

UNIVERSIDADE PAULISTA

**ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE
TECNOLOGIA DA INFORMAÇÃO.**

MIGUEL DE SOUZA VILAÇA NETO

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Paulista - UNIP, para a obtenção do título de mestre em Engenharia de Produção.

SÃO PAULO
2008

Livros Grátis

<http://www.livrosgratis.com.br>

Milhares de livros grátis para download.

UNIVERSIDADE PAULISTA

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO.

MIGUEL DE SOUZA VILAÇA NETO

Orientador: Prof. Dr. Antônio Roberto Pereira
Leite de Albuquerque
Área de Concentração: Engenharia de
Produção
Linha de Pesquisa: Modelos e Ferramentas
para Gestão da Informação
Projetos de Pesquisa: Reconhecimento de
Padrões em Projetos

Dissertação apresentada ao Programa de Pós-
Graduação em Engenharia de Produção da
Universidade Paulista.

SÃO PAULO
2008

VILAÇA, Miguel de Souza

Análise de Conformidade de Governança de Tecnologia da Informação / Miguel de Souza Vilaça Neto. São Paulo, 2008.
79 p.

Dissertação (Mestrado) – Universidade Paulista, 2008.

Área de Concentração: Engenharia de Produção.

Orientador: Dr. Antônio Roberto Pereira Leite de Albuquerque.

1. Governança de TI
2. Lógicas Não Clássicas.
3. Alinhamento Estratégico.

ERRATA

DEDICATÓRIA

A minha querida esposa Renata Raveli e meus filhos Giovani Vilaça e João Vilaça que me motivaram na conclusão deste trabalho.

AGRADECIMENTOS

Agradeço aos meus familiares que me incentivaram desde criança os valores de uma boa educação. Em especial agradeço meu Pai por sua fiel presença nos momentos mais difíceis da minha vida.

Ao meu Mestre Dr. Antônio R. P. L. Albuquerque por sua extrema paciência e sabedoria nas questões decisivas deste trabalho.

Ao meu Prof. Oduvaldo Vendrametto que tão bem entendeu minhas dificuldades e falhas.

A todos os docentes do Programa de Pós-graduação (Mestrado) em engenharia da Produção envolvidos diretamente ou indiretamente nessa minha jornada de sucesso.

EPÍGRAFE

“Gandhi encarna o maior gênio político de nossa civilização. Definiu o sentido concreto de uma política e soube encontrar em cada homem um inesgotável heroísmo quando descobre um objetivo e um valor para sua ação” (Albert Einstein).

RESUMO

VILAÇA, M. S. **Análise de Conformidade de Governança de Tecnologia da Informação**. Dissertação (Mestrado em Engenharia de Produção) - Instituto de Ciências Exatas e Tecnológicas, Universidade Paulista, 2008.

Palavras-chave: Governança de TI; Lógica Paraconsistente; COBIT;

O presente estudo descreve um método de avaliação de conformidade em Governança de Tecnologia da Informação por meio de avaliação de questionários. Baseando-se na comparação da opinião de lideranças com os especialistas de quatro áreas distintas de uma empresa do ramo de cosméticos. Para montagem das alternativas do questionário utilizou-se o *framework* COBIT, e no refinamento e análise dos resultados aplicou-se a Lógica Paraconsistente Anotada na qual visa tratar as opiniões inconsistentes dos especialistas e mitigar a subjetividade em questão. Esta mescla de uma teoria de análise e avaliação por especialistas, permite sugerir um indicador que representa o nível de conformidade da empresa em relação à escala de maturidade do COBIT. Com isso, é possível prever inconformidades com a Governança de TI.

ABSTRACT

VILAÇA, M. S. **IT Governance Compliance Analysis**. Dissertation (Master in Production Engineering) – Paulista University, São Paulo, 2008.

Keywords: IT Governance; Annotated Paraconsistente Logic; COBIT;

The present study describes a method for evaluation of compliance with IT (Information Technology) Governance through polls evaluation. Based on the leaderships opinions with specialists from four different areas from a company in the beauty industry. For developing the alternatives of the polls we will use the Cobit framework, and in the refinement and analysis of the results we will apply APL in which is sought to deal with the specialists' inconsistent opinions and to mitigate the subjectivity in topic. This mix of in analyzes theory and specialists evaluation, allows to suggest an indicator which represents the level of the company's compliance in relation to the theory maturity scale on COBIT. With that, it is possible to foresee non-compliance with IT Governance.

LISTA DE SIGLAS

OECD - Organization for Economic Co-operation and Development

ISACA - Information Systems Audit and Control Association

ITSEC - Information Technology Security Evaluation Criteria

TCSEC - Trusted Computer System Evaluation Criteria

IFAC - International Federation of Automatic Control

AICPA - American Institute of Certified Public Accountants

IIA - Institute of Internal Auditors

GAO - Government Accountability Office

ITGI - IT Governance Institute

ITIL - Information Technology Infrastructure Library

UML - Unified Modeling Language

LISTA DE FIGURAS

Figura 1 - Processos e domínios do Cobit (Fonte: www.consulting.com.br).....	22
Figura 2 - Objetivos de Controle (Fonte: www.consulting.com.br)	23
Figura 3 - Indicadores como mecanismo que ajuda a tomadas de decisão.....	28
Figura 4 - Design UML do método para avaliação de conformidade em Governança de TI.....	33
Figura 5 - Fluxograma do método para avaliação de conformidade em Governança de TI.....	40
Figura 6 - Escala com índices para classificação da conformidade.	43

LISTA DE TABELAS

Tabela 1 - Unidades de controle baseadas no Cobit.....	32
Tabela 2 - Unidades de Controle x Alternativas.....	34
Tabela 3 - Critérios correlacionados com os índices para classificação da conformidade.....	39
Tabela 4 - Avaliação dos especialistas.....	50
Tabela 5 - Índices resultantes de conformidade condizentes com os parâmetros estratégicos predefinidos.....	53
Tabela 6 - Grau de Contradição e decisão para avaliação final, Avaliação Conservadora.....	56
Tabela 7 - Grau de Contradição e decisão para avaliação final, avaliação Intermediária.....	57
Tabela 8 - Grau de Contradição e decisão para avaliação final, avaliação Otimista.....	59
Tabela 9 - Obtenção dos dois índices resultantes de conformidade, para área de conformidade SOX “planejar e organizar”.....	51
Tabela 10 - Adoção do maior índice de conformidade entre (cR ou cR1), para área de conformidade SOX “planejar e organizar”.....	62
Tabela 11 - Alocação do maior índice de conformidade na escala adotada, para área de conformidade SOX “planejar e organizar”.....	64
Tabela 12 - Quantidade de Alternativas avaliadas x Convergência da Opinião dos Especialistas, considerando os três parâmetros estratégicos.....	66
Tabela 13 - Quantidade de Alternativas avaliada x Índices de Conformidade.....	66
Tabela 14 - Resultado da avaliação da empresa - estudo de caso.....	57
Tabela 15 - Resultado Final.....	58

SUMÁRIO

1	INTRODUÇÃO	14
1.1	APRESENTAÇÃO DO ASSUNTO	14
1.2	OBJETIVOS DO TRABALHO	14
1.3	JUSTIFICATIVA DA PESQUISA	15
1.4	METODOLOGIA DE PESQUISA UTILIZADA	15
1.5	ESTRUTURA DO TRABALHO	15
2	REFERENCIAL TEORICO	17
2.1	GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO	17
2.1.1	ATO SARBANES-OXLEY	18
2.1.2	MEDINDO A ESTRATÉGIA	19
2.1.3	ADMINISTRAÇÃO DE TI	20
2.1.4	ALINHAMENTO ESTRATÉGICO	20
2.2	CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECNOLOGIES (COBIT)	21
2.3	A LÓGICA PARACONSISTENTE	23
2.4	A LÓGICA PARACONSISTENTE ANOTADA	24
2.5	BSC – BALANCED SCORECARD	26
2.6	MODELO DE GOVERNANÇA DE TI, A PARTIR DE INDICADORES DE DESEMPENHO	27
2.6.1	INDICADORES DE DESEMPENHO	27
2.6.2	CLASSIFICAÇÃO E BENEFÍCIOS DOS INDICADORES DE DESEMPENHO NA GESTÃO ESTRATÉGICA	28
3	MÉTODO DE PESQUISA	30
3.1	COLETA DOS DADOS	30
3.2	PREENCHIMENTO DO QUESTIONARIO	31
3.3	MODELO PROPOSTO PARA AVALIAÇÃO DE CONFORMIDADES EM GOVERNANÇA DE TI	31
3.4	FLUXOGRAMA	39
4	APLICAÇÃO DO MÉTODO	41
4.1	DESENVOLVIMENTO	41
5	APRESENTAÇÃO DOS RESULTADOS	64
5.1	RESULTADOS DA PESQUISA	66
5.2	COMPARAÇÃO DAS OPINIÕES DOS ESPECIALISTAS COM AS DAS SUAS LIDERANÇAS	67
6	CONCLUSÃO	69
7	REFERÊNCIAS BIBLIOGRÁFICAS	71
	ANEXO A – QUESTIONÁRIO	74

1 INTRODUÇÃO

1.1 APRESENTAÇÃO DO ASSUNTO

As empresas de capital aberto e fechado procuram, cada vez mais, aderir-se aos modelos de gestão de maiores aceitação do mercado. Neste trabalho utilizou-se o *framework* (sistema) Cobit, que por sua vez tem como objetivo fornecer boas práticas para a gestão de processo de Tecnologia da Informação (TI) .

Define-se por Governança de TI um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, aperfeiçoar a aplicação de recursos, reduzir custos, suportar as melhores decisões e conseqüentemente alinhar a TI aos negócios.

Junto a estes objetivos os auditores e fiscais do exercício da lei, monitoram e avaliam possíveis empresas a abrir seu capital na bolsa de valores, mitigando os escândalos financeiros envolvendo empresas com papéis na bolsa, como as do ano 2001, que motivaram o ato SOX de 2002, decretado pelo congresso Norte Americano. Este ato impõe as empresas de capital aberto a relatar suas finanças, acarretando uma grande exigência sobre toda área de TI.

1.2 OBJETIVOS DO TRABALHO

Demonstrar por meio de análise de opiniões, o grau de maturidade em que uma organização encontra-se em relação a sua aderência à Governança de TI, nos limites definidos no *framework Control Objectives for Information and Related Technologies* (Sistema Cobit).

O estudo foi realizado em uma empresa do ramo de cosméticos, utilizando o Cobit, com foco em análise de conformidade por meio da elaboração de uma metodologia baseada na Lógica Paraconsistente, que permite não só caracterizar a maturidade em relação a sua aderência à Governança de TI, como também comparar as opiniões de internas, de líderes com os seus próprios especialistas em quatro áreas distintas da empresa em questão.

1.3 JUSTIFICATIVA DA PESQUISA

A conformidade em Governança de TI é um grande passo para abrir o capital na bolsa de valores de uma corporação. E entretanto, para tal feito, é necessário haver uma análise geral sobre as principais áreas que definem a infraestrutura de TI. Os métodos clássicos de avaliação não se mostram maduros na identificação das não conformidades em Governança de TI. Portanto, o modelo proposto avalia de forma diferente essa questão, já que introduz a abordagem da Lógica Paraconsistente.

1.4 METODOLOGIA DE PESQUISA UTILIZADA

A metodologia adotada neste trabalho fundamenta-se na avaliação de um questionário de acordo com os objetivos de controle do Cobit em referência aos domínios da Governança de TI, em aderência a seção 404 da lei SOX (Sarbanes-Oxley).

O questionário é submetido a vários especialistas, que permite avaliar o grau de coerência dos avaliadores, que possibilitou perceber e compreender as principais dificuldades encontradas na avaliação de conformidade para este tipo de sistema de avaliação.

As questões dispostas no capítulo 4 estão de acordo com os objetivos de controle do Cobit, e foram desenvolvidas para ajudar uma organização a medir, como ela está em relação a sua aderência à Governança de TI, baseado em escala do sistema Cobit.

1.5 ESTRUTURA DO TRABALHO

Este trabalho consiste de seis capítulos, incluindo a introdução.

No capítulo 2 são apresentados os referenciais teóricos relacionados no trabalho, nos quais são abrangidos a Governança de TI, métricas e alinhamento estratégico, administração de TI, *frameworks* Cobit, BSC especializados em definir domínios sobre a Governança de TI, ferramentas de análise sobre lógicas

não clássicas, e classificação e benefícios dos indicadores de desempenho sobre a gestão estratégica.

No capítulo 3 descreve-se o método de pesquisa a ser aplicado no estudo de caso e apresenta-se o mecanismo utilizado para coletar e preencher as informações necessárias para avaliar o grau de conformidade em Governança de TI em uma empresa do ramo de cosméticos.

No capítulo 4 demonstra-se a aplicação do método, passo a passo, identificando as áreas de atuação dos avaliadores, seleção das alternativas e unidades de controle baseados nos domínios dos *frameworks* Cobit e Lógica Paraconsistente. Também expõe os critérios de mensuração de conformidade em Governança de TI, tabulação e aplicação dos questionários, definição do parâmetro estratégico, obtenção dos graus de conformidade (cR) e inexistência de conformidade (icR), além da análise das opiniões.

No capítulo 5 destacam-se os resultados qualitativos obtidos pela aplicação do método descrito, sobre ponderação e convergência das opiniões dos especialistas quanto à conformidade em Governança de TI das alternativas identificadas e avaliadas. E ainda descreve-se a comparação de visões de avaliadores extremamente importantes em corporações “líderes X especialistas”.

No capítulo 6 apresenta-se a conclusão sobre o método para avaliação da conformidade em Governança de TI, considerando a aplicação da metodologia proposta no estudo.

2 REFERENCIAL TEÓRICO

2.1 GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO

A informação é reconhecida pelas organizações, nos últimos anos, como um dos mais importantes recursos estratégicos que necessitam gerenciamento (WEILL & ROSS, 2004).

Atualmente, os sistemas e os serviços de TI desempenham papel vital na coleta, análise, produção e distribuição da informação indispensável à execução do negócio das organizações. Tornou-se essencial o reconhecimento de que a TI é crucial, estratégica e importante recurso, que precisa de investimento e gerenciamento apropriados.

O cenário motivou o surgimento do conceito de Governança de TI, do termo inglês “*IT Governance*”, por meio da qual se procura o alinhamento da TI com os objetivos da organização. Governança de TI define que a TI é fator essencial para a gestão financeira e estratégica de uma organização, e não apenas um suporte aos mesmos. Governança de TI pode ser definida como:

- Estrutura de relacionamentos entre processos para direcionar e controlar uma empresa de modo a atingir seus objetivos corporativos, por meio da agregação de valor e controle dos riscos pelo uso da TI e seus processos (ITGI, 2001);
- Capacidade organizacional exercida pelo conselho diretor, gerente executivo e gerente de TI de controlar o planejamento e implementação das estratégias de TI e, dessa forma, permitir a fusão de TI ao negócio (GREMBERGEN, 2003);
- Especificação das decisões corretas em um modelo que encoraje o comportamento desejável no uso de TI nas organizações (WEILL & ROSS, 2004).

Os princípios da Governança de TI visam garantir o alinhamento do uso de TI com os objetivos, estratégias e operacionalização do negócio. A estrutura de benefícios de TI no desempenho empresarial deve ser a base para o estabelecimento e a manutenção desse alinhamento.

2.1.1 A Lei Sarbanes-Oxley

“*Sarbanes-Oxley Act*” ou Lei Sarbanes-Oxley é uma lei norte-americana, assinada em 30 de julho de 2002, pelo senador Paul Sarbanes (democrata de Maryland) e pelo deputado Michael Oxley (republicano de Ohio).

Motivada por escândalos financeiros corporativos (entre eles o da Enron, que acabou por afetar drasticamente a empresa de auditoria Arthur Andersen), a lei foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores, causada pela aparente insegurança a respeito da governança adequada das empresas.

A Lei Sarbanes-Oxley passou a ser conhecida como Lei de Sarbox ou ainda SOX. Seu conjunto busca garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo regras para a criação de comitês e comissões encarregados de supervisionar suas atividades e operações. Os objetivos são mitigar riscos aos negócios, evitar a ocorrência de fraudes ou ter meios de identificar quando elas ocorrem, garantindo a transparência na gestão das empresas.

Atualmente, grandes empresas com operações financeiras no exterior seguem a Lei Sarbanes-Oxley. A Lei Sarbanes-Oxley afeta dezenas de empresas brasileiras que mantêm ADRs (*American Depositary Receipts*) negociadas na NYSE (*New York Stock Exchange*), como Petrobrás, Sabesp, TAM Linhas Aéreas, Brasil Telecom, Ultrapar (Ultragaz), Companhia Brasileira de Distribuição (Grupo Pão de Açúcar), Banco Itaú e Telemig Celular.

2.1.1.1 Requisitos da lei

1. Controlar a criação, edição e versão dos documentos em um ambiente de acordo com os padrões ISO, para controle de todos os documentos relativos à seção 404;
2. Cadastrar os riscos associados aos processos de negócios e armazenar os desenhos de processo;
3. Utilizar ferramentas como editor de texto e planilha eletrônica para criação e alteração dos documentos da seção 404;
4. Publicar em múltiplos *websites* os conteúdos da seção 404;
5. Gerenciar todos os documentos, controlando seus períodos de retenção e distribuição;
6. Digitalizar e armazenar todos os documentos que estejam em papel, ligados à seção 404.

2.1.1.2 Seção 404

A seção 404 determina a avaliação anual dos controles e procedimentos internos para emissão de relatórios financeiros. Além disso, o auditor independente da companhia deve emitir um relatório distinto que ateste a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros.

2.1.2 Medindo a estratégia

As medidas darão informações indispensáveis, vitais, pois toda a estratégia é construída em cima de princípios que se acredita serem fundamentais para a criação de valores para a organização. O acompanhamento dessas medidas indicará se será necessário ou não haver mudança ou até mesmo ser reescrita a estratégia.

Com base na medição, é possível avaliar o desempenho dos indicadores estratégicos e acompanhar se estão sendo alcançados os objetivos. Os indicadores e objetivos traduzem a visão e a estratégia empregadas. A tarefa de medir a estratégia requer constante acompanhamento e avaliação. A partir das

metas traçadas são avaliados os estágios rumo aos objetivos estratégicos (CORREIA et al., 2007).

2.1.3 Administração de TI

O interesse do uso de TI nas empresas e a inovação contínua propiciada pela TI criam vantagem tecnológica para a empresa. A utilização de tecnologias mais recentes está em alta entre as empresas qualificadas tecnologicamente. A meta estratégica para essas empresas será obter vantagem tecnológica sobre os concorrentes. O desenvolvimento de TI deve estar alinhado com o negócio da empresa para criar vantagens de negócio. Entretanto, na maioria das organizações as lacunas entre o que os usuários esperam e o que a TI pode fornecer continuam a existir por causa das seguintes razões:

- Falta de definição dos requisitos de negócio
- Falta de capacidade de esclarecer as prioridades
- Complexidade dos projetos
- Falta de comprometimento da alta direção
- Problemas de comunicação entre o negócio e a TI

Então, baseada nas razões acima, a administração de TI precisa ser proativa e direta na solução dos problemas e na administração dos recursos. Para apoiar essa necessidade surge a Governança de TI, que se preocupa com as operações e desempenho dos negócios, transformando e posicionando a TI para alcançar os requisitos de negócio.

2.1.4 Alinhamento estratégico

O alinhamento estratégico se refere a alinhar a TI às estratégias do negócio. A questão chave é verificar se os investimentos da empresa em TI estão em harmonia com os objetivos estratégicos da empresa, e ainda se está desenvolvendo capacidades necessárias para entregar valor ao negócio.

2.1.4.1 Objetivos estratégicos

- Especificar os objetivos.
- Desenvolver estratégias para alcançar os objetivos especificados.
- Desenhar planos de ações para programar as estratégias.

2.1.4.2 Benefícios do alinhamento estratégico

- Valor agregado aos produtos e serviços da empresa.
- Ajuda no posicionamento competitivo da empresa.
- Uso otimizado dos recursos.

“Para alcançar a Governança de TI, as organizações utilizam modelos que possuem as melhores práticas para a gestão de TI. Entre esses modelos, os de maiores aceitação são o Cobit (ITGI, 2000) e o ITIL (OGC, 2002).”

2.2 COBIT (*Control Objectives for Information and Related Technologies*).

Trabalho desenvolvido desde 1996 por *Information Systems Audit and Control Foundation* (Isaca). Tem como objetivo fornecer boas práticas para a gestão de processo de tecnologia da informação, eliminando divergências entre riscos de negócios, questões técnicas, controles e medidas de desempenho. O Cobit foi desenvolvido com base no consenso de especialistas de todo o mundo no que concerne às melhores práticas e metodologias, tais como códigos de conduta (Conselho Europeu, OECD e Isaca), critérios de qualificação para os sistemas e processos de TI (ITSEC, TCSEC, ISO9000, SPICE e *Common Criteria*), padrões profissionais para controle interno e auditoria (Coso, Ifac, AICPA, Cica, Isaca, IIA, PCIE e GAO), práticas de mercado e requerimentos legais, governamentais e específicos dos mercados que dependem fortemente de tecnologia.

Os métodos propostos pelo Cobit contêm uma estrutura que responde às necessidades de gerenciamento, controle e medida da TI, utilizados no processo de negócio da empresa, mediante a utilização de 34 objetivos de controle de alto nível.

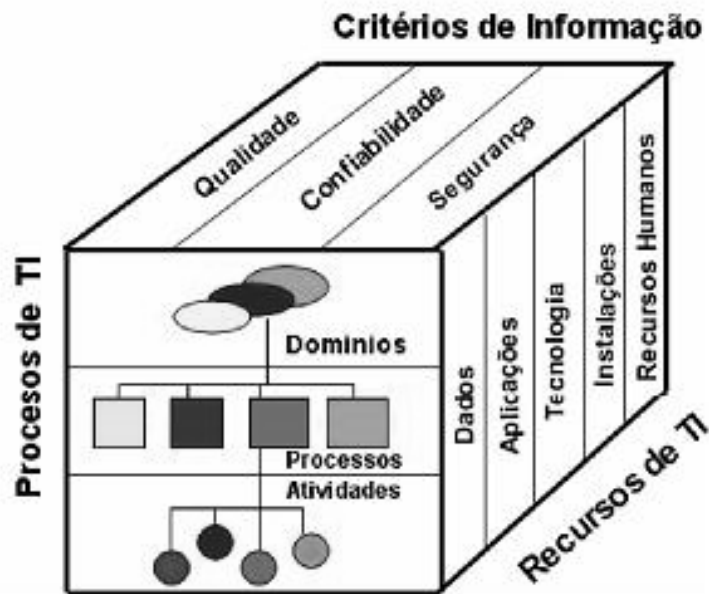


Figura 1 - Processos e domínios do Cobit (Fonte: www.consulting.com.br)

O Cobit define governança tecnológica como estrutura de relacionamentos entre processos para direcionar e controlar uma empresa, de modo a atingir os objetivos corporativos, agregando valor e risco controlado pelo uso da TI e de seus processos. O Cobit atende aos requisitos de um *framework* de controle. São eles:

- Define a linguagem comum para a área de TI e negócio
- Ajuda a atender aos requisitos regulatórios
- É padrão aceito entre empresas
- É orientado a processos
- É focado nos requisitos de negócio

Os métodos incluem:

- Elementos de medida de desempenho
- Fatores críticos de sucesso
- Modelo de maturidade

O Cobit está organizado em quatro grandes domínios: planejamento e organização, aquisição e implementação, entrega e suporte e, por último, monitoração. Os domínios são caracterizados por objetivos de controle e atividades executadas na governança tecnológica alinhada ao processo de negócio da empresa.

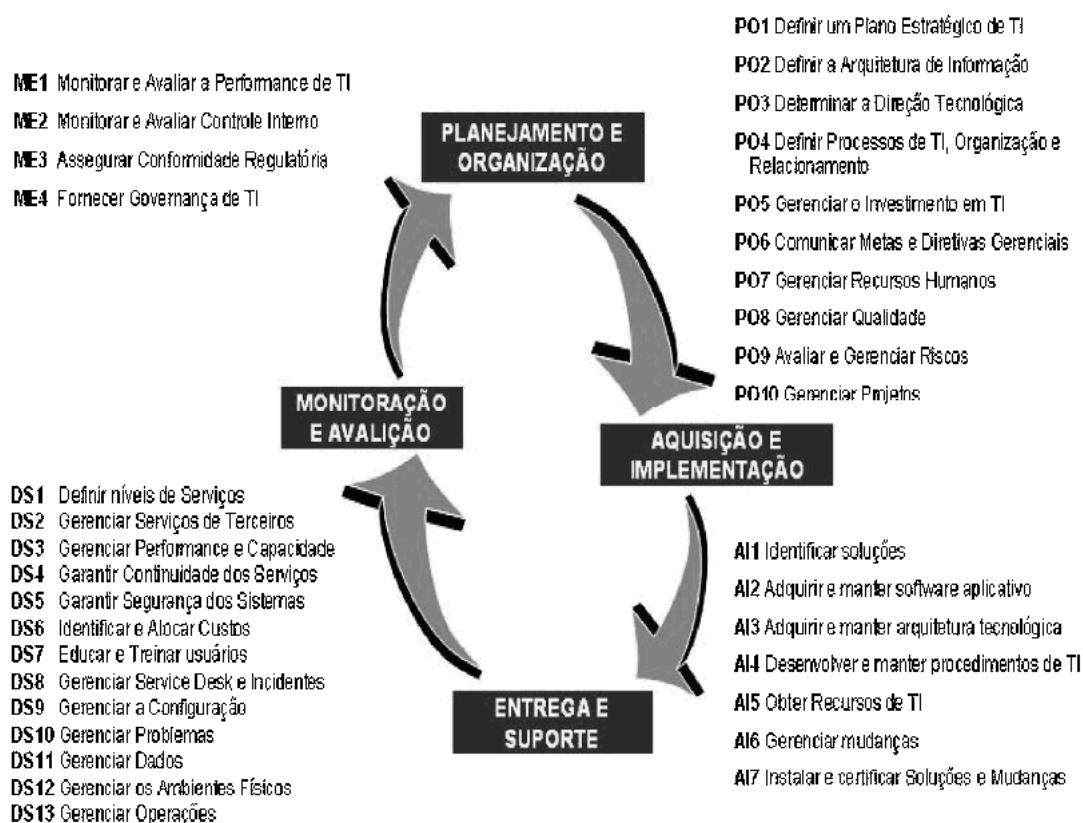


Figura 2 - Objetivos de Controle (Fonte: www.consulting.com.br)

2.3 A LÓGICA PARACONSISTENTE

A Lógica Paraconsistente teve como precursores o lógico russo N.A. Vasilev e o lógico polonês J. Lukasiewics. Ambos, em 1910, independentemente, publicaram trabalhos nos quais tratavam da possibilidade de uma lógica que não eliminasse as contradições. Todavia, os trabalhos desses autores, no tocante à paraconsistência, se restringiram à lógica aristotélica tradicional. Somente em 1948 e 1954 o lógico polonês S. Jaskowski e o lógico brasileiro N.C.A. da Costa, respectivamente, embora independentemente, construíram a Lógica Paraconsistente. Jaskowski formalizou um cálculo proposicional paraconsistente

denominado Cálculo Proposicional Discursivo (ou Discursivo), ao passo que Da Costa desenvolveu várias lógicas paraconsistentes contendo todos os níveis lógicos comuns. Também paralelamente, D. Nelson, em 1959, investigou os sistemas construtivos com negação forte, relacionados intimamente às idéias de paraconsistência.

Seja T uma teoria fundada sobre uma lógica L , e supondo-se que a linguagem de T e de L contenha um símbolo para a negação — se houver mais de uma negação, uma delas deve ser escolhida, pelas suas características lógico-formais, T diz-se inconsistente se ela possuir teoremas contraditórios; isto é, um é a negação do outro; caso contrário, T diz-se consistente. T diz-se trivial se todas as fórmulas de L — ou todas as fórmulas fechadas de L — forem teoremas de T ; em hipótese contrária, T diz-se não-trivial.

Analogamente, a mesma definição aplica-se a sistemas de proposições, conjunto de informações etc (levando-se em conta, naturalmente, o conjunto de suas conseqüências). Na lógica clássica e em muitas categorias de lógica, a consistência desempenha papel muito importante. Com efeito, na maioria dos sistemas lógicos usuais, uma teoria T é trivial, então T é inconsistente e reciprocamente uma lógica L chama-se paraconsistente se puder servir de base para teorias inconsistentes, mas não-triviais.

2.4 A LÓGICA PARACONSISTENTE ANOTADA

As lógicas paraconsistentes anotadas são famílias de lógicas não-clássicas, inicialmente empregadas em programação lógica. Posteriormente, várias aplicações foram estendidas por Blair, Subrahmanian, Kifer e outros. Por causa das aplicações obtidas, tornou-se conveniente um estudo dos fundamentos da lógica subjacente às linguagens de programação investigadas. Verificou-se que se tratava de uma Lógica Paraconsistente e que, em alguns casos, também continha características da lógica para completa e não-alética.

Os primeiros estudos sobre os fundamentos da LPA foram efetuados por DA COSTA et. al., 1991 (a); DA COSTA et. al., 1991 (b); ABE (1992). Em 1992, ABE estudou a lógica de predicados, teoria de modelos, teoria anotada de

conjuntos e alguns sistemas modais, estabelecendo-se estudo sistemático dos fundamentos das lógicas anotadas apontadas em trabalhos anteriores.

Outras aplicações dos sistemas anotados foram iniciadas por ABE, por volta de 1993, que, juntamente com discípulos, implementou a linguagem de programação paraconsistente Paralog (ÁVILA, ABE & PRADO 97), independentemente dos resultados de Subrahmanian. Tais idéias foram aplicadas na especificação de uma arquitetura, baseada na LPA, que integra vários sistemas computacionais – planejadores, base de dados, sistemas de visão etc – na construção de uma célula de manufatura (PRADO 96) e na representação de conhecimento por *Frames*, permitindo representar inconsistências e exceções (ÁVILA 96).

Em (ABE 99), (ABE 98), (ABE 01a) foram introduzidos circuitos digitais (portas lógicas Complement, And e Or), inspirados nas LPAs. Tais circuitos permitem sinais “conflitantes”, implementados em sua estrutura de modo não-trivial. Acreditamos que a contribuição dos circuitos elétricos paraconsistentes seja pioneira na área dos circuitos elétricos, abrindo novas vias de investigações. Nas pesquisas referentes, ainda na parte de hardware, a grande contribuição foi a edificação do analisador lógico – paraanalisador – que permite tratar conceitos de incerteza, inconsistência e paracompleteza (ABE 99a). Também baseados nas lógicas anotadas, foram construídos controladores lógicos – paracontrol, simuladores lógicos – parasim, dispositivo para tratamento de sinais – parasônico (ABE 03). Como materialização dos conceitos discutidos construiu-se o primeiro robô com hardware paraconsistente: protótipo I, que recebeu o nome de Emmy (DA SILVA FILHO, ABE 01), e está sendo construído o protótipo II.

Os sistemas anotados abarcam aspectos dos conceitos envolvidos em raciocínio não-monotônico, *defesiabile*, *default* e deontico (NAKAMATSU, ABE, SUZUKI 00).

Intuitivamente, na LPA bivalorada o que se faz é atribuir uma anotação (μ_1 ; μ_2), com μ_1 e μ_2 pertencentes ao intervalo fechado $[0; 1]$, a cada proposição elementar (atômica) p de tal modo que μ_1 traduza o grau de crença (ou evidência

favorável) que se tem em p e μ_2 , o grau de descrença (ou evidência contrária) (ABE, 1992).

O conjunto $[0; 1]^2$ ou $[0; 1] \times [0; 1]$, dotado de uma relação de ordem $*$ tal que $(\mu_1; \mu_2) * (\mu_1; \mu_2)$ se e somente se $\mu_1 = \mu_1$ e $\mu_2 = \mu_2$, onde $=$ é a relação de ordem total habitual dos números reais, constitui um reticulado (reticulado das anotações), que denominamos também Quadrado Unitário de Plano Cartesiano (QUPC). Cada par $(\mu_1; \mu_2)$ constitui um estado lógico. Destacam-se os seguintes estados lógicos extremos:

$(1; 0)$ representa, intuitivamente, crença total e nenhuma descrença (traduz um estado lógico que chamamos de verdade, representado por V);

$(0; 1)$ representa, intuitivamente, nenhuma crença e descrença total (traduz um estado lógico que chamamos de falsidade, representado por F);

$(1; 1)$ representa, intuitivamente, ao mesmo tempo crença e descrença totais (traduz um estado lógico que chamamos de inconsistência, representado por -), e

$(0; 0)$ indica ausência total de crença e de descrença (traduz um estado lógico que chamamos de paracompleteza ou de indeterminação, representado por ?).

2.5 BSC – BALANCED SCORECARD

O BSC (*Balanced Scorecard*) foi desenvolvido por Robert Kaplan e David Norton no início da década de 90. É um novo modelo de gestão estratégica, baseado em indicadores financeiros e não financeiros, vinculados à estratégia organizacional e divididos em quatro perspectivas de avaliação: perspectiva financeira, dos clientes, dos processos internos e do aprendizado e crescimento (KAPLAN, NORTON 1997).

O BSC é ferramenta que materializa a visão e a estratégia da empresa por meio de um mapa coerente com objetivos e medidas de desempenho, organizados segundo quatro perspectivas diferentes: financeira, do cliente, dos processos internos e do aprendizado e crescimento. Tais medidas devem ser interligadas para comunicar um pequeno número de temas estratégicos amplos, como o crescimento da empresa, a redução de riscos ou o aumento de produtividade.

Segundo seus criadores, KAPLAN & NORTON (1997: 09), “os objetivos e as medidas utilizadas no BSC não se limitam a um conjunto aleatório de medidas de desempenho financeiro e não financeiro, pois derivam de um processo hierárquico de cima para baixo, norteado pela missão e pela estratégia da unidade de negócios”.

O conceito do BSC tem sido aplicado nos processos de Tecnologia da Informação. Considerando que a área de TI é provedora de serviços internos, (HAES et al. 2004) sugerem que as perspectivas propostas originalmente pela metodologia do BSC devem ser mudadas para contribuição com a corporação, orientação para usuários, excelência operacional e orientação para o futuro. (Haes et al., 2004) citam também que a ligação entre o BSC Corporativo e o BSC da área de TI é considerada mecanismo de suporte para a Governança de TI.

2.6 MODELO DE GOVERNANÇA DE TI, A PARTIR DE INDICADORES DE DESEMPENHO

2.6.1 Indicadores de Desempenho

Por meio do sistema de medição de desempenho, gestores podem obter com maior facilidade informações de produtividade da empresa. Informações que auxiliam a tomada de decisão e em ações para processo de melhoria da produtividade e qualidade da empresa.

Medir processos é etapa inicial para se obter o controle e, conseqüentemente, a melhoria, ou seja, se o processo não é ou não pode ser mensurável, então também não poderá ser entendido, desta forma, um processo não entendido e não controlado, não poderá ser melhorado.

A utilização de indicadores ajuda o executivo a atuar com maior objetividade na tomada de decisão e direcionar atenção da alta administração nos problemas importantes.

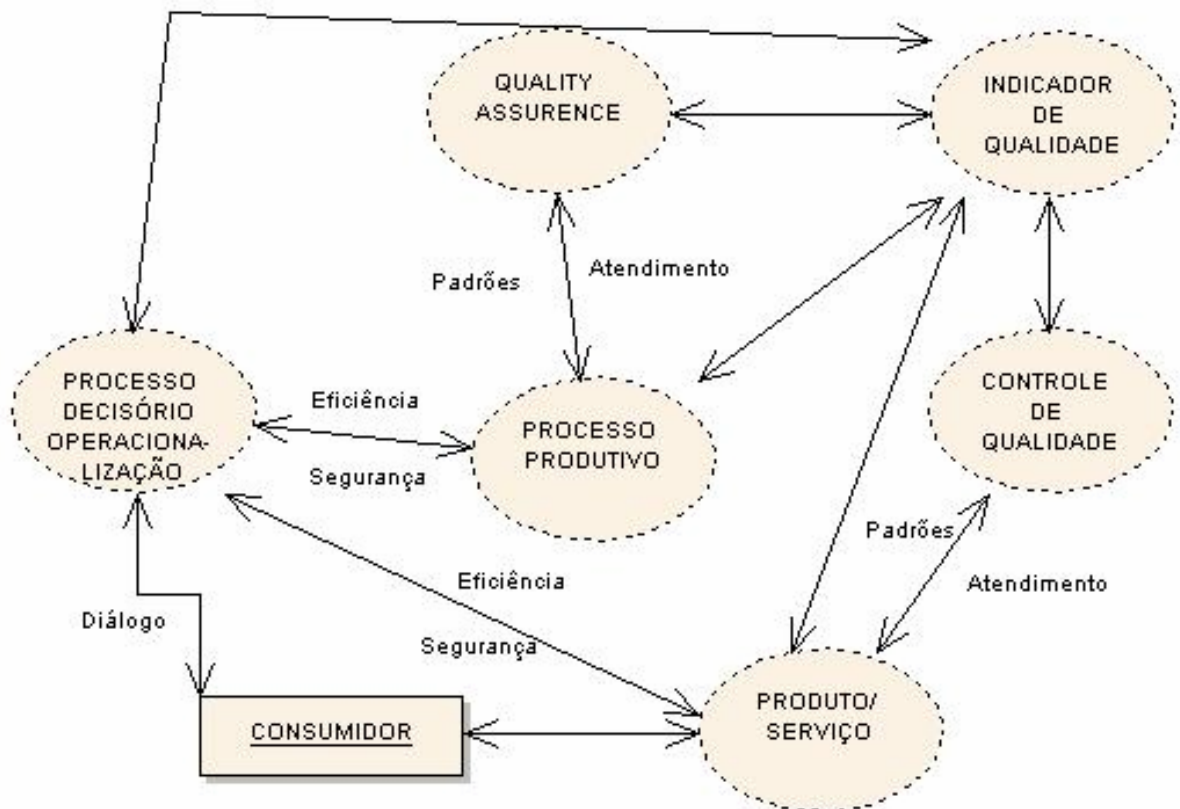


Figura 3 - Design UML Indicadores como mecanismo que ajuda a tomadas de decisão (baseado, Gil 1992).

2.6.2 Classificação e benefícios dos indicadores de desempenho na gestão estratégica

2.6.2.1 Indicadores de qualidade

Está ligado ao nível de satisfação do cliente, pois toda medida analisada pode ser considerada nova oportunidade de melhoria no atendimento das necessidades do cliente. Ou seja, conquistar qualidade é imprescindível para também conquistar o cliente. "Indicadores de qualidade são aqueles que medem diretamente os desempenhos relacionados às necessidades e satisfação dos clientes, através dos quais medimos os resultados de nosso trabalho na ótica dos usuários". (Sebrae, 1995).

2.6.2.2 Indicadores de produtividade

Mede o esforço em fazer algo. Ex: criar um produto mais personalizado às necessidades dos clientes, com menor custo e tempo possível. "Indicadores de produtividade medem o desempenho dos diferentes processos da empresa, o esforço em fazer coisas. Relacionam-se ao modo pelo qual são utilizados os recursos disponíveis". (Sebrae, 1995). "Indicadores de produtividade é a relação entre os resultados (outputs) e os recursos utilizados (inputs)".

2.6.2.3 Utilização dos indicadores

No controle de redução de variações, auto-avaliação no uso de medidas em processos, definir novas implementações, melhoria contínua na identificação da fonte de problemas, determinar eficiência dos processos, avaliação administrativa na análise de medições feitas para definição de eficiência.

Benefícios imediatos:

- Menos reuniões gerenciais
- Diminuição dos relatórios de desempenho
- Aumento do foco nas ações gerenciais
- Maior entendimento dos dados e interpretação das informações
- Melhor comunicação sobre metas e missões

Benefícios de médio e longo prazo:

- Quantidade de re-trabalho reduzida
- Redução do *Total Cost Ownership* (TCO)
- Redução nos fatores que impactam na produtividade
- Avaliação das decisões
- Ganho na produtividade gerencial

3 MÉTODO DE PESQUISA

A metodologia adotada durante este trabalho está fundamentada na utilização de um questionário de acordo com os domínios do Cobit, que foi desenvolvido para ajudar a empresa a medir a capacidade de reunir os objetivos de controle do Cobit que estão em aderência com a seção 404 do ato SOX, o qual possibilitou perceber e compreender as principais dificuldades encontradas na avaliação de uma empresa de TI. Esse questionário é submetido a liderança e a vários especialistas. A metodologia inclui a Lógica Paraconsistente, que permite avaliar o grau de coerência dos avaliadores, onde suas opiniões são requisitos necessários para aplicação do *framework* e dos conceitos da Lógica Paraconsistente, a fim de desenvolver um método para avaliação da conformidade de Governança de TI.

3.1 COLETA DOS DADOS

A partir de meados da década de 90 a internet vem sendo utilizada como ambiente de coleta em levantamentos de dados e experimentos nas diversas áreas. A aplicação de instrumentos de pesquisa por questionário na *World Wide Web* apresenta vantagens, como redução de custos, possibilidade de atingir segmentos populacionais amplos e diversificados, e facilidades na tabulação dos dados em bancos estatísticos. Há limitações de controle, como abertura diferenciada a fraudes, auto-seleção de participantes e diferenças dos meios técnicos disponíveis. Todavia, são problemas que podem ser neutralizados se forem tomadas algumas precauções.

O questionário foi disponibilizado em um *website* em que o respondente pudesse preenchê-lo via internet. Nesse método, o respondente interage com o instrumento via internet, usando seu próprio computador, *modem* e *browser*. O questionário (Anexo A) é composto por uma parte inicial, na qual o respondente preenche seus dados e os dados da organização.

3.2 PREENCHIMENTO DO QUESTIONÁRIO.

Os dados coletados devem seguir essas condições: cada questão tem 6 respostas possíveis, partindo do 0 até o 5. Se a organização marcar “3”, “4” ou “5” numa questão, significará que a empresa possui os objetivos de controle adequados naquela área. Por outro lado, se a empresa responder “0”, “1” ou “2” numa questão, significa que será necessário consultar o Cobit e verificar quais controles recomenda-se implantar para colocar a empresa na direção da aderência à SOX. Cada resposta possui um valor baseado na criticidade da demanda que a questão endereça. Respondendo a cada questão com o valor apropriado, por fim tem-se um total de pontos. Respostas “0” ou “1” são críticas para aderência à SOX, consideradas falha total de aderência, independentemente do valor total do questionário, isto é, não serão aceitas num processo de auditoria, e devem ser endereçadas independentemente do valor total alcançado no questionário.

3.3 MODELO PROPOSTO PARA AVALIAÇÃO DE CONFORMIDADES EM GOVERNANÇA DE TI

O modelo proposto para avaliação de conformidades em Governança de TI considera que o principal objetivo a ser alcançado é a melhoria do processo de tomada de decisão e avaliação da conformidade em Governança de TI, por meio da identificação e avaliação das unidades de controle baseadas no Cobit .

Quanto menos incerteza e divergência se tenham acerca do grau de conformidade avaliado pelos especialistas, mais assertiva e mais bem embasada será a decisão. Para que essa assertividade seja alcançada, o método proposto disponibiliza duas dimensões de análise:

A busca das informações de uma mesma base de dados proporciona resultados que consideram a incerteza e a divergência presentes nas opiniões dos diferentes especialistas, minimizando-as. Essa dimensão é importantíssima, visto que a percepção das alternativas, que depende tanto do conhecimento

sobre a empresa quanto das características cognitivas do indivíduo que o percebe registrando os aspectos observados da organização do qual faz parte, esses especialistas também atribuem significados e valores aos mesmos.

A necessidade dessa dimensão é justificada ainda pelo fato de que alguns especialistas tenderem a valorizar seu trabalho, de forma individualizada, procedimento que dificulta a comunicação, além de restringir, de maneira segmentada e dispersa, o conhecimento tecnológico do produto. Courtney (Kirkland & Viguerie 1997) alerta também para a armadilha de "se perceber incerteza de uma maneira binária - supondo que o mundo ou é certo e, portanto, aberto para previsões precisas sobre o futuro, ou é incerto e, portanto, completamente imprevisível".

Em seguida, apresenta as unidades de controle em referência, após avaliação qualitativa das conformidades, o qual sugere que sejam os prioritários na tomada de decisão.

A metodologia utilizada neste trabalho baseia-se na adoção parcial de elementos e pré-requisitos necessários para aplicação de conceitos da Lógica Paraconsistente, a fim de desenvolver um método para avaliação da conformidade. A figura 4 apresenta um escopo geral do método proposto em *design* UML:

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

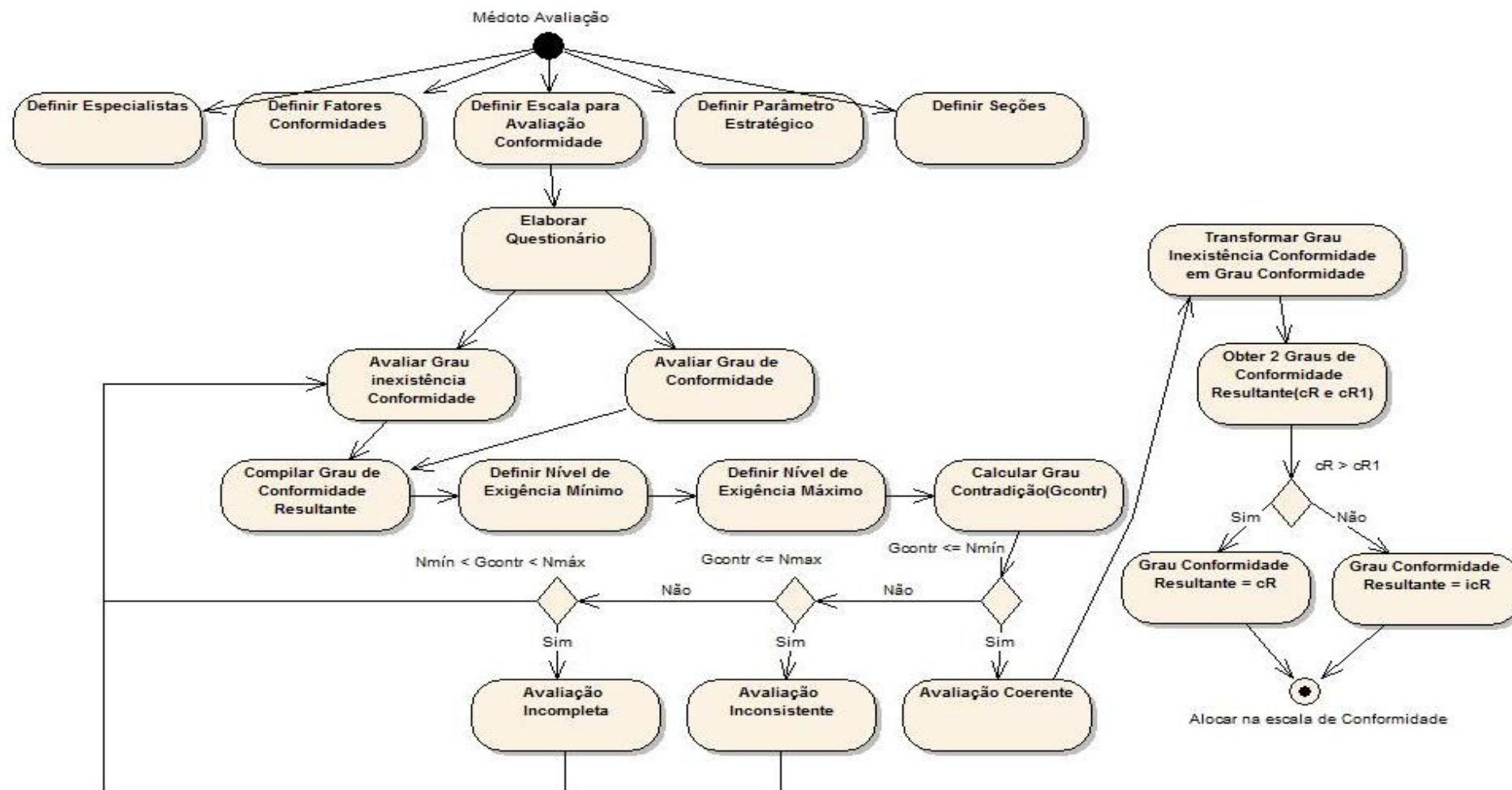


Figura 4 - Design UML do método para avaliação de conformidade em Governança de TI

Para o alcance do propósito do presente trabalho, sinteticamente adotaram-se 11 etapas de desenvolvimento, como segue:

1. Seleção das iniciativas a serem avaliadas.
2. Definição dos especialistas diretamente envolvidos nas áreas de abrangência de uma organização. A função dos especialistas é identificar e avaliar as unidades de controle baseadas nos *frameworks* descritos neste trabalho.
3. Identificação das unidades de controle utilizando-se o referencial teórico, com a avaliação de especialistas diretamente envolvidos na área em questão. Os especialistas verificam conjuntamente as especificações utilizadas ou definidas pela organização, suas origens, seus critérios de aplicação, aceitação, controle e certificação.
4. Estabelecimento das alternativas de cada uma das unidades de controle, ou seja, dos parâmetros que justificam a conformidade presente em cada uma das unidades identificadas. Essa etapa utiliza a escala de maturidade do Cobit.
5. Determinação de uma escala que servirá de base para avaliação da conformidade das seções por parte dos especialistas, com valores que variam de 0 a 5, bem como dos critérios correlacionados aos valores da escala. Quanto maior o valor na escala, maior a gravidade.
6. Elaboração de questionário de pesquisa em uma coleta de dados, cujas informações devem apresentar as unidades de controle e suas alternativas a eles associadas, identificadas nas etapas 3 e 4, e as respostas dos especialistas definidas na etapa 2, que avaliarão a conformidade.

Duas variáveis servem de parâmetro para a avaliação da conformidade, por meio dos valores da escala definida na etapa 5:

- Grau de conformidade (c);
- Grau de inexistência de conformidade (ic).

7. Aplicação do questionário para os especialistas em duas etapas:

- A primeira visa coletar o grau de conformidade (c), ou seja, o quão crítico cada especialista acredita que seja uma determinada unidade de controle, em caso de ocorrência do mesmo;
- Algum dia, após a finalização da primeira coleta, aplica-se novamente o mesmo questionário, para os mesmos especialistas, com o objetivo de coletar o grau de inexistência de conformidade (ic).

8. Definição do parâmetro estratégico que servirá de base para obtenção do índice resultante de conformidade e, posteriormente, para tomada de decisão por parte do gerente de projeto. Esse parâmetro está diretamente relacionado à estratégia do negócio, definida no plano diretor da organização, que pode apresentar-se, por exemplo, da seguinte forma:

- Conservadora (maior segurança possível para a tomada de decisão);
- Intermediária (decisão mais econômica, porém sujeita a riscos);
- Otimista (decisão mais arriscada / agressiva).

Considerando que a análise de conformidades de Governança de TI é, por natureza, uma atividade carregada de subjetividade, e que avaliações errôneas por parte dos especialistas podem impactar significativamente o alcance do sucesso da organização, é de se esperar que padrões organizacionais estabelecidos forneçam diretrizes para abordagem da avaliação da conformidade das unidades de controle identificados e avaliados (SALLES et al., 2007).

O método proposto flexibiliza a avaliação de conformidade ao permitir a criação de outros agrupamentos para o parâmetro estratégico, além dos especificados acima.

9. Obtenção dos graus de conformidade (cR) e inexistência de conformidade (icR) resultante, para cada fator e seção, com a utilização dos parâmetros lógicos paraconsistentes, cuja aplicação dependerá diretamente do parâmetro estratégico definido.

Segundo Da Costa 1974, a Lógica Paraconsistente utiliza três diferentes conectores para compilação das informações:

Operador **NOT** é definido por: $\text{NOT}(\mu_1; \lambda_1) = (\lambda_1; \mu_1)$. O operador NOT deve corresponder à negação da lógica anotada. Notemos que $\text{NOT } V = F$ e $\text{NOT } F = V$.

O operador **OR** é definido por: $(\mu_1; \lambda_1) \text{ OR } (\mu_2; \lambda_2) = (\text{Max}\{\mu_1, \mu_2\}; \text{Max}\{\lambda_1, \lambda_2\})$. Este operador tem o mesmo sentido da *disjunção* clássica, ou seja, de fazer a *maximização*.

O operador **AND** é definido por: $(\mu_1; \lambda_1) \text{ AND } (\mu_2; \lambda_2) = (\text{min}\{\mu_1, \mu_2\}; \text{min}\{\lambda_1, \lambda_2\})$. Seu sentido é o mesmo da *conjunção* clássica, ou seja, de fazer a *minimização*.

Para o **parâmetro estratégico conservador**, adota-se o maior índice de conformidade entre os avaliados pelos especialistas (maior *c*), bem como o menor índice de inexistência de conformidade (menor *ic*). Para isso aplica-se a técnica de maximização (OR) para *c* (conformidade) e a técnica de minimização (AND) para *ic* (inexistência de conformidade), como segue:

$$[(\text{Gr.A } c1)] \text{ OR } [(\text{Gr.B } c2)] \text{ OR } [(\text{Gr.C } c3)] \text{ OR } [(\text{Gr.D } c4)] \dots$$

$$[(\text{Gr.A } ic1)] \text{ AND } [(\text{Gr.B } ic2)] \text{ AND } [(\text{Gr.C } ic3)] \text{ AND } [(\text{Gr.D } ic4)] \dots$$

Para o **parâmetro estratégico otimista**, adota-se o menor índice de conformidade entre os avaliados pelos especialistas (menor *c*), bem como o maior índice de inexistência de conformidade (menor *ic*). Para isso aplica-se a técnica de minimização (AND) para *c*

(conformidade) e a técnica de maximização (OR) para *ic* (inexistência de conformidade), como segue:

$[(Gr.A\ c1)]\ AND[(Gr.B\ c2)]\ AND\ [(Gr.C\ c3)]\ AND[(Gr.D\ c4)]\ \dots$

$[(Gr.A\ ic1)]\ OR[(Gr.B\ ic2)]\ OR\ [(Gr.C\ ic3)]\ OR\ [(Gr.D\ ic4)]\ \dots$

Para o **parâmetro estratégico intermediário**, adota-se a mediana de ambos os índices (*c*) e (*ic*) avaliados, como segue:

MEDIANA (*c1*; *c2*; *c3*; *c4*)...

MEDIANA (*ic1*; *ic2*; *ic3*; *ic4*) ...

10. Avaliação final dos dados resultantes a partir de três importantes etapas:

- a. Cálculo do Grau de contradição (G_{contr}), onde $G_{contr} = [(\mu R1 + \mu R2) - 1]$. O valor resultante determinará quão convergentes são as opiniões dos diferentes especialistas acerca da conformidade das unidades de controle, ou seja, o grau de concordância entre os especialistas. O valor do grau de contradição é correspondente à distância do ponto de interpolação entre os graus de conformidade e de inexistência de conformidade.

No cálculo deve-se assumir o módulo dos graus de contradição resultantes, evitando valores negativos, os quais atrapalham a análise.

- b. Paralelamente é necessário definir os níveis de exigência mínimos ($N_{exig\ mínimo}$) e máximo ($N_{exig\ máximo}$), os quais, neste estudo, traduzirão os graus mínimo e máximo de contradição aceitos pelos gestores da empresa estudo de caso, quanto à convergência apresentada pelas opiniões expressas pelos diferentes especialistas acerca do índice de conformidade das unidades de controle, possibilitando a eles tomar decisões mais assertivas.

Como sugestão para definição dos níveis de exigência mínimo e máximo, pode ser efetuado um paralelo com a escala de

conformidade definida na etapa 5, considerando adicionalmente o parâmetro estratégico definido na etapa 8.

Sendo assim, assume-se que:

- i. $G_{\text{contr}} \leq N_{\text{exig mínimo aceitável}}$: *Avaliação Coerente*, ou seja, praticamente não há divergência de opiniões.

Decisão: a avaliação de conformidade das unidades de controle será realizada

- ii. $G_{\text{contr}} > N_{\text{exig máximo aceitável}}$: *Avaliação Inconsistente*, visto que a avaliação dos especialistas apresenta-se pouco confiável, por causa da grande divergência das opiniões.

Decisão: a avaliação da conformidade das unidades de controle será descartada

- iii. $N_{\text{exig mínimo}} < G_{\text{contr}} < N_{\text{exig máximo}}$: *Avaliação Incompleta*.

Decisão: sugere-se que nova pesquisa ou coleta de algumas informações adicionais seja realizada com os especialistas, para que os resultados estejam concretamente na escala de coerência ou, no pior caso, de inconsistente.

Essa definição dos parâmetros para análise do grau de contradição proporcionará a finalização da 1ª etapa, decisiva para continuidade da avaliação de conformidade.

- c. Para as unidades de controle cujo Grau de contradição (G_{contr}) apresentar-se menor ou igual ao Nível de Exigência mínima ($N_{\text{exig mínimo}}$) preestabelecida, a avaliação da conformidade é classificada como “Coerente”, aguardando as análises. Para que possamos avaliar a conformidade, é necessário determinar o índice de conformidade das unidades de controle, o qual torna-se possível da seguinte forma:

- i. Adotar o grau de conformidade resultante (cR);

- ii. Transformar o grau de inexistência de conformidade resultante (icR) também em grau de conformidade. Para isso basta que seja feita a subtração da unidade, ou seja, o complemento do grau de inexistência de conformidade resultante em relação à unidade = $1 - icR$. (ABE 2000);
- iii. Com isso, obteremos dois graus resultantes de conformidade (cR e $cR1$), os quais, de acordo com o conceito aplicado na pesquisa, Os índices de conformidade avaliados para cada unidade de controle os quais assumiremos o maior índice de conformidade entre os dois obtidos na etapa anterior (cR ou $cR1$).

Alocação do maior índice de conformidade resultante na escala de conformidade adotada, conforme Figura 1, e os resultados obtidos são os resultados finais alcançados com o uso do método proposto, apoiado nos parâmetros da Lógica Paraconsistente.

3.4 FLUXOGRAMA

O Fluxograma abaixo apresenta o método aqui descrito:

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

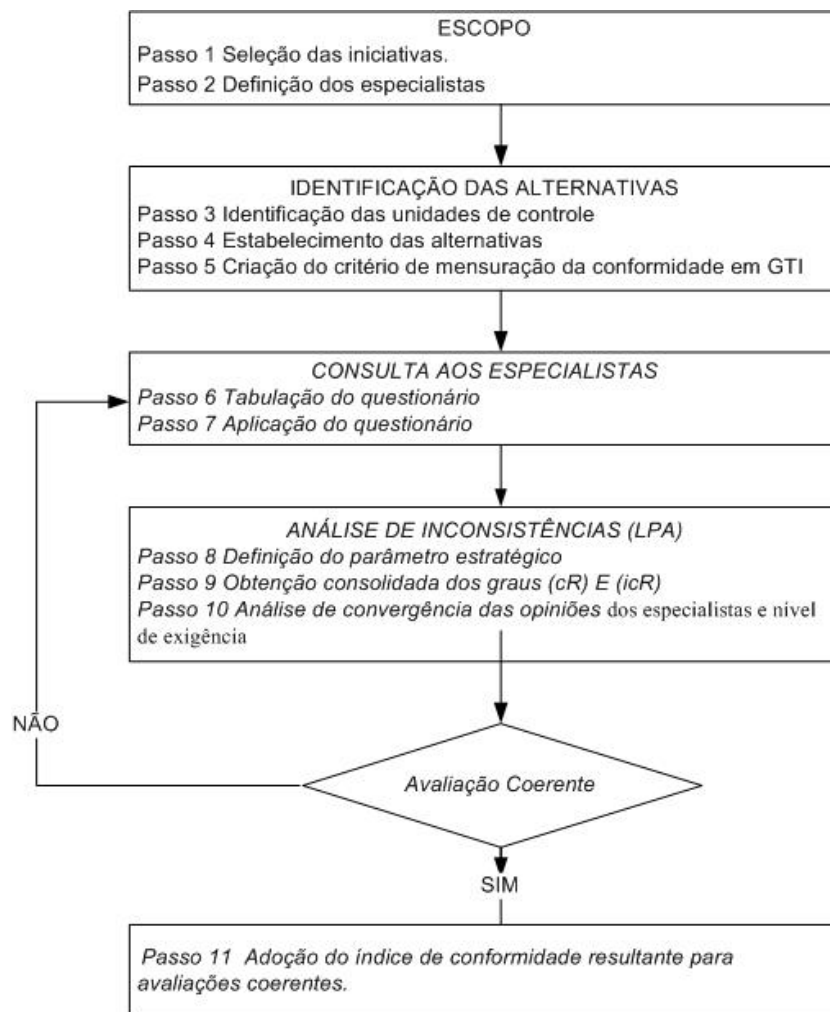


Figura 5 - Fluxograma do método para avaliação de conformidade em Governança de TI

4 APLICAÇÃO DO MÉTODO

4.1 DESENVOLVIMENTO

A metodologia de pesquisa descrita foi aplicada em um estudo de caso de uma empresa do ramo de cosméticos, como descrito a seguir:

Passo 1 - Seleção das iniciativas

Adotou-se um conjunto de iniciativas que definem o nível de conformidade de TI da empresa onde o método foi aplicado.

Passo 2 - Definição dos especialistas

Definiram-se quatro grupos distintos de especialistas:

Grupo A – Especialista Área de Planejamento

Grupo B – Especialista Área de Engenharia de Produtos

Grupo C – Especialista Área de Tecnologia

Grupo D – Especialista Área de Testes, conhecida por QA (*Quality Assurance*)

A seleção dos grupos de especialistas deu-se na separação em áreas distintas na organização. Desta forma, haverá a opinião dos mesmos que estão diretamente envolvidos nas principais áreas da organização.

Passo 3 - Identificação das unidades de controle

Identificaram-se 20 unidades de controle baseadas nos objetivos do Cobit, descritos na tabela 1, para a utilização do método proposto neste trabalho, os quais definem os indicadores relacionados ao nível de conformidade em Governança de TI.

Tabela 1 - Unidades de controle baseadas no Cobit.

Área Conformidade SOX	Unidades de Controle
Planejar e Organizar	A empresa possui um esquema para classificar dados em um dicionário ou catálogo de dados?
	A estrutura organizacional da empresa provê uma segregação de funções adequada?
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?
	Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?
	Sua empresa tem em andamento um programa que garanta a aderência ao SOX?
Adquirir e Implementar	Os requerimentos de segurança foram colhidos e documentados para todos os produtos de software que serão implementados em todos os sistemas que terão impacto nos relatórios financeiros da empresa?
	Os sistemas relacionados ao SOX foram construídos de acordo com padrões de configuração pré-definidos? Eles descrevem o Sistema Operacional e as configurações dos aplicativos que são necessários para se manter a segurança das aplicações e serviços que são executados nestes sistemas?
	Os sistemas relacionados ao SOX estão configurados para capturar os acessos dos usuários?
	Os sistemas relacionados ao SOX (incluindo infra-estrutura e rede) estão mantidos sob rígido
	Os sistemas relacionados ao SOX são testados e reconhecidos regularmente para garantir que configurações, privilégios e contas de usuários são apropriadas e consistentes com o que foi definido nas configurações e regras?
Entregar e Suportar	Sua empresa conduz inspeções regulares de segurança da informação em terceiros?
	Todos os sistemas e aplicativos envolvidos em (ou suportando) relatórios financeiros possuem controles de acesso e autenticação segura implementados de forma efetiva?
	As contas de usuários são gerenciadas de forma definida e continua com as devidas aprovações de <i>workflow</i> sobre seus proprietários e custodiantes? Existem LOGs e documentação referente a privilégios conferidos a contas de usuários?
	A empresa executa avaliações regulares sobre contas e privilégios?
	A empresa conduz testes regulares de segurança nos sistemas relacionados ao SOX de forma a certificar-se de que as configurações são as que deveriam ser e os sistemas permanecem seguros?
Monitorar e Avaliar	A empresa gerencia suas vulnerabilidades e aplica correções de forma uniforme através de todos os sistemas relacionados ao SOX?
	A empresa monitora a efetividade dos controles de segurança implementados para a aderência ao SOX?
	A empresa contrata terceiros com expertise específica para avaliar e conferir seus processos e controles de TI?
	A empresa envolve de forma pro ativa a auditoria interna antes de finalizar os planos de TI?
	A empresa realiza consultas a terceiros sobre a aderência às leis e regulamentações (ex. SOX e privacidade)?

Passo 4 - Estabelecimento das alternativas

Identificaram-se as 120 alternativas relacionadas às unidades de controle, que no estudo representaram à escala de medida do grau de conformidade (figura 6), nas alternativas selecionadas. Essa abordagem é derivada do modelo de maturidade para desenvolvimento de software, *Capability Maturity Model for Software* (SW-CMM), proposto pelo *Software Engineering Institute* (SEI).



Figura 6 - Escala com índices para classificação da conformidade. (Fonte: Cobit)

No desenvolvimento desse item não foi considerado se haverá ou não a conformidade, mas quais são as formas possíveis de avaliar certo tipo de alternativa. Após compilação dos dados, segue as alternativas (tabela 2), abaixo.

Tabela 2 - Unidades de Controle x Alternativas

Unidade de Controle	Alternativas
A empresa possui um esquema para classificarem dados em um dicionário ou catalogo de dados	Não existe definição para este item.
	A Empresa não tem um esquema de classificação da informação ou catalogo ou dicionário ou inventario de dados.
	Existe um esquema para algumas informações, mas sem documentação formal.
	Existe um esquema repetitivo, mas intuitivo, baseado no conhecimento interno da empresa.
	Existe um processo documentado.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
A estrutura organizacional da empresa provê uma segregação de funções adequada?	Não existe definição para este item.
	Não existe segregação de funções baseadas em regras.
	Existe alguma segregação, mas sem processos formais.
	Existe uma segregação apropriada com alguma documentação.
	Existem regras formalmente documentadas e que são revisadas regularmente.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	Não existe definição para este item.
	Não existe um escritório de segurança na empresa.
	A responsabilidade pelo gerenciamento da segurança é compartilhada através do gerenciamento das operações de TI da empresa.
	Existe um gerenciamento de segurança dedicado, mas que se reporta ao TI.
	O gerenciamento da segurança reporta-se ao gerenciamento corporativo no mesmo nível que um CIO.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?	Não existe definição para este item.
	Não existem políticas de segurança.
	Existem algumas políticas nas não são atualizadas nem abrangentes.
	Existem políticas para as maiores prioridades que afetam a aderência ao SOX (por ex:manutenção de contas, responsabilidades pela segurança, segregação de funções, controle de mudanças).
	Existe um conjunto completo e atualizado de políticas e acompanhamento de procedimentos.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	Não existe definição para este item.
	Não existem processos estabelecidos que produzam evidencias de aderência.
	Produziu-se um esforço de aderência, uma vez, no passado, mas nunca mais foi repetido.

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

	Existe um processo repetitivo, mas não é parte de um processo contínuo e atualizado.
	Existe um programa formal e continuado que provê evidências de aderência e o status para corrigir deficiências.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Os requerimentos de segurança foram colhidos e documentados para todos os produtos de software que serão implementados em todos os sistemas que terão impacto nos relatórios financeiros da empresa?	Não existe definição para este item.
	Não existem requerimentos de segurança especificados.
	Existem requerimentos de segurança especificados para alguns produtos, mas não de forma consistente.
	Existe um conjunto padrão de requerimentos de segurança que é usado para todos os softwares, mas não especificamente para os que impactam nos relatórios financeiros da empresa.
	Existem requerimentos de segurança documentados e utilizados na seleção de todos os softwares usados no ambiente SOX.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Os sistemas relacionados ao SOX foram construídos de acordo com padrões de configuração pré-definidos? Eles descrevem o Sistema Operacional e as configurações dos aplicativos que são necessários para se manter a segurança das aplicações e serviços que são executados nestes sistemas?	Não existe definição para este item.
	Não existem padrões. Os sistemas foram implantados e são operados conforme recebidos dos fornecedores.
	Existe alguma coisa feita pontualmente, mas não foi documentada.
	Existe um processo construído de forma intuitiva, mas a documentação ainda é inadequada.
	Existe um processo construído de forma disciplinada e documentada.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Os sistemas relacionados ao SOX estão configurados para capturar os acessos dos usuários	Não existe definição para este item.
	A função de LOG não está habilitada.
	A função de LOG está habilitada, mas o processo não captura todos os acessos, e/ou os registros são sobregravados de acordo com o tamanho do arquivo.
	A função de LOG está habilitada para todos os acessos e os LOGS são revisados, mas não arquivados.
	A função de LOG está habilitada, os LOGS são revisados e os registros são arquivados por um ano.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Os sistemas relacionados ao SOX (incluindo infra-estrutura e rede) estão mantidos sob rígido	Não existe definição para este item.
	Não existe controle de mudanças.
	Existem algumas anotações pontuais sobre mudanças, mas não existe nenhum processo ou mecanismo formal de controle.
	Existem vários mecanismos de controle de mudanças que são usados em vários tipos de sistemas, permitindo um efetivo, porém complicado controle.

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

	Existe um centralizado, consistente e bem documentado sistema de controle de mudanças usado para o ambiente SOX.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Os sistemas relacionados ao SOX são testados e reconhecidos regularmente para garantir que configurações, privilégios e contas de usuários são apropriadas e consistentes com o que foi definido nas configurações e regras?	Não existe definição para este item.
	Não existe um processo regular de avaliação.
	Existem reconhecimentos pontuais implementados apenas para sistemas importantes.
	Existem processos regulares de testes que verificam contas de usuários e configuração de sistemas, mas não estão documentados e/ou não são abrangentes.
	É abrangente, regular, bem documentada, reconhecidos oficialmente e com retorno para processos de correção nos processos deficientes.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Sua empresa conduz inspeções regulares de segurança da informação em terceiros	Não existe definição para este item.
	Não existe inspeção a serviços e produtos contratados de terceiros.
	Existem inspeções pontuais com um mínimo de evidencias documentadas aderentes aos padrões da empresa.
	Existem inspeções e evidencias documentada, mas não existem processos formais para revisar os terceiros para retificá-los ou reconhecê-los oficialmente.
	Existem inspeções regulares utilizando-se avaliações padrão e evidencias documentada da aderência ao SOX.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
Todos os sistemas e aplicativos envolvidos em (ou suportando) relatórios financeiros possuem controles de acesso e autenticação segura implementados de forma efetiva?	Não existe definição para este item.
	Os sistemas são configurados para autenticação, os usuários compartilham contas e/ou tem acesso de administrador em sistemas e aplicações envolvidos em relatórios financeiros.
	Os sistemas são configurados uma vez para cada usuário, mas não existe mais nada que garanta que as funções são segregadas ou que as interfaces estão expostas a acessos não autorizados.
	Os sistemas estão configurados para autenticação forte e as senhas não são compartilhadas, mas estas proteções são tratadas de modo pontual.
	Os sistemas e aplicações usam autenticação forte de modo consistente e existem mecanismos de prevenção contra acesso não autorizado. Existe reporte de direitos de acesso e uso de contas.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
As contas de usuários são gerenciadas de forma definida e continua com as devidas aprovações de workflow sobre seus proprietários e custodiantes? Existe	Não existe definição para este item.
	A empresa usa gerenciamento de usuários de forma intuitiva.
	Os usuários são gerenciados de forma intuitiva, mas existe alguma documentação e evidencia de que existem aprovações.

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

documentação referente a privilégios conferidos a contas de usuários?	Gerenciamento de usuário segue processos documentados de aprovação, mas os mecanismos são diferentes para os vários sistemas.
	Existe um processo único e centralizado de gerenciamento de usuários, com reporte integrado que é usado para todo gerenciamento relacionado ao SOX.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
A empresa executa avaliações regulares sobre contas e privilégios?	Não existe definição para este item.
	As contas são criadas, porém nunca mais são revistas ou avaliadas.
	Contas são revisadas de forma pontual quando os sistemas entram em manutenção, são modificados ou na suspeição de um problema.
	As contas são revisadas regularmente por sistemas e pelos custodiantes das aplicações a partir de informações obtidas junto aos donos e gestores da informação.
	As contas são revisadas regularmente através de um <i>workflow</i> automatizado com checagens e balanços providenciados pelos representantes do negócio, custodiantes dos sistemas e gerentes. Relatórios são providenciados automaticamente sob demanda.
Alto nível, seguindo as melhores práticas, otimizado e automatizado.	
A empresa conduz testes regulares de segurança nos sistemas relacionados ao SOX de forma a certificar-se de que as configurações são as que deveriam ser e os sistemas permanecem seguros?	Não existe definição para este item.
	Não existe qualquer tipo de teste.
	Existem avaliações de configuração de forma pontual, mas não existem testes de penetração.
	Existem testes de penetração e avaliação de configuração de forma pontual.
	Existem testes de penetração e análises de configuração em bases regulares para todos os sistemas SOX considerados críticos.
Alto nível, seguindo as melhores práticas, otimizado e automatizado.	
A empresa gerencia suas vulnerabilidades e aplica correções de forma uniforme através de todos os sistemas relacionados ao SOX?	Não existe definição para este item.
	Não existe nenhum mecanismo que rastreie vulnerabilidades (vírus, bugs de sistema, etc) e aplique patches ou correções.
	Monitoram-se as vulnerabilidades e aplicam-se correções, mas depende de grupos de administradores de sistemas e de rede e do tipo de sistema.
	Existe um gerenciamento efetivo das vulnerabilidades, mas não de forma uniforme. Está implementado por diferentes áreas em vários níveis de documentação e reporte.
	Existe rastreamento de vulnerabilidades e aplicação de correções de forma uniforme através de toda a empresa.
Alto nível, seguindo as melhores práticas, otimizado e automatizado.	
A empresa monitora a efetividade dos	Não existe definição para este item.

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

controles de segurança implementados para a aderência ao SOX?	A aderência é checada como parte da auditoria.
	Os controles são checados para determinar se continuam a operar como planejado, mas não são avaliados para checar se são efetivos no ambiente corporativo.
	Os controles são avaliados regularmente para checar sua efetividade, e mudanças são programadas como parte do processo de aderência aos projetos de atividades do.
	Os controles são avaliados e documentados de forma continua como parte das operações do Negocio. Aperfeiçoamentos nos controles são inerentes à operação do Negocio e TI.
	Alto nível, seguindo as melhores práticas, otimizado e automatizado.
A empresa contrata terceiros com expertise específica para avaliar e conferir seus processos e controles de TI?	Não existe definição para este item.
	Não existe avaliação independente.
	Existe alguma avaliação independente, mas é pontual.
	Existe avaliação independente para as novas políticas e sistemas, mas não existe reavaliação.
	Existe avaliação independente das políticas importantes, sistemas e aplicações.
Alto nível, seguindo as melhores práticas, otimizado e automatizado.	
A empresa envolve de forma pro ativa a auditoria interna antes de finalizar os planos de TI?	Não existe definição para este item.
	A auditoria é conduzida depois do desenho do plano estar completo.
	Seu impacto principal é depois que o sistema é organizado e preparado para entrar em produção.
	A auditoria é consultada em vários pontos durante o desenvolvimento e implementação.
	A auditoria é um membro importante no time de desenvolvimento e implementação.
Alto nível, seguindo as melhores práticas, otimizado e automatizado.	
A empresa realiza consultas a terceiros sobre a aderência às leis e regulamentações (ex. SOX e privacidade)?	Não existe definição para este item.
	Não existem consultas.
	O staff interno avalia os requerimentos legais de aderência.
	Existe alguma avaliação externa sobre aderência.
	Existe avaliação externa regular sobre a efetividade da aderência da empresa às leis e regulamentações.
Alto nível, seguindo as melhores práticas, otimizado e automatizado.	

Passo 5 - Criação do critério de mensuração da conformidade em Governança de TI

Determinou-se uma escala para avaliação da conformidade nas alternativas respondidas. Os critérios associados a cada um dos índices da figura 7 são apresentados na Tabela 1:

Tabela 3: Critérios correlacionados com os índices para classificação da conformidade.

Critério	Conformidade	%
Processos de gerenciamento não são aplicados.	Muito Baixa	0 - 0,10
Existem processos, mas desorganizados.	Baixa	0,11 - 0,30
Segue-se um processo definido	Moderada	0,31 - 0,50
Processos são documentados e comunicados	Média	
Processos são medidos e monitorados	Alta	0,51 - 0,80
As boas práticas são seguidas e automatizadas	Muito Alta	0,81 - 1

Passo 6 - Tabulação do questionário

Elaborou-se um questionário em uma planilha Excel, cujas linhas apresentam as unidades de controle (seções) e as alternativas associadas aos especialistas que avaliaram a conformidade das unidades de controle.

Passo 7 - Aplicação do questionário

Aplicou-se o questionário a especialistas e foram coletados o grau de conformidade (c) e o grau de inexistência de conformidade (ic) associado a cada uma das 120 alternativas (tabela 4) com nomenclatura representada por A, de alternativa, seguido de sua ordem de 001 a 120.

Tabela 4 - Avaliação dos especialistas, para área de conformidade SOX “planejar e organizar”.

Área Conformidade SOX	Unidade de Controle	Alternativas	GRUPO A - Especialista Área de Planejamento		Grupo B - Especialista Área de Engenharia		Grupo C - Especialista Área de Tecnologia		Grupo D - Especialista Área de QA	
			c1	ic1	c1	ic1	c1	ic1	c1	ic1
Planejar e Organizar	A empresa possui um esquema para classificarem dados em um dicionário ou catalogo de dados	A001	0,15	0,9	0,11	0,9	0,3	0,5	0,1	0,65
		A002	0,05	0,9	0,2	0,9	0,4	0,75	0,3	0,2
		A003	0,25	0,7	0,9	0,9	0,3	0,75	0,3	0,2
		A004	0,2	0,7	0,81	0,9	0,3	0,75	0,2	0,75
		A005	0,9	0	0,81	0,2	0,5	0,1	1	0,01
		A006	0,45	0,2	0,5	0	0,7	0,5	0,9	0,4
	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0,35	0,5	0,4	0,2	0,5	0,7	0,6	0,5
		A008	0,65	0,5	0,2	0	0,4	0,2	0,1	0,2
		A009	0,75	0	0,8	0	0,8	0,2	0,6	0,2
		A010	0,75	0	0,8	0	0,8	0,2	0,6	0
		A011	0,15	0,8	0,2	0,9	0,7	0,8	0,2	0,65
		A012	0,25	0,2	0,7	0,7	0,7	0,4	0,81	0,65
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0,15	0,2	0,6	0,7	0,6	0,4	0,6	0,6
		A014	0,35	0,5	0,5	0,2	0,6	0,7	0,1	0,6
		A015	0,08	0,7	0,6	0,9	0,5	0,7	0,1	0,6
		A016	0,05	0,5	0,3	0,9	0,5	0,5	0,2	0,6
		A017	0,6	0	0,7	0	0,7	0,2	1	0
		A018	0,85	0,2	0,9	0	0,8	0,3	1	0
	Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?	A019	0,85	0,2	0,9	0	0,8	0,2	1	0
		A020	0,9	0	0,81	0	0,7	0	1	0
		A021	0,6	0,1	0,6	0,2	0,7	0,1	0,6	0,2

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

		A022	0,2	0,8	0,11	0,9	0,5	0,2	0,5	0,975
		A023	0,1	0,8	0,11	0,9	0,5	0,5	0,5	0,8
		A024	0,25	0,8	0,2	0,9	0,4	1	0,4	0
	Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	A025	0,55	0,2	0,4	0,2		0,2	1	0
		A026	0,95	0	0,4	0,2	0,8	0	1	0
		A027	0,95	0,1	0,5	0,2	0,7	0,2	1	0
		A028	0,7	0,1	0,1	0,2	0,8	0,2	0,9	0,15
		A029	0,4	0,2	0,3	0,4	0,7	0,1	0,51	0,35
		A030	0,5	0	0,81	0	0,8	0	0,7	0

Passo 8 - Definição do parâmetro estratégico

Adotaram-se os parâmetros estratégicos conservador, intermediário e otimista para a avaliação dos índices resultantes da conformidade em Governança de TI advindos da opinião dos especialistas.

Passo 9 - Obtenção consolidada dos graus de conformidade (cR) e inexistência de conformidade (icR)

Os graus de conformidade (cR) e inexistência de conformidade (icR) resultantes de cada alternativa por unidade de controle foram compilados e, a partir da aplicação da Lógica Paraconsistente, verificou-se considerando as avaliações conservadora, intermediária e otimista, logo na tabela 6.

Tabela 6 - Índices resultantes de conformidade condizentes com os parâmetros estratégicos predefinidos, para área de conformidade SOX “planejar e organizar”.

Área Conformidade SOX	Unidade de Controle	Alternativas	Parâmetro Estratégico Conservador		Parâmetro Estratégico Intermediário		Parâmetro Estratégico Otimista	
			c1	ic1	c1	ic1	c1	ic1
Planejar e Organizar	A empresa possui um esquema para classificar dados em um dicionário ou catalogo de dados	A001	0,35	0,5	0,5	0,2	0,6	0,7
		A002	0,08	0,7	0,6	0,9	0,5	0,7
		A003	0,05	0,5	0,3	0,9	0,5	0,5
		A004	0,6	0	0,7	0	0,7	0,2
		A005	0,85	0,2	0,9	0	0,8	0,3
		A006	0,85	0,2	0,9	0	0,8	0,2
	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0,9	0	0,81	0	0,7	0
		A008	0,6	0,1	0,6	0,2	0,7	0,1
		A009	0,2	0,8	0,11	0,9	0,5	0,2
		A010	0,1	0,8	0,11	0,9	0,5	0,5
		A011	0,35	0,5	0,5	0,2	0,6	0,7
		A012	0,08	0,7	0,6	0,9	0,5	0,7
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0,05	0,5	0,3	0,9	0,5	0,5
		A014	0,6	0	0,7	0	0,7	0,2
		A015	0,85	0,2	0,9	0	0,8	0,3
		A016	0,85	0,2	0,9	0	0,8	0,2
		A017	0,9	0	0,81	0	0,7	0
		A018	0,6	0,1	0,6	0,2	0,7	0,1
	Sua empresa tem e mantém um	A019	0,2	0,8	0,11	0,9	0,5	0,2

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

		Parâmetro Estratégico Conservador		Parâmetro Estratégico Intermediário		Parâmetro Estratégico Otimista	
conjunto completo de Políticas de Segurança?	A020	0,1	0,8	0,11	0,9	0,5	0,5
	A021	0,6	0,1	0,6	0,2	0,7	0,1
	A022	0,2	0,8	0,11	0,9	0,5	0,2
	A023	0,1	0,8	0,11	0,9	0,5	0,5
	A024	0,25	0,8	0,2	0,9	0,4	1
Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	A025	0,55	0,2	0,4	0,2	0	0,2
	A026	0,95	0	0,4	0,2	0,8	0
	A027	0,95	0,1	0,5	0,2	0,7	0,2
	A028	0,7	0,1	0,1	0,2	0,8	0,2
	A029	0,4	0,2	0,3	0,4	0,7	0,1
	A030	0,5	0	0,81	0	0,8	0

Passo 10 - Análise de convergência das opiniões

- a. Calcularam-se os Graus de contradição resultantes (Gcontr);
- b. Determinaram-se os níveis de exigência mínimo ($N_{\text{exig mínimo}}$) e máximo ($N_{\text{exig máximo}}$) para aceitabilidade dos Graus de contradição, efetuando paralelo com a escala de conformidade da Figura 1, da seguinte forma:

iv. Parâmetro estratégico conservador: $(N_{\text{exig mínimo}}) \leq 0,10 / (N_{\text{exig máximo}}) > 0,3$

v. Parâmetro estratégico intermediário: $(N_{\text{exig mínimo}}) \leq 0,30 / (N_{\text{exig máximo}}) > 0,5$

vi. Parâmetro estratégico otimista: $(N_{\text{exig mínimo}}) \leq 0,50 / (N_{\text{exig máximo}}) > 0,8$

Após definição, os parâmetros para análise do grau de contradição de cada uma dos 120 alternativas, foram analisados e sua categorização final, como “Coerente”, “Inconsistente” ou “Incompleta”. logo abaixo nas tabelas 6,7 e 8

Tabela 6 - Grau de Contradição e decisão para avaliação final, para área de conformidade SOX “planejar e organizar” - Avaliação Conservadora

Área Conformidade SOX	Unidade de Controle	Alternativas	Parâmetro Estratégico Conservador		0,1	0,3	<= Nível de Exigência Mínimo e Máximo aceitável
			cR	icR	Gcontr	cR1	Resultado da Análise
Planejar e Organizar	A empresa possui um esquema para classificar dados em um dicionário ou catalogo de dados	A001	0,5	0,7	-0,2	0,3	AVALIAÇÃO INCOMPLETA
		A002	0,6	0,9	-0,5	0,1	AVALIAÇÃO INCONSISTENTE
		A003	0,5	0,6	-0,1	0,4	AVALIAÇÃO COERENTE
		A004	0,8	0,4	-0,2	0,6	AVALIAÇÃO INCOMPLETA
		A005	0,4	0,6	0,0	0,4	AVALIAÇÃO COERENTE
		A006	0,3	0,5	0,2	0,5	AVALIAÇÃO INCOMPLETA
	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0,7	0,7	-0,4	0,3	AVALIAÇÃO INCONSISTENTE
		A008	0,5	0,0	0,5	1,0	AVALIAÇÃO INCONSISTENTE
		A009	0,3	0,3	0,4	0,7	AVALIAÇÃO INCONSISTENTE
		A010	0,8	0,5	-0,3	0,5	AVALIAÇÃO INCOMPLETA
		A011	0,5	0,5	0,0	0,6	AVALIAÇÃO COERENTE
		A012	0,5	0,5	0,0	0,6	AVALIAÇÃO COERENTE
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0,0	0,0	1,0	1,0	AVALIAÇÃO INCONSISTENTE
		A014	0,2	0,7	0,2	0,4	AVALIAÇÃO INCOMPLETA
		A015	0,5	0,7	-0,2	0,4	AVALIAÇÃO INCOMPLETA
		A016	0,5	0,7	-0,2	0,4	AVALIAÇÃO INCOMPLETA
		A017	0,4	0,7	-0,1	0,3	AVALIAÇÃO COERENTE
		A018	0,3	0,9	-0,2	0,1	AVALIAÇÃO INCOMPLETA

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

	Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?	A019	0,0	0,0	1,0	1,0	AVALIAÇÃO INCONSISTENTE
		A020	0,3	0,8	-0,1	0,2	AVALIAÇÃO COERENTE
		A021	0,8	0,1	0,1	0,9	AVALIAÇÃO COERENTE
		A022	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
		A023	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
		A024	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
	Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	A025	0,0	0,0	1,0	1,0	AVALIAÇÃO COERENTE
		A026	0,7	0,5	-0,2	0,5	AVALIAÇÃO COERENTE
		A027	0,3	0,6	0,1	0,4	AVALIAÇÃO COERENTE
		A028	0,1	0,8	0,1	0,2	AVALIAÇÃO COERENTE
		A029	0,2	0,5	0,3	0,5	AVALIAÇÃO COERENTE
		A030	0,0	0,2	0,8	0,8	AVALIAÇÃO COERENTE

Tabela 7 - Grau de Contradição e decisão para avaliação final, para área de conformidade SOX “planejar e organizar” – Avaliação Intermediária.

Área Conformidade SOX	Unidade de Controle	Alternativas	Parâmetro Estratégico Intermediário		0,3	0,5	<= Nível de Exigência Mínimo e Máximo aceitável
			cR	icR	Gcontr	cR1	Resultado da Análise
Planejar e Organizar	A empresa possui um esquema para classificar dados em um dicionário ou catalogo de dados	A001	0,5	0,7	-0,2	0,3	AVALIAÇÃO COERENTE
		A002	0,6	0,9	-0,5	0,1	AVALIAÇÃO INCOMPLETA
		A003	0,5	0,6	-0,1	0,4	AVALIAÇÃO COERENTE
		A004	0,8	0,4	-0,2	0,6	AVALIAÇÃO COERENTE
		A005	0,4	0,6	0,0	0,4	AVALIAÇÃO COERENTE
		A006	0,3	0,5	0,2	0,5	AVALIAÇÃO COERENTE

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0,7	0,7	-0,4	0,3	AVALIAÇÃO INCOMPLETA
		A008	0,5	0,0	0,5	1,0	AVALIAÇÃO INCOMPLETA
		A009	0,3	0,3	0,4	0,7	AVALIAÇÃO INCOMPLETA
		A010	0,8	0,5	-0,3	0,5	AVALIAÇÃO COERENTE
		A011	0,5	0,5	0,0	0,6	AVALIAÇÃO COERENTE
		A012	0,5	0,5	0,0	0,6	AVALIAÇÃO COERENTE
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0,0	0,0	1,0	1,0	AVALIAÇÃO INCONSISTENTE
		A014	0,2	0,7	0,2	0,4	AVALIAÇÃO COERENTE
		A015	0,5	0,7	-0,2	0,4	AVALIAÇÃO COERENTE
		A016	0,5	0,7	-0,2	0,4	AVALIAÇÃO COERENTE
		A017	0,4	0,7	-0,1	0,3	AVALIAÇÃO COERENTE
		A018	0,3	0,9	-0,2	0,1	AVALIAÇÃO COERENTE
	Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?	A019	0,0	0,0	1,0	1,0	AVALIAÇÃO INCONSISTENTE
		A020	0,3	0,8	-0,1	0,2	AVALIAÇÃO COERENTE
		A021	0,8	0,1	0,1	0,9	AVALIAÇÃO COERENTE
		A022	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
		A023	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
		A024	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
	Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	A025	0,0	0,0	1,0	1,0	AVALIAÇÃO COERENTE
		A026	0,7	0,5	-0,2	0,5	AVALIAÇÃO COERENTE
		A027	0,3	0,6	0,1	0,4	AVALIAÇÃO COERENTE
		A028	0,1	0,8	0,1	0,2	AVALIAÇÃO COERENTE
		A029	0,2	0,5	0,3	0,5	AVALIAÇÃO COERENTE
		A030	0,0	0,2	0,8	0,8	AVALIAÇÃO COERENTE

Tabela 8 - Grau de Contradição e decisão para avaliação final, para área de conformidade SOX “planejar e organizar” – Avaliação Otimista.

Área Conformidade SOX	Unidade de Controle	Alternativas	Parâmetro Estratégico Intermediário		0,5	0,8	<= Nível de Exigência Mínimo e Máximo aceitável
			cR	icR	Gcontr	cR1	Resultado da Análise
Planejar e Organizar	A empresa possui um esquema para classificar dados em um dicionário ou catálogo de dados	A001	0,5	0,7	-0,2	0,3	AVALIAÇÃO COERENTE
		A002	0,6	0,9	-0,5	0,1	AVALIAÇÃO COERENTE
		A003	0,5	0,6	-0,1	0,4	AVALIAÇÃO COERENTE
		A004	0,8	0,4	-0,2	0,6	AVALIAÇÃO COERENTE
		A005	0,4	0,6	0,0	0,4	AVALIAÇÃO COERENTE
		A006	0,3	0,5	0,2	0,5	AVALIAÇÃO COERENTE
	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0,7	0,7	-0,4	0,3	AVALIAÇÃO COERENTE
		A008	0,5	0,0	0,5	1,0	AVALIAÇÃO COERENTE
		A009	0,3	0,3	0,4	0,7	AVALIAÇÃO COERENTE
		A010	0,8	0,5	-0,3	0,5	AVALIAÇÃO COERENTE
		A011	0,5	0,5	0,0	0,6	AVALIAÇÃO COERENTE
		A012	0,5	0,5	0,0	0,6	AVALIAÇÃO COERENTE
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0,0	0,0	1,0	1,0	AVALIAÇÃO INCONSISTENTE
		A014	0,2	0,7	0,2	0,4	AVALIAÇÃO COERENTE
		A015	0,5	0,7	-0,2	0,4	AVALIAÇÃO COERENTE
		A016	0,5	0,7	-0,2	0,4	AVALIAÇÃO COERENTE
		A017	0,4	0,7	-0,1	0,3	AVALIAÇÃO COERENTE
		A018	0,3	0,9	-0,2	0,1	AVALIAÇÃO COERENTE
	Sua empresa tem e mantém um conjunto completo de	A019	0,0	0,0	1,0	1,0	AVALIAÇÃO INCONSISTENTE
		A020	0,3	0,8	-0,1	0,2	AVALIAÇÃO COERENTE

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

	Políticas de Segurança?	A021	0,8	0,1	0,1	0,9	AVALIAÇÃO COERENTE
		A022	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
		A023	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
		A024	0,8	0,2	0,0	0,8	AVALIAÇÃO COERENTE
	Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	A025	0,0	0,0	1,0	1,0	AVALIAÇÃO COERENTE
		A026	0,7	0,5	-0,2	0,5	AVALIAÇÃO COERENTE
		A027	0,3	0,6	0,1	0,4	AVALIAÇÃO COERENTE
		A028	0,1	0,8	0,1	0,2	AVALIAÇÃO COERENTE
		A029	0,2	0,5	0,3	0,5	AVALIAÇÃO COERENTE
		A030	0,0	0,2	0,8	0,8	AVALIAÇÃO COERENTE

Passo 11 - Adoção do índice de conformidade resultante para avaliações coerentes.

Foram obtidos dois índices resultantes de conformidade (cR e cR1) para as alternativas cuja avaliação da conformidade foi classificada como “Coerente”.

Tabela 9 - Obtenção dos dois índices resultantes de conformidade, para área de conformidade SOX “planejar e organizar”.

Área Conformidade SOX	Unidade de Controle	Alternativas	Parâmetro Estratégico Conservador		0,3
			cR	icR	cR1
Planejar e Organizar	A empresa possui um esquema para classificar dados em um dicionário ou catalogo de dados	A001	0,5	0,7	0,3
		A002	0,6	0,9	0,1
		A003	0,5	0,6	0,4
		A004	0,8	0,4	0,6
		A005	0,4	0,6	0,4
		A006	0,3	0,5	0,5
	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0,7	0,7	0,3
		A008	0,5	0,0	1,0
		A009	0,3	0,3	0,7
		A010	0,8	0,5	0,5
		A011	0,5	0,5	0,6
		A012	0,5	0,5	0,6
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0,0	0,0	1,0
		A014	0,2	0,7	0,4
		A015	0,5	0,7	0,4
		A016	0,5	0,7	0,4
		A017	0,4	0,7	0,3
		A018	0,3	0,9	0,1
	Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?	A019	0,0	0,0	1,0
		A020	0,3	0,8	0,2
		A021	0,8	0,1	0,9
		A022	0,8	0,2	0,8
		A023	0,8	0,2	0,8
		A024	0,8	0,2	0,8
	Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	A025	0,0	0,0	1,0
		A026	0,7	0,5	0,5
		A027	0,3	0,6	0,4
		A028	0,1	0,8	0,2
		A029	0,2	0,5	0,5
		A030	0,0	0,2	0,8

Em seguida, assumiu-se o maior índice de conformidade dentre os dois obtidos na etapa anterior (cR ou cR1), somente para as avaliações classificadas como “Coerente”, conforme Figura 15.

Tabela 70 - Adoção do maior índice de conformidade entre (cR ou cR1), para área de conformidade SOX “planejar e organizar”.

Área Conformidade SOX	Unidade de Controle	Alternativas	Parâmetro Estratégico Conservador		0,3	<= Nível de Exigência Mínimo e Máximo aceitável	Maior Valor de cR e cR1
			cR	icR	cR1	Resultado da Análise	
Planejar e Organizar	A empresa possui um esquema para classificar dados em um dicionário ou catálogo de dados	A001	0,5	0,7	0,3	AVALIAÇÃO INCOMPLETA	
		A002	0,6	0,9	0,1	AVALIAÇÃO INCONSISTENTE	
		A003	0,5	0,6	0,4	AVALIAÇÃO COERENTE	0,5
		A004	0,8	0,4	0,6	AVALIAÇÃO INCOMPLETA	
		A005	0,4	0,6	0,4	AVALIAÇÃO COERENTE	0,4
		A006	0,3	0,5	0,5	AVALIAÇÃO INCOMPLETA	
	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0,7	0,7	0,3	AVALIAÇÃO INCONSISTENTE	
		A008	0,5	0,0	1,0	AVALIAÇÃO INCONSISTENTE	
		A009	0,3	0,3	0,7	AVALIAÇÃO INCONSISTENTE	
		A010	0,8	0,5	0,5	AVALIAÇÃO INCOMPLETA	
		A011	0,5	0,5	0,6	AVALIAÇÃO COERENTE	0,6
		A012	0,5	0,5	0,6	AVALIAÇÃO COERENTE	0,6
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0,0	0,0	1,0	AVALIAÇÃO INCONSISTENTE	
		A014	0,2	0,7	0,4	AVALIAÇÃO INCOMPLETA	

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

		A015	0,5	0,7	0,4	AVALIAÇÃO INCOMPLETA	
		A016	0,5	0,7	0,4	AVALIAÇÃO INCOMPLETA	
		A017	0,4	0,7	0,3	AVALIAÇÃO COERENTE	0,4
		A018	0,3	0,9	0,1	AVALIAÇÃO INCOMPLETA	
	Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?	A019	0,0	0,0	1,0	AVALIAÇÃO INCONSISTENTE	
		A020	0,3	0,8	0,2	AVALIAÇÃO COERENTE	0,3
		A021	0,8	0,1	0,9	AVALIAÇÃO COERENTE	0,9
		A022	0,8	0,2	0,8	AVALIAÇÃO COERENTE	0,8
		A023	0,8	0,2	0,8	AVALIAÇÃO COERENTE	0,8
		A024	0,8	0,2	0,8	AVALIAÇÃO COERENTE	0,8
	Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	A025	0,0	0,0	1,0	AVALIAÇÃO COERENTE	1
		A026	0,7	0,5	0,5	AVALIAÇÃO COERENTE	0,7
		A027	0,3	0,6	0,4	AVALIAÇÃO COERENTE	0,4
		A028	0,1	0,8	0,2	AVALIAÇÃO COERENTE	0,2
		A029	0,2	0,5	0,5	AVALIAÇÃO COERENTE	0,5
A030		0,0	0,2	0,8	AVALIAÇÃO COERENTE	0,8	

1. Alocou-se para cada alternativa o maior índice de conformidade resultante na escala de conformidade adotada (tabela 10).

Tabela 81 - Alocação do maior índice de conformidade na escala adotada, para área de conformidade SOX “planejar e organizar”.

Área Conformidade SOX	Unidade de Controle	Alternativas	Parâmetro Estratégico Conservador		0,3	<= Nível de Exigência Mínimo e Máximo aceitável	Maior Valor de cR e cR1	Conformidade Final
			cR	icR	cR1			
Planejar e Organizar	A empresa possui um esquema para classificar dados em um dicionário ou catálogo de dados	A001	0,5	0,7	0,3	AVALIAÇÃO INCOMPLETA		
		A002	0,6	0,9	0,1	AVALIAÇÃO INCONSISTENTE		
		A003	0,5	0,6	0,4	AVALIAÇÃO COERENTE	0,5	MODERADO
		A004	0,8	0,4	0,6	AVALIAÇÃO INCOMPLETA		
		A005	0,4	0,6	0,4	AVALIAÇÃO COERENTE	0,4	MODERADO
		A006	0,3	0,5	0,5	AVALIAÇÃO INCOMPLETA		
	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0,7	0,7	0,3	AVALIAÇÃO INCONSISTENTE		
		A008	0,5	0,0	1,0	AVALIAÇÃO INCONSISTENTE		
		A009	0,3	0,3	0,7	AVALIAÇÃO INCONSISTENTE		
		A010	0,8	0,5	0,5	AVALIAÇÃO INCOMPLETA		
		A011	0,5	0,5	0,6	AVALIAÇÃO COERENTE	0,6	ALTO
		A012	0,5	0,5	0,6	AVALIAÇÃO COERENTE	0,6	ALTO
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0,0	0,0	1,0	AVALIAÇÃO INCONSISTENTE		
		A014	0,2	0,7	0,4	AVALIAÇÃO INCOMPLETA		
		A015	0,5	0,7	0,4	AVALIAÇÃO INCOMPLETA		

ANÁLISE DE CONFORMIDADE DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

		A016	0,5	0,7	0,4	AVALIAÇÃO INCOMPLETA		
		A017	0,4	0,7	0,3	AVALIAÇÃO COERENTE	0,4	MODERADO
		A018	0,3	0,9	0,1	AVALIAÇÃO INCOMPLETA		
	Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?	A019	0,0	0,0	1,0	AVALIAÇÃO INCONSISTENTE		
		A020	0,3	0,8	0,2	AVALIAÇÃO COERENTE	0,3	BAIXO
		A021	0,8	0,1	0,9	AVALIAÇÃO COERENTE	0,9	MUITO ALTO
		A022	0,8	0,2	0,8	AVALIAÇÃO COERENTE	0,8	ALTO
		A023	0,8	0,2	0,8	AVALIAÇÃO COERENTE	0,8	ALTO
		A024	0,8	0,2	0,8	AVALIAÇÃO COERENTE	0,8	ALTO
	Sua empresa tem em andamento um programa que garanta a aderência ao SOX?	A025	0,0	0,0	1,0	AVALIAÇÃO COERENTE	1	MUITO ALTO
		A026	0,7	0,5	0,5	AVALIAÇÃO COERENTE	0,7	ALTO
		A027	0,3	0,6	0,4	AVALIAÇÃO COERENTE	0,4	MODERADO
		A028	0,1	0,8	0,2	AVALIAÇÃO COERENTE	0,2	BAIXO
		A029	0,2	0,5	0,5	AVALIAÇÃO COERENTE	0,5	MODERADO
		A030	0,0	0,2	0,8	AVALIAÇÃO COERENTE	0,8	ALTO

5 APRESENTAÇÃO DOS RESULTADOS

5.1 RESULTADOS DA PESQUISA

Destacam-se os resultados qualitativos obtidos pela aplicação do método aqui descrito: ponderação e convergência da opinião dos especialistas quanto à conformidade em Governança de TI das alternativas identificadas e avaliadas nas tabelas a seguir:

Tabela 12 - Quantidade de Alternativas avaliadas x Convergência da Opinião dos Especialistas, considerando os três parâmetros estratégicos.

Convergência de Opiniões dos Especialistas	Parâmetro Estratégico Conservador		Parâmetro Estratégico Intermediário		Parâmetro Estratégico Otimista	
	Qtde de Alternativas	%	Qtde de Alternativas	%	Qtde de Alternativas	%
AVALIAÇÃO COERENTE	84	70%	101	84%	116	97%
AVALIAÇÃO INCONSISTENTE	7	6%	5	4%	4	3%
AVALIAÇÃO INCOMPLETA	29	24%	14	12%	0	0%
TOTAL	120	100%	120	100%	120	100%

Tabela 13 - Quantidade de Alternativas avaliada x Índices de Conformidade

Conformidade	Parâmetro Estratégico Conservador		Parâmetro Estratégico Intermediário		Parâmetro Estratégico Otimista	
	Qtde de Alternativas	%	Qtde de Alternativas	%	Qtde de Alternativas	%
MUITO BAIXO	0	0%	0	0%	2	0%
BAIXO	0	0%	11	10%	14	100%
MODERADO / MEDIO	4	5%	13	12%	45	
ALTO	22	25%	64	57%	47	0%
MUITO ALTO	61	70%	25	22%	12	0%
TOTAL	87	100%	113	100%	120	100%

5.2 COMPARAÇÃO DAS OPINIÕES DOS ESPECIALISTAS ÀS DAS SUAS LIDERANÇAS

Os índices de conformidade resultantes do método aqui apresentado foram comparados aos índices de conformidade adotados pela empresa escolhida para aplicação do mesmo, da seguinte forma:

Verificaram-se quais índices de conformidade são atualmente utilizados pela empresa em estudo, o método para cálculo da conformidade baseia-se integralmente na avaliação por um único especialista, de forma bem simplificada. Os índices de conformidade resultantes estão discriminados na Figura 19.

Tabela 14 - Resultado da avaliação da empresa - estudo de caso.

Área Conformidade SOX	Unidade de Controle	Alternativas	Conformidade Avaliada pela Empresa Estudo de Caso
Planejar e Organizar	A empresa possui um esquema para classificarem dados em um dicionário ou catálogo de dados	A001	0.4
		A002	0.4
		A003	0.4
		A004	1
		A005	0.7
		A006	0.7
	A estrutura organizacional da empresa provê uma segregação de funções adequada?	A007	0.7
		A008	1
		A009	0.4
		A010	1
		A011	0.4
		A012	0.4
	O escritório de segurança se reporta ao mais alto nível gerencial da empresa?	A013	0.4
		A014	1
		A015	1
		A016	1
		A017	1
		A018	1
	Sua empresa tem e mantém um conjunto completo de Políticas de Segurança?	A019	0.4
		A020	0.4
		A021	0.4
		A022	0.4
		A023	0.4
		A024	0.4

Para existir a comparação entre os índices de conformidade obtidos por meio do método proposto e os índices calculados pela sistemática adotada na empresa na qual o método aqui descrito foi aplicado, adotou-se um índice de coerência. Esse índice nada mais é do que a diferença máxima aceitável entre os resultados obtidos pelos dos dois diferentes métodos. Em suma, estipulou-se 0,30 como referência.

Comparação dos métodos: se o maior valor de cR (índice de conformidade resultante obtido com o método aqui descrito, na passo 11 do capítulo 3) subtraído do índice de conformidade adotado pela empresa em estudo for menor ou igual ao índice de coerência definido de 0,30, interpreta-se que ambos os métodos proporcionaram a mesma avaliação para as unidades de controle, classificando a comparação como “Coerente”. Caso contrário, as avaliações utilizando os dois diferentes métodos não foram convergentes, sugerindo “Reavaliação”.

Tabela 15 - Resultado Final

Convergência de Opiniões dos Especialistas	Parâmetro Estratégico Conservador		Parâmetro Estratégico Intermediário		Parâmetro Estratégico Otimista	
	Qtde de Alternativas	%	Qtde de Alternativas	%	Qtde de Alternativas	%
REAVALIAR	54	45%	27	22%	0	0%
COERENTE	37	31%	84	70%	120	100%
AVALIAÇÃO NÃO-CONCLUSIVA	29	24%	9	8%	0	0%
TOTAL	120	100%	120	100%	120	100%

As avaliações não-conclusivas estão diretamente relacionadas às alternativas cujas avaliações foram classificadas como “Inconsistente” ou “Incompleta”.

6 CONCLUSÃO

Este estudo apresenta um método para avaliação da conformidade em Governança de TI e sua aplicação em empresa do ramo de cosméticos, onde por meio de avaliação de questionários com 120 alternativas, baseadas nos objetivos do *framework* Cobit e utilizando Lógica Paraconsistente associada a uma técnica de análise de respostas .

Considerando a aplicação da metodologia proposta no estudo, por meio de análise de opiniões, a avaliação do grau de maturidade em que uma organização encontra-se em relação a sua aderência à Governança de TI, nos limites definidos pelo Cobit, apoiado em conceitos da Lógica Paraconsistente como um dos critérios de análise.

Os resultados demonstram que trabalho é uma maneira diferente dos métodos convencionais, mostrando-se extremamente ágil e adequado para os fins propostos, onde por sua vez leva consideração vários parâmetros estratégicos diretamente relacionados ao plano estratégico de uma corporação. Neste método a exposição das avaliações realizadas por diferentes especialistas, é muito mais valiosa e precisa do que quando realizada somente por um único especialista, embora permita que o mesmo desconsidere, ainda que inadvertidamente, alguns objetivos não diretamente relacionados ao foco de sua atividade, podendo assim diminuir a confiabilidade da avaliação por ele proposta. Por causa da possibilidade de integração de opiniões de diversos especialistas, bem como de múltiplos objetivos e alternativas, pode-se dizer que os resultados apresentados pelo método descrito são matematicamente mais confiáveis, além de reduzir a dependência da empresa, em momentos críticos de decisão, da opinião de um único especialista.

Este método de análise e avaliação contribui para o processo de tomada de decisão por parte das lideranças de uma organização, de modo que todas decisões baseadas nestes resultados são muito mais precisas e diretas para a imediata definição de ações preventivas, que minimizam o acontecimento dessas inconformidades, resultando em consequência uma maior aderência com a Governança de TI em consequência a SOX.

Como a avaliação de conformidade não trata de decisões futuras, mas do futuro da decisão tomada hoje, ao se manter, por exemplo, a avaliação da conformidade de alternativa de uma forma conservadora (maximização de valores), considera-se sempre os maiores índices de conformidade, avaliados pelos especialistas, em cada uma das alternativas, e os resultados oriundos da utilização do método aqui descrito adaptam-se a essa realidade, o que não acontece no método adotado pela empresa focalizada como caso em estudo. Isso significa que, se um especialista em desenvolvimento de software e um segundo especialista de engenharia avaliam a conformidade de uma alternativa com um índice baixo (0,1) e um terceiro especialista de Qualidade avalia a conformidade com um índice alto (0,9), um índice de conformidade média/moderada (0,55) seria obtido, caso uma média aritmética dos valores fosse calculada, o que é procedimento bastante comum. No entanto, esse resultado despreza parcialmente a experiência do terceiro especialista acerca da conformidade associada à alternativa em questão.

O método aqui descrito é estratégico ao apresentar em seus resultados, de forma clara, que quanto maior o grau de conformidade em Governança de TI a se manter dentro de uma organização, menores serão os investimentos e os custos requeridos para subsidiar as ações preventivas necessárias, mantendo um planejamento mais confiável em longo prazo. Ou seja, quanto mais conservador for o posicionamento estratégico da empresa, mais índices com alto grau de conformidade resultarão das avaliações, exigindo com isso maiores dispêndios financeiros para mitigá-los.

A avaliação de conformidade por meio do método descrito cria condições para que as lideranças decidirem rapidamente a ação mais adequada a ser tomada diante de oportunidades e ameaças, minimizando a falta de aderência ao SOX, maximizando as vantagens competitivas dentro do ambiente concorrencial em que atuam e explorando melhor as oportunidades de mercado.

7 REFERÊNCIAS BIBLIOGRÁFICAS

- ARAGON, AGUINALDO FERNANDES; FERRAZ, VLADIMIR. **Implantando a Governança de TI**. Rio de Janeiro: Brasport, 2006
- ARNAUD, VICTOR GONÇALVES. **Governança de tecnologia da informação: em busca do alinhamento com a estratégia da organização**. 2007. Dissertação (Mestrado em Engenharia Industrial) - Pontifícia Universidade Católica, Rio de Janeiro, 2007.
- BERNARDES, MAURO CÉSAR; MOREIRA, EDSON DOS SANTOS. **Um Modelo para Inclusão da Governança da Segurança da Informação no Escopo da Governança Organizacional**. Instituto de Ciências Matemáticas e de Computação – ICMC. São Carlos: Universidade de São Paulo, 1999.
- BERTO, MARCIEL FRANCISCO; ABE, JAIR MINORO. **Lógica Paraconsistente Anotada Evidencial Em: Uma Análise Dos Fatores Críticos De Sucesso Para Implementação De Sistemas Erp**. Programa de Mestrado em Engenharia de Produção – UNIP: São Paulo, 2004.
- CACIATO, L. M., **Métricas e metodologias do gerenciamento de TI** Disponível em: http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=980, acessado em 10 de março de 2006.
- CARVALHO, FÁBIO ROMÉU; BRUNSTEIN, ISRAEL; ABE, JAIR MINORO. **Um Estudo de Tomada de Decisão Baseado em Lógica Paraconsistente Anotada: Avaliação do Projeto de uma Fábrica** Revista Pesquisa e Desenvolvimento Engenharia de Produção n.1, p. 47-62, São Paulo, 2003.
- Consulting Tecnologia & Sistemas. **Treinamento em Gestão Empresarial** Disponível em: <http://www.consulting.com.br>, acessado em 22 de maio de 2007.
- CORREIA, PAULO ALVES et al. **Benefícios da utilização do framework Cobit 4.0 através de indicadores de desempenho apoiados ao Balanced Scorecard**. Programa de Mestrado Profissional em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2007.
- DA COSTA, N.C.A. et al, **Lógica Paraconsistente Aplicada**, São Paulo: Atlas, 1999.
- FAGUNDES, EDUARDO MAYER. **COBIT Um kit de ferramentas para a excelência na gestão de TI**. Programa de Mestrado Mackenzie, São Paulo 2004.

- THOMPSON-FLORES, E.A.L. **Governança Corporativa no Brasil e o Papel dos Investidores Institucionais**. Tese de Doutorado. Dept. de Engenharia Industrial. PUC, Rio de Janeiro, 2004.
- GAMA, FERNANDA DE ASSIS. **Governança de tecnologia da informação: um estudo em empresas brasileiras** f. 76 Dissertação (Mestrado em Ciências Contábeis) – Programa de Pós-Graduação em Ciências Contábeis, Fundação Instituto Capixaba de Pesquisas em Contabilidade, Economia e Finanças, Vitória, 2006.
- GIL, A. L. **Qualidade Total nas Organizações: indicadores de qualidade, gestão econômica da qualidade, sistemas especialistas de qualidade**. Atlas: São Paulo, 1992.
- GROVES, ROBERT et al. **Survey Methodology**. Wiley-Interscience, 2004.
- ITGI-THE IT GOVERNANCE INSTITUTE **COBIT Control Objectives for information and related Technology**. United States of America, [S.I.], 2000.
- ITGI-THE IT GOVERNANCE INSTITUTE **Information Security Governance: Guidance for Boards of Directors and Executive Management**, USA, [S.I.], 2001.
- KAPLAN, R. S.; NORTON, D. P. **The Balanced Scorecard – Measures that drive performance**. Harvard Business Review. Boston, v. 70, n. 1, p. 71-79, 1992.
- KAPLAN, R. S.; NORTON, D. P. **A Estratégia em Ação: Balanced Scorecard**. Tradução de Luiz Euclides Frazão Filho. 15 ed. Rio de Janeiro: Campus, 1997.
- KAPLAN, R. S.; NORTON, D. P. **Organizações orientadas para a estratégia: como as empresas que adotam o Balanced Scorecard prosperam no novo ambiente de negócios** Rio de Janeiro: Campus, 2000a.
- NELSON D. **Negation and separation of concepts in constructive systems**, A. Heyting (ed.), **Constructivity in Mathematics**, 208–225, North-Holland, Amsterdam, 1959.
- MAHMOOD, M. A. e SZEWCZAK, E. J. **Measuring Information Technology Investment Payoff: Contemporary Approaches**. Hershey: Idea Group Publishing, 1999a.
- MARTIN, N, SANTOS, L., DIAS, J. **Governança empresarial, riscos e controles internos: A emergência de um novo modelo de controladoria**. Revista Contabilidade & Finanças, São Paulo: USP, n. 34, p. 7 - 22, 2004.
- MUNIZ, Gleydson Paiva. **Mecanismos de Governança na Terceirização dos serviços de Tecnologia da Informação: Uma Análise em Empresas do**

Estado do ES. Fundação Instituto Capixaba de Pesquisas em Contabilidade, Economia e Finanças, Vitória, 2006.

PETERSON R. R. **Information Strategies and Tactics for Information Technology Governance**, in **Strategies for Information Technology Governance**, Van Grembergen W: Idea Group Publishing, 2003.

REIS, NÉLIO FERNANDO; ABE, JAIR MINORO. **Análise De Cenários Através Da Lógica Paraconsistente Anotada**, Programa de Mestrado em Engenharia de Produção Universidade Paulista, São Paulo, 2006.

Serviço Brasileiro de Apoio às Micro e Pequenas Empresas, Sebrae. **Indicadores de competitividade para micro e pequenas empresas industriais no Brasil**, Serviço Brasileiro de Apoio às Micro e Pequenas Empresas, Sebrae, Brasília, 1993.

TOLEDO, JOSÉ CARLOS; OPRIME, PEDRO CARLOS. **Sistema de indicadores de desempenho da qualidade do produto e do processo: concepção e implantação em uma empresa do setor de auto peças**. ENANPAD Encontro da Associação Nacional de Pós-graduação e Pesquisa em Administração, 1996.

WEILL, PETER; ROSS, JEANNE W. **Governança de TI – Tecnologia da Informação** São Paulo: M. Books, 2004.

ANEXO A – Questionário

1. A empresa possui um esquema para classificar dados em um dicionário ou catálogo de dados?
 - a. A empresa não tem um esquema de classificação da informação ou catálogo ou dicionário ou inventário de dados (0.2)
 - b. Existe um esquema para algumas informações, mas sem documentação formal. (0.4)
 - c. Existe um esquema repetitivo, mas intuitivo, baseado no conhecimento interno da empresa. (0.6)
 - d. Existe um processo documentado. (0.8)
 - e. Alto nível, seguindo as melhores práticas, otimizado e automatizado. (1.0)

2. A estrutura organizacional da empresa provê uma segregação de funções adequada?
 - a. Não existe segregação de funções baseadas em regras.
 - b. Existe alguma segregação, mas sem processos formais.
 - c. Existe uma segregação apropriada com alguma documentação.
 - d. Existem regras formalmente documentadas e que são revisadas regularmente.
 - e. Alto nível, seguindo as melhores práticas, otimizado e automatizado.

3. O escritório de segurança se reporta ao mais alto nível gerencial da empresa?
 - a. Não existe um escritório de segurança na minha empresa.
 - b. A responsabilidade pelo gerenciamento da segurança é compartilhada através do gerenciamento das operações de TI da empresa.
 - c. Existe um gerenciamento de segurança dedicado, mas que se reporta ao TI.
 - d. O gerenciamento da segurança reporta-se ao gerenciamento corporativo no mesmo nível que um CIO.
 - e. Alto nível, seguindo as melhores práticas, otimizado e automatizado.

4. Sua empresa tem e mantém um conjunto completo de políticas de segurança?
 - a. Não existem políticas de segurança.
 - b. Existem algumas políticas, mas não são atualizadas nem abrangentes.
 - c. Existem políticas para as maiores prioridades que afetam a aderência ao SOX (por ex: manutenção de contas, responsabilidades pela segurança, segregação de funções, controle de mudanças).
 - d. Existe um conjunto completo e atualizado de políticas e acompanhamento de procedimentos.
 - e. Alto nível, seguindo as melhores práticas, otimizado e automatizado.

5. Sua empresa tem em andamento um programa que garanta a aderência ao SOX?

- a. Não existem processos estabelecidos que produzam evidências de aderência.
- b. Produziu-se um esforço de aderência uma vez, no passado, mas nunca mais foi repetido.
- c. Existe um processo repetitivo, mas não é parte de um processo contínuo e atualizado.
- d. Existe um programa formal e continuado que provê evidências de aderência e o status para corrigir deficiências.
- e. Alto nível, seguindo as melhores práticas, otimizado e automatizado.

6. Os requerimentos de segurança foram colhidos e documentados para todos os produtos de software que serão implementados em todos os sistemas com impacto nos relatórios financeiros da empresa?

- a. Não existem requerimentos de segurança especificados.
- b. Existem requerimentos de segurança especificados para alguns produtos, mas não de forma consistente.
- c. Existe um conjunto padrão de requerimentos de segurança que é usado para todos os softwares, mas não especificamente para os que impactam nos relatórios financeiros da empresa.
- d. Existem requerimentos de segurança documentados e utilizados na seleção de todos os softwares usados no ambiente SOX.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

7. Os sistemas relacionados ao SOX foram construídos de acordo com padrões de configuração predefinidos? Eles descrevem o sistema operacional e as configurações dos aplicativos que são necessários para se manter a segurança das aplicações e serviços executados nesses sistemas?

- a. Não existem padrões. Os sistemas foram implantados e são operados conforme recebidos dos fornecedores.
- b. Existe alguma coisa feita pontualmente, mas não foi documentada.
- c. Existe um processo construído de forma intuitiva, mas a documentação ainda é inadequada.
- d. Existe um processo construído de forma disciplinada e documentada.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

8. Os sistemas relacionados ao SOX estão configurados para capturar os acessos dos usuários e dos administradores?

- a. A função de LOG não está habilitada.
- b. A função de LOG está habilitada, mas o processo não captura todos os acessos e/ou os registros são sobregravados de acordo com o tamanho do arquivo.
- c. A função de LOG está habilitada para todos os acessos, e os LOGs são revisados, mas não arquivados.
- d. A função de LOG está habilitada, os LOGs são revisados e os registros são arquivados por um ano.

- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.
9. Os sistemas relacionados ao SOX (incluindo infra-estrutura e rede) estão mantidos sob rígido controle de mudanças?
- a. Não existe controle de mudanças.
 - b. Existem algumas anotações pontuais sobre mudanças, mas não existe nenhum processo ou mecanismo formal de controle.
 - c. Existem vários mecanismos de controle de mudanças usados em vários tipos de sistemas, permitindo um efetivo porém complicado controle.
 - d. Existe um centralizado, consistente e bem documentado sistema de controle de mudanças usado para o ambiente SOX.
 - e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.
10. Os sistemas relacionados ao SOX são testados e reconhecidos regularmente para garantir que configurações, privilégios e contas de usuários são apropriados e consistentes com o que foi definido nas configurações e regras?
- a. Não existe um processo regular de avaliação.
 - b. Existem reconhecimentos pontuais implementados apenas para sistemas importantes.
 - c. Existem processos regulares de testes que verificam contas de usuários e configuração de sistemas, mas não estão documentados e/ou não são abrangentes.
 - d. É abrangente, regular, bem documentados, reconhecidos oficialmente e com retorno para processos de correção nos processos deficientes.
 - e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.
11. Sua empresa conduz inspeções regulares de segurança da informação em terceiros (fornecedores de produtos e serviços de TI) para determinar se oferecem proteção adequada em termos de exatidão, confidencialidade e integridade da informação e serviços envolvidos nos relatórios financeiros ou serviços de suporte a esses relatórios?
- a. Não existe inspeção em serviços e produtos contratados de terceiros.
 - b. Existem inspeções pontuais, com um mínimo de evidências documentadas aderentes aos padrões da empresa.
 - c. Existem inspeções e evidências documentadas, mas não existem processos formais para re-visitar os terceiros para recertificá-los ou reconhecê-los oficialmente.
 - d. Existem inspeções regulares utilizando-se avaliações padrão e evidências documentadas da aderência ao SOX.
 - e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.
12. Todos os sistemas e aplicativos envolvidos em (ou suportando) relatórios financeiros possuem controles de acesso e autenticação segura, implementados de forma efetiva?

- a. Os sistemas são configurados para autenticação, os usuários compartilham contas e/ou têm acesso de administrador em sistemas e aplicações envolvidos em relatórios financeiros.
- b. Os sistemas são configurados uma vez para cada usuário, mas não existe mais nada que garanta que as funções são segregadas ou que as interfaces estão expostas a acessos não autorizados.
- c. Os sistemas estão configurados para autenticação forte e as senhas não são compartilhadas, mas essas proteções são tratadas de modo pontual.
- d. Os sistemas e aplicações usam autenticação forte, de modo consistente, e existem mecanismos de prevenção contra acesso não autorizado. Existe reporte de direitos de acesso e uso de contas.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

13. As contas de usuários são gerenciadas de forma definida e contínua com as devidas aprovações de *workflow* sobre seus proprietários e custodiantes? Existem LOGs e documentação referentes a privilégios conferidos a contas de usuários?

- a. A empresa usa gerenciamento de usuários de forma intuitiva.
- b. Os usuários são gerenciados de forma intuitiva, mas existe alguma documentação e evidência de que existem aprovações.
- c. Gerenciamento de usuário segue processos documentados de aprovação, mas os mecanismos são diferentes para os vários sistemas.
- d. Existe um processo único e centralizado de gerenciamento de usuários, com reporte integrado, que é usado para todo o gerenciamento relacionado ao SOX.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

14. A empresa executa avaliações regulares sobre contas e privilégios?

- a. As contas são criadas, porém nunca mais são revistas ou avaliadas.
- b. Contas são revisadas de forma pontual quando os sistemas entram em manutenção, são modificados ou na suspeição de um problema.
- c. As contas são revisadas regularmente por sistemas e pelos custodiantes das aplicações a partir de informações obtidas junto aos donos e gestores da informação.
- d. As contas são revisadas regularmente por meio de um *workflow* automatizado com checagens.
- e. Balanços providenciados pelos representantes do negócio, custodiantes dos sistemas e gerentes. Relatórios são providenciados automaticamente sob demanda.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

15. A empresa conduz testes regulares de segurança nos sistemas relacionados ao SOX de forma a certificar-se de que as configurações são as que deveriam ser e (se) os sistemas permanecem seguros?

- a. Não existe qualquer tipo de teste.
- b. Existem avaliações de configuração de forma pontual, mas não existem testes de penetração.
- c. Existem testes de penetração e avaliação de configuração de forma pontual.
- d. Existem testes de penetração e análises de configuração em bases regulares para todos os sistemas SOX considerados críticos.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

16. A empresa gerencia suas vulnerabilidades e aplica correções de forma uniforme a partir de todos os sistemas relacionados ao SOX?

- a. Não existe nenhum mecanismo que rastreie vulnerabilidades (vírus, *bugs* de sistema, etc) e aplique *patches* ou correções.
- b. Monitoram-se as vulnerabilidades e aplicam-se correções, mas depende de grupos de administradores de sistemas e de rede e do tipo de sistema.
- c. Existe um gerenciamento efetivo das vulnerabilidades, mas não de forma uniforme. Está implementado por diferentes áreas em vários níveis de documentação e reporte.
- d. Existem rastreamento de vulnerabilidades e aplicação de correções de forma uniforme em toda a empresa.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

17. A empresa monitora a efetividade dos controles de segurança implementados para a aderência ao SOX?

- a. A aderência é checada como parte da auditoria.
- b. Os controles são checados para determinar se continuam a operar como planejado, mas não são avaliados para checar se são efetivos no ambiente corporativo.
- c. Os controles são avaliados regularmente para checar sua efetividade, e mudanças são programadas como parte do processo de aderência aos projetos
- d. Os controles são avaliados e documentados de forma contínua como parte das operações do negócio. Aperfeiçoamentos nos controles são inerentes à operação do negócio e TI.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

18. A empresa contrata terceiros com expertise específico para avaliar e conferir seus processos e controles de TI?

- a. Não existe avaliação independente.
- b. Existe alguma avaliação independente, mas é pontual.
- c. Existe avaliação independente para as novas políticas e sistemas, mas não existe reavaliação.
- d. Existe avaliação independente das políticas importantes, sistemas e aplicações.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

19. A empresa envolve de forma proativa a auditoria interna antes de finalizar os planos de TI?

- a. A auditoria é conduzida depois do desenho do plano estar completo.
- b. A auditoria é consultada, mas seu impacto principal é depois que o sistema é organizado e preparado para entrar em produção.
- c. A auditoria é consultada em vários pontos durante o desenvolvimento e implementação.
- d. A auditoria é membro importante no time de desenvolvimento e implementação.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

20. A empresa realiza consultas a terceiros sobre a aderência às leis e regulamentações (ex. SOX e privacidade)?

- a. Não existem consultas.
- b. O staff interno avalia os requerimentos legais de aderência.
- c. Existe alguma avaliação externa sobre aderência.
- d. Existe avaliação externa regular sobre a efetividade da aderência da empresa às leis e regulamentações.
- e. Alto nível, seguindo as melhores práticas, otimizados e automatizados.

Livros Grátis

(<http://www.livrosgratis.com.br>)

Milhares de Livros para Download:

[Baixar livros de Administração](#)

[Baixar livros de Agronomia](#)

[Baixar livros de Arquitetura](#)

[Baixar livros de Artes](#)

[Baixar livros de Astronomia](#)

[Baixar livros de Biologia Geral](#)

[Baixar livros de Ciência da Computação](#)

[Baixar livros de Ciência da Informação](#)

[Baixar livros de Ciência Política](#)

[Baixar livros de Ciências da Saúde](#)

[Baixar livros de Comunicação](#)

[Baixar livros do Conselho Nacional de Educação - CNE](#)

[Baixar livros de Defesa civil](#)

[Baixar livros de Direito](#)

[Baixar livros de Direitos humanos](#)

[Baixar livros de Economia](#)

[Baixar livros de Economia Doméstica](#)

[Baixar livros de Educação](#)

[Baixar livros de Educação - Trânsito](#)

[Baixar livros de Educação Física](#)

[Baixar livros de Engenharia Aeroespacial](#)

[Baixar livros de Farmácia](#)

[Baixar livros de Filosofia](#)

[Baixar livros de Física](#)

[Baixar livros de Geociências](#)

[Baixar livros de Geografia](#)

[Baixar livros de História](#)

[Baixar livros de Línguas](#)

[Baixar livros de Literatura](#)
[Baixar livros de Literatura de Cordel](#)
[Baixar livros de Literatura Infantil](#)
[Baixar livros de Matemática](#)
[Baixar livros de Medicina](#)
[Baixar livros de Medicina Veterinária](#)
[Baixar livros de Meio Ambiente](#)
[Baixar livros de Meteorologia](#)
[Baixar Monografias e TCC](#)
[Baixar livros Multidisciplinar](#)
[Baixar livros de Música](#)
[Baixar livros de Psicologia](#)
[Baixar livros de Química](#)
[Baixar livros de Saúde Coletiva](#)
[Baixar livros de Serviço Social](#)
[Baixar livros de Sociologia](#)
[Baixar livros de Teologia](#)
[Baixar livros de Trabalho](#)
[Baixar livros de Turismo](#)