version 1.3**: improving processes for developing better products and services. Pittsburgh: Carnegie Mellon University, 2010.

SORENSEN, Eva. Measuring the accountability of collaborative innovation. **The Innovation Journal**: The Public Sector Innovation Journal, v. 17, n. 1, p. 2-18, 2012.

SPEARS, Janine L.; BARKI, Henri. User participation in information systems security risk management. **MIS Quarterly**, v. 34, n. 3, p. 503-522, 2010.

SPHINX BRASIL. **Manual do Sphinx v5**. Canos: Sphinx Brasil, 2007.

SYMONS, Craig. **IT governance framework**: structures, processes and communication. Cambridge: Forrester Reserarch Inc, 2005.

TAROUCO, Hiury Hakim; GRAEML, Alexandre Reis. Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias, **RAM**, v. 46, n. 1, p. 07-18, 2011.

THURNER, Reinhold. Key success factor: IT resource management. **COBIT® Focus**: Using COBIT®, Val IT, Risk IT, BMIS and ITAF, v. 2, p. 12-16, 2010.

VAHIDNIA, M. H.; ALESHEIKH, A.; ALIMOHAMMAI, A.; BASSIRI, A. Fuzzy analytical hierarchy process in gis application. **The International Archives of the Photogrammetry, Remote Sensinf and Spatial Information Sciences**. v. 37, n. 2, p. 593-596, 2008.

VALENTE, Daniel de Oliveira. **Compreendendo o alinhamento estratégico entre as áreas de negócio e a área de TI nas empresas**: uma proposta de análise e medição. 2006. Dissertação (Mestrado em Administração) – Programa de Pós-Graduação e Pesquisa em Administração e Economia – Faculdade de Economia e Finanças IBMEC. Rio de Janeiro, 2006.

VAN GREMBERGEN, Wim; DE HAES, Steven. **Enterprise governance of information technology**: achieving strategic alignment and value. New York: Springer, 2009.

VAN GREMBERGEN, Wim; DE HAES, Steven; GULDENTOPS, Erick. Structures, processes and relational mechanisms for IT governance. In: VAN GREMBERGEN, Wim. **Strategies for information technology governance**. Hershey, PA: Idea Group Publishing . 2004. p. 1-36.

VASARHELYI, Miklos A.; ALLES, Michael G. The “now” economy and the traditional accounting reporting model: opportunities and challenges for AIS research. **International Journal of Accounting Information Systems**, v.9, n. 4, p. 227-239, 2008.

VERHOEF, Chris. Quantifying the effects of IT governance rules. **Science of Computer Programming**, v. 67, n. 2-3, p. 247-277, 2007.

WEILL, Peter; ROSS, Jeanne. A matrixed approach to designing IT governance. **MIT Sloan Management Review**, v. 46, n. 2, p. 26–34, 2005.

WEILL, Peter; ROSS, Jeanne. **Governança de tecnologia da informação**. São Paulo: Books do Brasil, 2006.

WESTBY, Jody R.; ALLEN, Julia H. **Governing for entreprise security (GES)**: implementation guide. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2007.

WILKIN, Carla L.; CHENHALL, Robert H. A review of IT governance: a taxonomy to inform accounting information systems. **Journal of Information Systems**, v. 24, n, 2, p. 107-146, 2010.

APÊNDICES

APÊNDICE A – Categorização dos Relatórios de Gerenciamento de Riscos

(Continua)

Código	Descrição	ALFA	BANCOGMAC	BANCOOB	BANESE	BANESTES	BANPARA	BANRISUL	BB	BIC	BMG	BNDES	BNPPARIBAS	BRADESCO	BTGPACTUAL	CEF	CITIBANK	DAYCOVAL	DEUTSCHE	FIBRA	INDUSVAL	ITAU	JPMORGANCHASE	MERCANTILDOBRASIL	PINE	RABOBANK	RURAL	SAFRA	SANTANDER	VOLKSWAGEN	VOTORANTIM
PO4	Define e capacita estrutura de RH para documentação, atendimento de demandas e incidentes.	X	X	X		X		X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PO5	Gerencia investimentos em recursos para infraestrutura, segurança, proteção de ativos e desenvolvimento de controles (mensurando e alocando custos, inibindo desvios e usos indevidos).			X		X		X	X	X			X		X	X				X		X	X	X	X		X	X	X	X	
PO6	Comunica metas, políticas e diretrizes à equipe de TI para estabelecer responsabilidades e exigir prestação de contas.	X		X		X		X	X	X					X	X													X		
PO9	Gerencia ameaças, incidentes e vulnerabilidades, corretiva e preventivamente.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PO10	Usa planos: de nível de qualidade, utilização de recursos e prazos para gerenciar projetos de TI.																															

(Continuação)

Código	Descrição	ALFA	BANCOGMAC	BANCOOB	BANESE	BANESTES	BANPARA	BANRISUL	BB	BIC	BMG	BNDES	BNPPARIBAS	BRADESCO	BTGPACTUAL	CEF	CITIBANK	DAYCOVAL	DEUTSCHE	FIBRA	INDUSVAL	ITAU	JPMORGANCHASE	MERCANTILDOBRASIL	PINE	RABOBANK	RURAL	SAFRA	SANTANDER	VOLKSWAGEN	VOTORANTIM
AI7	Instala e certifica novas soluções e mudanças.					X		X	X	X			X	X		X	X	X		X	X	X		X	X		X	X	X	X	X
ES1A	Define responsabilização pela entrega e suporte dos serviços de TI.			X				X	X	X			X			X												X	X		
ES1B	Define transparência na entrega e suporte dos serviços de TI.			X				X																								
ES1C	Define prestação de contas pela entrega e suporte dos serviços de TI.																						X									
ES2A	Gerencia (responsabiliza) os serviços de TI realizados por terceiros.																															
ES2B	Gerencia (exige transparência) nos serviços de TI realizados por terceiros.							X																								
ES2C	Gerencia (exige prestação de contas) dos serviços de TI realizados por terceiros.																															
ES3	Monitora e avalia operações, processos, capacidade e desempenho da TI.		X	X	X	X		X	X	X			X	X		X	X	X		X		X	X	X	X			X	X		X

(Continuação)

Código	Descrição	ALFA	BANCOGMAC	BANCOOB	BANESE	BANESTES	BANPARA	BANRISUL	BB	BIC	BMG	BNDES	BNPPARIBAS	BRADESCO	BTGPACTUAL	CEF	CITIBANK	DAYCOVAL	DEUTSCHE	FIBRA	INDUSVAL	ITAU	JPMORGANCHASE	MERCANTILDOBRASIL	PINE	RABOBANK	RURAL	SAFRA	SANTANDER	VOLKSWAGEN	VOTORANTIM
ES5	Garante qualidade, confiabilidade e segurança dos sistemas e das informações.			X		X		X			X	X	X		X	X			X	X	X	X	X	X	X	X	X	X	X	X	X
ES11	Gerencia acesso, arquivamento e descarte de dados, fornecendo produtos e serviços com transparência nas informações para atender às necessidades dos usuários.		X			X			X	X	X	X		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
MO2	Monitora e avalia o controle interno.	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X
MO3A	Responsabiliza e indica sanções quanto à conformidade aos requisitos externos.					X										X																X
MO3B	Exige transparência quanto à conformidade aos requisitos externos.					X							X																			
MO3C	Exige prestação de conta das ações e decisões quanto à conformidade aos requisitos externos.					X									X													X				
MO4	Fornece modelo governança de TI.																															
GTIA1	Segue políticas, procedimento, processos e controles da estratégia de proteção e segurança.	X	X	X	X	X	X	X	X	X	X	X		X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X		

(Continuação)

Código	Descrição	ALFA	BANCOGMAC	BANCOOB	BANESE	BANESTES	BANPARA	BANRISUL	BB	BIC	BMG	BNDES	BNPPARIBAS	BRADESCO	BTGPACTUAL	CEF	CITIBANK	DAYCOVAL	DEUTSCHE	FIBRA	INDUSVAL	ITAU	JPMORGANCHASE	MERCANTILDOBRASIL	PINE	RABOBANK	RURAL	SAFRA	SANTANDER	VOLKSWAGEN	VOTORANTIM
GTIC1	Garante conformidade legal e regulamentar com requisitos internos e externos.					X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X		X	X	X	X	X	X	X
GTIC4	Reestabelece confiança, integridade e responsabilidade após períodos de crise.									X	X	X		X	X	X		X				X				X					X
GTIE1	Permite a inexistência de conflitos entre o principal e o agente.	X			X	X		X										X						X				X			
GTIE2	Envolve princípios de honestidade, integridade, fairness e preocupação com o outro.								X	X				X				X	X		X	X		X			X		X	X	X
GTICR2	Guia as ações para a continuidade do negócio.		X	X	X	X	X	X		X	X	X	X	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X	X
GTICR4	Formula planos para gestão de crises e incidentes.	X	X	X		X	X	X		X	X	X	X	X	X	X	X	X		X	X	X		X	X	X	X	X	X	X	X
GTIGR1	Define, supervisiona e monitora a eficácia estratégia na proteção das informações.	X	X			X			X	X					X	X		X	X	X		X	X	X	X	X	X			X		X
ACCR1	Responsabiliza ações e tomadas de decisão quanto à supervisão, monitoramento, controle e gestão da TI.			X						X			X										X						X		
ACCR2	Acompanha o processo de melhoria das normas e práticas internacionais.		X		X			X	X	X	X	X	X	X	X	X	X		X	X		X		X	X	X	X		X	X	X

(Conclusão)

Código	Descrição	ALFA	BANCOGMAC	BANCOOB	BANESE	BANESTES	BANPARA	BANRISUL	BB	BIC	BMG	BNDES	BNPPARIBAS	BRADESCO	BTGPACTUAL	CEF	CITIBANK	DAYCOVAL	DEUTSCHE	FIBRA	INDUSVAL	ITAU	JPMORGANCHASE	MERCANTILDOBRASIL	PINE	RABOBANK	RURAL	SAFRA	SANTANDER	VOLKSWAGEN	VOTORANTIM
ACCP1	Gera informações significantes para o cumprimento dos objetivos, estratégias e padrões de desempenho.		X							X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ACCP3	Observa a interdependência entre os recursos de TI (pessoas, aplicações, infraestrutura e informações) na gestão dos recursos de TI.			X			X	X		X	X	X				X			X												

APÊNDICE B – Significância: Critérios X Léxicos_Risco

Nível de significância entre os Critérios e Léxico_Risco
PO9 / An_Lex_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Risco p = **1,1%** ; qui² = **21,27** ; gdl = **9** (**S**)
PO5 / An_Lex_Risco p = **0,5%** ; qui² = **23,84** ; gdl = **9** (**MS**)
PO6 / An_Lex_Risco p = **<0,1%** ; qui² = **37,21** ; gdl = **9** (**MS**)
PO10 / An_Lex_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Risco p = **<0,1%** ; qui² = **35,84** ; gdl = **9** (**MS**)
ES1A / An_Lex_Risco p = **<0,1%** ; qui² = **32,83** ; gdl = **9** (**MS**)
ES1B / An_Lex_Risco p = **44,9%** ; qui² = **8,87** ; gdl = **9** (**NS**)
ES1C / An_Lex_Risco p = **11,9%** ; qui² = **14,11** ; gdl = **9** (**PS**)
ES2A / An_Lex_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Risco p = **84,0%** ; qui² = **4,94** ; gdl = **9** (**NS**)
ES2C / An_Lex_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Risco p = **8,8%** ; qui² = **15,11** ; gdl = **9** (**PS**)
ES5 / An_Lex_Risco p = **2,6%** ; qui² = **18,86** ; gdl = **9** (**S**)
ES11 / An_Lex_Risco p = **21,4%** ; qui² = **11,99** ; gdl = **9** (**NS**)
MO2 / An_Lex_Risco p = **13,2%** ; qui² = **13,74** ; gdl = **9** (**PS**)
MO3A / An_Lex_Risco p = **<0,1%** ; qui² = **34,28** ; gdl = **9** (**MS**)
MO3B / An_Lex_Risco p = **3,3%** ; qui² = **18,18** ; gdl = **9** (**S**)
MO3C / An_Lex_Risco p = **8,0%** ; qui² = **15,43** ; gdl = **9** (**PS**)
MO4 / An_Lex_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Risco p = **53,8%** ; qui² = **7,97** ; gdl = **9** (**NS**)
GTIC1 / An_Lex_Risco p = **0,4%** ; qui² = **24,06** ; gdl = **9** (**MS**)
GTIC4 / An_Lex_Risco p = **0,3%** ; qui² = **24,69** ; gdl = **9** (**MS**)
GTIE1 / An_Lex_Risco p = **2,9%** ; qui² = **18,54** ; gdl = **9** (**S**)
GTIE2 / An_Lex_Risco p = **52,5%** ; qui² = **8,09** ; gdl = **9** (**NS**)
GTICR2 / An_Lex_Risco p = **67,0%** ; qui² = **6,68** ; gdl = **9** (**NS**)
GTICR4 / An_Lex_Risco p = **19,0%** ; qui² = **12,44** ; gdl = **9** (**NS**)
GTIGR1 / An_Lex_Risco p = **15,5%** ; qui² = **13,17** ; gdl = **9** (**NS**)
ACCR1 / An_Lex_Risco p = **1,2%** ; qui² = **21,18** ; gdl = **9** (**S**)
ACCR2 / An_Lex_Risco p = **3,4%** ; qui² = **18,09** ; gdl = **9** (**S**)
ACCP1 / An_Lex_Risco p = **44,3%** ; qui² = **8,94** ; gdl = **9** (**NS**)
ACCP2 / An_Lex_Risco p = **2,6%** ; qui² = **18,93** ; gdl = **9** (**S**)

APÊNDICE C – Significância: Critérios X Léxicos_Estratégia

Nivel de significância entre so Critérios e Léxico-Estratégia
PO9 / An_Lex_Estratégia p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Estratégia p = **2,3%** ; qui² = **25,08** ; gdl = **13** (**S**)
PO5 / An_Lex_Estratégia p = **<0,1%** ; qui² = **44,03** ; gdl = **13** (**MS**)
PO6 / An_Lex_Estratégia p = **<0,1%** ; qui² = **35,26** ; gdl = **13** (**MS**)
PO10 / An_Lex_Estratégia p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Estratégia p = **<0,1%** ; qui² = **56,36** ; gdl = **13** (**MS**)
ES1A / An_Lex_Estratégia p = **0,1%** ; qui² = **34,02** ; gdl = **13** (**MS**)
ES1B / An_Lex_Estratégia p = **<0,1%** ; qui² = **45,22** ; gdl = **13** (**MS**)
ES1C / An_Lex_Estratégia p = **<0,1%** ; qui² = **38,21** ; gdl = **13** (**MS**)
ES2A / An_Lex_Estratégia p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Estratégia p = **5,6%** ; qui² = **21,98** ; gdl = **13** (**PS**)
ES2C / An_Lex_Estratégia p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Estratégia p = **<0,1%** ; qui² = **42,29** ; gdl = **13** (**MS**)
ES5 / An_Lex_Estratégia p = **0,3%** ; qui² = **31,16** ; gdl = **13** (**MS**)
ES11 / An_Lex_Estratégia p = **1,0%** ; qui² = **27,76** ; gdl = **13** (**MS**)
MO2 / An_Lex_Estratégia p = **4,9%** ; qui² = **22,43** ; gdl = **13** (**S**)
MO3A / An_Lex_Estratégia p = **<0,1%** ; qui² = **46,34** ; gdl = **13** (**MS**)
MO3B / An_Lex_Estratégia p = **32,2%** ; qui² = **14,77** ; gdl = **13** (**NS**)
MO3C / An_Lex_Estratégia p = **18,6%** ; qui² = **17,29** ; gdl = **13** (**NS**)
MO4 / An_Lex_Estratégia p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Estratégia p = **0,5%** ; qui² = **29,95** ; gdl = **13** (**MS**)
GTIC1 / An_Lex_Estratégia p = **0,9%** ; qui² = **28,19** ; gdl = **13** (**MS**)
GTIC4 / An_Lex_Estratégia p = **1,4%** ; qui² = **26,72** ; gdl = **13** (**S**)
GTIE1 / An_Lex_Estratégia p = **<0,1%** ; qui² = **40,79** ; gdl = **13** (**MS**)
GTIE2 / An_Lex_Estratégia p = **<0,1%** ; qui² = **35,60** ; gdl = **13** (**MS**)
GTICR2 / An_Lex_Estratégia p = **6,6%** ; qui² = **21,39** ; gdl = **13** (**PS**)
GTICR4 / An_Lex_Estratégia p = **1,2%** ; qui² = **27,12** ; gdl = **13** (**S**)
GTIGR1 / An_Lex_Estratégia p = **4,7%** ; qui² = **22,59** ; gdl = **13** (**S**)
ACCR1 / An_Lex_Estratégia p = **0,6%** ; qui² = **29,27** ; gdl = **13** (**MS**)
ACCR2 / An_Lex_Estratégia p = **1,2%** ; qui² = **27,19** ; gdl = **13** (**S**)
ACCP1 / An_Lex_Estratégia p = **69,1%** ; qui² = **10,03** ; gdl = **13** (**NS**)
ACCP2 / An_Lex_Estratégia p = **<0,1%** ; qui² = **42,93** ; gdl = **13** (**MS**)

APÊNDICE D – Significância: Critérios X Léxicos_Desempenho

Nível de significância entre os Critérios e Léxico_Desempenho
PO9 / An_Lex_Desempenho p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Desempenho p = **<0,1%** ; qui² = **75,56** ; gdl = **20** (**MS**)
PO5 / An_Lex_Desempenho p = **0,1%** ; qui² = **44,96** ; gdl = **20** (**MS**)
PO6 / An_Lex_Desempenho p = **<0,1%** ; qui² = **53,45** ; gdl = **20** (**MS**)
PO10 / An_Lex_Desempenho p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Desempenho p = **0,1%** ; qui² = **44,73** ; gdl = **20** (**MS**)
ES1A / An_Lex_Desempenho p = **<0,1%** ; qui² = **46,27** ; gdl = **20** (**MS**)
ES1B / An_Lex_Desempenho p = **<0,1%** ; qui² = **81,04** ; gdl = **20** (**MS**)
ES1C / An_Lex_Desempenho p = **0,8%** ; qui² = **38,22** ; gdl = **20** (**MS**)
ES2A / An_Lex_Desempenho p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Desempenho p = **<0,1%** ; qui² = **56,35** ; gdl = **20** (**MS**)
ES2C / An_Lex_Desempenho p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Desempenho p = **<0,1%** ; qui² = **65,98** ; gdl = **20** (**MS**)
ES5 / An_Lex_Desempenho p = **<0,1%** ; qui² = **48,68** ; gdl = **20** (**MS**)
ES11 / An_Lex_Desempenho p = **<0,1%** ; qui² = **66,41** ; gdl = **20** (**MS**)
MO2 / An_Lex_Desempenho p = **1,0%** ; qui² = **37,64** ; gdl = **20** (**MS**)
MO3A / An_Lex_Desempenho p = **0,8%** ; qui² = **38,22** ; gdl = **20** (**MS**)
MO3B / An_Lex_Desempenho p = **5,8%** ; qui² = **30,76** ; gdl = **20** (**PS**)
MO3C / An_Lex_Desempenho p = **45,7%** ; qui² = **20,02** ; gdl = **20** (**NS**)
MO4 / An_Lex_Desempenho p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Desempenho p = **0,1%** ; qui² = **45,27** ; gdl = **20** (**MS**)
GTIC1 / An_Lex_Desempenho p = **2,0%** ; qui² = **35,02** ; gdl = **20** (**S**)
GTIC4 / An_Lex_Desempenho p = **0,5%** ; qui² = **40,31** ; gdl = **20** (**MS**)
GTIE1 / An_Lex_Desempenho p = **<0,1%** ; qui² = **49,36** ; gdl = **20** (**MS**)
GTIE2 / An_Lex_Desempenho p = **<0,1%** ; qui² = **77,21** ; gdl = **20** (**MS**)
GTICR2 / An_Lex_Desempenho p = **17,4%** ; qui² = **25,77** ; gdl = **20** (**NS**)
GTICR4 / An_Lex_Desempenho p = **18,9%** ; qui² = **25,34** ; gdl = **20** (**NS**)
GTIGR1 / An_Lex_Desempenho p = **2,4%** ; qui² = **34,36** ; gdl = **20** (**S**)
ACCR1 / An_Lex_Desempenho p = **<0,1%** ; qui² = **73,22** ; gdl = **20** (**MS**)
ACCR2 / An_Lex_Desempenho p = **<0,1%** ; qui² = **53,26** ; gdl = **20** (**MS**)
ACCP1 / An_Lex_Desempenho p = **0,3%** ; qui² = **42,16** ; gdl = **20** (**MS**)
ACCP2 / An_Lex_Desempenho p = **<0,1%** ; qui² = **51,28** ; gdl = **20** (**MS**)

APÊNDICE E – Significância: Critérios X Léxicos_TI

Nível de significância entre os Critérios e Léxico_TI
PO9 / An_Lex_TI p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_TI p = **1,4%** ; qui² = **44,24** ; gdl = **26** (**S**)
PO5 / An_Lex_TI p = **0,2%** ; qui² = **51,32** ; gdl = **26** (**MS**)
PO6 / An_Lex_TI p = **<0,1%** ; qui² = **72,86** ; gdl = **26** (**MS**)
PO10 / An_Lex_TI p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_TI p = **<0,1%** ; qui² = **84,12** ; gdl = **26** (**MS**)
ES1A / An_Lex_TI p = **<0,1%** ; qui² = **61,28** ; gdl = **26** (**MS**)
ES1B / An_Lex_TI p = **0,5%** ; qui² = **48,08** ; gdl = **26** (**MS**)
ES1C / An_Lex_TI p = **<0,1%** ; qui² = **65,62** ; gdl = **26** (**MS**)
ES2A / An_Lex_TI p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_TI p = **<0,1%** ; qui² = **69,39** ; gdl = **26** (**MS**)
ES2C / An_Lex_TI p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_TI p = **<0,1%** ; qui² = **88,70** ; gdl = **26** (**MS**)
ES5 / An_Lex_TI p = **<0,1%** ; qui² = **90,20** ; gdl = **26** (**MS**)
ES11 / An_Lex_TI p = **24,3%** ; qui² = **30,61** ; gdl = **26** (**NS**)
MO2 / An_Lex_TI p = **0,7%** ; qui² = **47,09** ; gdl = **26** (**MS**)
MO3A / An_Lex_TI p = **<0,1%** ; qui² = **70,40** ; gdl = **26** (**MS**)
MO3B / An_Lex_TI p = **8,5%** ; qui² = **36,40** ; gdl = **26** (**PS**)
MO3C / An_Lex_TI p = **<0,1%** ; qui² = **66,77** ; gdl = **26** (**MS**)
MO4 / An_Lex_TI p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_TI p = **<0,1%** ; qui² = **74,29** ; gdl = **26** (**MS**)
GTIC1 / An_Lex_TI p = **3,2%** ; qui² = **40,80** ; gdl = **26** (**S**)
GTIC4 / An_Lex_TI p = **3,8%** ; qui² = **40,16** ; gdl = **26** (**S**)
GTIE1 / An_Lex_TI p = **<0,1%** ; qui² = **86,06** ; gdl = **26** (**MS**)
GTIE2 / An_Lex_TI p = **<0,1%** ; qui² = **60,05** ; gdl = **26** (**MS**)
GTICR2 / An_Lex_TI p = **17,5%** ; qui² = **32,58** ; gdl = **26** (**NS**)
GTICR4 / An_Lex_TI p = **0,7%** ; qui² = **46,94** ; gdl = **26** (**MS**)
GTIGR1 / An_Lex_TI p = **20,3%** ; qui² = **31,71** ; gdl = **26** (**NS**)
ACCR1 / An_Lex_TI p = **0,2%** ; qui² = **51,50** ; gdl = **26** (**MS**)
ACCR2 / An_Lex_TI p = **<0,1%** ; qui² = **100,03** ; gdl = **26** (**MS**)
ACCP1 / An_Lex_TI p = **0,2%** ; qui² = **50,91** ; gdl = **26** (**MS**)
ACCP2 / An_Lex_TI p = **<0,1%** ; qui² = **56,31** ; gdl = **26** (**MS**)

APÊNDICE F – Significância: Critérios X Léxicos_Segurança

Nível de significância entre os Critérios e Lex_Segurança
PO9 / An_Lex_Segurança p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Segurança p = **0,4%** ; qui² = **59,04** ; gdl = **33** (**MS**)
PO5 / An_Lex_Segurança p = **<0,1%** ; qui² = **64,37** ; gdl = **33** (**MS**)
PO6 / An_Lex_Segurança p = **<0,1%** ; qui² = **81,00** ; gdl = **33** (**MS**)
PO10 / An_Lex_Segurança p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Segurança p = **<0,1%** ; qui² = **146,63** ; gdl = **33** (**MS**)
ES1A / An_Lex_Segurança p = **<0,1%** ; qui² = **70,53** ; gdl = **33** (**MS**)
ES1B / An_Lex_Segurança p = **0,3%** ; qui² = **59,73** ; gdl = **33** (**MS**)
ES1C / An_Lex_Segurança p = **0,7%** ; qui² = **56,54** ; gdl = **33** (**MS**)
ES2A / An_Lex_Segurança p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Segurança p = **<0,1%** ; qui² = **65,53** ; gdl = **33** (**MS**)
ES2C / An_Lex_Segurança p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Segurança p = **<0,1%** ; qui² = **80,21** ; gdl = **33** (**MS**)
ES5 / An_Lex_Segurança p = **<0,1%** ; qui² = **76,31** ; gdl = **33** (**MS**)
ES11 / An_Lex_Segurança p = **<0,1%** ; qui² = **67,96** ; gdl = **33** (**MS**)
MO2 / An_Lex_Segurança p = **9,8%** ; qui² = **43,83** ; gdl = **33** (**PS**)
MO3A / An_Lex_Segurança p = **<0,1%** ; qui² = **69,93** ; gdl = **33** (**MS**)
MO3B / An_Lex_Segurança p = **<0,1%** ; qui² = **97,96** ; gdl = **33** (**MS**)
MO3C / An_Lex_Segurança p = **<0,1%** ; qui² = **92,43** ; gdl = **33** (**MS**)
MO4 / An_Lex_Segurança p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Segurança p = **<0,1%** ; qui² = **79,98** ; gdl = **33** (**MS**)
GTIC1 / An_Lex_Segurança p = **<0,1%** ; qui² = **85,33** ; gdl = **33** (**MS**)
GTIC4 / An_Lex_Segurança p = **3,8%** ; qui² = **48,71** ; gdl = **33** (**S**)
GTIE1 / An_Lex_Segurança p = **<0,1%** ; qui² = **116,60** ; gdl = **33** (**MS**)
GTIE2 / An_Lex_Segurança p = **<0,1%** ; qui² = **106,80** ; gdl = **33** (**MS**)
GTICR2 / An_Lex_Segurança p = **1,5%** ; qui² = **53,15** ; gdl = **33** (**S**)
GTICR4 / An_Lex_Segurança p = **0,4%** ; qui² = **59,05** ; gdl = **33** (**MS**)
GTIGR1 / An_Lex_Segurança p = **27,7%** ; qui² = **37,32** ; gdl = **33** (**NS**)
ACCR1 / An_Lex_Segurança p = **<0,1%** ; qui² = **66,96** ; gdl = **33** (**MS**)
ACCR2 / An_Lex_Segurança p = **<0,1%** ; qui² = **82,51** ; gdl = **33** (**MS**)
ACCP1 / An_Lex_Segurança p = **<0,1%** ; qui² = **89,45** ; gdl = **33** (**MS**)
ACCP2 / An_Lex_Segurança p = **<0,1%** ; qui² = **80,10** ; gdl = **33** (**MS**)

APÊNDICE G – Significância: Critérios X Léxicos_Responsabilidade

Nível de significância entre os Critérios e Lex_Responsabilidade
PO9 / An_Lex_Responsabilidade p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **56,19** ; gdl = **25** (**MS**)
PO5 / An_Lex_Responsabilidade p = **17,5%** ; qui² = **31,44** ; gdl = **25** (**NS**)
PO6 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **62,09** ; gdl = **25** (**MS**)
PO10 / An_Lex_Responsabilidade p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **104,75** ; gdl = **25** (**MS**)
ES1A / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **56,68** ; gdl = **25** (**MS**)
ES1B / An_Lex_Responsabilidade p = **0,3%** ; qui² = **48,58** ; gdl = **25** (**MS**)
ES1C / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **58,55** ; gdl = **25** (**MS**)
ES2A / An_Lex_Responsabilidade p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Responsabilidade p = **22,0%** ; qui² = **30,11** ; gdl = **25** (**NS**)
ES2C / An_Lex_Responsabilidade p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **110,46** ; gdl = **25** (**MS**)
ES5 / An_Lex_Responsabilidade p = **0,5%** ; qui² = **46,73** ; gdl = **25** (**MS**)
ES11 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **69,69** ; gdl = **25** (**MS**)
MO2 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **64,56** ; gdl = **25** (**MS**)
MO3A / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **97,95** ; gdl = **25** (**MS**)
MO3B / An_Lex_Responsabilidade p = **0,4%** ; qui² = **47,44** ; gdl = **25** (**MS**)
MO3C / An_Lex_Responsabilidade p = **1,9%** ; qui² = **41,83** ; gdl = **25** (**S**)
MO4 / An_Lex_Responsabilidade p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **74,02** ; gdl = **25** (**MS**)
GTIC1 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **57,82** ; gdl = **25** (**MS**)
GTIC4 / An_Lex_Responsabilidade p = **20,5%** ; qui² = **30,53** ; gdl = **25** (**NS**)
GTIE1 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **74,91** ; gdl = **25** (**MS**)
GTIE2 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **78,49** ; gdl = **25** (**MS**)
GTICR2 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **82,89** ; gdl = **25** (**MS**)
GTICR4 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **100,71** ; gdl = **25** (**MS**)
GTIGR1 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **65,36** ; gdl = **25** (**MS**)
ACCR1 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **67,65** ; gdl = **25** (**MS**)
ACCR2 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **88,17** ; gdl = **25** (**MS**)
ACCP1 / An_Lex_Responsabilidade p = **1,1%** ; qui² = **44,06** ; gdl = **25** (**S**)
ACCP2 / An_Lex_Responsabilidade p = **<0,1%** ; qui² = **83,61** ; gdl = **25** (**MS**)

APÊNDICE H – Significância: Critérios X Léxicos_Transparência

Nível de significância entre os Critérios e Lex_Transparência
PO9 / An_Lex_Transparência p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Transparência p = **<0,1%** ; qui² = **41,20** ; gdl = **13** (**MS**)
PO5 / An_Lex_Transparência p = **2,8%** ; qui² = **24,34** ; gdl = **13** (**S**)
PO6 / An_Lex_Transparência p = **5,2%** ; qui² = **22,21** ; gdl = **13** (**PS**)
PO10 / An_Lex_Transparência p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Transparência p = **<0,1%** ; qui² = **48,79** ; gdl = **13** (**MS**)
ES1A / An_Lex_Transparência p = **4,7%** ; qui² = **22,61** ; gdl = **13** (**S**)
ES1B / An_Lex_Transparência p = **2,6%** ; qui² = **24,62** ; gdl = **13** (**S**)
ES1C / An_Lex_Transparência p = **0,3%** ; qui² = **31,13** ; gdl = **13** (**MS**)
ES2A / An_Lex_Transparência p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Transparência p = **<0,1%** ; qui² = **59,77** ; gdl = **13** (**MS**)
ES2C / An_Lex_Transparência p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Transparência p = **4,2%** ; qui² = **22,95** ; gdl = **13** (**S**)
ES5 / An_Lex_Transparência p = **19,8%** ; qui² = **17,02** ; gdl = **13** (**NS**)
ES11 / An_Lex_Transparência p = **<0,1%** ; qui² = **62,30** ; gdl = **13** (**MS**)
MO2 / An_Lex_Transparência p = **40,1%** ; qui² = **13,63** ; gdl = **13** (**NS**)
MO3A / An_Lex_Transparência p = **0,3%** ; qui² = **31,73** ; gdl = **13** (**MS**)
MO3B / An_Lex_Transparência p = **59,1%** ; qui² = **11,24** ; gdl = **13** (**NS**)
MO3C / An_Lex_Transparência p = **98,6%** ; qui² = **4,38** ; gdl = **13** (**NS**)
MO4 / An_Lex_Transparência p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Transparência p = **17,6%** ; qui² = **17,53** ; gdl = **13** (**NS**)
GTIC1 / An_Lex_Transparência p = **<0,1%** ; qui² = **36,93** ; gdl = **13** (**MS**)
GTIC4 / An_Lex_Transparência p = **1,6%** ; qui² = **26,19** ; gdl = **13** (**S**)
GTIE1 / An_Lex_Transparência p = **<0,1%** ; qui² = **43,22** ; gdl = **13** (**MS**)
GTIE2 / An_Lex_Transparência p = **<0,1%** ; qui² = **45,31** ; gdl = **13** (**MS**)
GTICR2 / An_Lex_Transparência p = **10,5%** ; qui² = **19,64** ; gdl = **13** (**PS**)
GTICR4 / An_Lex_Transparência p = **3,6%** ; qui² = **23,50** ; gdl = **13** (**S**)
GTIGR1 / An_Lex_Transparência p = **<0,1%** ; qui² = **38,61** ; gdl = **13** (**MS**)
ACCR1 / An_Lex_Transparência p = **32,2%** ; qui² = **14,77** ; gdl = **13** (**NS**)
ACCR2 / An_Lex_Transparência p = **0,9%** ; qui² = **27,88** ; gdl = **13** (**MS**)
ACCP1 / An_Lex_Transparência p = **25,7%** ; qui² = **15,85** ; gdl = **13** (**NS**)
ACCP2 / An_Lex_Transparência p = **2,1%** ; qui² = **25,27** ; gdl = **13** (**S**)

APÊNDICE I – Significância: Critérios X Léxicos_Prestação_de_Contas

Nível de significância entre os Critérios e Lex_Prestação
PO9 / An_Lex_Prestação p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Prestação p = **0,5%** ; qui² = **33,10** ; gdl = **15** (**MS**)
PO5 / An_Lex_Prestação p = **0,7%** ; qui² = **31,79** ; gdl = **15** (**MS**)
PO6 / An_Lex_Prestação p = **6,4%** ; qui² = **24,09** ; gdl = **15** (**PS**)
PO10 / An_Lex_Prestação p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Prestação p = **<0,1%** ; qui² = **70,64** ; gdl = **15** (**MS**)
ES1A / An_Lex_Prestação p = **2,9%** ; qui² = **26,99** ; gdl = **15** (**S**)
ES1B / An_Lex_Prestação p = **14,2%** ; qui² = **20,83** ; gdl = **15** (**PS**)
ES1C / An_Lex_Prestação p = **0,1%** ; qui² = **36,64** ; gdl = **15** (**MS**)
ES2A / An_Lex_Prestação p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Prestação p = **12,6%** ; qui² = **21,34** ; gdl = **15** (**PS**)
ES2C / An_Lex_Prestação p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Prestação p = **<0,1%** ; qui² = **46,17** ; gdl = **15** (**MS**)
ES5 / An_Lex_Prestação p = **10,4%** ; qui² = **22,15** ; gdl = **15** (**PS**)
ES11 / An_Lex_Prestação p = **1,1%** ; qui² = **30,15** ; gdl = **15** (**S**)
MO2 / An_Lex_Prestação p = **0,4%** ; qui² = **33,32** ; gdl = **15** (**MS**)
MO3A / An_Lex_Prestação p = **0,7%** ; qui² = **31,95** ; gdl = **15** (**MS**)
MO3B / An_Lex_Prestação p = **0,4%** ; qui² = **33,37** ; gdl = **15** (**MS**)
MO3C / An_Lex_Prestação p = **6,9%** ; qui² = **23,79** ; gdl = **15** (**PS**)
MO4 / An_Lex_Prestação p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Prestação p = **0,1%** ; qui² = **37,36** ; gdl = **15** (**MS**)
GTIC1 / An_Lex_Prestação p = **0,5%** ; qui² = **32,96** ; gdl = **15** (**MS**)
GTIC4 / An_Lex_Prestação p = **1,5%** ; qui² = **29,23** ; gdl = **15** (**S**)
GTIE1 / An_Lex_Prestação p = **<0,1%** ; qui² = **44,57** ; gdl = **15** (**MS**)
GTIE2 / An_Lex_Prestação p = **<0,1%** ; qui² = **51,33** ; gdl = **15** (**MS**)
GTICR2 / An_Lex_Prestação p = **0,3%** ; qui² = **34,29** ; gdl = **15** (**MS**)
GTICR4 / An_Lex_Prestação p = **<0,1%** ; qui² = **52,85** ; gdl = **15** (**MS**)
GTIGR1 / An_Lex_Prestação p = **0,3%** ; qui² = **34,75** ; gdl = **15** (**MS**)
ACCR1 / An_Lex_Prestação p = **0,8%** ; qui² = **31,39** ; gdl = **15** (**MS**)
ACCR2 / An_Lex_Prestação p = **1,1%** ; qui² = **30,14** ; gdl = **15** (**S**)
ACCP1 / An_Lex_Prestação p = **49,7%** ; qui² = **14,38** ; gdl = **15** (**NS**)
ACCP2 / An_Lex_Prestação p = **<0,1%** ; qui² = **37,78** ; gdl = **15** (**MS**)

APÊNDICE J – Significância: Critérios X Gerenciamento de Riscos

Nível de Significância entre os Critérios e Gerenciamento de Riscos
PO9 / An_Lex_Gerenciamento_de_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **201,65** ; gdl = **77** (**MS**)
PO5 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **177,81** ; gdl = **77** (**MS**)
PO6 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **194,93** ; gdl = **77** (**MS**)
PO10 / An_Lex_Gerenciamento_de_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **285,28** ; gdl = **77** (**MS**)
ES1A / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **177,06** ; gdl = **77** (**MS**)
ES1B / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **182,63** ; gdl = **77** (**MS**)
ES1C / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **137,54** ; gdl = **77** (**MS**)
ES2A / An_Lex_Gerenciamento_de_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **161,61** ; gdl = **77** (**MS**)
ES2C / An_Lex_Gerenciamento_de_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **217,92** ; gdl = **77** (**MS**)
ES5 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **156,14** ; gdl = **77** (**MS**)
ES11 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **163,27** ; gdl = **77** (**MS**)
MO2 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **155,48** ; gdl = **77** (**MS**)
MO3A / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **197,35** ; gdl = **77** (**MS**)
MO3B / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **147,98** ; gdl = **77** (**MS**)
MO3C / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **149,87** ; gdl = **77** (**MS**)
MO4 / An_Lex_Gerenciamento_de_Risco p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **169,27** ; gdl = **77** (**MS**)
GTIC1 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **163,42** ; gdl = **77** (**MS**)
GTIC4 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **134,52** ; gdl = **77** (**MS**)
GTIE1 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **226,12** ; gdl = **77** (**MS**)
GTIE2 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **219,47** ; gdl = **77** (**MS**)
GTICR2 / An_Lex_Gerenciamento_de_Risco p = **0,7%** ; qui² = **111,09** ; gdl = **77** (**MS**)
GTICR4 / An_Lex_Gerenciamento_de_Risco p = **0,2%** ; qui² = **117,46** ; gdl = **77** (**MS**)
GTIGR1 / An_Lex_Gerenciamento_de_Risco p = **0,2%** ; qui² = **117,08** ; gdl = **77** (**MS**)
ACCR1 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **173,32** ; gdl = **77** (**MS**)
ACCR2 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **219,41** ; gdl = **77** (**MS**)
ACCP1 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **153,24** ; gdl = **77** (**MS**)
ACCP2 / An_Lex_Gerenciamento_de_Risco p = **<0,1%** ; qui² = **192,71** ; gdl = **77** (**MS**)

APÊNDICE K – Significância: Critérios X *Accountability*

Nível de significância entre os Critérios e a Accountability
PO9 / An_Lex_Accountability p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
PO4 / An_Lex_Accountability p = **<0,1%** ; qui² = **101,68** ; gdl = **41** (**MS**)
PO5 / An_Lex_Accountability p = **0,1%** ; qui² = **74,45** ; gdl = **41** (**MS**)
PO6 / An_Lex_Accountability p = **<0,1%** ; qui² = **96,32** ; gdl = **41** (**MS**)
PO10 / An_Lex_Accountability p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
AI7 / An_Lex_Accountability p = **<0,1%** ; qui² = **168,01** ; gdl = **41** (**MS**)
ES1A / An_Lex_Accountability p = **<0,1%** ; qui² = **101,82** ; gdl = **41** (**MS**)
ES1B / An_Lex_Accountability p = **<0,1%** ; qui² = **82,48** ; gdl = **41** (**MS**)
ES1C / An_Lex_Accountability p = **<0,1%** ; qui² = **85,30** ; gdl = **41** (**MS**)
ES2A / An_Lex_Accountability p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES2B / An_Lex_Accountability p = **<0,1%** ; qui² = **97,49** ; gdl = **41** (**MS**)
ES2C / An_Lex_Accountability p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
ES3 / An_Lex_Accountability p = **<0,1%** ; qui² = **136,61** ; gdl = **41** (**MS**)
ES5 / An_Lex_Accountability p = **3,5%** ; qui² = **58,83** ; gdl = **41** (**S**)
ES11 / An_Lex_Accountability p = **<0,1%** ; qui² = **127,19** ; gdl = **41** (**MS**)
MO2 / An_Lex_Accountability p = **<0,1%** ; qui² = **100,68** ; gdl = **41** (**MS**)
MO3A / An_Lex_Accountability p = **<0,1%** ; qui² = **126,44** ; gdl = **41** (**MS**)
MO3B / An_Lex_Accountability p = **0,2%** ; qui² = **72,02** ; gdl = **41** (**MS**)
MO3C / An_Lex_Accountability p = **4,2%** ; qui² = **57,92** ; gdl = **41** (**S**)
MO4 / An_Lex_Accountability p = **100,0%** ; qui² = **0,00** ; gdl = **0** (**NS**)
GTIA1 / An_Lex_Accountability p = **<0,1%** ; qui² = **102,77** ; gdl = **41** (**MS**)
GTIC1 / An_Lex_Accountability p = **<0,1%** ; qui² = **103,50** ; gdl = **41** (**MS**)
GTIC4 / An_Lex_Accountability p = **0,2%** ; qui² = **72,68** ; gdl = **41** (**MS**)
GTIE1 / An_Lex_Accountability p = **<0,1%** ; qui² = **140,38** ; gdl = **41** (**MS**)
GTIE2 / An_Lex_Accountability p = **<0,1%** ; qui² = **126,47** ; gdl = **41** (**MS**)
GTICR2 / An_Lex_Accountability p = **<0,1%** ; qui² = **99,68** ; gdl = **41** (**MS**)
GTICR4 / An_Lex_Accountability p = **<0,1%** ; qui² = **118,85** ; gdl = **41** (**MS**)
GTIGR1 / An_Lex_Accountability p = **<0,1%** ; qui² = **108,34** ; gdl = **41** (**MS**)
ACCR1 / An_Lex_Accountability p = **<0,1%** ; qui² = **94,13** ; gdl = **41** (**MS**)
ACCR2 / An_Lex_Accountability p = **<0,1%** ; qui² = **131,30** ; gdl = **41** (**MS**)
ACCP1 / An_Lex_Accountability p = **0,9%** ; qui² = **65,40** ; gdl = **41** (**MS**)
ACCP2 / An_Lex_Accountability p = **<0,1%** ; qui² = **127,30** ; gdl = **41** (**MS**)