UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM MODELO DE CONFIANÇA APLICADO AOS PROCESSOS DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

DAYSE DE MELLO BENZI

ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JÚNIOR

TESE DE DOUTORADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: 030/TESE/2008
BRASÍLIA, DF: AGOSTO/2008.
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UM MODELO DE CONFIANÇA APLICADO AOS PROCESSOS DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

DAYSE DE MELLO BENZI

TESE DE DOUTORADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR.

APROVADO POR:

_____

RAFAEL TIMÓTEO DE SOUSA JÚNIOR
DOUTOR, UNB (ORIENTADOR)

_____

PAULO ROBERTO DE LIRA GONDIM
DOUTOR, UNB (EXAMINADOR INTERNO)

_____

GEORGES AMVAME NZE
DOUTOR, UNB (EXAMINADOR INTERNO)

_____

RICARDO MATOS CHAIM
DOUTOR, FGV (EXAMINADOR EXTERNO)

_____

MURILO BASTOS DA CUNHA
DOUTOR, UNB (EXAMINADOR EXTERNO)

BRASÍLIA, DF, 21 DE AGOSTO DE 2008.

FICHA CATALOGRÁFICA

Benzi, Dayse de Mello, Um Modelo de Confiança Aplicado aos Processos de Gestão da Tecnologia da Informação. [Distrito Federal], 2008.xiv, 142 p., 297 mm (ENE/FT/UnB, Doutor, Engenharia Elétrica, 2008).
Tese de Doutorado – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.

1. Tecnologia da Informação	2. Gestão da Tecnologia da Informação
3. Confiança	4. Risco
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Benzi, Dayse de Mello (2008). Modelo de Confiança Aplicado aos Processos de Gestão da Tecnologia da Informação**.** Tese de Doutorado, Publicação ENE. 030/2008, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 146 p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Dayse de Mello Benzi
TITULO DA TESE: Um Modelo de Confiança Aplicado aos Processos de Gestão da Tecnologia da Informação

GRAU/ANO: Doutor / 2008

_____

Dayse de Mello Benzi
SQS 104 Bloco K 202
CEP: 70.722-080, Brasília - DF
Tel. 55 – 61 – 32268075 / dayse@redes.unb.br

DEDICATÓRIA

Aos meus filhos, pela compreensão nos momentos de ausência que foram dedicados ao desenvolvimento desse trabalho, e ao meu marido pelo companheirismo e motivação.

AGRADECIMENTOS

Agradeço a todos que contribuiram de alguma maneira para a realização desse trabalho. Em especial ao meu orientador professor Rafael Timóteo de Sousa Jr., por ter acreditado na minha competência quando me aceitou como sua aluna para orientação. Pelas horas dedicadas durante o curso na elaboração desse trabalho, pelo incentivo e amizade proporcionando o melhor ambiente possível para que essa pesquisa pudesse fluir de forma agradável.

Ao programa de pós-graduação em engenharia elétrica pela apoio dispensado.

À CAPES, à École Superieur d'Électricité - SUPELEC, Rennes - França e aos professores Christophe Bidan, co-orientador no exterior, e Ludovic Mé, Chefe do Grupo de Pesquisa Securité des Systemes d'Information et Reseaux - SSIR, por terem criado condições que possibilitaram a realização do estágio doutoral agregando a minha pesquisa, conhecimento de área de excelência.

De maneira especial a minha família, meu marido e meus filhos pelo apoio irrestrito em todos os momentos de minha vida.

RESUMO

UM MODELO DE CONFIANÇA APLICADO AOS PROCESSOS DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

A tese apresenta um modelo de confiança aplicado aos processos de gestão da tecnologia da informação. Discorre sobre definições de confiança explicitando alguns tipos da confiança e apresenta modelos de confiança aplicados em áreas distintas. Focaliza a governança de TI, enfatizando a necessidade do alinhamento com as estratégias organizacionais e a harmonização com a atividade-fim das empresas.

Para isso aborda os impactos da confiança na governança de TI, onde estudos recentes identificam que organizações com uma governança de TI ajustada ao negócio obtêm vantagens em relação às demais. Nesse contexto aborda o entendimento de que o rumo seguro está vinculado à confiança que contribui para o alcance dos resultados objetivados pela gestão, desde que seja controlada e medida, levando a que as organizações de TI adquiram maior eficácia no alinhamento da TI com a estratégia organizacional.

A validação do Modelo proposto foi realizada por intermédio de um estudo de caso em uma organização real onde foi elaborado um diagnóstico da situação, empregando requisitos consagrados de confiança associados aos processos pertinentes de gestão de TI. Em tal processo foram cumpridas todas as fases previstas na elaboração do Modelo, desde o planejamento até a tabulação dos resultados obtidos após a implantação das respostas às questões formuladas o que foi feito de modo a permitir a verificação dos impactos da confiança, atividade na qual se contou com o auxílio de um sistema eletrônico desenvolvido para essa finalidade.

ABSTRACT

A TRUST MODEL APPLYED TO INFORMATION TECHNOLOGY MANAGEMENT PROCESSES

This dissertation presents a model of trust in the management of the information technology. It presents relevant aspects on the use of trust on the Information Technology (IT) Management. It comments on the definitions of trust relates the contemporary business environment to crescent risks, as far as trust is concerned, based on the complexity deriving from globalized relationships. It focuses IT management, emphasizing the necessity of alignment with the organizational strategies and the harmonization with the end-activity of the companies.

To do so it approaches the impacts of the trust in IT management where recent studies identify that organizations whose IT management is business-focused run less risks and get advantages in relation to others. In this context, it approaches the understanding that the safe route is tied to the trust, which may provide highly desirable results to management, as long as they are controlled and measured, making IT organizations to acquire greater effectiveness in their alignment to the organizational strategy.

The application of the model consisted of a case study in the DMB Organization which was drafted a result and a diagnosis of the situation, employing requirements enshrined in trust associated with the relevant procedures of management. In this application have been completed all stages in developing the model, from planning to the tabulation of results after the deployment of the questions raised what was done to enable the verification of the impacts of trust, an activity which had the aid of an electronic system designed for that purpose.

SUMÁRIO

1.INTRODUÇÃO 1
1.1.JUSTIFICATIVA 2
1.2.APRESENTAÇÃO DO TEMA 3
1.3.OBJETIVOS 4
1.3.1.Objetivo Geral 4
1.3.2.Objetivos Específicos 4

2.CONFIANÇA 5
2.1.TIPOS DE CONFIANÇA 7
2.2.REQUISITOS DE CONFIANÇA 9
2.3.APLICAÇÕES DA CONFIANÇA 11
2.3.1.O Modelo HTrust 12
2.3.2.O Modelo para Confiança em Redes Dinâmicas 13
2.3.3.O Modelo de Confiança para e-business 16
2.3.4.O Modelo para o Gerenciamento de Confiança em Serviços Móveis 19
2.4.TRABALHOS SOBRE CONFIANÇA 24

3.GESTÃO DA TECNOLOGIA DA INFORMAÇÃO 26
3.1.ALINHAMENTO DA TI COM A ESTRATÉGIA DE NEGÓCIOS 27
3.1.1.Harmonia Decorrente das Governança de TI 30
3.2.OS RISCOS 33
3.3.COBIT 35
3.4.ESTRUTURA DO COBIT 36
3.5.CONFIANÇA E A GESTÃO DA TECNOLOGIA DA INFORMAÇÃO .39
3.5.1.Processos e Métricas 40
3.5.1.1.Definir o Plano Estratégico de TI 41
3.5.1.2.Definir a Arquitetura da Informação 41
3.5.1.3.Definir a Direção Tecnológica 41
3.5.1.4.Definir os Processos de TI, Organização e Relacionamentos 42
3.5.1.5.Definir o Controle dos Investimentos de TI 42
3.5.1.6.Estabelecer os Objetivos de Gerenciamento e Direção 43
3.5.1.7.Gerenciar Recursos Humanos de TI 43
3.5.1.8.Estabelecer o Controle de Qualidade 43
3.5.1.9.Avaliar e Controlar o Risco de TI 44
3.5.1.10.Gerenciar Projetos 44
3.5.1.11.Identificar Soluções Automatizadas 44
3.5.1.12.Adquirir e Manter Software de Aplicação 45
3.5.1.13.Adquirir e Manter Infra-estrutura de Tecnologia 45
3.5.1.14.Instalar e Validar Soluções e Mudanças 45
3.5.1.15.Definir e Gerenciar Níveis de Serviço 45
3.5.1.16.Definir e Gerenciar Serviços Terceirizados 46

3.5.1.17.Estabelecer e Serviço Contínuo 46
3.5.1.18.Estabelecer a Segurança dos Sistemas 46
3.5.1.19.Identificar e Alocar Custos 46
3.5.1.20.Gerenciar Central de Serviço e Incidentes 47
3.5.1.21.Gerenciar a Configuração 47
3.5.1.22.Gerenciar Problemas 47
3.5.1.23.Gerenciar Dados 47
3.5.1.24.Gerenciar Ambiente Físico 48
3.5.1.25.Gerenciar Operações 48
3.5.1.26.Monitorar e Avaliar Desempenho de TI 48
3.5.1.27.Monitorar e Avaliar Controle Interno 48
3.5.1.28.Estabelecer a Conformidade Regulamentar 49
3.5.1.29.Fornecer Governança de TI 49
3.5.2.Métricas 49

4.METODOLOGIA 56
4.1.MODELO DE CONFIANÇA 56
4.2.ARQUITETURA DO MODELO 67
4.2.1.Planejamento 67
4.2.2.Mecanismos para Obtenção do Grau de Confiança 67
4.2.3.Base de Conhecimento 68
4.3.IMPLEMENTAÇÃO DO MODELO 68
4.3.1.Mecanismo de Avaliação 68
4.3.2.Ações de Confiança 69
4.3.3.Sistema de Apoio 71
4.3.4.Interação com o Usuário 72

5.VALIDAÇÃO DO PROJETO 73
5.1.FOCO DA PESQUISA 73
5.2.NÍVEL ESTRATÉGICO 73
5.3.NÍVEL DE EXECUÇÃO 74
5.4.UNIVERSO DA PESQUISA 77
5.5.APLICAÇÃO DA PESQUISA 78
5.6.RESULTADOS ENCONTRADOS 78
5.6.1.Planejamento 79
5.6.2.Controle 80
5.6.3.Implementação 82
5.6.4.Entrega 84
5.6.5.Suporte 86
5.6.6.Monitoramento 88
5.7.CONSIDERAÇÕES FINAIS 90

6. CONCLUSÕES 95
6.1. SUGESTÕES PARA PESQUISAS FUTURAS 96

7. REFERÊNCIAS 98

ANEXOS **107**
ANEXO A – COLETA DE INFORMAÇÕES SOBRE OS PROCESSOS DE TI **108**
Anexo A.1 – Planejamento **108**
Anexo A.2 – Controle **110**
Anexo A.3 – Implementação **112**
Anexo A.4 – Entrega **114**
Anexo A.5 – Suporte **116**
Anexo A.6 – Monitoramento **118**

ANEXO B – SISTEMA GERENCIAMENTO TI BASEADO EM CONFIANÇA **120**
Anexo B.1 – Tela de Entrada **120**
Anexo B.2 – Tela de Acesso à Pesquisa (questionário) **121**
Anexo B.3 – Tela de Acesso aos Resultados **122**
Anexo B.4 – Tela de Acesso aos Resultados Totais por Fator **123**
Anexo B.5 – Tela de Acesso aos Resultados de Cada Fator por Setor **124**
Anexo B.6 – Tela de Acesso aos Resultados de Cada Fator por Setor **125**
Anexo B.7 – Tela de Acesso ao Resultado Total **126**

ANEXO C – PAINEL DE ACOMPANHAMENTO DA DMB **127**

ANEXO D - PUBLICAÇÕES REALIZADAS DURANTE PESQUISA DA TESE **128**

LISTA DE TABELAS

TABELA 1 – REQUISITOS DE CONFIANÇA [47] 10
TABELA 2 - RELAÇÃO DE TRABALHOS SOBRE CONFIANÇA 24
TABELA 3 - MATRIZ DE ARRANJOS DE TI 29
TABELA 4 - RELAÇÃO ELEMENTOS DA GESTÃO DE TI - PLANEJAMENTO X MÉTRICAS. 50
TABELA 5 - RELAÇÃO ELEMENTOS DA GESTÃO DE TI - CONTROLE X MÉTRICAS. 51
TABELA 6 - RELAÇÃO ELEMENTOS DA GESTÃO DE TI - IMPLEMENTAÇÃO X MÉTRICAS. 52
TABELA 7 - RELAÇÃO ELEMENTOS DA GESTÃO DE TI - ENTREGA X MÉTRICAS. 53
TABELA 8 - RELAÇÃO ELEMENTOS DA GESTÃO DE TI – SUPORTE X MÉTRICAS. 54
TABELA 9 - RELAÇÃO ELEMENTOS DA GESTÃO DE TI - MONITORAMENTO X MÉTRICAS. 55
TABELA 10 - REQUISITOS DE CONFIANÇA 57
TABELA 11 – PROCESSOS UTILIZADOS NO MODELO 58
TABELA 12 – QUESTIONÁRIO PLANEJAMENTO 59
TABELA 13 - QUESTIONÁRIO CONTROLE 60
TABELA 14 - QUESTIONÁRIO IMPLEMENTAÇÃO 61
TABELA 15 - QUESTIONÁRIO ENTREGA 63
TABELA 16 - QUESTIONÁRIO SUPORTE 64
TABELA 17 – MONITORAMENTO 65
TABELA 18 - ASSOCIAÇÃO DOS REQUISITOS DE CONFIANÇA COM OS MECANISMOS E MÉTRICAS DE TI. 66
TABELA 19- CLASSIFICAÇÃO DA CONFIANÇA 68
TABELA 20 – CLASSIFICAÇÃO DA CONFIANÇA 70
TABELA 21 - CARACTERIZAÇÃO DOS ESPECIALISTAS RELACIONADOS AOS SETORES 77
TABELA 22 - PLANEJAMENTO 79
TABELA 23 - CONTROLE 80
TABELA 24 – ITENS VERIFICADOS DO PROCESSO CONTROLE 81
TABELA 25 - IMPLEMENTAÇÃO 82
TABELA 26 - ITENS VERIFICADOS NO PROCESSO IMPLEMENTAÇÃO 82
TABELA 27 - ENTREGA 85
TABELA 28 - ITENS ENTREGA 85
TABELA 29 - SUPORTE 86
TABELA 30 - ITENS DO PROCESSO SUPORTE 87
TABELA 31 - MONITORAMENTO 88

TABELA 32 – ITENS VERIFICADOS DO PROCESSO MONITORAMENTO 89
TABELA 33 - RESULTADO DA DMB 90

LISTA DE FIGURAS

FIGURA 1 - MODELO ESTRATÉGICO DE ALINHAMENTO 27
FIGURA 2 - HARMONIZAÇÃO DE ESTRATÉGIAS E ORGANIZAÇÃO 30
FIGURA 3 - ESTRUTURA DO COBIT 36
FIGURA 4 - CONCEPÇÃO DO MODELO DE CONFIANÇA 57
FIGURA 5 - ARQUITETURA DO MODELO 67
FIGURA 6 - MECANISMO DE AVALIAÇÃO 69
FIGURA 7 - SISGESCON 71
FIGURA 8 - ORGANOGRAMA CDS 75
FIGURA 9 - ORGANOGRAMA CIT 76
FIGURA 10 - RESULTADO ÁREA DE TI DA DMB 79
FIGURA 11 - RESULTADO PLANEJAMENTO 80
FIGURA 12 - RESULTADO IMPLEMENTAÇÃO 84
FIGURA 13 - RESULTADO IMPLEMENTAÇÃO- DMB 84
FIGURA 14 - RESULTADO SUPORTE 84
FIGURA 15 - PAINEL DE ACOMPANHAMENTO 91
FIGURA 16 - NÍVEL BAIXO DE CONFIANÇA 92
FIGURA 17 - NÍVEL MÉDIO DE CONFIANÇA 92
FIGURA 18 - CATEGORIA SUPORTE DE TI 93
FIGURA 19 - NÍVEL ALTO DE CONFIANÇA 94

LISTA DE SIGLAS

CDS	Centro de Desenvolvimento de Sistemas
CIT	Centro Integrado de Telemática
CG	Computação Global
CT	Centro de Telemática
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
ERM	Enterprize Risk Management
ODG	Órgão de Direção Geral
ODS	Órgão de Direção Setorial
ODTI	Órgão de Direção de TI
SAM	Strategic Alignment Model
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

1. INTRODUÇÃO

O ambiente no qual se inserem as organizações se apresenta cada vez mais globalizado e competitivo. Elas necessitam, para a interação otimizada nas diversas áreas de atuação, de informações confiáveis e conhecimentos atualizados, encontrando na Tecnologia da Informação (TI) um veículo para agregar valores aos seus produtos e serviços.

Para a sua utilização plena e eficaz, deve-se considerar que o que não se controla, não pode ser gerenciado, sendo esta a primeira premissa quando queremos falar sobre Gerenciamento da TI, ou seja, controlar para poder gerenciar.

O gerenciamento sofre impactos positivos de uma série de fatores. A presente pesquisa concentra-se em um deles, a confiança, buscando melhor conhecê-la, por meio do tratamento de seus modelos e mecanismos com o foco da sua utilização para avaliação de seus níveis nas diversas áreas da TI.

Esta introdução apresenta a justificativa da escolha do tema a ser pesquisado, bem como define um contexto de aplicação, aborda a questão da pesquisa e os objetivos propostos.

Na seqüência, o capítulo 2 traz uma abordagem conceitual sobre a confiança discorrendo sobre os principais requisitos, mecanismos e aplicações. Discorre ainda, com foco na utilização da confiança, sobre tipos, modelos e trabalhos publicados.

O capítulo 3 apresenta o contexto da gestão da TI e os elementos que farão parte do modelo a ser adotado na realização da pesquisa. Nele são abordados aspectos relevantes da iteração da TI com os negócios, os riscos envolvidos bem como o seu relacionamento com a confiança. Os processos de TI são abordados no que se refere a sua implementação no modelo adotado.

O capítulo 4 apresenta o método de pesquisa envolvendo as etapas para sua realização, melhor especificando o contexto e as técnicas de coleta e de análise de dados. Nele é apresentada a metodologia empregada discorrendo sobre o modelo proposto, no

que se refere a arquitetura, implementação, mecanismos de avaliação e ainda sobre o sistema desenvolvido em apoio a aplicação da pesquisa.

Apresenta-se no capítulo 5, um estudo de caso que foi realizado com a finalidade de aplicação real do modelo desenvolvido, o que proporcionou o respaldo necessário para a elaboração de recomendações e conclusão.

1.1. JUSTIFICATIVA

Esta justificativa aborda aspectos sobre a escolha do foco do trabalho – Medição de Confiança – e do campo que se pretende desenvolver a pesquisa – Modelos de Gestão de Tecnologia da Informação.

Atualmente, o ambiente de negócios diversificado, com a Internet ultrapassando as limitações geográficas e estabelecendo ligações à distância, requer informações depuradas e confiáveis. Assim sendo, a auditoria empresarial ligada ao foco do trabalho, que avalia as referidas informações, vem sendo objeto de recentes pesquisas que revelam ser a questão da confiança um assunto de grande complexidade, mas bastante promissor como um dos novos paradigmas e soluções de segurança da informação. A confiança pode ser aplicada tanto na detecção como na prevenção de problemas de segurança. Tais aspectos têm um grande impacto nas interações que os usuários realizam entre si e com as organizações.

Atualmente a governança está na agenda de muitas organizações, levando ao desenvolvimento de modelos de alto nível. Somente esse procedimento não significa que a gestão esteja realmente ajustada à organização. A concepção do modelo a ser utilizado é a primeira etapa, sendo que somente em etapas seguintes será obtida uma solução sustentável.

Então, na implementação de medidas para a adoção de um modelo de governança de TI eficiente, a organização deverá ser analisada de forma a serem empreendidas medidas que visem a atenuar as deficiências encontradas e a adoção de procedimentos de correção e de ajuste.

O procedimento acima carece ainda, no campo da pesquisa, de ações no sentido de formalização de níveis de confiança, de forma a garantir a efetividade da gestão organizacional.

1.2. APRESENTAÇÃO DO TEMA

Esta tese propõe a criação de um modelo de confiança aplicado aos processos da gestão de tecnologia da informação, produzido a partir dos mecanismos que suportam o surgimento da confiança.

Considerando os conflitos, contradições e indefinições no que se refere à confiança em ambiente computacional, e abordando a grande complexidade e abstração dos conceitos envolvidos no estudo [59], verifica-se que na busca de soluções técnicas existe considerável espaço para pesquisa acrescentando conhecimentos à investigação que tem sido muito explorada na literatura internacional especializada [48], já que a aplicação dessas soluções é intensamente exigida nos ambientes empresariais de tecnologia da informação.

Assim, são analizados os fatores que suportam o surgimento de comportamento confiável nos citados ambientes, em analogia com o comportamento humano acerca do estabelecimento da confiança [52]. A análise desses fatores permitiu o desenvolvimento de instrumento adequado ao estabelecimento de modelo para tratamento de confiança na Governança de TI.

Focalizando então a Governança de TI, constitui-se em diferencial desejável a inclusão de mecanismos que garantam a segurança da informação, possibilitando a avaliação de riscos por método adequado, bem como o estabelecimento de modelos da confiança.

A confiança relaciona-se ao fornecimento, por parte dos sistemas, de informações apropriadas aos gerentes para tomada de decisão, relatórios financeiros precisos e informações adequadas aos órgãos normatizadores sobre o cumprimento das normas legais. Além disso, ela assegura que os processos críticos e os serviços de TI sejam monitorados, e qualquer incidente ou falha de alta prioridade, seja encaminhada e

resolvida. Os serviços requerem que níveis mais elevados de confiança sejam implementados para minimizar a probabilidade de uma falha ou interrupção de um determinado serviço.

O gerenciamento de confiança tem buscado soluções tecnológicas, abandonando a abstração relatada em muitas das definições de confiança e adotando metodologias de controle com elevado aporte computacional. Com este enfoque, para que se tenha uma Governança de TI amplamente confiável, torna-se apropriado a criação de um modelo de confiança aplicado aos processos de gestão da tecnologia da informação.

1.3. OBJETIVOS

A seguir apresentam-se os objetivos geral e específicos da pesquisa realizada que focaliza a medição da confiança utilizando os modelos de gestão de TI.

1.3.1. Objetivo Geral

O trabalho tem como objetivo geral apresentar uma proposta de um modelo de confiança aplicado aos processos de gestão da tecnologia da informação.

1.3.2. Objetivos Específicos

Os objetivos específicos foram:

a) Identificar e descrever de forma sistemática os principais mecanismos e tipos de tratamento da confiança à gestão de TI de uma organização.

b) Analisar os fatores que apoiam o surgimento de comportamento confiável, objetivando a criação de modelo para estabelecimento da confiança;

c) Adaptar técnicas existentes e elaborar de novas técnicas para estabelecimento da confiança;

d) Identificar os processos de TI onde à confiança deverá ser verificada;

e) Elaborar requisitos de confiança a serem relacionados aos processos de TI.

f) Testar e validar o modelo.

2. CONFIANÇA

Nos relacionamentos em múltiplos campos de atuação, para uma otimização da real interação entre a entidade ou pessoa prestadora de serviço e os beneficiados ou usuários, verifica-se ser a confiança um componente imprescindível. Mayer *et al* [46], citam ser a mesma importante em muitas áreas, tais como: comunicação, liderança, administração por objetivos, negociação, teoria dos jogos, reconhecimento de *performance,* relações de trabalho e implementação de grupos de trabalho auto-gerenciáveis. Por esse amplo emprego, nas oportunidades em que se torna necessário estabelecer a sua compreensão e definição, observa-se a possibilidade do surgimento de interpretações conflitantes, caracterizadas pela ausência de princípios claros. Keen *et al* [37] coerente com a constatação, chega a afirmar que a "confiança está tornando-se cada vez mais importante, mas ainda não se sabe o que realmente ela significa".

O sociólogo Diego Gambetta [25] busca garantir a manutenção do objetivo de ser o mais fiel possível ao modelo de confiança humano, trazendo a convicção de ser a confiança algo extremamente subjetivo e difícil (praticamente impossível) de se definir um padrão. Numa relação entre dois agentes não existe a garantia da reciprocidade do grau de confiança entre ambos, pois cada um poderá confiar no outro em dosagens distintas. A decisão de começar uma interação ou não com outro agente, depende do nível de confiança estabelecido entre ambas as partes, do contexto e do risco envolvido.

Fruto dessa dificuldade, a confiança é muitas vezes definida de forma mais especializada e voltada para a área de interesse do pesquisador. Como exemplo, Fukuyama [24] relaciona confiança e sociedade contemporânea e Luftman [38] confiança e sistemas sociais. Prosseguindo na especialização, Pillatt [50] usa uma definição de confiança, dentro do ambiente de *e-business*, voltada de uma maneira muito específica para tópicos tais como autenticação e habilidade para o pagamento de produtos e/ou serviços solicitados. Porém, este tipo de definição é bastante restrito à medição da confiança com relação ao comprador e não dá suporte para a medição da confiança das demais entidades transacionais participantes da negociação. Manchala [40, 41], tenta ver

a confiança de uma maneira mais genérica, mensurando-a com base na transação como um todo e não em alguns parâmetros específicos de uma entidade. Neste caso, as informações referentes a todas as entidades participantes da transação e do produto/serviço negociado são abstraídas servindo de base para uma medição mais genérica da confiança.

Ao buscar um conceito mais amplo, baseado em objetivos, abordando aspectos relacionados à honestidade, competência e confiabilidade, ultrapassa-se a fronteira do termo em si e adentra-se em parâmetros que poderão se relacionar facilmente com termos tais como autorização, autenticação e validação. É verdade que esses termos poderão ser usados de forma intercambiável como afirma Grandison e Sloman, [27], ao considerarem ser a autorização o resultado do refinamento de um relacionamento de confiança, ou seja, a delegação de direitos de acesso para uma entidade transacional desempenhar ações específicas em um alvo específico e a autenticação como sendo a verificação da identidade de uma entidade, a qual pode ser desempenhada por meio de senha, serviços confiáveis de autenticação ou por meio de certificados.

Grandison [28] contribui para aprofundar o entendimento sobre confiança ao especificar ser a mesma "a convicção quantificada por um usuário com respeito à competência, honestidade, segurança e confiança de uma entidade dentro de um contexto especificado". Amplia esse conceito definindo ser a entidade competente quando for capaz de executar corretamente, e em tempo razoável, as funções esperadas. Ser honesta quando fôr verdadeira e não enganar (acidentalmente ou não) ou cometer fraude. Ser segura quando assegurar o sigilo dos ativos e prevenir o acesso sem autorização a eles.

Jones [36] acrescenta que a confiança, é definida pela *European Commission Joint Research Centre* como sendo "a propriedade de um relacionamento de negócio, de maneira que possa ser dado crédito aos parceiros de negócios e às transações desempenhadas com eles".

Gambetta [25] define confiança em termos matemáticos como *Trust* (ou, simetricamente, desconfiança), sendo ela um determinado nível de probabilidade subjetiva com que o agente avalia que outro agente ou grupo de agentes irão realizar uma

ação especial, tanto antes que possa acompanhar tais ações (ou de forma independente ou a sua capacidade de ser cada vez capazes de controlá-lo), e em um contexto em que ela afeta a sua própria ação. Quando dizemos que alguém é confiável, significa implicitamente que é alta a probabilidade de que ele irá executar uma ação que é benéfica ou pelo menos não prejudicial a nós, sendo essa constatação suficiente para que possamos nos engajar em alguma forma de cooperação com ele. Correspondentemente, quando dizemos que alguém é pouco confiável, torna-se baixa a probabilidade de que se possa estabelecer uma cooperação com ele.

Assim é possível verificar que as definições ora tendem para relacionamentos interpessoais, ora para os negócios e prestação de serviços, podendo ao quantificar níveis de confiança, abrir um amplo espectro de áreas de pesquisa, abordando numerosas nuances das ciências humanas, bem como das exatas.

2.1. TIPOS DE CONFIANÇA

O amplo espectro da confiança nos leva a dividir, segundo a área de aplicação e de acordo com as distintas definições, os relacionamentos facilitados e levados a excelentes níveis de interações baseados em confiança interpessoal, confiança interinstitucional e confiança pessoa/instituição. Grassi [29], configurando uma abordagem interessante para os objetivos deste trabalho, especifica que segundo Lyons e Mehta [39], confiança é questão de grau, indo da confiança completa até sua completa ausência, em que o comportamento oportunista será a regra. Eles analisam o papel da confiança em facilitar relações de troca eficientes, considerando a abordagem de dois mecanismos distintos que dão suporte à confiança, a confiança socialmente orientada e a confiança auto-interessada.

A confiança socialmente orientada considera aspectos do passado - *backward-looking*, ao analisar os mecanismos sociais realizados pela comunidade de indivíduos que, intencional ou inadvertidamente, sustentam a confiança, e as suas conseqüências. Dogson [20] denomina esta visão da confiança de *goodwill trust,* onde o reconhecimento de que o comportamento é localizado dentro de uma arena social leva à noção de

confiança para uma orientação baseada em normas; as relações sociais são experimentadas em certos modos normativos, ou mutuamente entendidas.

A confiança auto-interessada é entendida instrumentalmente aplicando a teoria dos jogos para modelar a interação entre agentes cujos interesses parcialmente conflitam e parcialmente convergem. A confiança surge como conseqüência de um cálculo cuidadoso, ou da criação intencional de incentivos em resposta direta à presença de risco comportamental. Os custos e benefícios relativos de ser confiante ou confiável são mensuráveis, e eles são avaliados dentro dos limites da relação de troca. Portanto, a confiança auto-interessada, ao contrário da anterior, é fundamentalmente baseada em futuro - *"forward-looking*", com agentes sendo confiantes ou confiáveis somente até o ponto em que eles esperam que tal comportamento renda um retorno direto.

Grassi [29] ressalta ainda que "os autores, ao distinguirem os dois tipos de confiança acima descritos, não propõem que um seja universalmente verdadeiro e o outro não, nem que haja lugar para somente um tipo de confiança em cada relacionamento. Eles podem ser usados para reforçar um ao outro, apesar de estarem provavelmente presentes em diferentes combinações de importância relativa. Seria errado propor que eles são igualmente importantes. É possível que um tipo seja dominante em um grupo de firmas e o outro, em outros". Lyons e Mehta [39] afirmam ser "amplamente possível que os mesmos indivíduos venham a agir com confiança socialmente orientada com respeito a um parceiro comercial, mas somente com confiança auto-interessada com respeito a outro".

Domenico e Macri [21], citando Couch *et al* [14] acrescentam que a pesquisa sobre confiança avançou para dois tipos distintos: a Confiança em Geral, que é a expectativa em relação às pessoas em geral, e a Confiança Relacional que é o relacionamento com parceiros específicos. O primeiro verifica a propensão ou predisposição do indivíduo a confiar, enquanto a segunda abordagem refere-se à fé que as pessoas possuem em um relacionamento, que segundo Rempel, Holmes e Zanna, *apud* Couch *et al*. [14] podem ser influenciadas por características e ações de um dos parceiros. A confiança em geral, relacionando-se com a confiança socialmente orientada, aborda

expectativa que deriva de experiências passadas, dependendo do quanto um indivíduo acredita na honestidade humana ou também de traços da sua personalidade.

Enfatizando, Mayer *et al*. [46] acrescenta que as pessoas diferem na sua propensão a confiar, sendo a propensão o desejo de acreditar nos outros, influenciando em quem se irá acreditar. Pessoas com diferentes experiências de desenvolvimento, tipos de personalidade e bagagem cultural podem variar na sua propensão a confiar.

Marsh [46] também discorre sobre tipos de confiança, ressaltando que ela se apresenta com diversos aspectos. E visando o seu esclarecimento, apresentou um formalismo que fornece uma ferramenta para uma discussão mais precisa sobre como mensurar a confiança por meio de aspectos práticos envolvendo definição e implementação de um modelo, que segundo o próprio Marsh, pode ser utilizado por agentes artificiais para a tomada de decisões baseada em confiança. Nesse modelo ele considera a confiança básica, a geral e a situacional, sendo que em sua visão a situacional é a mais importante em situações de cooperação. A condição básica é que uma vez que a confiança situacional estiver acima de um determinado valor a cooperação acontecerá, sendo que no seu cálculo devem ser levados em consideração vários aspectos, como por exemplo, a importância e a utilidade.

2.2. REQUISITOS DE CONFIANÇA

Segundo Gambetta [26], a confiança pode ser quantificada com valores entre ZERO e UM, onde ZERO representa total desconfiança e UM a confiança cega e total em um outro indivíduo. A partir dessa afirmativa pode-se trabalhar com o pressuposto de que a confiança pode ser medida, e sendo assim poderão ser atribuídas requisitos de confiança e seus indicadores.

Para o contexto específico deste trabalho, os requisitos de confiança selecionados [47] estão incluídos no quadro 1.

Tabela 1 – Requisitos de Confiança [47]

Requisitos de Confiança	
Adequabilidade	Qualidade de ser adequável; capacidade de se ajustar, se acomodar, se amoldar.
Atraso	Ação ou efeito de atrasar; retardamento, afrouxamento.
Benevolência	Qualidade daquele que é benévolo; que quer bem; bem intencionado.
Capacidade	Qualidade de satisfazer a certo fim; idoneidade; habilitação; aptidão.
Capacitação	Tornar capaz; dar capacidade.
Conformidade	Qualidade do que é conforme ou de quem se conforma; analogia; identidade; semelhança.
Consistência	Estado ou qualidade de consistente; estado de uma coisa que promete durar ou não ter mudança; perseverança.
Criticidade	Forma de se tornar crítico; Relativo a, ou indicativo de um estado no qual alguma qualidade, propriedade ou fenômeno passam por uma alteração determinada ou drástica.
Disponibilidade	Qualidade daquele ou daquilo que é ou está disponível; coisa ou coisas disponíveis.
Freqüência	Ação de freqüentar; afluência, concorrência de gente; repetição com curtos intervalos de um ato ou sucesso.
Inconsistência	Qualidade de inconsistente; falta de consistência; falta de base.

Inoperabilidade	Sem possibilitar a faculdade de ser operado.
Qualidade	Atributo, condição natural, propriedade pela qual algo ou alguém se individualiza, distinguindo-se dos demais; maneira de ser, essência, natureza; excelência, virtude, talento.
Redundância	Qualidade de redundante; superfluidade de palavras; pleonasmo; superabundância. R. de estilo: abuso de ornatos no discurso.
Reputação	Ato ou efeito de reputar; fama, renome; conceito em que uma pessoa é tida; bom ou mau nome: Ter boa reputação.
Rotatividade	Qualidade de rotativo; alternância.
Satisfação	Ato ou efeito de satisfazer ou de satisfazer-se; qualidade ou estado de satisfeito; contentamento, prazer.
Sustentabilidade	Qualidade de sustentável; que pode ser sustentado.
Vulnerabilidade	Caráter ou qualidade de vulnerável; que se pode vulnerar; diz-se do lado fraco de um assunto ou questão, e do ponto por onde alguém pode ser atacado ou ofendido.

2.3. APLICAÇÕES DA CONFIANÇA

Com base nos parâmetros conhecidos de obtenção e manutenção da confiança, surgiram modelos para o seu gerenciamento, que buscam a obtenção da garantia da consistência de informações necessárias às varias formas de atividades. Abaixo serão descritos alguns desses modelos.

2.3.1. O Modelo *HTrust*

O *HTrust*, definido por Capra [13], é um modelo de gerenciamento da confiança humana e um *framework* que facilita a obtenção da confiança em sistemas e aplicações móveis. Em particular proporciona a formação e a disseminação da confiança em rede, e a derivação de novos relacionamentos formados a partir desses (evolução da confiança). O *framework* considera cada agente móvel como auto-ajustável, com um portfólio de credenciais utilizadas para provar a outros agentes a sua confiabilidade em um ambiente móvel *ad-hoc*. No que se refere à estrutura de gerência de confiança, o *HTrust* disponibiliza funções customizadas para prospecção do nível de confiança dos usuários.

Para descrever este modelo de confiança considera-se que o mesmo tem uma abordagem dinâmica, o que possibilita decrementar ou incrementar o grau de confiança de um agente em relação a outro, sem realizar consultas ao mesmo.

O modelo aborda os contextos social e transacional. Sendo auto-ajustável, utiliza a troca de informações de confiança, em contexto social, sobre agentes que estão interligados em uma rede composta de usuários. O contexto transacional é a rede composta por produtores e consumidores que tem a necessidade de interagir por meio de serviços, utilizando as informações de confiança do contexto social para formar, disseminar e evoluir a confiança de agentes da rede. A autenticação das informações de confiança de um agente pode ser feita por meio de criptografia de chave pública onde cada agente possui o seu par de chaves pública e privada.

O modelo é composto por disseminação da confiança, formação da confiança e evolução da confiança, onde um agente A que dá o voto de confiança a um outro agente B é chamado de *Trustor*, e o agente B recebe o nome de *Trustee*.

A obtenção de informações de confiança por agentes pode ser feita por experiências diretas ou por recomendações.

As experiências diretas ocorrem quando há uma interação entre os agentes colaboradores. Durante esse relacionamento o modelo *framework* coleta o histórico das interações, que é armazenado no ambiente local dos agentes, de forma que qualquer A

que pretenda interagir com B possa verificar antecipadamente o histórico de interações de B.

As recomendações são indicações feitas por agentes que já tiveram uma interação. Essas recomendações são fornecidas por agentes que pertencem ao contexto social e dessa forma o componente de disseminação de confiança do modelo realiza a publicação com o propósito de difundir a confiança deste agente no contexto social. A partir de então, a informação de confiança é utilizada pelo componente de formação de confiança que irá predizer a credibilidade do agente B (*Trustee*). Assim sendo, considerando que ocorra uma interação entre os agentes A e B, é necessário que A obtenha um *feedback* para assim inferir a credibilidade de B percebida por A. Isso será utilizado como um dado de entrada para o componente de evolução de confiança, que por sua vez, terá como objetivo atualizar as informações de confiança armazenadas no ambiente local do agente A.

2.3.2. O Modelo para Confiança em Redes Dinâmicas

Este modelo de confiança proposto por Carbone *et al* [12], tem por base a Computação Global (CG), derivada da ciência da computação e da tecnologia da computação. O Sistema de Computação Global é composto por entidades que são autônomas, descentralizadas, móveis, dinamicamente configuráveis, e capazes de operar com informações parciais. Tais sistemas, como por exemplo, a Internet, ficam com facilidade muito complexos, e apresentam necessidade de garantir a segurança da propriedade.

Este modelo formaliza a confiança baseando-se em definições das ciências humanas. Sua proposta é transferir um modelo semelhante ao modelo de confiança humana para o cenário computacional, ao elaborar seu sistema baseado em confiança.

O trabalho de McKnight e Chervany [44], utilizado neste modelo, apresenta uma classificação de confiança oriunda da sociologia, psicologia, administração, economia, e ciências políticas. Assim sendo a confiança é classificada em seis categorias:

1) Disposição - quando uma entidade *A* tem inclinação a confiar em *B*;

2) Situação - quando *A* tem confiança em *B*, apenas quando se encontra em um determinado cenário;

3) Estrutura - quando *A* confia em *B* impessoalmente por causa da estrutura de *B*;

4) Convicção - quando *A* acredita que *B* é fidedigno;

5) Intenção – quando *A* está disposto a se sujeitar a *B*;

6) Comportamento - quando *A* voluntariamente se sujeita a *B*.

O modelo permite a classificação por categoria com relação à confiança da entidade *Trustee* que é dada por: competência, benevolência, integridade e possibilidade de atribuição.

De acordo com Carbone e Sassone [24], com um bom modelo matemático e por meio de estruturas complexas, é possível representar combinações de tipos de confiança para o cenário da computação global.

De acordo com Santos [57], "o sistema de gerenciamento da confiança é composto de: mecanismo de confiança e mecanismo de risco que juntos fazem parte do principal. O mecanismo de confiança é o responsável por atualizar informações de confiança obtidas por meio de observações diretas ou indiretas (evidências também são consideradas neste modelo) e fornecer informações de confiança como entrada para o mecanismo de risco o qual dará um *feedback*, com informações para os procedimentos do principal como, por exemplo, à atualização da entrada para mecanismo de confiança."

Os aspectos principais deste modelo são: a formação, evolução e propagação da confiança.

O *framework* utiliza a função *GTrust* para associar a cada Principal B um grau de confiança que um outro Principal tem nele.

A função *GTrust* representa o menor ponto fixo do arranjo universal de políticas locais, a teoria do ponto fixo, abaixo descrita, é utilizada para desenvolver a teoria de políticas de segurança.

Para f : A → A, a ε A é dito Ponto Fixo de f se f(a) = a.

a é o menor ponto fixo de f se para todo a'ε A, tal que f(a') = a', temos a → a'.

Assim a função *GTrust* tem a seguinte representação:

GTrust : Principal → Principal → *TrustDegree*

A função *GTrust*(A) associa a cada principal B o grau de confiança que A tem em B. Desta forma uma direção é tomada para o modelo de política local.

TrustPolicy : *GTrust* → Principal → *TrustDegree*

A função *TrustPolicy* tem como objetivo dar uma estrutura de confiança que deve ser seguida, esta estrutura também é definida por meio da teoria de ponto fixo.

Como os domínios destas funções são completos e parcialmente ordenados, o grau de confiança utiliza relações de ordem possibilitando a aplicação da Teoria de Ponto Fixo de acordo com *TrustDegree*. Santos [57] estabelece os seguintes cenários:

a) Um principal *A* pergunta a *B* informações sobre *C*. Uma das grandes preocupações desse modelo é não confundir confiança com o conhecimento sobre um principal, pois isto pode fazer com que *B* demore um pouco mais a responder e assim faça com que *A* tome uma decisão errada, fazendo com que o ponto fixo evolua o grau de confiança que *A* tem em *C* para o grau mais baixo.

b) Outro possível cenário é que *B* pode estar temporariamente *offline* ou ainda não está pronto para falar com *A*. Em função disto são mantidas duas estruturas de ordem para os valores de confiança, são eles a ordenação da confiança e a ordenação da informação.

O grau de credibilidade é representado da seguinte forma: o menor elemento representa desconfiança absoluta e o maior elemento representa confiança absoluta. O grau de conhecimento é representado da mesma forma, onde dado um intervalo o menor elemento representa desconhecimento e o maior elemento representa conhecimento total sobre um principal.

Neste modelo, o campo da teoria da ordenação é fortemente utilizado para calcular a função de confiança global e a ordenação de informação, utiliza um *framework* que possibilita a construção da estrutura de confiança, por meio da construção de intervalos, preservando a noção natural da incerteza.

2.3.3. O Modelo de Confiança para *e-business*

Ao propor um modelo para o tratamento de confiança sobre transações de *e-business*, Pillatt [50] considera que a medição da confiança sobre essas transações começa a se tornar imprescindível, visto o papel que o *e-business* tem assumido com relação ao volume de negócios no cenário mundial, bem como o grande crescimento de usuários da Internet, os quais se tornam potenciais clientes e/ou empreendedores de soluções de *e-business*.

Na consideração do modelo são estabelecidas questões a serem respondidas para que o *e-business* possa prosperar com segurança por seus participantes. Essas questões são as seguintes:

1) "Você confia suficientemente na Internet para enviar eletronicamente as economias de sua vida ao seu parceiro comercial?",

2) "Quanto você está disposto a arriscar?",

3) "Você está seguro da identidade da pessoa ou empresa que está no outro lado da linha?",

4) "Você está certo de que receberá o produto e/ou serviço solicitado e na data combinada?",

5) “Você está certo que será recompensado pelo produto e/ou serviço fornecido?”,

6) “Você realmente acredita que as informações confidenciais envolvidas na transação serão mantidas em segurança?”.

Além disso, o *e-business* atua de forma distinta de um ambiente presencial. No presencial a integridade, a honestidade e a sinceridade dos participantes da negociação são avaliadas, e no *e-business* se requer uma visão mais complexa do que as simplistas visões de um ambiente *off-line*, para as especificações de métricas e modelos.

O surgimento de novas demandas com relação à confiança, bem como a indefinição com relação ao seu atual conceito, uma lista de requisitos genéricos de confiança pode ser de fundamental importância na especificação de um sistema de *e-business* coerente com a nova realidade do ambiente de negócios.

Os requisitos genéricos de confiança para um sistema de *e-business* são:

a) Privacidade de informações confidenciais, notadamamente aquelas relacionadas com produto, cliente, pagamento e negociação. As entidades transacionais devem ter acesso apenas às informações que lhes dizem respeito.

b) Integridade de informações críticas: Deve-se estar seguro que toda informação cuja integridade é fundamental para o correto desfecho da negociação não foi danificada ou deformada durante a transmissão.

c) Disponibilidade de informações críticas: Informações tais como características do produto ou serviço disponibilizado, devem estar acessíveis a quem delas necessitar dentro de um período de tempo aceitável.

d) Identificação de objetos digitais facilitando, desta forma, a verificação do caminho percorrido pelos mesmos e a prevenção contra cópias não autorizadas.

e) Prevenção contra cópias ou uso de informações críticas sem a devida autorização. Organizações fornecedoras de mercadorias digitais, tais como música e vídeos, por exemplo, preocupam-se com a disponibilização das mesmas, apenas àqueles que realmente pagaram.

f) Possibilidade de reaver o caminho percorrido pelos objetos digitais permitindo, desta forma, a criação de *logs* que serão úteis para evitar o repúdio.

g) Verificação da qualidade das mercadorias digitais: A qualidade da mercadoria digital deve ajustar-se ao acordado entre as entidades transacionais envolvidas na negociação.

h) Gerenciamento de riscos: Os participantes de uma negociação necessitam identificar prováveis ameaças, tais como mudança drástica e repentina de perfil por parte de uma entidade transacional participante da negociação, o que pode indicar a não veracidade das credenciais.

i) Autenticação de informações de pagamento: O vendedor/fornecedor necessita estar seguro de que as informações referentes ao pagamento disponibilizadas pelo cliente, ou até mesmo por outro vendedor, são genuínas.

À medida que se almeja atender aos requisitos de confiança acima listados, torna-se necessária a especificação de um modelo de confiança que seja capaz de avaliar os três principais componentes de um sistema de *e-business* – entidades transacionais, infra-estrutura e informação – e, com base nesta avaliação, mensurar a confiabilidade da ação que está sendo desempenhada envolvendo algum propósito.

Com a ajuda do modelo de confiança as ações, ou seja, operações tais como compra e venda de mercadorias e/ou serviços, troca de informações ou utilização de parte da infra-estrutura, podem ser divididas dentro de duas categorias: autorizadas e não autorizadas. A classificação da ação dentro destas categorias irá depender do grau de confiabilidade a ela atribuído pelo modelo de confiança.

2.3.4. O Modelo para o Gerenciamento de Confiança em Serviços Móveis

O Modelo para o Gerenciamento de Confiança em Serviços Móveis, proposto por Santos [57] tem como foco principal as redes *Wireless* 802:11. Foi estabelecido que o grande mercado para os serviços móveis deverá ser mais eficiente com redes de grande alcance como *WiMax,* onde provavelmente a grande procura por serviços de gerenciamento de confiança ocorrerá, já que o grau de confiança pode ser um ponto decisivo para muitas pessoas na hora de decidir onde almoçar, ou qual serviço de mecânica chamar. Desta forma, um modelo de gerenciamento de confiança pode ser um divisor de águas que decidirá quem vencerá uma concorrência.

Focalizando as redes de pequeno alcance (*Wireless* 802.11) delineia-se um forte mercado para aplicação de um sistema de gerenciamento de confiança, como por exemplo, num campus universitário, onde existem muitos serviços prestados à comunidade acadêmica. Esses serviços poderão ser prestados a pessoas munidas de dispositivos móveis (com cartão para acesso a redes *Wireless*), para acessar os mesmos em campus com essa cobertura. Nesse contexto, o grau de confiança funciona como uma indicação, já que o grau de confiança é dado por clientes e, inevitavelmente, está interligado à qualidade dos serviços prestados, e a competência da pessoa que se propõem a prestar os serviços.

O Modelo para Gerenciamento de Confiança em Serviços Móveis foi pensado para redes *Wireless* estruturadas, sendo assim o modelo centralizado vem em primeira opção, sendo acessível a um número maior de pessoas. A mobilidade deste modelo não será afetada, pois o objetivo é gerenciar a reputação de serviços dentro de uma área coberta com essas redes.

A formação de confiança de maneira simples e objetiva será feita por meio de questionários que devem ser respondidos, ou seja, devem ser atribuídos valores dentro de um determinado intervalo. O modelo solicita a todas as pessoas que já utilizaram serviços que tenham um sistema para o gerenciamento de confiança, que avaliem os mesmos fornecendo valores "inteiros positivos” dentro do intervalo [0,10].

O questionário aborda os seguintes questionamentos:

1. Há um domínio daquilo que se pretende fazer, por parte do prestador de serviços?

2. A qualidade do serviço prestado é condizente com o custo benefício?

3. O tempo de espera e/ou pontualidade é satisfatório?

Após o preenchimento dos questionários será definido em qual intervalo se encontra a confiança de um serviço. Os intervalos são os seguintes:

Confiança Baixa - [0, 4];

Confiança Média - [5, 6];

Confiança Alta - [7, 10];

Para obter a confiança inicial de um serviço será necessário que um usuário X atribua valores de confiança que ele tem em um serviço Y, seguindo os itens citados acima. Feito isso, o componente "definir confiança" irá calcular por meio de média ponderada o valor da confiança que X tem em relação ao serviço prestado por Y.

Para execução do cálculo, o componente definir confiança estabelece pesos para cada pergunta do questionário, atribuindo o peso 5 para a primeira questão, 4 para a segunda e 1 para a terceira.

Os pesos e os valores serão definidos por:

$$Pesos = \sum f_i \text{ e } valores = \sum x_i$$

Desta forma para obtermos o nível de confiança inicial basta utilizar a função abaixo.

$$\delta = \frac{\Sigma x_i f_i}{\Sigma f_i}$$

Este valor será armazenado num banco de dados e caso um outro usuário K interaja com o serviço Y, será feito o mesmo cálculo descrito anteriormente para obtermos a confiança que K tem em relação ao serviço Y. Porém é necessário definir uma nova confiança "geral", ou seja, uma confiança gerada com base na confiança que X teve em Y e que K teve em Y e assim sucessivamente. Para inferir este tipo de confiança o componente "definir confiança" definirá uma média entre os respectivos valores de confiança.

O sistema também utiliza pesos que variam de [0, 1], a fim de valorizar as opiniões mais recentes dos usuários em relação aos serviços prestados, conforme a representação abaixo.

$$\gamma_j \varepsilon [0,1]$$

Todos os graus de confiança, dados no instante em que será calculando o grau de confiança geral, terão sempre peso 1 e serão chamados de Y. Os graus de confiança σ serão chamados de σ' se são recentes e σ'' se são graus já armazenados.

O grau de confiança geral é calculado da seguinte forma:

$$\delta = \frac{\Sigma^{n}_{i=1} \gamma'_i \sigma'_i + \Sigma^{n}_{j=1} \gamma''_i \sigma_j}{\Sigma^{n}_{i=1} i + \Sigma^{m}_{j=1} 1\ \gamma_j}$$

Onde para qualquer γi σj temos γj ε [0,1] e γi=1

A disseminação do nível de confiança, uma parte importante do modelo, é feita por meio de mensagens enviadas pelo próprio local que presta o serviço.

Como exemplo considera-se o seguinte cenário: uma pessoa, sem conhecimento dos serviços está transitando por uma área com cobertura *Wireless*. Ela recebe mensagens dos locais que prestam serviços, que a detectam por meio de um sensor de presença. Para melhor qualidade o cliente detectado poderia receber além das informações dos serviços,

o grau de confiança geral dos mesmos, e as indicações de três a cinco usuários com os respectivos graus de confiança avaliados por eles.

Um ponto importante neste cenário de disseminação da confiança é a criação de uma rede de amizade entre os usuários em função dos serviços, criando a possibilidade de tomar conhecimento do grau de confiança atribuído por outras pessoas em relação a serviços desconhecidos por um usuário.

O intervalo de confiança da área de cobertura em questão é disseminado por meio de mensagens expedidas em relação aos serviços disponíveis.

A função decorrente é expressa da seguinte forma:

$$\delta\ (ser) \in [0,10], \text{ onde } ser \in \varphi$$

O conjunto φ representa o conjunto de serviços disponíveis em uma área coberta por redes *Wireless*.

Cada usuário poderá ter uma rede de amigos para recomendação de algum serviço de seu interesse, da seguinte forma:

Se um usuário A tem como amigo para serviços de *xerox* o usuário B, ele A pode fazer uma requisição ao usuário B sobre bons serviços de *xerox*, ou até mesmo o usuário B (sem receber requisições) pode recomendar ao usuário A os melhores serviços no campus.

Este serviço pode ter implementado um modelo de chave publica e privada para verificar a identidade do usuário requisitante e do usuário recomendador.

$$\Psi rec(keyA) \rightarrow B$$

A função Ψrec(keyA) faz a requisição a B para que ele envie sugestões de bons serviços. O usuário B retorna uma função de recomendação descrita por:

$$\xi \sigma B(keyB) \rightarrow A$$

Esta função indica os serviços com o maior nível de confiança, na opinião de B.

Neste modelo a evolução (acréscimo ou decréscimo) da confiança se dá principalmente em função dos pesos atribuídos às questões que irão definir o grau de confiança de um serviço. O principal problema é que pessoas podem atribuir valores a fim de diminuir o grau de confiança de um determinado serviço ou atribuir valores com o objetivo de aumentar o grau de confiança de um serviço. Estes usuários são chamados de agentes maliciosos, e a detecção destes agentes é uma das maiores dificuldades e sem essa detecção não é possível manter a qualidade do serviço de confiança.

O modelo proposto aposta em estratégias simples para detectar agentes maliciosos, como a utilização de *logs* para que possam ser feitas comparações entre as avaliações armazenadas. Desta forma, é possível verificar se uma pessoa está dando um grau de confiança muito acima do que a maioria das pessoas ou muito abaixo, e a partir daí já é possível observar os agentes maliciosos em potencial. Certamente por meio de pesquisas de campo e estudos estatísticos (em função do serviço prestado) é possível determinar o tempo de observação de um agente malicioso em potencial, e então após este instante todo o grau de confiança atribuído pelo agente malicioso será desconsiderado da média.

Outra técnica utilizada na tentativa de evitar agentes maliciosos é utilizar uma função de troca de pesos. Desta forma, as questões utilizadas para definir o grau de confiança nunca terão um peso fixo e assim se um agente a cada hora está com uma identificação (o que certamente dificulta o uso da técnica anterior) e se ele costumeiramente atribui o valor máximo na primeira questão, daqui a algum tempo este valor terá um peso mais baixo em função da rotação de pesos.

Assim sendo, o modelo se propõe a gerenciar a confiança que uma pessoa tem em relação a um serviço oferecido. A utilização deste modelo também incentiva o aumento da qualidade dos serviços prestados por aumentar a competitividade.

2.4. TRABALHOS SOBRE CONFIANÇA

Apesar de a confiança ter sido estudada durante décadas em disciplinas variadas, atualmente pode-se considerar que passou a existir um maior interesse na análise do seu significado e da sua aplicação por métodos teóricos empíricos. O desenvolvimento tecnológico associado à globalização criou necessidades de interação de pessoas e organizações afastadas geograficamente, o que acrescentou às relações formais e presenciais um componente diversificado no sentido de confiabilidade. Esse contexto proporcionou um acréscimo em pesquisas e estudos acerca do tema, sendo alguns deles relacionados na tabela 2:

Tabela 2 - Relação de Trabalhos sobre Confiança

Autor	**Título do Trabalho**	**Abordagem**	**Contexto**
Huotari Iivonen [34]	*Managing Knowledge-Based Organizations Through Trust*	Conceito de confiança em geral e no contexto de Gestão do Conhecimento	Organizacional
Iivonen [35]	*Trust Building as a Management Strategy*	Confiança como estratégia de administração	Organizacional
Harisalo Stenvall [30]	*Trust as Capital: The Foundation of Management*	Framework de confiança no comportamento organizacional	Organizacional
Sonnenwald [59]	*Managing Cognitive and Affective Trust in the Conceptual R&D Organization*	Administração de confiança cognitiva e afetiva em uma organização on-line	Redes e Comunidades Online
Davenport McLaughlin [17]	*Interpersonal Trust in Online Partnerships: The Challenge of Representation*	Confiança interpessoal e confiança em sociedades on-line	Redes e Comunidades Online
Öörni, Kaleva, [49]	*Usability of Websites Contributing to Trust in E-commerce*	Confiança no comércio eletrônico	Individual e Organizacional
Harisalo Stenvall [31]	*Citizens' Trust in Ministries*	Confiança na administração pública	Individual e Organizacional
Blomqvist Ståhle [9]	*Trust in Technology Partnerships*	Confiança no contexto da formação do relacionamento tecnológico	Redes e Comunidades Online

Mandelli [43]	*Exploring the Origins of New Transaction Costs in Connected Societies*	Papel da confiança na administração moderna e nos custos de transação em sociedades on-line	Economia Global e sociedade
Mandelli [42]	*Self-Organization and New Hierarchies in Complex Evolutionary Value Networks*	Confiança organizacional e modelo teórico de redes de cognitivas de valor	Economia Global e sociedade
Falcone [23]	*A Belief-Based Model of Trust*	Análise sócio-cognitiva de confiança em nível de sistema	Sistemas de Informação
Dias [19]	Confiança no Documento Eletrônico	Requisitos de segurança de documentos em papel eletrônico	Sistemas de Informação

Como se verifica a confiança é abordada em variados contextos, dentre eles o contexto organizacional onde já foram apresentados estudos que aprofundaram a pesquisa da aplicação da confiança em aspectos referentes ao planejamento estratégico e comportamento organizacional, praticamente inexistindo abordagens em aspectos de sua aplicação na governança de TI, assunto proposto na presente pesquisa.

Assim sendo, no que se refere ao contexto organizacional contribuíram para a pesquisa os trabalhos de Huotari e Iivonen [34], Iivonen [35], Harisalo e Stenvall [30], Öörni e Kaleva, [49], Harisalo e Stenvall [31]. Da mesma forma por tratarem de sistemas de informação contribuíram os trabalhos de Falcone [23] e Dias [19].

3. GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

De Haes e Van Grembergen [18] pesquisaram que na literatura acadêmica e profissional, os artigos que mencionam em seu título a governança, começaram a surgir em 1999, com o artigo de Sambamurthy e Smud [28], "Arranjos para a Governança de Tecnologia da Informação: Uma Teoria de Contingências Múltiplas", e em 2000 com o artigo "*The Balanced Scorecard and IT Governance*" de Van Grembergen [60]. Assim concluíram que o conceito de governança emergiu há poucos anos, o que não quer dizer que os muitos dos elementos subjacentes da discussão estratégica do alinhamento da TI com o negócio, tema central da governança, não atraíssem a atenção há mais tempo.

Ainda esses autores enfatizaram que, mesmo com o avanço do conhecimento, é comum encontrar organizações onde a TI se insere como uma atividade estanque, implementando seus processos e controlando a si mesma, caminhando paralelamente, sem convergência com a governança organizacional. Tal procedimento pouco contribui para a geração de valor na organização e por outro lado, quase sempre, leva a uma falta de sintonia e ajuste entre a atividade-fim e a plataforma tecnológica que tem por finalidade proporcionar uma base sólida para a habilitação de excelente desempenho estratégico.

Nesta conjuntura proliferam ações limitadas pouco controladas, onde a tática supera a estratégia, em ambientes onde os processos e as responsabilidades não se apresentam com a desejável definição. Com a desculpa da fluidez do mundo competitivo e da urgência do negócio, como resultados colhem-se clientes insatisfeitos, produtos de pouca qualidade, impactos na imagem organizacional e a inevitável perda de receita.

Os mesmos estudos, em contrapartida, levantam que organizações com uma governança de TI ajustadas ao negócio, com foco no tratamento adequado da informação, têm suas ações facilitadas no intuito de aproveitar as oportunidades e correm menos riscos diante das ameaças potenciais.

3.1. ALINHAMENTO DA TI COM A ESTRATÉGIA DE NEGÓCIOS

O alinhamento estratégico entre o negócio e a TI é definido por Duffy [22] como o processo e o objetivo de conseguir vantagem competitiva desenvolvendo e sustentando um relacionamento simbiótico entre o negócio e a TI. A idéia do alinhamento estratégico é facilmente compreendida, mas as organizações não alcançam este objetivo com facilidade. Para auxiliá-las Henderson e Venkatraman [32] desenvolveram um modelo de alinhamento estratégico para conceituar e dirigir a gerência estratégica da TI (Figura 1). Estes autores foram os primeiros a descrever de uma maneira clara o inter-relacionamento entre as estratégias de negócio e de TI, criando o Modelo Estratégico de Alinhamento, (*Strategic Alignment Model*, *SAM)*, descrito por Smaczny [56]. Muitos autores usaram este modelo em pesquisas mais aprofundadas, dentre eles, Luftman e Brier [38], Burn e Szeto [10] e Smaczny [58].

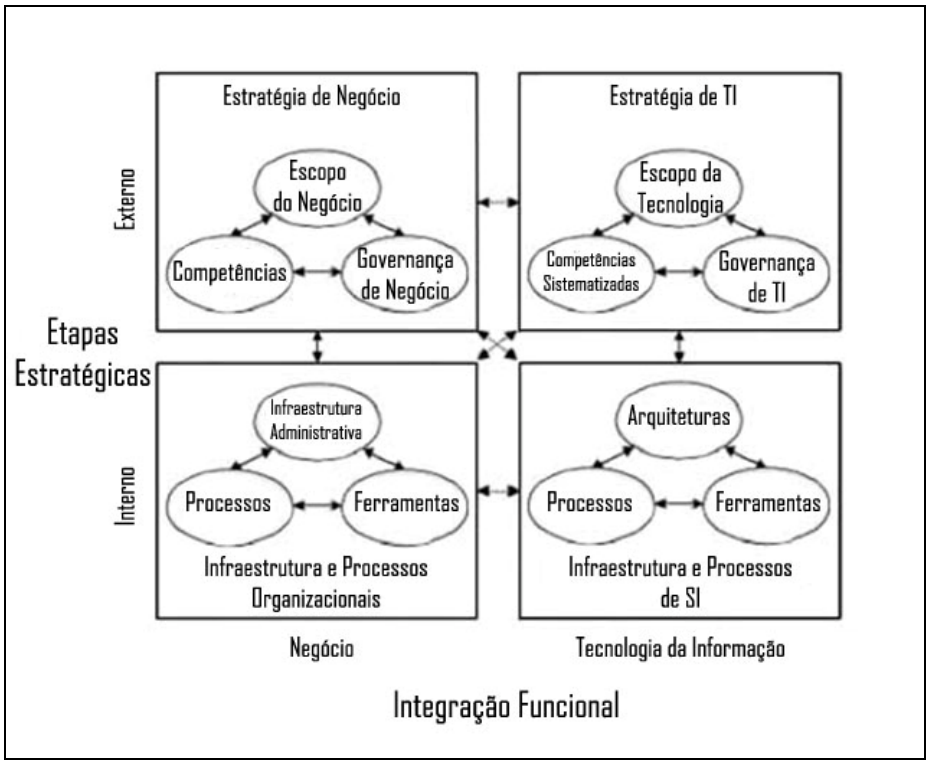


Figura 1 - Modelo Estratégico de Alinhamento

No que se refere à contribuição que uma governança deve proporcionar à manutenção de um alinhamento estratégico e eficaz, Webb [62], apud Sambamurthy e Smud [28], definem três modalidades preliminares de governança de TI: centralizada, descentralizada, e federativa. A adoção de uma modalidade centralizada é indicada quando a decisão está delimitada a pequena quantidade de funções com capacidade para tal. Uma modalidade descentralizada tem reflexo em um número maior de configurações, mas descentraliza o poder e dificulta o alinhamento; é típica da organização divisional e/ou de gerentes de linha. Já a modalidade federativa e suas várias configurações se relacionam com os aspectos da decisão, balanceando entre a alta gerência e a estrutura divisional e/ou de gerência de linha.

Weill e Ross [63] expandiram estes conceitos e estabeleceram uma combinação de cinco decisões necessárias, que inter-relacionadas com seis possibilidades de quem deve ter a atribuição de decidir, constituem uma matriz de arranjos ajustada à atividade de cada empresa. São cinco as decisões-chave:

a) Princípios de TI, que esclarecem o papel de negócio de TI;

b) Arquitetura de TI, que define os requisitos de integração e padronização;

c) Infraestrutura de TI, que determina os serviços compartilhados e de suporte;

d) Necessidade de aplicações de negócio, que especifica a necessidade comercial de aplicações de TI, comprada ou desenvolvida internamente; e

e) Investimentos e priorização de TI, que priorizam quais iniciativas financiar e quanto gastar.

Os direitos decisórios são listados em seis arquétipos, ou tipo de pessoa envolvida em tomar uma decisão de TI:

a) Monarquia de negócio, representada pelos altos gerentes;

b) Monarquia de TI, representada pelos especialistas em TI;

c) Feudalismo, onde cada unidade de negócio toma decisões independentes;

d) Federalismo, caracterizando uma combinação entre o centro corporativo e as unidades de negócio, com ou sem o envolvimento do pessoal de TI;

e) Duopólio de TI, com o envolvimento do grupo de TI e de algum outro grupo Tal como a alta gerência ou os líderes das unidades de negócio; e

f) Anarquia, onde as tomadas de decisão são individuais ou por pequenos grupos de modo isolado.

Esta matriz de arranjos, tabela 3, conforme Weill e Ross [63] organiza o processo decisório, mas para que o mesmo seja otimizado e monitorado, torna-se necessária a formulação e a implementação de mecanismos de governança, tais como processos formais, desenhos descritivos funcionais e estabelecimento de grupos ou comitês para assessoramento e apoio à decisão.

Tabela 3 - Matriz de Arranjos de TI

DECISÃO / ARQUÉTIPO	Princípios de TI	Arquitetura de TI	Estratégias de infra-estrutura de TI	Necessidades de aplicações de negócio	Investimentos em TI
Monarquia de negócio					
Monarquia de TI					
Feudalismo					
Federalismo					
Duopólio					
Anarquia					
Não se sabe					

3.1.1. Harmonia Decorrente das Governança de TI

Uma governança de TI deve buscar harmonizar as estratégias e organização da empresa com os arranjos de governança de TI, que por sua vez devem estar monitoradas por metas de desempenho de negócios conforme exemplificado por Weill e Ross [63] na Figura 2.

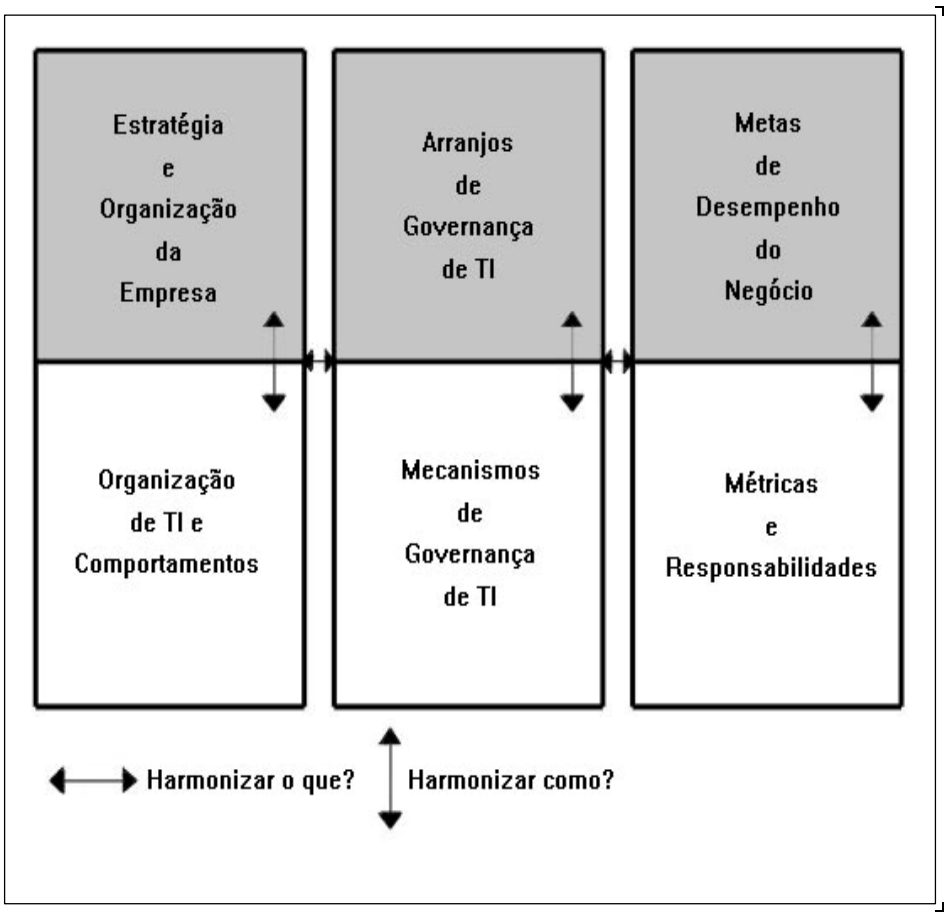


Figura 2 - Harmonização de Estratégias e Organização

A estratégia e a organização da empresa deverão ser estabelecidas e definidas por meio de diretrizes que estabeleçam uma organização de TI baseada em comportamentos desejáveis. Por exemplo, para uma empresa com uma estratégia de desenvolvimento de uma cultura do tipo uma firma – uma equipe poderá ser estabelecida a diretriz operacional de simplificar a sua arquitetura geral para facilitar o compartilhamento e a integração.

Os arranjos de governança de TI são implementados por meio de mecanismos que facilitem a continuidade harmônica do processo decisório. Um exemplo é estabelecer a participação do *Chief Information Officer (CIO)* no comitê executivo, bem como a participação de *CIOs* das unidades de negócio no comitê central de tecnologia.

As metas de desempenho do negócio nas unidades centralizadas devem ser traduzidas por métricas homogêneas, e em contrapartida, por métricas distintas para as unidades de negócio de empresas que buscam a agilidade e rapidez.

Em relação aos mecanismos de governança de TI, Weill e Ross [63] estabelecem que uma governança eficaz adota três tipos diferentes de mecanismos para implementar a Governança de TI:

a) Estruturas de tomadas de decisão

Unidades e papéis organizacionais responsáveis por tomar decisões de TI como comitês, equipes executivas e gerentes de relacionamento entre negócios e TI.

b) Processos de alinhamento

Processos formais para assegurar que os comportamentos cotidianos sejam consistentes com as políticas de TI e contribuam com as decisões. Incluem processos de avaliação e proposta de investimentos em TI, processo de tratamento de exceções de arquitetura, acordo de níveis de serviços – Service Level Agreement - SLA, cobrança reversa e métrica, acompanhamento de projetos e rastreamento formal do valor do negócio.

c) Abordagens de Comunicação

Comunicados, porta-vozes, canais e esforços de educação que disseminam os princípios e as políticas da governança de TI e os resultados dos processos decisórios em TI. Incluem comunicados da alta gerência, comitês formais, portais baseados na *Web*, escritório do CIO ou da governança de TI e trabalho com dissidentes.

Dentre os diagnósticos que poderão ser adotados, como exemplo, Araújo [1] sugere os seguintes passos:

a) Analisar o relacionamento de TI com a alta administração para verificar se, independentemente da estrutura existente, a TI tem uma visão clara das necessidades do negócio e a qual velocidade e agilidade deve atender.

b) Analisar os papéis e responsabilidades em TI, onde se enfatiza que inicialmente deve a organização desenhar os seus processos, verificando depois quem irá executar funções na cadeia decisória. Tal procedimento evita que uma segregação inadequada de funções possa comprometer os processos já em sua concepção.

c) Implementar um mapeamento de todos os processos existentes, de forma a ter bem claro o que necessita ser formalizado.

d) Analisar os processos existentes para eventuais propostas de modificações, tal como extinção, substituição ou modificação.

e) Levantar os riscos que possam comprometer o negócio, relacionando quais riscos poderão comprometer o funcionamento de cada processo e os impactos decorrentes.

f) Implementar um mapeamento dos controles existentes que mitigam os riscos identificados, verificando se os mesmos realmente suportam as necessidades dos processos e conseqüentemente do negócio.

Considerando o resultado do diagnóstico, e buscando um alinhamento organizacional com a visão estratégica e uma harmonização de procedimentos, que beneficiem a estrutura decisória, poderão ser adotados modelos e metodologias de desenvolvimento que visem o ajuste e a adequação da organização.

3.2. OS RISCOS

Atualmente existem muitas exigências de regulamentação e controle que indicam às empresas novos procedimentos para sua adequação a essa realidade. A conjuntura apresenta também inúmeras oportunidades de frustrar as expectativas de usuários e investidores, tornando evidente a importância do controle de risco, pois a sua falta poderá ocasionar uma quebra da confiança extremamente danosa para os negócios.

Existe todo um relacionamento entre o ambiente, as oportunidades e o risco, pois as empresas de porte atuam em um ambiente globalizado. O aumento do espectro de atuação ampliou as oportunidades mas tornou maior a complexidade dos relacionamentos, trazendo embutidos um potencial mais elevado da ocorrência de erros, ou seja, uma maior amplitude de risco.

Rodrigues [54] defende que o processo de Gestão de Riscos visa identificar previamente os eventos que possam trazer impactos para os resultados da organização, classificar estes eventos como risco ou oportunidade, formular estratégias e ações para minimizar os possíveis efeitos negativos e potencializar os positivos e diminuir, assim, a ocorrência de "surpresas".

Barton *et al* [8] estabelece que "o risco é a possibilidade de alguma coisa dar errado. Fatores de risco são as condições que dão origem a essa possibilidade. O risco é um resultado e não algo que se possa gerir ou controlar diretamente. Os fatores de risco, como as causas, sim. Ao gerir o risco, a maioria das empresas presta atenção ao resultado e não à causa, o que provoca erros". Assim sendo, a visão do gerenciamento de risco deve ser ampliada, tornando-se holística, de forma a monitorar os primórdios, o estabelecimento dos fatores que poderão proporcionar efeitos negativos para os negócios.

Como exemplo, ressalta-se que, para possibilitar essa visão ampliada, surgiram as técnicas de gestão holística do risco, designadas por *Enterprise Risk Management* (ERM*),* que quando aplicadas corretamente, têm se constituído em uma ferramenta de gestão poderosa. O ERM aborda os principais riscos da empresa num determinado nível,

tendo como característica ser variável, pela especificidade dos riscos inerentes a cada empresa abordada.

O ERM, também conhecido como COSO I [16], é composto por oito componentes inter-relacionados, cujas principais características são descritas pelo COSO em seu *Executive Summary*, sendo elas:

a) Ambiente de Controle: é a base de como o risco é percebido e tratado pelas pessoas envolvidas, considerando a filosofia de gestão de riscos e o apetite de risco (disposição de tolerar riscos), a integridade e os valores éticos, e o ambiente operacional.

b) Definição de Objetivos: o ERM garante que a Administração adotou um processo para definirem objetivos e que os objetivos selecionados suportam e estão alinhados à missão da instituição e são consistentes com o apetite de risco.

c) Identificação de Eventos: devem ser identificados todos os tipos de eventos, internos e externos, que podem afetar o alcance dos objetivos da instituição, devendo ser distinguidos os riscos das oportunidades.

d) Avaliação de Riscos: os riscos internos e externos à instituição são analisados, considerando a probabilidade e a severidade das ameaças, como bases para determinar os riscos relevantes e como estes devem ser gerenciados.

e) Tratamento dos Riscos: a Administração seleciona a opção adequada - evitar, aceitar, reduzir ou compartilhar riscos - desenvolvendo uma série de ações (controles) para alinhar os riscos com a tolerância e o apetite de risco.

f) Atividades de Controle: políticas e procedimentos são definidos e implementados para ajudar a garantir que o tratamento de risco foi corretamente realizado, de forma que os objetivos estratégicos possam ser alcançados.

g) Informação e Comunicação: as informações relevantes são identificadas, capturadas e comunicadas de forma oportuna e adequada, o que possibilita que as pessoas necessárias as recebam com o nível de conteúdo apropriado para que possam executar suas atividades.

h) Monitoração: monitorar em âmbito global e fazer as alterações quando necessárias. A monitoração é feita por atividades contínuas de gestão, por auditorias internas ou externas (periódicas ou especiais), ou por ambas.

Uma vez implementado, o ERM irá reduzir ou transferir riscos, sendo, porém, necessário avaliar sua eficácia em relação aos objetivos de controle e, devido às mudanças de estratégias organizacionais, se eles continuam efetivos ao longo do tempo.

Assim sendo, o ERM é uma abordagem sistemática segundo a qual os fatores de risco e os programas de atenuação são considerados em relação ao negócio como um todo, interna e externamente. É também pró-ativo, buscando controlar o risco, desde o início, por meio do monitoramento do comportamento organizacional, onde são balanceados com os controles institucionais, tais como as políticas e os procedimentos previamente estabelecidos.

Barton *et al* [8] ressaltam que "quando corretamente implantado, o ERM exige trabalho árduo e comprometido da alta gestão. Entretanto, para as empresas que praticam o ERM com eficácia, as recompensas podem ser: liderança de mercado, crescimento contínuo, subida dos preços das ações e confiança dos investidores".

3.3. COBIT

O *Control Objectives for Information and related Technology* (COBIT®*)* [15] é uma estrutura e conjunto de ferramentas de suporte que permite o preenchimento de lacunas no gerenciamento da TI com os respectivos requisitos de controle, questões técnicas e riscos de negócio e comunicar o nível de controle às partes interessadas. O COBIT possibilita o desenvolvimento de uma política clara e de boas práticas para controle de TI dentro das empresas. O COBIT é constantemente atualizado e harmonizado com outros padrões. Por essa razão, ele se tornou o integrador das melhores técnicas de TI e a estrutura guarda-chuva da governança de TI que auxilia no entendimento e gerenciamento dos riscos e benefícios associados com TI. A estrutura de processos do COBIT e sua abordagem avançada, orientada aos negócios de alto nível, dão uma visão que permeia a TI facilitando as tomadas de decisão.

3.4. ESTRUTURA DO COBIT

A estrutura completa do COBIT pode ser exibida graficamente como na figura 3, com o modelo de processo do COBIT, de quatro domínios, contendo trinta e quatro processos genéricos, gerenciando os recursos de TI para fornecer informação para o negócio conforme os requisitos de governança e negócios.

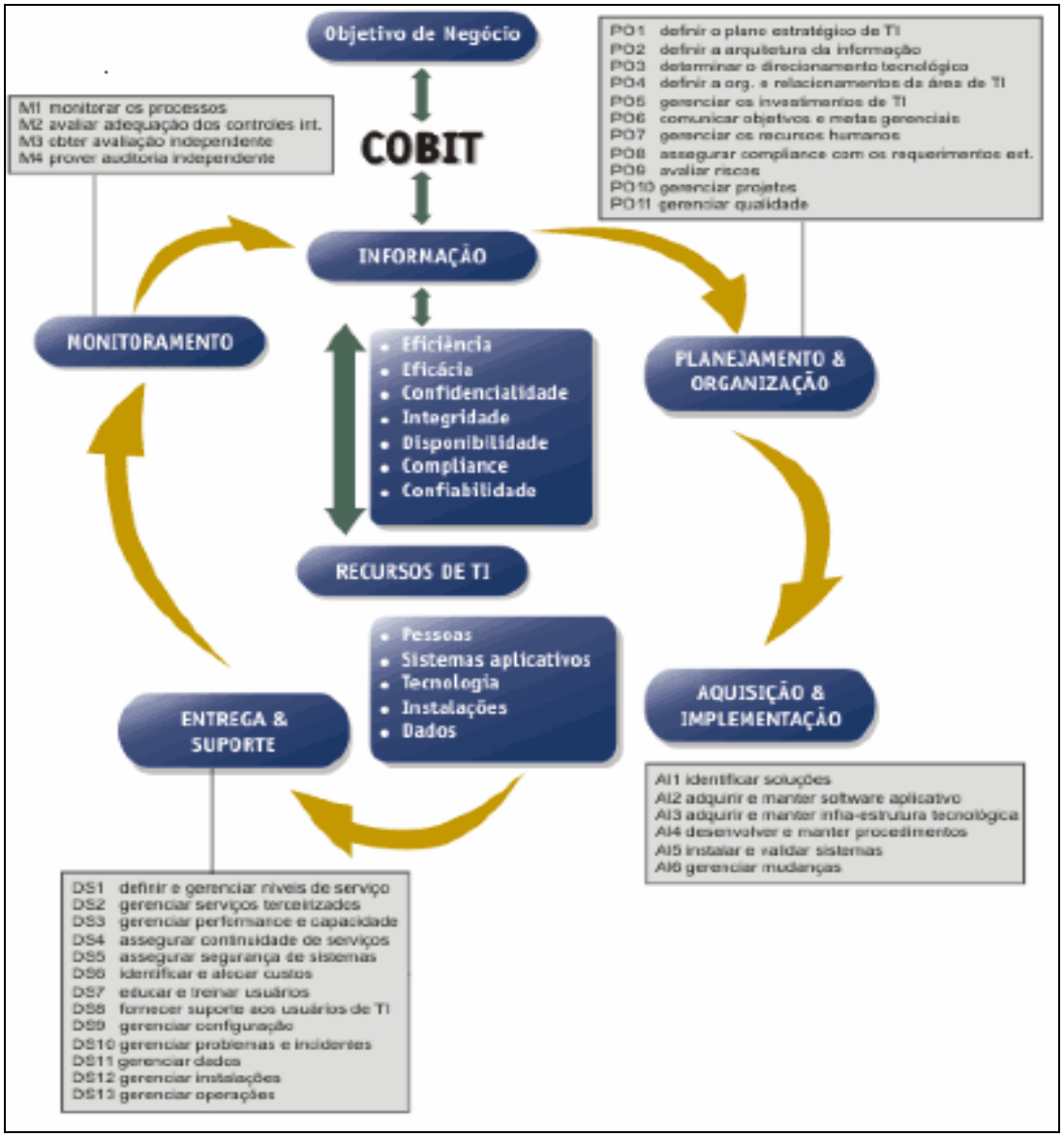


Figura 3 - Estrutura do COBIT

A estrutura do *COBIT* fornece um modelo de processos de TI, de referência e uma linguagem comum para que qualquer pessoa numa empresa possa compreender e gerenciar as atividades de TI. Incorporar um modelo operacional e uma linguagem comum para todas as partes do negócio envolvidas em TI é um dos mais importantes e iniciais passos para a boa governança. Ele também fornece uma estrutura para medir e monitorar o desempenho de TI, comunicando com os provedores de serviços e integrando as melhores práticas de gerenciamento. Um modelo de processo que favorece a atribuição de propriedade do processo, permitindo que responsabilidades e autoridade sejam definidas.

Para governar TI efetivamente, é importante considerar as atividades e riscos dentro de TI que precisam ser gerenciados. Isto pode ser resumido com os seguintes domínios:

a) PLANEJAR E ORGANIZAR (PO)

Este domínio compreende estratégias e táticas e se preocupa com a identificação da forma que TI pode melhor contribuir com a realização dos objetivos de negócio. Além disso, a realização da visão estratégica precisa ser planejada, comunicada e gerenciada para diferentes perspectivas. Finalmente, uma organização apropriada bem como infra-estrutura tecnológica deve ser posicionada. Este domínio normalmente conduz às seguintes questões de gerenciamento:

- As estratégias de TI e de negócio estão alinhadas?
- A empresa está conseguindo um ótimo uso de seus recursos?
- Todas as pessoas na organização entendem os objetivos de TI?
- Os riscos da TI estão sendo compreendidos e gerenciados?
- A qualidade dos sistemas de TI está apropriada para as necessidades do negócio?

b) ADQUIRIR E IMPLEMENTAR (AI)

Para perceber a estratégia de TI, as soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, bem como implementadas e integradas nos processos do negócio. Além disso, mudanças e manutenção de sistemas existentes devem ser cobertas por esses domínios para certificar-se de que as soluções continuam atendendo aos objetivos do negócio. Este domínio normalmente conduz às seguintes questões de gerenciamento:

- Os novos projetos são adequados para fornecer soluções que atendam as necessidades do negócio?
- Os novos projetos estão aptos a serem entregues no prazo e dentro do orçamento?
- Os novos sistemas funcionarão adequadamente quando implementados?
- As mudanças serão realizadas sem perturbar as operações de negócio correntes?

c) ENTREGAR E DAR SUPORTE (DS)

Este domínio está relacionado com o fornecimento atual de serviços requeridos, os quais incluem fornecimento de serviços, gerenciamento de segurança e continuidade, suporte técnico para usuários, gerenciamento de dados e de instalações operacionais. Ele normalmente conduz às seguintes questões de gerenciamento:

- Os serviços de TI estão sendo fornecidos em alinhamento com as prioridades do negócio?
- Os custos de TI estão otimizados?
- A força de trabalho (os empregados) está capacitada a utilizar os sistemas de TI de forma produtiva e segura?
- A confidencialidade, integridade e disponibilidade estão adequadamente posicionadas?

d) MONITORAR E AVALIAR (ME)

Este domínio trata do gerenciamento de desempenho, monitoração do controle interno, conformidade regulatória e provimento de governança já que todos os processos de TI precisam ser regularmente avaliados com o passar do tempo para assegurar sua qualidade e conformidade com os requisitos de controle. Ele normalmente conduz às seguintes questões de gerenciamento:

- O desempenho de TI é medido a fim de detectar problemas antes que seja tarde?
- O gerenciamento assegura que os controles internos são efetivos e eficientes?
- O desempenho de TI pode ser ligado às metas de negócio?
- Risco, controle, conformidade e desempenho são medidos e relatados?

3.5. CONFIANÇA E A GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

O estudo da confiança confirma que a mesma está diretamente relacionada com os níveis de desenvolvimento das sociedades, que se apresenta de forma mais evoluída de acordo com a confiabilidade dos relacionamentos dos indivíduos entre si e desses com as organizações. Robinson e Jackson [53] ressaltam que a confiança relaciona-se com a fé nas pessoas, que está provavelmente ligada ao fato de que alguém manterá sua palavra, ou seja, existe um envolvimento de risco pois essa palavra poderá não ser mantida.

Bacharach e Gambetta [7] afirmam que existem sinais que os indivíduos usam para interpretar a confiabilidade dos outros e, além disso, a repetição ou a ausência desses sinais poderão, por sua incidência, proporcionar respostas matemáticas, ou seja, proporcionar medições. Dessa forma verifica-se que a confiança envolve risco e pode ser medida. Couch *et al* [14] acrescentam que existem pelo menos duas escalas diferentes de confiança: "confiança no parceiro" (em uma pessoa específica) e "confiança generalizada" (nas pessoas em geral, na natureza humana).

Esses dois aspectos, medição e risco, nos reportam à gestão de TI, pois a gerenciamento envolve medição e o risco é inerente aos serviços de TI. Assim, na aplicação da confiança à governança de TI verifica-se que muitos pontos importantes são abordados, pois quanto mais alto o nível da confiança mais alto o nível de relacionamento e menor o risco dos serviços de TI, garantindo relacionamentos ajustados, comunicação eficiente e maior facilidade na implementação de ajustes necessários à condução da TI nas organizações [2].

A formalização da aplicação da confiança na gestão de TI estimula a concepção e implementação de modelo computacional, que poderá ser concebido após elaboração de diagnóstico de maturidade da gestão.

Os mesmos estudos, em contrapartida, levantam que organizações com uma gestão de TI ajustada ao negócio, com foco no tratamento adequado da informação, têm suas ações facilitadas no intuito de aproveitar as oportunidades e correm menos riscos diante das ameaças potenciais.

Com esse foco Weill e Ross [63] enfatizam que a Gestão de TI é "implementada por meio de um conjunto de mecanismos que se bem concebidos, bem compreendidos e transparentes promovem comportamentos desejáveis em termos de TI. Por outro lado se os mecanismos forem mal implementados, os arranjos de Gestão não trarão os resultados esperados".

Para isso, foram estabelecidos os parâmetros sob os quais a confiança poderá ser avaliada e quantificada, sendo então adequada a utilização de tópicos já consagrados e presentes em mecanismos de apoio ao gerenciamento e de auditoria existentes no mercado e levantados segundo as principais decisões e uma prospecção realizada em mais de duzentas empresas, como no caso da pesquisa de Weill e Ross [63].

3.5.1. Processos e Métricas

Na elaboração do Modelo foram considerados os processos do COBIT com aspectos relevantes à obtenção dos níveis confiança, além do emprego de métricas consideradas adequadas a sua medição.

3.5.1.1. Definir o Plano Estratégico de TI

O planejamento estratégico de TI é necessário para controlar e direcionar todos os recursos de TI em alinhamento com as prioridades e estratégia de negócio. A função de TI e as partes interessadas pelo negócio são responsáveis por garantir que dos projetos e portfólios executivos de serviços resultem em valores inestimáveis.

O plano estratégico deve realçar o entendimento das partes interessadas no que diz respeito à oportunidade e limitação da TI, avaliar o atual desempenho e esclarecer o nível de investimento requerido. A estratégia de negócio e prioridade devem ser pautados nos portfólios executivos e determinados pelo plano tático de TI, o qual estabelece objetivos concisos, planos e tarefas bem definidos e aceitos pelo negócio e pela TI.

3.5.1.2. Definir a Arquitetura da Informação

Os sistemas de informação devem criar e atualizar regularmente um modelo de informação de negócio e definir os sistemas apropriados para otimizar o uso desta informação. Isto abarca o desenvolvimento de um dicionário de dados corporativo com as regras sintáticas de dados da organização, esquema de classificação de dados e níveis de segurança. Este processo melhora a qualidade de decisão do gerenciamento certificando-se de que informações seguras e confiáveis sejam geradas, permitindo racionalizar os recursos de sistemas de informação para subsidiar as estratégias de negócio de forma apropriada. Este processo de TI também é requerido para aumentar a responsabilidade solidária sobre a integridade e segurança dos dados e para melhorar a efetividade e controle do compartilhamento da informação por meio das aplicações e entidades.

3.5.1.3. Definir a Direção Tecnológica

A função dos serviços de informação determina a direção da tecnologia para manter o rumo do negócio. Isto demanda a criação de um plano de infra-estrutura tecnológica além da arquitetura base, de forma a estabelecer e gerenciar expectativas realísticas do que a tecnologia pode oferecer em termos de produtos, serviços e

disseminação de mecanismos. O plano deve ser regularmente atualizado em todos os aspectos: arquitetura de sistemas, direção tecnológica, planos de aquisição, padrões, migração de estratégias e contingência. Isto permite reação imediata às mudanças no ambiente competitivo, economia de escala no preenchimento de vagas dos sistemas de informação e investimentos bem como interoperabilidade de plataformas e aplicações aperfeiçoada.

3.5.1.4. Definir os Processos de TI, Organização e Relacionamentos

Uma organização de TI deve ser definida levando-se em consideração os requisitos de pessoal, habilidades, funções, responsabilidade geral, autoridade, papéis, responsabilidades individuais e supervisão. Esta organização deve ser adequada segundo uma estrutura de processo de TI que garanta transparência e controle bem como o envolvimento de executivos seniores e gerenciamento de negócio. Um comitê estratégico deve atuar como uma comissão de supervisão de TI além de uma ou mais comissões de direção, na qual o negócio e a TI participe, devendo determinar priorização dos recursos de TI coerente com as necessidades do negócio. Os processos, as políticas administrativas e os procedimentos precisam ser estabelecidos para todas as funções, com especial atenção para o controle, a garantia, o gerenciamento de risco, a segurança da informação, a propriedade de sistemas e dados e segregação de deveres. Para atender oportunamente as exigências do negócio, a TI deve estar envolvida nos processos relevantes de decisão.

3.5.1.5. Definir o Controle dos Investimentos de TI

Estabelece e mantém a estrutura para controlar os programas de investimentos voltados à TI que envolvem custos, benefícios, prioridade dentro do orçamento, ou seja, um processo de orçamento formal e gerenciamento afinado com o orçamento. Trabalha com as partes interessadas para identificar e controlar os custos totais e os benefícios dentro do contexto estratégico da TI e dos planos críticos e inicia, ainda, ação corretiva onde for necessária. O processo alimenta a parceria entre a TI e as partes interessadas do negócio, permitindo o efetivo e eficiente uso dos recursos da TI, dando transparência e atribuindo responsabilidade contábil (*accountability*) no custo total da propriedade, a relação dos benefícios do negócio e o retorno sobre os investimentos voltados à TI.

3.5.1.6. Estabelecer os Objetivos de Gerenciamento e Direção

O gerenciamento deve desenvolver uma estrutura de controle das políticas de comunicação de TI na empresa. Um programa de comunicação contínuo deve ser implementado para articular as missões, os objetivos de serviços, as políticas e seus procedimentos, aprovado e apoiado pelo gerenciamento. A comunicação proporciona suporte na concretização dos objetivos de TI e garante a conscientização e o entendimento dos negócios e riscos de TI, seus objetivos e direção. O processo deve garantir conformidade com as leis e regulamentos relevantes.

3.5.1.7. Gerenciar Recursos Humanos de TI

Adquire, mantém e motiva uma força de trabalho competente para criar e distribuir os serviços de TI dentro da empresa. Isto é alcançado seguindo práticas comuns e definidas de apoio ao recrutamento, treinamento, avaliação de desempenho, promoção e finalização. Este processo é crítico pois as pessoas vão se tornando bens importantes e a governança e ambiente de controle interno são severamente dependentes da motivação e da competência do pessoal.

3.5.1.8. Estabelecer o Controle de Qualidade

Um sistema de controle de qualidade deve ser desenvolvido e mantido, incluindo processo comprovado de aquisição, desenvolvimento e padrões. Isto possibilita o planejamento, implementação e manutenção do sistema de gerenciamento de qualidade fornecendo requisitos, procedimentos e políticas de qualidade com clareza. Os requisitos de qualidade devem estabelecer indicadores quantificáveis e alcançáveis. As melhorias contínuas são alcançadas por meio de monitoramento contínuo, análise e ação sobre os desvios e transmição dos resultados às partes interessadas. O gerenciamento de qualidade é essencial para assegurar que a TI esteja agregando valores ao negócio de forma transparente.

3.5.1.9. Avaliar e Controlar o Risco de TI

Cria e mantém uma estrutura de gerenciamento de risco. A estrutura documenta um nível de risco de TI aceitável, abrandando as estratégias e aceitação sobre os riscos residuais, também minimizados a um nível aceitável. O resultado da avaliação deve ser compreensível às partes interessadas e expressado em termos financeiros, para permitir que as partes interessadas (*stakeholders*) equilibrem o risco a um nível de tolerância aceitável.

3.5.1.10. Gerenciar Projetos

Estabelecimento de programa e estrutura de gerenciamento de projeto para todos os projetos de TI. A estrutura deve garantir a correta priorização e coordenação de todos os projetos. Deve incluir um plano mestre, aplicação de recursos, definição dos benefícios aprovados pelos usuários, caminho planejado de entrega, garantia de qualidade, plano de teste formal, revisão de teste pós-implantação para garantir o gerenciamento de risco de projeto e agregação de valor ao negócio. Esta aproximação (nível) reduz o risco de custos inesperados e cancelamento de projetos, melhora as comunicações e envolvimento entre o negócio e os usuários finais, garante os valores e qualidades dos benefícios dos projetos e maximiza suas contribuições aos programas de investimentos na TI disponibilizada.

3.5.1.11. Identificar Soluções Automatizadas

A necessidade de nova aplicação ou função requer análises antes da aquisição ou criação para garantir que os requisitos de negócio sejam satisfeitos em um caminho efetivo e eficiente. Este processo contempla a definição das necessidades, consideração de fontes alternativas, revisão de viabilidade econômica e tecnológica, execução das análises de risco e análises de custo-benefício e conclusão de uma decisão final de "desenvolver" ou "comprar". Todos esses passos permitem à organização minimizar o custo para adquirir e implementar soluções adequadas aos seus objetivos de negócio.

3.5.1.12. Adquirir e Manter Software de Aplicação

As aplicações devem estar disponíveis em conformidade com os requisitos do negócio. Este processo contempla o esquema das aplicações, a inclusão apropriada dos requisitos de segurança e controle de programa, e o atual desenvolvimento e configuração de acordo com os padrões. Isto permite à organização suportar apropriadamente as operações de negócio com as aplicações automatizadas corretas.

3.5.1.13. Adquirir e Manter Infra-estrutura de Tecnologia

As organizações devem ter processos para a aquisição, implementação e atualização da infra-estrutura de tecnologia. Isto requer um método planejado de aquisição, manutenção e proteção da infra-estrutura em alinhamento com as estratégias tecnológicas aceitas e a provisão de desenvolvimento e dos ambientes de teste. Isto garante o contínuo apoio tecnológico às aplicações de negócio.

3.5.1.14. Instalar e Validar Soluções e Mudanças

Novos sistemas necessitam ser colocados em operação uma vez que seus desenvolvimentos tenham sido concluídos. Para tanto, é necessário teste apropriado em um ambiente dedicado com exaustivo teste de dados, definição de expansão e instruções de migração, planejamento de versão e promoção vigente para produção e uma revisão pós-implementação. Isto garante que os sistemas operacionais sejam alinhados com as expectativas e resultados esperados.

3.5.1.15. Definir e Gerenciar Níveis de Serviço

A comunicação efetiva entre o Gerenciamento de TI e os clientes de negócio referente aos serviços requisitados é disponibilizado por uma definição documentada e em conformidade com os serviços de TI e níveis de serviço. Este processo também inclui monitoramento e relato oportuno às partes interessadas na realização dos níveis de serviço. Este processo permite o alinhamento entre os serviços de TI e os requisitos dos negócios relacionados.

3.5.1.16. Definir e Gerenciar Serviços Terceirizados

A necessidade de assegurar que os serviços prestados por terceiros satisfaçam os requisitos de negócio requer um efetivo gerenciamento de processo de serviços terceirizados. Este processo é realizado definindo claramente os papéis, responsabilidades e expectativas dos acordos das partes terceirizadas bem como revisando e monitorando tais acordos para efetividade e conformidade. O efetivo gerenciamento dos serviços terceirizados minimiza os riscos de negócio associados com os fornecedores de serviços despreparados.

3.5.1.17. Estabelecer e Serviço Contínuo

Gerenciamento do processo de estabelecimento de serviço contínuo, de forma a satisfazer o requisito do negócio de TI de assegurar impacto mínimo no negócio no caso de interrupção do serviço de TI.

3.5.1.18. Estabelecer a Segurança dos Sistemas

A necessidade de manter a integridade da informação e proteger os ativos de TI requer um processo de gerenciamento de segurança. Este processo inclui estabelecer e manter os papéis e responsabilidades sobre a segurança de TI, políticas, padrões e procedimentos. O gerenciamento de segurança também inclui a execução de monitoramento de segurança e teste periódico, além da implementação de ações corretivas para as deficiências na segurança ou nos incidentes. O efetivo gerenciamento de segurança protege todos os recursos de TI para minimizar o impacto sobre o negócio, no que diz respeito à vulnerabilidade na segurança e respectivos incidentes.

3.5.1.19. Identificar e Alocar Custos

A necessidade de um sistema justo e eqüitativo de alocação de custo de TI para os negócios requer uma medição precisa dos custos de TI e acordo com os usuários do negócio em uma alocação razoável. Este processo contempla a construção e operação de um sistema para capturar, alocar e registrar os custos de TI aos usuários dos serviços. Um

sistema justo de alocação permite ao negócio tomar decisões mais embasadas acerca do uso dos serviços.

3.5.1.20. Gerenciar Central de Serviço e Incidentes

A resposta efetiva e oportuna às questões e problemas dos usuários de TI requer uma central de serviço, bem planejada e executada, e um processo de gerenciamento de incidente. Este processo engloba o estabelecimento de função da central de atendimento com respectivo registro, hierarquização de incidente, análises de tendência, raiz do problema e resolução. Os benefícios do negócio conferem aumento de produtividade por meio de rápida resolução das dúvidas dos usuários. Em complementação a isso, o negócio pode mapear a origem dos problemas (tal como treinamento deficiente de usuário) por meio de relatório efetivo.

3.5.1.21. Gerenciar a Configuração

Neste processo está incluída uma coletânea de configuração inicial de informação, o estabelecimento de linhas bases, informação de configuração de auditoria e verificação e um repositório de configuração conforme necessidade. Um efetivo gerenciamento de configuração facilita grandemente a disponibilidade do sistema, minimiza as questões de produção e soluciona os problemas com mais rapidez.

3.5.1.22. Gerenciar Problemas

O efetivo gerenciamento de problemas requer a identificação e classificação dos problemas, análise de suas origens e respectiva resolução. Esse processo de gerenciamento também contempla a identificação de recomendações para melhoria, manutenção dos registros de problemas e revisão da situação das ações corretivas. Um efetivo processo de gerenciamento de problemas melhora os níveis de serviço, reduz os custos e melhora a conveniência e satisfação do cliente.

3.5.1.23. Gerenciar Dados

O efetivo gerenciamento de dados requer a identificação dos requisitos de dados. Esse processo também contempla o estabelecimento de procedimentos efetivos para

controlar a biblioteca de mídia, cópia de segurança (*backup*), recuperação de dados (*recovery*) e a disposição da mídia (fornecimento). O efetivo gerenciamento dos dados ajuda a assegurar a qualidade, perda de tempo e disponibilidade dos dados de negócio.

3.5.1.24. Gerenciar Ambiente Físico

A proteção do pessoal e equipamento de informática requer instalações físicas bem planejadas e gerenciadas. O processo de gerenciamento do ambiente físico inclui a definição dos requisitos dos locais físicos, seleção apropriada das facilidades e dos processos efetivos de projeto para o monitoramento dos fatores ambientais e gerenciamento dos acessos físicos. O efetivo gerenciamento do ambiente físico reduz as interrupções do negócio por danos dos equipamentos de informática e pessoal.

3.5.1.25. Gerenciar Operações

O processamento completo e preciso dos dados requer um gerenciamento efetivo de processamento de dados e manutenção dos *hardwares*. Este processo inclui a definição das políticas e procedimentos das operações para o gerenciamento efetivo do processamento esquematizado, proteção de saída sensível, monitoramento de infra-estrutura e manutenção preventiva de *hardware*. O efetivo gerenciamento das operações ajuda a manter a integridade dos dados e reduzir a lentidão do negócio e os custos de operação de TI.

3.5.1.26. Monitorar e Avaliar Desempenho de TI

O efetivo gerenciamento de desempenho de TI exige um processo de monitoramento, o qual abrange a definição de indicadores de desempenho relevantes, um sistemático e oportuno relatório de desempenho e pronta ação sobre os desvios. O monitoramento é necessário para certificar-se de que os procedimentos estão sendo tomados corretamente em alinhamento com as políticas e direções estabelecidas.

3.5.1.27. Monitorar e Avaliar Controle Interno

Estabelecer um programa de controle interno de TI efetivo requer um processo de monitoramento bem definido. Nesse processo inclui-se o monitoramento e relatório das

exceções de controle, dos resultados da auto-avaliação e revisões das partes terceirizadas. Um benefício importante no monitoramento do controle interno é prover garantia no que diz respeito às eficientes e efetivas operações e conformidades com as leis e regulamentos aplicáveis.

3.5.1.28. Estabelecer a Conformidade Regulamentar

A efetiva supervisão regulamentar requer o estabelecimento de um processo de revisão independente para assegurar a conformidade com as leis e regulamentos. Este processo envolve um caráter de auditoria, a independência do auditor, éticas e padrões profissionais, planejamento, o desempenho do trabalho de auditoria, a reportagem e acompanhamento das atividades de auditoria. O propósito desse processo é fornecer garantia positiva relacionada à conformidade com as leis e regulamentos relacionados à TI.

3.5.1.29. Fornecer Governança de TI

Estabelecer uma estrutura de governança efetiva abrange a definição das estruturas organizacionais, dos processos, da liderança, dos papéis e respectivas responsabilidades para assegurar que os investimentos de TI sejam alinhados e segmentados em conformidade com as estratégias e objetivos da empresa.

3.5.2. Métricas

As métricas foram selecionadas a partir de requisitos de confiança e associadas aos processos de TI vinculados aos fatores de TI (planejamento, controle, implementação, entrega, suporte e monitoramento) [4]. Essas métricas incidem em cada item relacionado aos requisitos de confiança, o que possibilita a avaliação segundo sua importância e relevância. As tabelas 2, 3, 4, 5, 6 e 7 apresentam os relacionamentos de confiança propostos.

Tabela 4 - Relação Elementos da Gestão de TI - Planejamento x Métricas.

PLANEJAMENTO		
PROCESSOS	**REQUISITOS DE CONFIANÇA**	**MÉTRICAS**
Definir o Plano Estratégico de TI	**Sustentabilidade**	Porcentagem dos objetivos de TI no plano estratégico de TI que sustenta o plano estratégico de negócio;
	Conformidade	Porcentagem dos projetos de TI no portfólio executivo de projeto de TI que pode ser diretamente relacionado ao plano tático de TI;
	Atraso	Atraso entre a atualização do plano estratégico de TI e a atualização do plano tático de TI.
Definir a Arquitetura de TI	**Redundância**	Percentual de elementos de dados redundantes/duplicados
	Conformidade	Percentual de aplicações em desconformidade com a arquitetura da informação
	Freqüência	Freqüência das atividades de validação dos dados
Definir a Direção da TI	**Inconsistência**	Número e tipo de desvios do plano de infra-estrutura de tecnologia
	Freqüência	Freqüência da revisão/atualização do plano de infra-estrutura de tecnologia
	Conformidade	Número de plataformas de tecnologia por função dentro da empresa.
Definir os Processos de TI, Organização e Relacionamento	**Conformidade**	Percentual de funções com descrições de autoridades e posições documentadas
	Consistência	Número de unidades/processos de negócios não suportados pela TI da organização, mas que deveriam ser suportados, de acordo com a estratégia
	Consistência	Número de núcleos das atividades de TI fora da TI da organização que não são aprovados ou submetidos aos padrões organizacionais de TI
Estabelecer o Gerenciamento do Investimento de TI	**Qualidade**	Percentual da redução da unidade de custo dos serviços de TI distribuídos
	Consistência	Percentual de desvio do valor orçamentário comparado com o orçamento total
	Qualidade	Percentual dos gastos com a TI expressos por indexadores de valor de negócios (por exemplo, vendas/serviços crescem devido ao aumento da conectividade)

Tabela 5 - Relação Elementos da Gestão de TI - Controle x Métricas.

CONTROLE		
PROCESSOS	**REQUISITOS DE CONFIANÇA**	**MÉTRICAS**
Estabelecer os Objetivos de Gerenciamento e Direção	**Consistência**	Número de interrupção de negócio devido à falha de serviço de TI
	Conformidade	Percentual de partes interessadas que entendem a estrutura de controle do negócio.
	Conformidade	Percentual das partes interessadas controle do negócio. que não estejam em conformidade com a política
Estabelecer o Gerenciamento dos Recursos Humanos de TI	**Satisfação**	Nível de satisfação das partes interessadas com as experiências e habilidades do pessoal de TI
	Rotatividade	Rotatividade de pessoal de TI na empresa
	Capacidade	Percentual de pessoas certificadas de acordo com as necessidades de serviço
Estabelecer o Controle da Qualidade	**Satisfação**	Percentual das partes interessadas satisfeitas com a qualidade da TI (avaliado segundo a importância)
	Qualidade	Percentual de processos de TI formalmente revisados pela garantia de qualidade numa base periódica que atinja as metas e objetivos de qualidade e os objetivos como um todo
	Qualidade	Percentual dos processos em fase de revisão de certificação de qualidade (QA)
Avaliar e Gerenciar os Riscos de TI	**Criticidade**	Percentual de objetivos de TI críticos contemplados pela avaliação de risco
	Criticidade	Percentual dos riscos de TI críticos identificados pelos planos de ação desenvolvidos
	Conformidade	Percentual dos planos de ação de controle de risco aprovado para implementação
Controlar os Projetos	**Conformidade**	Percentual de expectativas das reuniões de projetos das partes interessadas (sobre o tempo, sobre os requisitos das reuniões e orçamentos – pesados com base na importância)
	Conformidade	Percentual de recebimento de projetos revistos após sua implementação
	Qualidade	Percentual de projetos que seguem os padrões e práticas de gerenciamento de projetos

Tabela 6 - Relação Elementos da Gestão de TI - Implementação x Métricas.

IMPLEMENTAÇÃO		
PROCESSOS	**REQUISITOS DE CONFIANÇA**	**MÉTRICAS**
Identificar as Soluções Automatizadas	**Consistência**	Número de projetos onde os benefícios declarados não foram alcançados devido às presunções incorretas de viabilidade
	Consistência	Percentual de estudos de viabilidades interrompidos pelos seus respectivos proprietários de processo
	Satisfação	Percentual de usuários satisfeitos com as funcionalidades apresentadas
Adquirir e Manter Softwares de Aplicação	**Consistência**	Número de problemas de produção por aplicação causando visível inatividade
	Satisfação	Porcentagem de usuários satisfeitos com a funcionalidade oferecida
Adquirir e Manter a Infra-estrutura de Tecnologia	**Conformidade**	Percentual de plataformas que não estejam em alinhamento com a arquitetura de TI definida bem como os padrões tecnológicos
	Consistência	Número de processos de negócios críticos sustentados por infra-estrutura obsoleta (ou à deriva de ser)
	Consistência	Número de componentes de infra-estrutura que não sejam mais suportáveis (ou que tendem a não ser suportadas num futuro próximo)
Gerenciar Mudanças	**Consistência**	Número de desvios ou erros de dados causados por especificações imprecisas ou avaliação de impacto incompleta
	Consistência	Retrabalho de infra-estrutura ou aplicação causado por especificações de mudanças inadequadas
	Qualidade	Percentuais de mudanças seguem os processos de controle de mudança formais
Instalar e Validar Soluções e Mudanças	**Consistência**	Tempo improdutivo do aplicativo (inoperância) ou manutenção de dados causados por teste inadequado
	Qualidade	Percentual de sistemas que atendam os benefícios esperados tais como os medidos pelo processo pós-implementação

Tabela 7 - Relação Elementos da Gestão de TI - Entrega x Métricas.

ENTREGA		
PROCESSOS	**REQUISITOS DE CONFIANÇA**	**MÉTRICAS**
Definir e Gerenciar Níveis de Serviço	**Satisfação**	Percentual das partes interessadas satisfeitas com os níveis de entrega de serviço acima do esperado
	Consistência	Número de serviços prestados inexistentes no catálogo
	Conformidade	Número de reuniões de revisão de SLA formal com os negócios por ano
Gerenciar Serviços de Terceirizados	**Satisfação**	Número de queixas de usuário devido aos serviços contratados
	Adequabilidade	Percentual de fornecedores que atendam claramente os requisitos definidos e níveis de serviço
Assegurar Serviço Contínuo	**Inoperabilidade**	Número de horas perdidas por usuários por mês devido inoperância de sistema (outages) não planejada
	Conformidade	Número de processo de negócios críticos confiados à TI não contemplados no plano de continuidade de TI
Assegurar Segurança dos Sistemas	**Reputação**	Número de reputação negativa dos incidentes de conhecimento público
	Adequabilidade	Número de sistemas cujos requisitos de segurança não estão de acordo
	Vulnerabilidade	Número de violações na distribuição dos deveres
Educar e Treinar os Usuários	**Capacitação**	Número de chamadas no centro de atendimento devido a falta de treinamento de usuário
	Satisfação	Percentual de partes interessadas satisfeitas com o treinamento recebido
	Atraso	Atraso no tempo entre a identificação da necessidade de treinamento e a sua respectiva efetivação

Tabela 8 - Relação Elementos da Gestão de TI – Suporte x Métricas.

SUPORTE		
PROCESSOS	**REQUISITOS DE CONFIANÇA**	**MÉTRICAS**
Gerenciar Central de Serviço e Incidentes	**Satisfação**	Satisfação do usuário com a primeira instância do atendimento
	Qualidade	Percentual de incidentes resolvidos dentro do período de tempo estipulado/aceitável
Gerenciar a Configuração	**Conformidade**	Número de questões de conformidade de negócio causadas pela configuração imprópria dos recursos
	Consistência	Número de desvios identificados entre o repositório de configuração e as configurações dos recursos atuais
	Conformidade	Percentual de licenças adquiridas e não contabilizadas no rol do repositório
Gerenciar os Problemas	**Vulnerabilidade**	Número de problemas recorrentes com impacto sobre os negócios
	Qualidade	Percentual de problemas resolvidos dentro do período de tempo programado
	Freqüência	Freqüência de registros ou atualizações de problemas existentes, com base na severidade do problema.
Gerenciar os Dados	**Disponibilidade**	Pela satisfação do usuário com a disponibilidade dos dados
	Qualidade	Pelo percentual de incidentes onde os dados sensíveis foram restabelecidos com sucesso após a mídia ter sido disponibilizada
Gerenciar o Ambiente Físico	**Consistência**	Pelo tempo improdutivo conseqüente de incidentes no ambiente físico
	Vulnerabilidade	Pelo número de incidentes devido às falhas ou violação do ambiente físico
	Freqüência	Pela freqüência avaliação de risco físico e revisões

Tabela 9 - Relação Elementos da Gestão de TI - Monitoramento x Métricas.

MONITORAMENTO		
PROCESSOS	**REQUISITOS DE CONFIANÇA**	**MÉTRICAS**
Gerenciar as Operações	**Adequabilidade**	Número de níveis de serviço impactados pelos incidentes operacionais
	Consistência	Horas de inoperância imprevistas dos sistemas causadas por incidentes operacionais
	Conformidade	Percentual de recursos de hardwares inseridos nos cronogramas de manutenção preventiva
Monitorar e Avaliar o Desempenho de TI	**Grau de Satisfação**	Grau de satisfação das entidades de gerenciamento e governança com o relatório de desempenho
	Adequabilidade	Número de ações de aperfeiçoamento segmentadas pelas atividades de monitoramento
	Qualidade	Percentual de processos críticos monitorados
Monitorar e Avaliar o Controle Interno	**Vulnerabilidade**	Número de falhas no controle principal
	Qualidade	Número de iniciativas de melhoramento de controle
	Qualidade	Número e abrangente das auto-avaliações de controle
Assegurar o Cumprimento das Normas Regulamentares	**Conformidade**	Custo da não conformidade com a TI, inclusive multas e penalidades
	Atraso	Tempo médio de atraso entre a identificação das questões de conformidades externas
	Conformidade	Freqüência das revisões de conformidades
Fornecer Governança de TI	**Freqüência**	Freqüência dos relatórios da comissão sobre a TI às partes interessadas (inclusive maturidade)
	Freqüência	Freqüência dos relatórios da TI à comissão (inclusive maturidade)
	Freqüência	Freqüência das revisões independentes da conformidade da TI

4. METODOLOGIA

Segundo Pozzebon e Freitas [51] Hoppen *et al* [33], a correta utilização dos métodos de pesquisa disponíveis é condição indispensável para o bom desenvolvimento da mesma, bem como da confiabilidade dos resultados obtidos. Embora o método não seja condição suficiente para o sucesso de uma pesquisa, ele é uma condição indispensável, uma vez que sem ele os resultados obtidos são de difícil aceitação, e quando um conhecimento é obtido pelo método científico, qualquer pesquisador que repita a investigação nas mesmas circunstâncias, obterá o mesmo resultado, desde que os mesmos cuidados sejam tomados Campomar [11].

Foi realizada uma pesquisa de natureza exploratória, tendo em vista a necessidade de compreensão de determinado fenômeno. Para alcançar os objetivos propostos, foram utilizados dados qualitativos e quantitativos: os dados qualitativos foram obtidos por meio da pesquisa bibliográfica e modelagem das técnicas objeto do estudo, já os dados quantitativos pela coleta de dados realizada em forma de entrevistas e questionários.

4.1. MODELO DE CONFIANÇA

Na elaboração do Modelo foram empregados aspectos relevantes ao gerenciamento da TI, adaptado do COBIT, confirmados por uma posterior verificação (diagnóstico). A figura 4 representa as etapas seguidas na elaboração do Modelo.

Figura 4 - Concepção do Modelo de Confiança

Na implementação do modelo para gerenciamento da confiança foram estabelecidos, correspondentes às ações de confiança, os seguintes etapas:

1. Confiança – Nesta etapa foi realizada a seleção dos parâmetros ou aspectos necessários para obtenção dos níveis de confiança, foram selecionados requisitos de confiança representados na tabela 10. .

Tabela 10 - Requisitos de Confiança

Requisitos de Confiança	Conformidade	Consistência	Disponibilidade	Criticidade
Benevolência	Qualidade	Inoperabilidade	Inconsistência	Freqüência
Capacidade	Adequabilidade	Rotatividade	Reputação	Atraso
Redundância	Sustentabilidade	Capacitação	Vulnerabilidade	Satisfação

2. Gerenciamento de TI – Foi realizado estudo exploratório sobre a gestão da tecnologia da informação em aspectos relevantes, visando determinar o contexto e os mecanismos de TI necessários à aplicação do Modelo.

Para o contexto deste trabalho foram adaptados aspectos considerados pertinentes do COBIT (Control Objectives for Information and Related Technology), a tabela 11 apresenta os processos selecionados.

Tabela 11 – Processos utilizados no Modelo

PLANEJAMENTO	CONTROLE	IMPLEMENTAÇÃO	ENTREGA	SUPORTE	MONITORA-MENTO
Plano Estratégico	Comunicar Objetivos e Direção da Gestão	Soluções Automatizadas	Gestão de Níveis de Serviço	Gestão de Serviço e Incidentes	Gestão de Operações
Arquitetura da Informação	RH de TI	Aquisição e Manutenção de SW	Gestão de Serviços Tercerizados	Gestão de Configuração	Monitoramento e Avaliação do Desempenho de TI
Direção Tecnológica	Controle e Qualidade	Aquisição e Manutenção de Infra Estrutura	Assegurar Serviço Contínuo	Gestão de Problemas	Monitoramento e Avaliação do Controle Interno
Processos de TI	Avaliação da Gestão de Riscos	Gestão de Mudanças	Segurança de Sistemas	Gestão de Dados	Assegurar o Cumprimento de Normas Regulamentares
Gestão de Investimento de TI	Controle de Projetos	Instalação e Validação de Soluções de Mudanças	Treinamento de Usuários	Gestão de Ambiente Físico	Gestão de TI

3. Verificação – Realizou-se um levantamento das métricas a serem aplicadas ao gerenciamento de TI, com o objetivo de conferir os valores obtidos e atribuídos a cada aspecto de confiança. Assim foi elaborado os questionários para o referido levantamento constante nas tabelas 12 a 17.

Tabela 12 – Questionário Planejamento

PLANEJAMENTO		
I. Em relação Plano Estratégico de TI, informar:		Niveis de Confiança (0,1 – 10)
1.	O percentual dos objetivos de TI no plano estratégico de TI que sustentam o plano estratégico de negócio.	
2.	O percentual dos projetos de TI no portfólio executivo de projeto de TI que pode ser diretamente traçado de volta para o plano tático de TI.	
3.	O percentual de atraso entre a atualização do plano estratégico de TI e a atualização do plano tático de TI.	
II. Em relação a Arquitetura da Informação, indicar:		
1.	O percentual de elementos de dados redundantes/duplicados.	
2.	O percentual de aplicações em desconformidade com a arquitetura da informação.	
3.	A freqüência das atividades de validação dos dados.	
III. Em relação a Direção da Tecnologia, indicar:		
1.	Número de desvios do plano de infra-estrutura de tecnologia.	
2.	Freqüência da revisão/atualização do plano de infra-estrutura de tecnologia.	
3.	Número de plataformas de tecnologia por função dentro da empresa.	
IV. Em relação aos Processos de TI, Organização e Relacionamento,informar:		
1.	Percentual de funções com descrições de autoridades e posições documentadas.	
2.	Número de unidades/processos de negócios não suportados pela TI da organização, mas que deveriam ser suportados, de acordo com a estratégia.	

3.	Número de núcleos das atividades de TI fora da TI da organização que não são aprovados ou submetidos aos padrões organizacionais de TI.	
V. Em relação ao Gerenciamento do Investimento de TI, apontar:		
1.	Percentual da unidade de custo dos serviços de TI distribuídos reduzidos.	
2.	Percentual de desvio do valor orçamentário comparado com o orçamento total.	
3.	Percentual dos gastos com a TI expressos por indexadores de valor de negócios (por exemplo, vendas/serviços crescem devido ao aumento da conectividade)	

Tabela 13 - Questionário Controle

CONTROLE		
VI. Em relação a Comunicar os Objetivos e a Direção do Gerenciamento		Niveis de Confiança (0,1 – 10)
1.	Número de interrupção de negócio devido à falha de serviço de TI.	
2.	Percentual de partes interessadas que entendem a estrutura de controle do negócio.	
3.	Percentual das partes interessadas que em conformidade com a política.	
VII. Controle os Recursos Humanos de TI, informar:		
1.	Nível de satisfação das partes interessadas com as experiências e habilidades do pessoal de TI.	
2.	Rotatividade de pessoal de TI na empresa.	
3.	Percentual de pessoas certificadas de acordo com as necessidades de serviço.	
VIII. Em relação ao Controle a Qualidade, apontar:		
1.	Percentual das partes interessadas satisfeitas com a qualidade da TI (avaliado segundo a importância).	
2.	Percentual de processos de TI formalmente revisados pela	

	garantia de qualidade numa base periódica que atinja as metas e objetivos de qualidade e os objetivos como um todo.	
3.	Percentual dos processos em fase de revisão de certificação de qualidade (QA).	
IX. Em relação a Avaliação e Gerenciamento dos Riscos de TI, indicar:		
1.	Percentual de objetivos de TI críticos contemplados pela avaliação de risco.	
2.	Percentual dos riscos de TI críticos identificados pelos planos de ação desenvolvidos.	
3.	Percentual dos planos de ação de controle de risco aprovado para implementação.	
X. Em relação ao Controle os Projetos, apontar:		
1.	Percentual de expectativas das reuniões de projetos das partes interessadas (sobre o tempo, sobre os requisitos das reuniões e orçamentos – pesados com base na importância).	
2.	Percentual de recebimento de projetos revistos após sua implementação.	
3.	Percentual de projetos que seguem os padrões e práticas de gerenciamento de projetos.	

Tabela 14 - Questionário Implementação

IMPLEMENTAÇÃO		
XI. Em relação a identificação das soluções automatizadas, indicar:		Niveis de Confiança (0,1 – 10)
1.	Número de projetos onde os benefícios declarados não foram alcançados devido às presunções incorretas de viabilidade.	
2.	Percentual de estudos de viabilidades interrompidos pelos seus respectivos proprietários de processo.	
3.	Percentual de usuários satisfeitos com as funcionalidades apresentadas.	
XII. Em relação a aquisição e manutenção de softwares de aplicação, apontar:		
1.	Percentual do número de problemas de produção por	

	aplicação causando visível inatividade.	
2.	Porcentagem de usuários satisfeitos com a funcionalidade oferecida.	
XIII. Em relação a aquisição e manutenção da infra-estrutura de Tecnologia, informar:		
1.	Percentual de plataformas que estejam em alinhamento com a arquitetura de TI definida bem como os padrões tecnológicos.	
2.	Número de processos de negócios críticos sustentados por infra-estrutura obsoleta (ou à deriva de ser).	
3.	Número de componentes de infra-estrutura que não sejam mais suportáveis (ou que tendem a não ser suportadas num futuro próximo).	
XIV. Em relação ao gerenciamento de mudanças, indicar:		
1.	Percentual de desvios ou erros de dados causados por especificações imprecisas ou avaliação de impacto incompleta.	
2.	Percentual de retrabalho de infra-estrutura ou aplicação causado por especificações de mudanças inadequadas.	
3.	Percentual de mudanças que seguem os processos de controle de mudança formais.	
XV. Em relação a instalação e validação das soluções e Mudanças, informar:		
1.	Percentual de tempo improdutivo do aplicativo (inoperância) ou manutenção de dados causados por teste inadequado.	
2.	Percentual de sistemas que atendam os benefícios esperados tais como os medidos pelo processo pós-implementação.	

Tabela 15 - Questionário Entrega

ENTREGA		
XVI. Em relação a Definição do Gerenciamento dos Níveis de Serviço, indicar:		Niveis de Confiança (0,1 – 10)
1.	Percentual das partes interessadas satisfeitas com os níveis de entrega de serviço acima do esperado.	
2.	Percentual dos serviços prestados inexistentes no catálogo.	
3.	Percentual de reuniões de revisão de SLA formal com os negócios por ano.	
XII. Em relação a aquisição e manutenção de softwares de aplicação, apontar:		
1.	Percentual do número de problemas de produção por aplicação causando visível inatividade.	
2.	Porcentagem de usuários satisfeitos com a funcionalidade oferecida.	
XIII. Em relação a aquisição e manutenção da infra-estrutura de Tecnologia, informar:		
1.	Percentual de plataformas que estejam em alinhamento com a arquitetura de TI definida bem como os padrões tecnológicos.	
2.	Número de processos de negócios críticos sustentados por infra-estrutura obsoleta (ou à deriva de ser).	
3.	Número de componentes de infra-estrutura que não sejam mais suportáveis (ou que tendem a não ser suportadas num futuro próximo).	
XIV. Em relação ao gerenciamento de mudanças, indicar:		
1.	Percentual de desvios ou erros de dados causados por especificações imprecisas ou avaliação de impacto incompleta.	
2.	Percentual de retrabalho de infra-estrutura ou aplicação causado por especificações de mudanças inadequadas.	
3.	Percentual de mudanças que seguem os processos de controle de mudança formais.	
XV. Em relação a instalação e validação das soluções e Mudanças, informar:		

1.	Percentual de tempo improdutivo do aplicativo (inoperância) ou manutenção de dados causados por teste inadequado.	
2.	Percentual de sistemas que atendam os benefícios esperados tais como os medidos pelo processo pós-implementação.	

Tabela 16 - Questionário Suporte

SUPORTE		
XXI. Em relação ao Gerenciamento da Central de Serviço e Incidentes, indicar:		Niveis de Confiança (0,1 – 10)
1.	Percentual da satisfação do usuário com a primeira instância do atendimento.	
2.	Percentual de incidentes resolvidos dentro do período de tempo estipulado/aceitável.	
3.	Percentual da taxa de desistência.	
XXII.Em relação ao Gerenciamento da Configuração, informar:		
1.	Percentual de questões de conformidade de negócio causadas pela configuração imprópria dos recursos.	
2.	Percentual de desvios identificados entre o repositório de configuração e as configurações dos recursos atuais.	
XXIII.Em relação ao Gerencia os Problemas, indicar:		
1.	Número de problemas recorrentes com impacto sobre os negócios.	
2.	Percentual de problemas resolvidos dentro do período de tempo programado.	
3.	Freqüência de registros ou atualizações de problemas existentes, com base na severidade do problema.	
XXIV.Em relação ao Gerenciamento dos Dados, apontar:		
1.	Percentual da satisfação do usuário com a disponibilidade dos dados.	
2.	Percentual de incidentes onde os dados sensíveis foram restabelecidos com sucesso após a mídia ter sido disponibilizada.	
XXV.Em relação ao Gerenciamento do Ambiente Físico, indicar:		
1.	Percentual do tempo improdutivo conseqüente de incidentes no	

	ambiente físico.	
2.	Percentual de incidentes devido às falhas ou violação do ambiente físico.	
3.	Percentual da freqüência avaliação de risco físico e revisões.	

Tabela 17 – Monitoramento

MONITORAMENTO		
XXVI.Em relação ao Gerenciamento das Operações, informar:		Niveis de Confiança (0,1 – 10)
1.	Percentual do número de níveis de serviço impactados pelos incidentes operacionais.	
2.	Percentual das horas de inoperância imprevistas dos sistemas causadas por incidentes operacionais.	
XXVII.Em relação ao Monitoramento e Avaliação do Desempenho de TI, indicar:		
1.	Percentual de questões de conformidade de negócio causadas pela configuração imprópria dos recursos.	
2.	Percentual de desvios identificados entre o repositório de configuração e as configurações dos recursos atuais.	
XXVIII.Em relação ao Monitoramento e Avaliação do Controle Interno, informar:		
1.	Percentual de falhas no controle principal.	
2.	Percentual de iniciativas de melhoramento de controle.	
3.	Percentual abrangente das auto-avaliações de controle.	
XXIX.Em relação a Assegurar o Cumprimento das Normas Regulamentares,indicar:		
1.	Percentual do custo da não conformidade com a TI, inclusive multas e penalidades.	
2.	Percentual de Tempo médio de atraso entre a identificação das questões de conformidades externas.	
3.	Percentual Freqüência das revisões de conformidades.	
XXX.Em relação a fornecer Governança de TI, indicar:		
1.	Percentual da freqüência dos relatórios da comissão sobre a TI às	

	partes interessadas (inclusive maturidade).	
2.	Percentual da freqüência dos relatórios da TI à comissão (inclusive maturidade).	
3.	Percentual da freqüência das revisões independentes da conformidade da TI.	

4. Definição de confiança aplicada a gestão da TI – Nesta etapa foi elaborada definição da confiança relacionada à TI, de forma a depurar os aspectos aplicáveis à destinação do Modelo. Estes aspectos em conjunto com fatores pertinentes da confiança proporcionaram o necessário respaldo à seguinte definição de gestão da confiança referida à TI: "Trata-se da atividade que concebe, avalia, implanta e monitora os mecanismos adequados ao estabelecimento de estruturas de tomadas de decisão, processos de alinhamento de negócios com a TI e meios de comunicação para a obtenção dos comportamentos desejáveis, ou seja, que possam ser avaliados como confiáveis, de forma a possibilitar a focalização da tecnologia nos objetivos empresariais"[3], exemplificados na tabela 18.

Tabela 18 - Associação dos requisitos de confiança com os mecanismos e métricas de TI.

PROCESSOS	REQUISITOS DE CONFIANÇA	MÉTRICAS
Definir a Arquitetura de TI	**Redundância**	**Percentual de elementos de dados redundantes/duplicados**
	Conformidade	**Percentual de aplicações em desconformidade com a arquitetura da informação**
	Freqüência	**Freqüência das atividades de validação dos dados**

5. Criação do Modelo – A partir das fases anteriores foi definido um Modelo para estabelecer os mecanismos de tratamento da confiança no contexto da gestão da TI.

4.2. ARQUITETURA DO MODELO

O modelo proposto é apresentado em três etapas: planejamento, mecanismos para obtenção do grau de confiança e base de conhecimento, mostrado na Arquitetura do Modelo, figura 5.

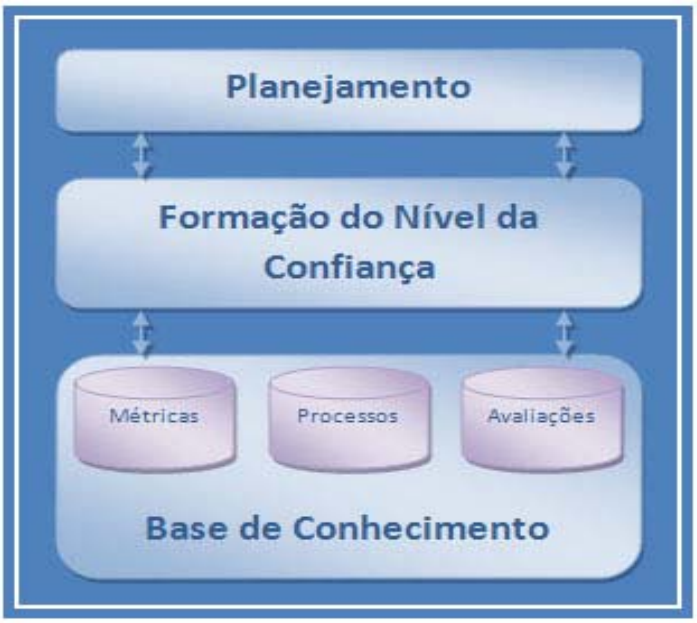


Figura 5 - Arquitetura do Modelo

4.2.1. Planejamento

Nessa etapa é estabelecido o ambiente onde a pesquisa será aplicada, definindo o grupo de pessoas relacionados a cada grupo de processos envolvidos, a periodicidade da aplicação e outros ajustes necessários e importantes para a execução da pesquisa.

4.2.2. Mecanismos para Obtenção do Grau de Confiança

Nessa etapa é apresentado um questionário (Anexo A) com fulcro na pesquisa, para resposta segundo a seletividade estabelecida no planejamento, visando uma prospecção da confiança associada as atividades da TI na organização. São implementados os processos selecionados, segundo métricas pré-estabelecidas possibilitando avaliação das categorias de TI com base nos requisitos de confiança.

Os resultados obtidos a partir das métricas são classificados em faixa de valores ao invés de um valor absoluto, proporcionando uma maior flexibilidade para a implantação das mesmas em vários cenários diferenciados (pequenas, médias e grandes empresas) [56,50]. Sendo assim, poderão ser utilizados valores classificados em: (1) Baixa, (2) Média e (3) Alta em relação ao nível de confiança alcançado. Adotou-se, conforme necessidades e informação dos gestores da TI, as seguintes faixas de valores conforme mostrado na tabela 19:

Tabela 19- Classificação da Confiança

Intervalos	Nível de Confiança	Nível de Risco
[0, 0.49]	Confiança Baixa	Risco Alto
[0.5, 0.69]	Confiança Média	Risco Médio
[0.7, 1.0]	Confiança Alta	Risco Baixo

4.2.3. Base de Conhecimento

Nessa etapa são organizadas as avaliações, os processos e as métricas selecionadas, como um repositório de informação de forma a possibilitar estudos futuros em relação à confiança na gestão da TI da organização segundo as necessidades elaboradas.

4.3. IMPLEMENTAÇÃO DO MODELO

4.3.1. Mecanismo de Avaliação

Para uma Organização ter a sua TI avaliada segundo a confiança, inicialmente é realizado um planejamento onde são estabelecidas as condições de execução, antecedendo a obtenção do nível de confiança. Segundo o resultado obtido, será carregada a Base de Conhecimento e/ou reiniciada a avaliação nos casos de níveis médios e baixos de confiança, conforme mostrado na figura 6.

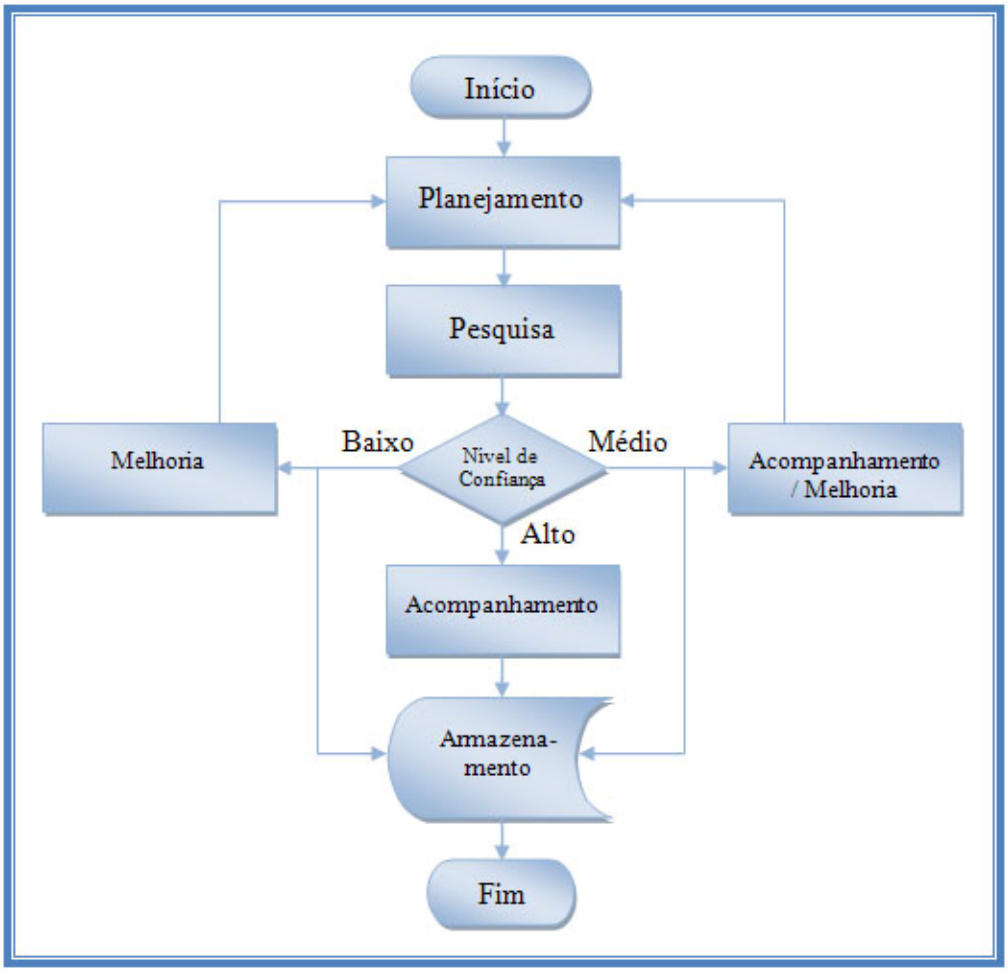


Figura 6 - Mecanismo de Avaliação

4.3.2. Ações de Confiança

- Formação da confiança – Na formação da confiança, etapa Planejamento, é feito um levantamento das informações sobre as áreas de TI envolvidas. Na etapa Pesquisa, são aplicados questionários aos grupos de envolvidos, gestores/usuários, distribuídos por atividades de cada processo nas áreas da TI, para a atribuição de valores dentro de um determinado intervalo. Sendo assim, o sistema para o gerenciamento de confiança é abastecido com as avaliações que utilizam valores "inteiros positivos" dentro do intervalo [0,1].

- Obtenção do nível da confiança – é feita pela consolidação dos valores obtidos em cada questionário, etapa pesquisa, a classificação da confiança se dá a partir do

cálculo das métricas atribuídas a cada Fator/Subfator/Item classificando-as segundo as faixas dos níveis de confiança/risco. Considera-se Item cada pergunta a ser respondida pelos pesquisados. Os Itens são agrupados em assuntos correlatos denominados Subfatores. Os Subfatores são agrupados segundo os processos Planejamento, Controle, Implementação, Entrega, Suporte e Monitoramento.

A obtenção do nível da confiança é feita após consolidação das respostas do questionário, determinando o intervalo onde se encontra a confiança a partir dos Fatores/Subfatores/Itens verificados. Os intervalos com os critérios de classificação constantes na tabela 20.

Tabela 20 – Classificação da Confiança

Intervalos	Nível de Confiança	Nível de Risco
[0, 0.49]	Confiança Baixa	Risco Alto
[0.5, 0.69]	Confiança Média	Risco Médio
[0.7, 1.0]	Confiança Alta	Risco Baixo

- Evolução da confiança – a cada nova avaliação pode-se comparar com a anterior visando monitorar a evolução da confiança no contexto. Indicam-se novas avaliações para o nível de confiança baixo em todas as situações. No caso de nível médio, deverá ser reavaliado somente quando este encontrar-se na faixa inferior do seu nível de avaliação.

- Atualização da base do conhecimento - são mantidas as informações relacionadas às avaliações realizadas e todos os resultados obtidos, bem como as diversas classificações.

4.3.3. Sistema de Apoio

Para possibilitar a interação dos gestores/usuários com a pesquisa, de forma eletrônica, foi implementado um sistema denominado Sistema de Gestão de TI baseado em Confiança (SISGESCON). O SISGESCON foi desenvolvido na linguagem JSP (Java Server Pages) com AJAX (Asynchronous Javascript And XML) e Javascript, utilizando Banco de Dados MYSQL. O sistema disponibiliza o questionário e realiza as operações necessárias para a obtenção do nível de confiança, figura 7. Por intermédio do sistema é possível manter um histórico dos resultados em uma base de dados, possibilitando estudos comparativos bem como prospecção dos níveis de confiança em determinada organoização.

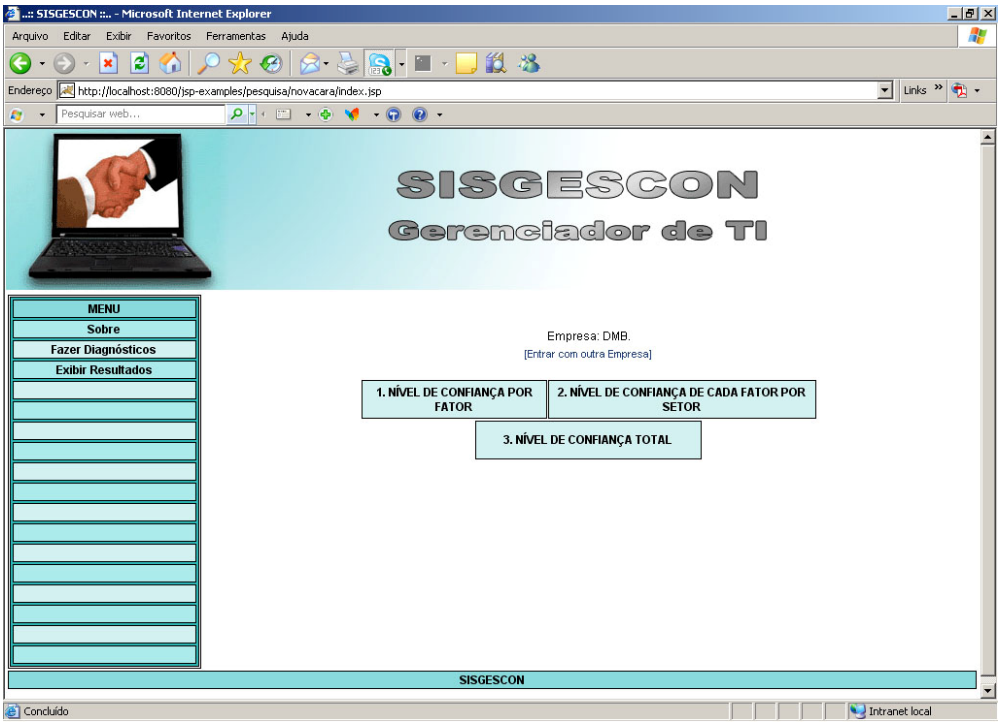


Figura 7 - Sisgescon

4.3.4. Interação com o Usuário

A camada de interação é responsável pela coordenação da integração entre o usuário e o sistema por meio da tradução das ações do usuário pela ativação de uma determinada funcionalidade do sistema, também permitindo que os resultados destas ações possam ser observados.

Nesta camada, para a realização do diagnóstico, é necessário que inicialmente, o usuário se identifique preenchendo as informações sobre o seu setor e sua organização, assim é possível inicar o diagnóstico. Cada etapa do questionário deve ser respondido apenas pelos responsáveis do setor relacionado. Para a visualização do resultado é necessário ter permissão que fica a critério do patrocinador.

5. VALIDAÇÃO DO PROJETO

5.1. FOCO DA PESQUISA

O teste de campo da pesquisa foi realizado na área de tecnologia da informação e comunicações (TIC) de uma Organização Governamental doravante denominada DMB, no primeiro trimestre de 2008, tornando-se então relevante a descrição da sua estrutura organizacional no que se refere à TIC na instituição.

As diversas atividades da DMB são definidas e tratadas nos níveis estratégicos em um Órgão de Direção Geral (ODG), e em níveis táticos ou de execução nos Departamentos denominados Órgãos de Direção Setoriais (ODS). A TIC está vinculada ao ODG a uma Subchefia, que trata de todas as modalidades de informações e no nível tático, ao Órgão de Direção de TI (ODTI). Os funcionários que se dedicam às atividades de TIC, nos diversos níveis, são engenheiros eletrônicos e de telemática, analistas de sistemas e de informática.

5.2. NÍVEL ESTRATÉGICO

A Subchefia do ODG tem como competências, dentre outras, planejar, orientar, coordenar e avaliar, no nível de direção geral, as atividades referentes aos Sistemas de informações organizacionais, comunicações e informática objetivando a modernização do Sistema de Controle da DMB e a otimização do processo decisório no âmbito da Instituição;

Para isso, integra a estrutura organizacional da Subchefia, uma Seção de Tecnologia da Informação.

O ODTI recebeu na Diretriz Estratégica de Comunicações e Informática da DMB as seguintes atribuições:

a) Desenvolver a prospecção e projetos nos campos das aplicações da tecnologia da informação;

b) Propor ao ODG, quando for o caso, as medidas necessárias à atualização das estruturas e diretrizes orientadoras do funcionamento do Sistema de Comunicações e Informática;

c) Elaborar os planos Básicos de Comunicações e de Informática de sua responsabilidade;

d) Estudar e propor ao ODG os procedimentos relativos à gestão dos recursos humanos das áreas de comunicações e informática;

e) Promover estudos, pesquisas e atividade sistemática de prospecção sobre o ciclo de vida das tecnologias adotadas no âmbito do Sistema de Comunicações e Informática;

f) Promover a integração com os sistemas congêneres das demais Organizações Governamentais e outros Órgãos;

g) Propor os padrões e soluções técnicas para a segurança da informação no âmbito dos sistemas;

h) Propor ao ODG a metodologia para avaliação dos sistemas.

Para gerir essas atribuições o ODTI se organiza em uma Assessoria de Tecnologia da Informação com Seções de Comunicações, Informática, Segurança da Informação, Planejamento e Gestão e Informações.

Para a execução das atividades o ODTI coordena e comanda as ações de um Centro de Desenvolvimento de Sistemas (CDS) e de Centros de Telemática (CT) localizados geograficamente de forma a propiciar apoio aproximado aos Órgãos Regionais subordinados.

5.3. NÍVEL DE EXECUÇÃO

O CDS é uma área complexa com um quadro de cargos de 168 funcionários, de nível universitário e técnico, com a missão de conceber, desenvolver, integrar e

aperfeiçoar sistemas, programas, aplicativos e estruturas lógicas dos diversos sistemas corporativos e sistemas de informações operacionais da DMB, atribuídos ao ODTI. Destaca-se a sua finalidade de realizar a prospecção e o desenvolvimento de sistemas pertinentes às áreas de comunicações, informática e de informações organizacionais de interesse da DMB.

Para isso o CDS se estrutura no que se refere à sua atividade fim, em uma Divisão de Sistemas com Seções de Gerência de Produto, de Analistas, de Arquitetura, de Desenvolvimento e de Apoio, uma Divisão de Engenharia com Seções de Prospecção, de Segurança da Informação, de Projetos com um Laboratório e de um Núcleo de Estudos de Software Livre e uma Divisão de Planejamento, Coordenação e Controle, conforme figura 8.

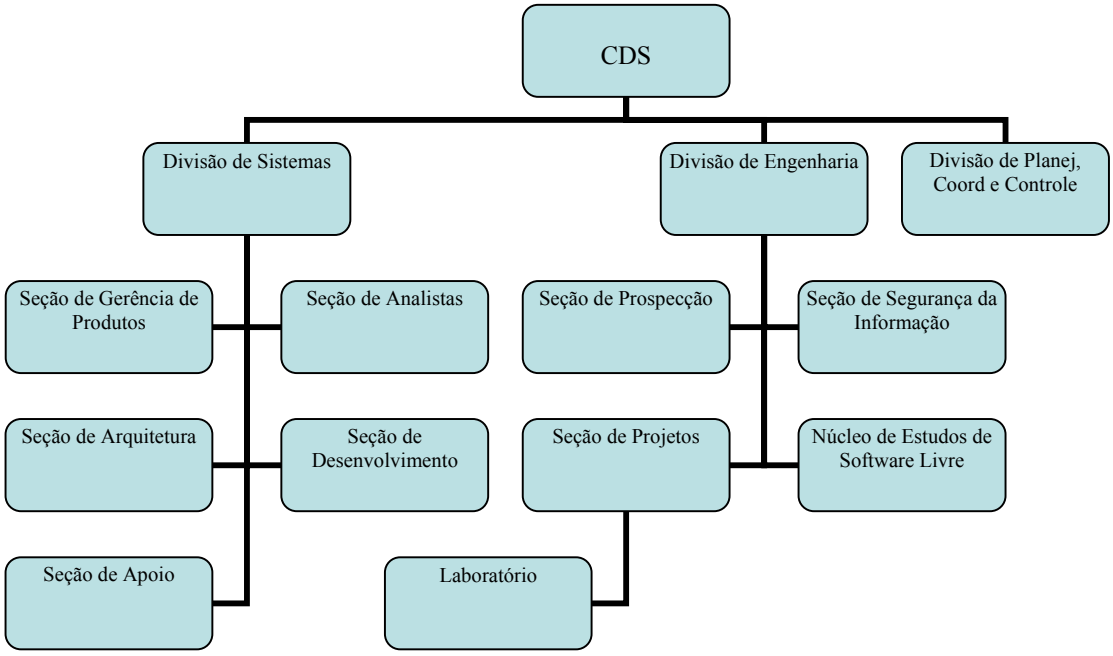


Figura 8 - Organograma CDS

Para o tratamento da infra-estrutura e suporte o ODTI enquadra Centros de Telemática sendo um deles, o Centro Integrado de Telemática da DMB (CIT), sediado em Brasília, sendo o responsável pela coordenação e direção dos demais centros. O CIT

apresenta um quadro de 295 funcionários (engenheiros, analistas de sistemas e técnicos) e tem como missão proporcionar a base física e lógica para a operação dos sistemas de Informática e Comunicações e realizar a manutenção dos sistemas em produção, além de manter em bom nível de operacionalidade a Rede de Comunicação de Dados e a manutenção das Bases de Dados Corporativos.

Para isso o CIT se estrutura no que se refere à sua atividade fim, conforme figura 9, em uma Divisão Técnica com Seções de Sistemas, de Redes e de Gerencia (Subseções de Segurança e de Desempenho), uma Divisão de Operação com Seção de Operações Combinadas (Subseções de Aplicativos, de Administração de Banco de Dados, de Supervisão Técnica e de Armazenamento), Seção de Redes e Seção de Atendimento a Usuários, e uma Divisão de Tratamento de Imagem com Seções de Geração de Imagens, Processo e Controle de Qualidade, Arquivo e Reconhecimento de Imagem e de Administração e Apoio, constantes na figura 9.

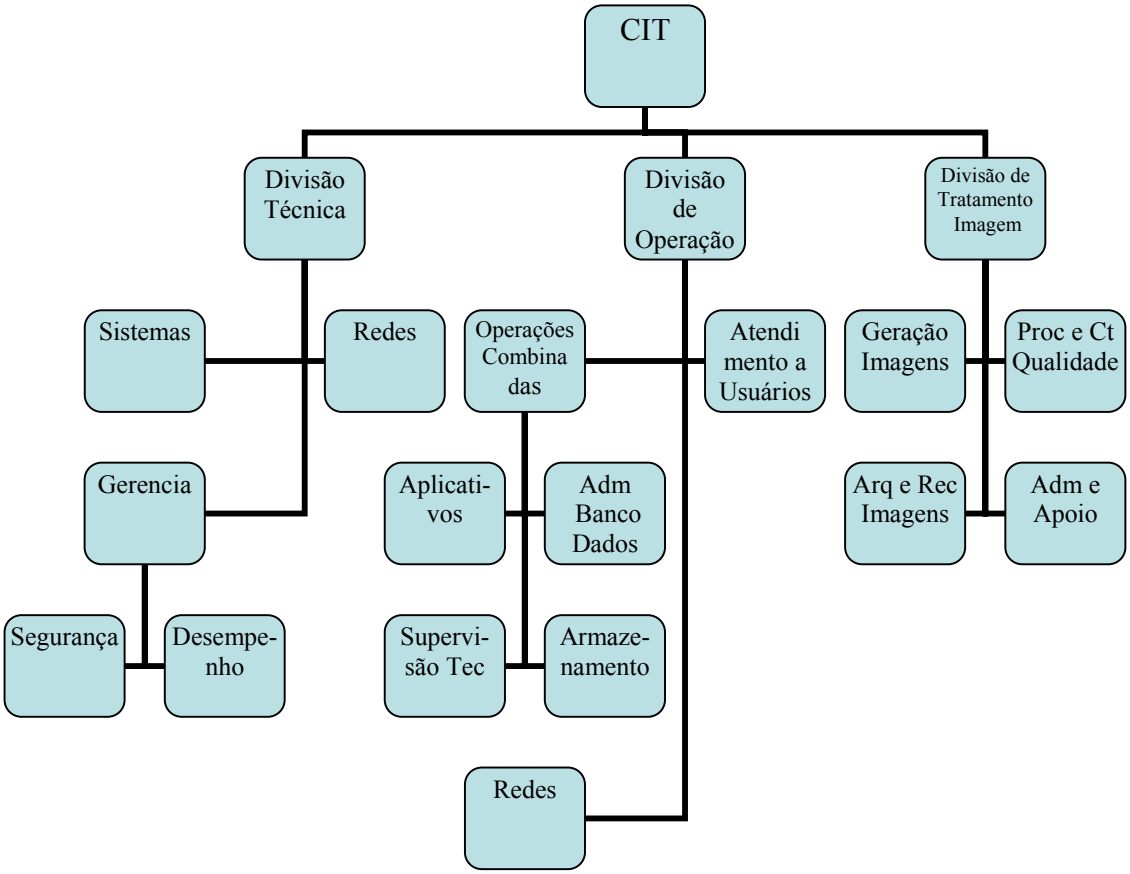


Figura 9 - Organograma CIT

Subordinados ao CIT, sete Centros de Telemática, localizam-se em Porto Alegre, Rio de Janeiro, São Paulo, Manaus, Recife, Campo Grande e Brasília, com uma estrutura de cerca de 70 funcionários com mesmas características dos que estão lotados no CIT.

5.4. UNIVERSO DA PESQUISA

Os funcionários da DMB que participaram da presente pesquisa, para tabulação de dados, foram agrupados segundo os níveis decisórios na sua estrutura de TIC, ou seja, responderam o questionário nos itens PLANEJAMENTO e CONTROLE, 12 funcionários da Seção de TI da Subchefia do ODG e 08 funcionários da Assessoria de TI do ODTI. Responderam nos itens IMPLEMENTAÇÃO e ENTREGA 25 funcionários do CDS e nos itens SUPORTE e MONITORAMENTO 26 do CIT e 14 do CTA de Brasília, totalizando 85 participantes escolhidos segundo a forma descrita a seguir.

A tabela 21 apresenta a relação entre os respondentes da pesquisa, caracterizados segundo suas especialidades no contexto da estrutura e seus setores, bem como a relação dos participantes por total de especialistas.

Tabela 21 - Caracterização dos especialistas relacionados aos setores

Setores / Processos	Estratégio		Execução		
	ODG Gestores	ODTI Gestores	CDS Analistas	CIT Analistas	CTA Analistas
Planejamento Controle	12/15	08/12			
Implementação Entrega			25/168		
Suporte Monitoramento				26/295	14/40

5.5. APLICAÇÃO DA PESQUISA

Inicialmente foi realizada uma reunião com representantes das citadas organizações, onde foi dado conhecimento do foco da pesquisa e do embasamento teórico da aplicabilidade da confiança, de forma a estabelecer facilitadores na estrutura da referida pesquisa. Nessa ocasião foi estabelecido, com esses facilitadores, o compromisso da divulgação aos pesquisados dos conceitos relevantes da confiança bem como da escolha dos que funcionalmente sofreriam o impacto de uma monitoração da confiabilidade da tecnologia da informação.

5.6. RESULTADOS ENCONTRADOS

Do resultado da pesquisa depreende-se que o nível de confiança na área de TI da DMB é médio, representado na figura 10 onde é apresentando áreas onde existem oportunidades de melhoria e outras onde existe a necessidade de medidas corretivas visando a diminuição do risco.

Conforme delimitado no sistema de avaliação, os tópicos com nível alto de confiança devem ser mantidos, os de média confiança devem ser acompanhados e/ou melhorados e os de baixa confiança deverão ser melhorados tendo em vista o conseqüente índice elevado de risco.

As faixas de valores dos níveis de confiança foram multiplicados por 10 para melhor visualização na figura, então o intervalo para os cálculos continuam de [0,1] e para representação de [0, 10].

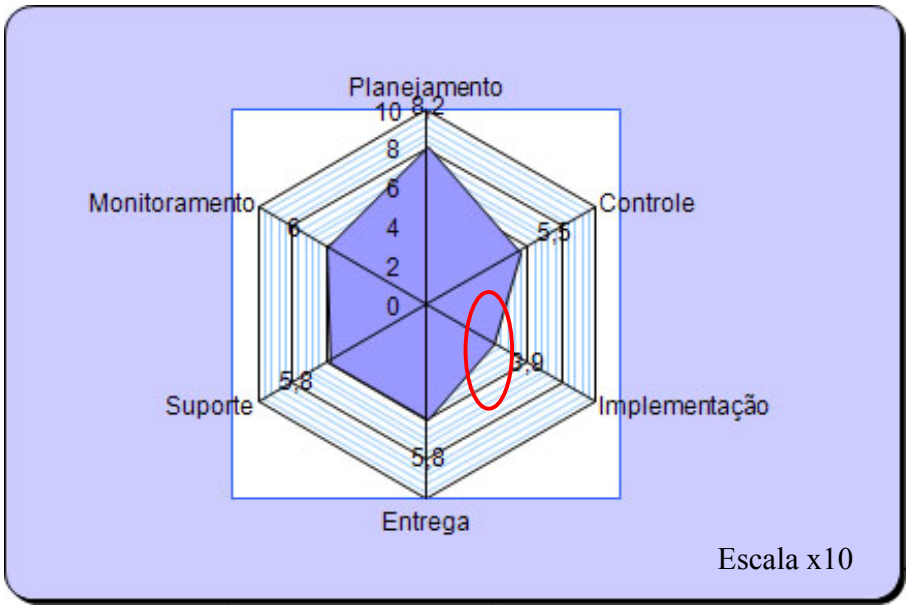


Figura 10 - Resultado Área de TI da DMB

5.6.1. Planejamento

Aprofundando a análise no que se refere ao Planejamento, é mostardo na tabela 22, verifica-se que o desempenho da DMB é elevado alcançando a média de 8,2, com todos os índices posicionados como de nível alto de confiança.

Tabela 22 - Planejamento

ÍNDICE	NÍVEL DE CONFIANÇA	AÇÃO
Todos	Alto	Acompanhamento

Para uma melhor visualização do resultado, é possível a representação gráfica, onde pode-se observar os níveis da confiança alcançados, constante na figura 11.

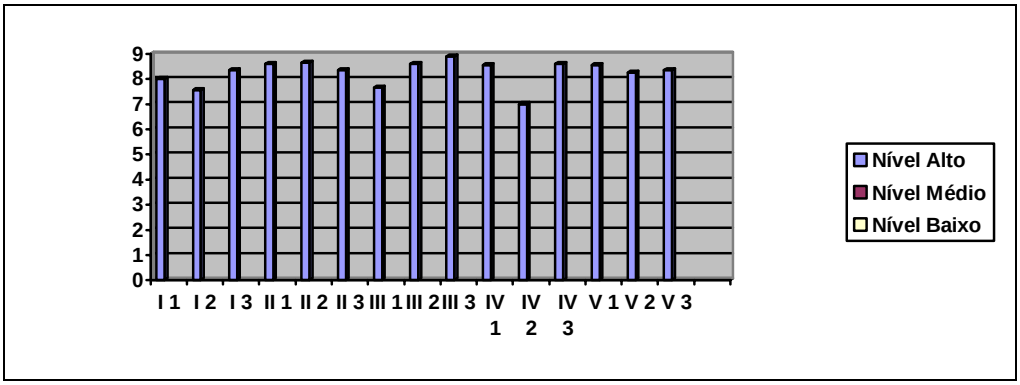


Figura 11 - Resultado Planejamento

5.6.2. Controle

Aprofundando a análise no que se refere ao Controle, verifica-se que o desempenho da DMB é moderado alcançando a média de 5,5, com índices, posicionados nos três níveis de confiança, preponderando o nível médio de confiança conforme é apresentado na tabela 23.

Tabela 23 - Controle

ÍNDICE	NÍVEL DE CONFIANÇA	AÇÃO
VII 3	Alto	Acompanhamento
VI 1,2,3 VII 1,2 VIII 1 IX 1 X 1,2,3	Médio	Acompanhamento e/ou Melhoramento
VIII 2,3 IX 2,3	Baixo	Melhoramento

Os itens que foram verificados constam na tabela 24.

Tabela 24 – Itens verificados do processo Controle

VI. Em relação a Comunicar os Objetivos e a Direção do Gerenciamento	
1.	Número de interrupção de negócio devido à falha de serviço de TI.
2.	Percentual de partes interessadas que entendem a estrutura de controle do negócio.
3.	Percentual das partes interessadas que em conformidade com a política.
VII. Controle os Recursos Humanos de TI, informar:	
1.	Nível de satisfação das partes interessadas com as experiências e habilidades do pessoal de TI.
2.	Rotatividade de pessoal de TI na empresa.
3.	Percentual de pessoas certificadas de acordo com as necessidades de serviço.
VIII. Em relação ao Controle a Qualidade, apontar:	
1.	Percentual das partes interessadas satisfeitas com a qualidade da TI (avaliado segundo a importância).
2.	Percentual de processos de TI formalmente revisados pela garantia de qualidade numa base periódica que atinja as metas e objetivos de qualidade e os objetivos como um todo.
3.	Percentual dos processos em fase de revisão de certificação de qualidade (QA).
IX. Em relação a Avaliação e Gerenciamento dos Riscos de TI, indicar:	
1.	Percentual de objetivos de TI críticos contemplados pela avaliação de risco.
2.	Percentual dos riscos de TI críticos identificados pelos planos de ação desenvolvidos.
3.	Percentual dos planos de ação de controle de risco aprovado para implementação.
X. Em relação ao Controle os Projetos, apontar:	
1.	Percentual de expectativas das reuniões de projetos das partes interessadas (sobre o tempo, sobre os requisitos das

	reuniões e orçamentos – pesados com base na importância).
2.	Percentual de recebimento de projetos revistos após sua implementação.
3.	Percentual de projetos que seguem os padrões e práticas de gerenciamento de projetos.

5.6.3. Implementação

Aprofundando a análise no que se refere à Implementação, verifica-se que o desempenho da DMB é baixo alcançando a média de 3,9, com a maioria dos índices posicionados no nível de confiança baixo, conforme é apresentado na tabela 25.

Tabela 25 - Implementação

ÍNDICE	NÍVEL DE CONFIANÇA	AÇÃO
XI 3 XIV 2	Médio	Acompanhamento e/ou Melhoramento
XI 1,2 XII 1,2 XIII 1,2,3 XIV 1,3 XV 1,2	Baixo	Melhoramento

Os itens verificados podem ser conferidos na tabela 26.

Tabela 26 - Itens verificados no processo Implementação

XI. Em relação a identificação das soluções automatizadas, indicar:	
1.	Número de projetos onde os benefícios declarados não foram alcançados devido às presunções incorretas de viabilidade.
2.	Percentual de estudos de viabilidades interrompidos pelos seus respectivos proprietários de processo.
3.	Percentual de usuários satisfeitos com as funcionalidades apresentadas.

XII. Em relação a aquisição e manutenção de softwares de aplicação, apontar:	
1.	Percentual do número de problemas de produção por aplicação causando visível inatividade.
2.	Porcentagem de usuários satisfeitos com a funcionalidade oferecida.
XIII. Em relação a aquisição e manutenção da infra-estrutura de Tecnologia, informar:	
1.	Percentual de plataformas que estejam em alinhamento com a arquitetura de TI definida bem como os padrões tecnológicos.
2.	Número de processos de negócios críticos sustentados por infra-estrutura obsoleta (ou à deriva de ser).
3.	Número de componentes de infra-estrutura que não sejam mais suportáveis (ou que tendem a não ser suportadas num futuro próximo).
XIV. Em relação ao gerenciamento de mudanças, indicar:	
1.	Percentual de desvios ou erros de dados causados por especificações imprecisas ou avaliação de impacto incompleta.
2.	Percentual de retrabalho de infra-estrutura ou aplicação causado por especificações de mudanças inadequadas.
3.	Percentual de mudanças que seguem os processos de controle de mudança formais.
XV. Em relação a instalação e validação das soluções e Mudanças, informar:	
1.	Percentual de tempo improdutivo do aplicativo (inoperância) ou manutenção de dados causados por teste inadequado.
2.	Percentual de sistemas que atendam os benefícios esperados tais como os medidos pelo processo pós-implementação.

A representação gráfica do resultado do processo de implementação pode ser observado na figura 12.

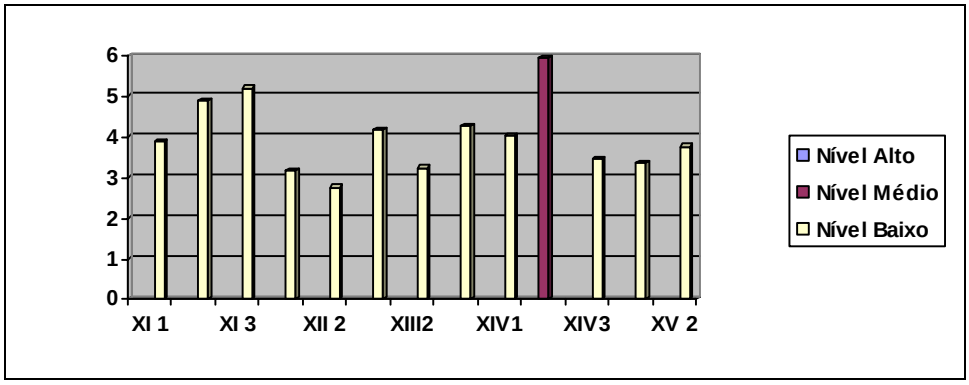


Figura 12 - Resultado Implementação

Nesse caso, para o saneamento dos itens de elevado risco, busca-se a visualização dos Subfatores de nível baixo de confiança, mostrados na figura 13.

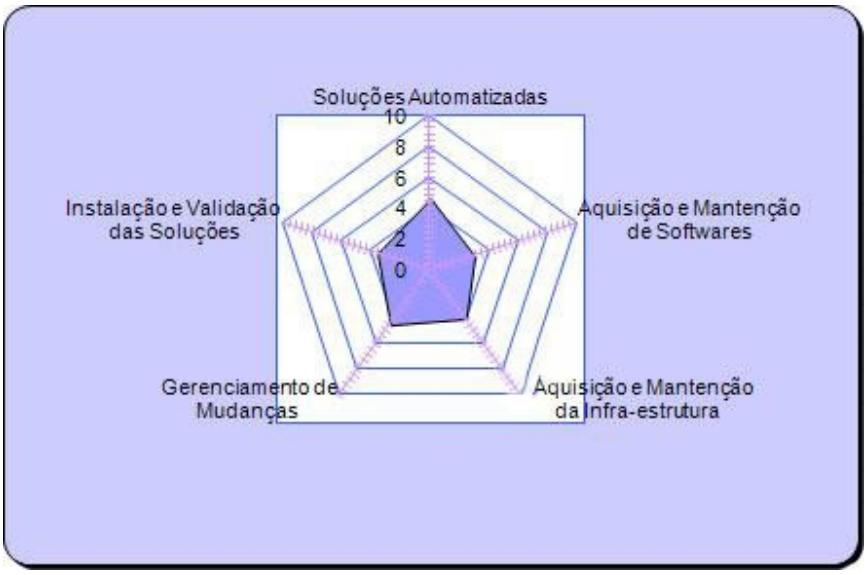


Figura 13 - Resultado Implementação - DMB

5.6.4. Entrega

Aprofundando a análise no que se refere à Entrega, verifica-se que o desempenho da DMB é moderado alcançando a média de 5,8, com índices posicionados nos três

níveis de confiança, preponderando o nível médio de confiança conforme é apresentado na tabela 27.

Tabela 27 - Entrega

ÍNDICE	NÍVEL DE CONFIANÇA	AÇÃO
VIII 1 XX 2	Alto	Acompanhamento
VI 1,3 VII 1,2 XIX 1,2,3 XX 1,3	Médio	Acompanhamento e/ou Melhoramento
VI 2 VII 3 VIII 2	Baixo	Melhoramento

Os itens selecionados para verificação podem ser observados na tabela 28.

Tabela 28 - Itens Entrega

XVI. Em relação a Definição do Gerenciamento dos Níveis de Serviço, indicar:	
1.	Percentual das partes interessadas satisfeitas com os níveis de entrega de serviço acima do esperado.
2.	Percentual dos serviços prestados inexistentes no catálogo.
3.	Percentual de reuniões de revisão de SLA formal com os negócios por ano.
XII. Em relação a aquisição e manutenção de softwares de aplicação, apontar:	
1.	Percentual do número de problemas de produção por aplicação causando visível inatividade.
2.	Porcentagem de usuários satisfeitos com a funcionalidade oferecida.
XIII. Em relação a aquisição e manutenção da infra-estrutura de Tecnologia, informar:	
1.	Percentual de plataformas que estejam em alinhamento com a arquitetura de TI definida bem como os padrões tecnológicos.
2.	Número de processos de negócios críticos sustentados por infra-

	estrutura obsoleta (ou à deriva de ser).
3.	Número de componentes de infra-estrutura que não sejam mais suportáveis (ou que tendem a não ser suportadas num futuro próximo).
XIV. Em relação ao gerenciamento de mudanças, indicar:	
1.	Percentual de desvios ou erros de dados causados por especificações imprecisas ou avaliação de impacto incompleta.
2.	Percentual de retrabalho de infra-estrutura ou aplicação causado por especificações de mudanças inadequadas.
3.	Percentual de mudanças que seguem os processos de controle de mudança formais.
XV. Em relação a instalação e validação das soluções e Mudanças, informar:	
1.	Percentual de tempo improdutivo do aplicativo (inoperância) ou manutenção de dados causados por teste inadequado.
2.	Percentual de sistemas que atendam os benefícios esperados tais como os medidos pelo processo pós-implementação.

5.6.5. Suporte

No que se refere à Suporte, verifica-se que o desempenho da DMB é moderado alcançando a média de 5,8, com índices posicionados nos três níveis de confiança, preponderando o nível médio de confiança conforme é apresentado na tabela 29.

Tabela 29 - Suporte

ÍNDICE	NÍVEL DE CONFIANÇA	AÇÃO
XXI 1	Alto	Acompanhamento
XXI 2,3 XXII 3 XXIII 1,2,3 XXIV 1,2 XXV 1,3	Médio	Acompanhamento e/ou Melhoramento
XXII 1,2 XXV 2	Baixo	Melhoramento

O itens utilizados foram os constantes na tabela 30.

Tabela 30 - Itens do processo Suporte

XXI. Em relação ao Gerenciamento da Central de Serviço e Incidentes, indicar:	
1.	Percentual da satisfação do usuário com a primeira instância do atendimento.
2.	Percentual de incidentes resolvidos dentro do período de tempo estipulado/aceitável.
3.	Percentual da taxa de desistência.
XXII.Em relação ao Gerenciamento da Configuração, informar:	
1.	Percentual de questões de conformidade de negócio causadas pela configuração imprópria dos recursos.
2.	Percentual de desvios identificados entre o repositório de configuração e as configurações dos recursos atuais.
XXIII.Em relação ao Gerencia os Problemas, indicar:	
1.	Número de problemas recorrentes com impacto sobre os negócios.
2.	Percentual de problemas resolvidos dentro do período de tempo programado.
3.	Freqüência de registros ou atualizações de problemas existentes, com base na severidade do problema.
XXIV.Em relação ao Gerenciamento dos Dados, apontar:	
1.	Percentual da satisfação do usuário com a disponibilidade dos dados.
2.	Percentual de incidentes onde os dados sensíveis foram restabelecidos com sucesso após a mídia ter sido disponibilizada.
XXV.Em relação ao Gerenciamento do Ambiente Físico, indicar:	
1.	Percentual do tempo improdutivo conseqüente de incidentes no ambiente físico.
2.	Percentual de incidentes devido às falhas ou violação do ambiente físico.
3.	Percentual da freqüência avaliação de risco físico e revisões.

A representação gráfica do Resultado Suporte pode ser observado na figura 14.

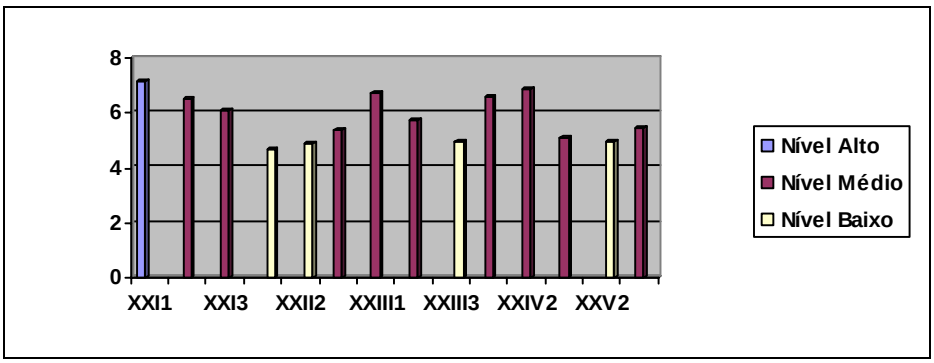


Figura 14 - Resultado Suporte

5.6.6. Monitoramento

Aprofundando a análise no que se refere ao Monitoramento, verifica-se que o desempenho da DMB é moderado alcançando a média de 6,0, com índices posicionados nos três níveis de confiança, preponderando o nível médio de confiança conforme é apresentado na tabela 31.

Tabela 31 - Monitoramento

ÍNDICE	NÍVEL DE CONFIANÇA	AÇÃO
XXVI 1,2 XXIX 1,3	Alto	Acompanhamento
XXVII 1,2,3 XXIX 2 XXX 1,2,3	Médio	Acompanhamento e/ou Melhoramento
XXVIII 1,2,3	Baixo	Melhoramento

Os itens verificados são apresentados na tabela 32.

Tabela 32 – Itens verificados do processo Monitoramento

XXVI.Em relação ao Gerenciamento das Operações, informar:	
1.	Percentual do número de níveis de serviço impactados pelos incidentes operacionais.
2.	Percentual das horas de inoperância imprevistas dos sistemas causadas por incidentes operacionais.
XXVII.Em relação ao Monitoramento e Avaliação do Desempenho de TI, indicar:	
1.	Percentual de questões de conformidade de negócio causadas pela configuração imprópria dos recursos.
2.	Percentual de desvios identificados entre o repositório de configuração e as configurações dos recursos atuais.
XXVIII.Em relação ao Monitoramento e Avaliação do Controle Interno, informar:	
1.	Percentual de falhas no controle principal.
2.	Percentual de iniciativas de melhoramento de controle.
3.	Percentual abrangente das auto-avaliações de controle.
XXIX.Em relação a Assegurar o Cumprimento das Normas Regulamentares,indicar:	
1.	Percentual do custo da não conformidade com a TI, inclusive multas e penalidades.
2.	Percentual de Tempo médio de atraso entre a identificação das questões de conformidades externas.
3.	Percentual Freqüência das revisões de conformidades.
XXX.Em relação a fornecer Governança de TI, indicar:	
1.	Percentual da freqüência dos relatórios da comissão sobre a TI às partes interessadas (inclusive maturidade).
2.	Percentual da freqüência dos relatórios da TI à comissão (inclusive maturidade).
3.	Percentual da freqüência das revisões independentes da conformidade da TI.

Após aplicação da pesquisa e implantação dos resultados no SISGESCOM o resultado final da rodada de confiança pode ser observado na tabela 33.

Tabela 33 - Resultado da DMB

FATOR	MÉDIA	INTERVALO	NIVEL DE CONFIANÇA	RISCO
Planejamento	8,2	0,7<C< 1,0	Alta	Baixo
Controle	5,5	0,5<C<0,69	Média	Médio
Implementação	3,9	0,0<C<0,49	Baixa	Alto
Entrega	5,8	0,5<C<0,69	Média	Médio
Suporte	5,8	0,5<C<0,69	Média	Médio
Monitoramento	6,0	0,5<C<0,69	Média	Médio
Total	5,9	0,5<C<0,69	Média	Médio

5.7. CONSIDERAÇÕES FINAIS

Para a validação, no estudo de caso referente à Organização, foram cumpridas todas as fases previstas na elaboração do Modelo, desde o planejamento até a tabulação dos resultados obtidos após a implantação das respostas às questões formuladas no SIGESCON. O questionário encontra-se disponível no Anexo A, podendo ser relacionado com os resultados apresentados nas tabelas deste Capítulo referentes a cada um dos Itens/Subfatores/Fatores. O resultado apresentado servirá para ativar as medidas necessárias para a melhoria dos Itens considerados de nível médio ou baixo de confiança, com reflexos relevantes ao desempenho da TI na DMB. O caminho a ser seguido no SISGESCON está explicitado no Anexo B. O resultado final é representado em um painel de acompanhamento que proporciona uma visualização da confiabilidade da TI da Organização tem objetico dar apoio à decisão, pois apresenta como um estímulo visual da situação da confiabilidade da TI apontando a situação em relacão a confiança dos macros processos , conforme mostrado na figura 15.

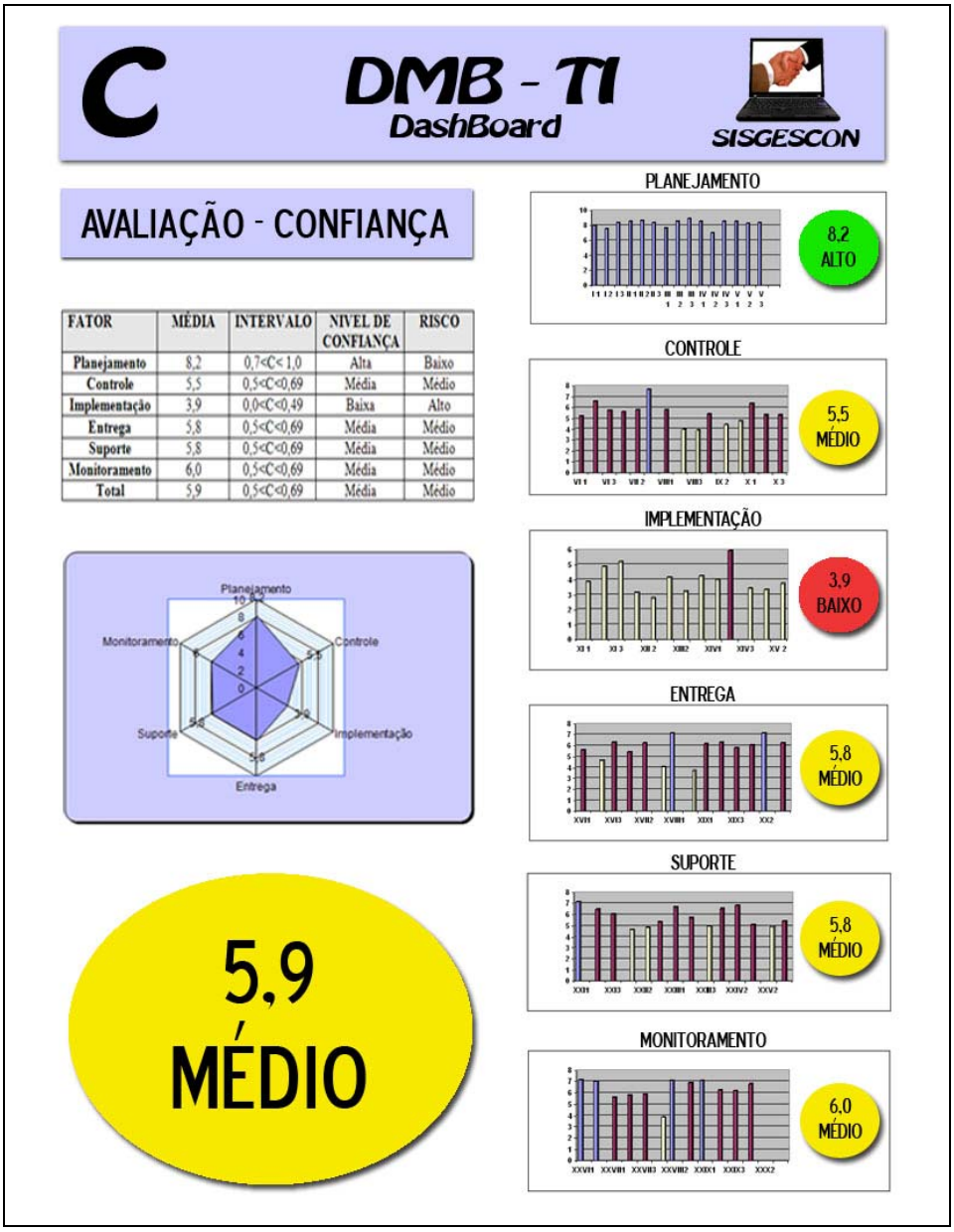


Figura 15 - Painel de Acompanhamento

Para proporcionar uma visão geral da forma gráfica de representação de organizações avaliadas em sua TI segundo os parâmetros de confiança apresentados nessa tese, apresentam-se nas figuras 19, 20 e 22 outras organizações com avaliações de níveis baixo, médio e alto de confiança [5].

As organizações com nível baixo de confiança, conforme figura 16, apresentaram o resultado das métricas em sua totalidade ou em sua maioria abaixo do nível cinco.

Figura 16 - Nível Baixo de Confiança

A figura 17 apresenta o resultado das métricas em sua totalidade ou em sua maioria entre o nível cinco e o nível sete, o que corresponde a Organizações com o nível médio de confiança.

Figura 17 - Nível Médio de Confiança

A partir da avaliação feita na figura 18, nível médio de confiança, pode-se verificar em um nível mais abaixo, mais detalhado, o que estaria causando a diminuição da confiança, ou seja, onde estaria localizado o problema, conforme mostrado na figura 20.

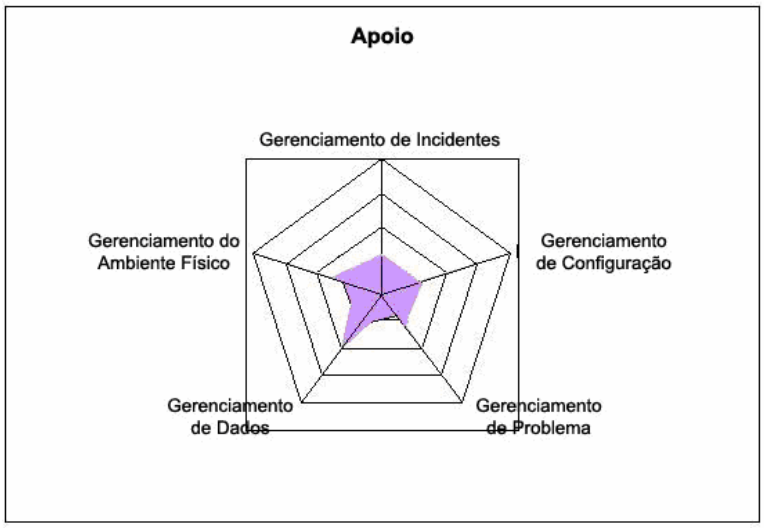


Figura 18 - Categoria Suporte de TI

A representação da figura 21 refere-se a Organizações com nível alto de confiança, pois o resultado das métricas em sua totalidade ou em sua maioria suplanta o nível sete.

Figura 19 - Nível Alto de Confiança

Todos os aspectos de confiança que após a avaliação se encontraram em zona de risco, nível de confiança abaixo de 5, foram relacionados para ações corretivas.

Os demais foram incluídos em uma base de dados como conhecimento útil para soluções futuras.

6. CONCLUSÕES

Ao longo desta tese foram delineados, onde pertinentes, os vínculos entre a gestão da TI e a confiança, dimensionando suas potencialidades e definindo as reais vantagens da harmonia entre estes dois importantes parâmetros.

Em nosso tempo, a TI vem proporcionando às organizações, de todos os ramos de atividade, a possibilidade de ações ágeis e seguras no tratamento das informações, justificando os elevados investimentos que atrai. Para que esses recursos sirvam para a melhoria do desempenho operacional tornam-se necessárias ações integradas, em todos os níveis, das necessidades de negócio com a base tecnológica de apoio.

Essas ações quando concentradas na esfera tática, com visão limitada e como soluções de problemas imediatos ou de pouca abrangência, não agregam valor e por estarem em um nível menos estratégico apresentam pouca abrangência e assim prejudicam a confiança, pois o "apagar incêndios" não contribui para o entendimento da visão e da potencialidade da organização.

Assim a confiança coloca-se como importante ativo na credibilidade das organizações, atraindo investimentos e possibilidades favoráveis nas negociações em geral. Mas tendo em vista ser uma característica marcante da confiança a larga abrangência da sua definição, verificou-se que para o objetivo buscado, a confiança a ser focada no estudo da gestão de tecnologia da informação, se afasta dos conceitos voltados para relacionamentos interpessoais e se aproxima dos direcionados a negócios e prestação de serviços, ou seja, busca a racionalidade deixando de lado aspectos emocionais. A racionalidade traz implícita a possibilidade de medição, de quantificação, ou seja, a possibilidade de ser expressa em números.

Este trabalho apresentou modelos de medição da confiança aplicados a áreas distintas, o que viabilizou a sua medição na gestão da TI. O emprego de ferramenta de qualidade de comprovada utilização, depurada pela associação a requisitos de confiança universalizados pelo uso, respaldou a tese e amparou, como uma solução tecnológica, o

Modelo apresentado, abordando o foco da questão e possibilitando a consecução dos objetivos propostos.

A aplicação do Modelo apresenta a tendência de trazer melhoria por proporcionar um instrumento de controle pertinente e acordado com uma cultura organizacional moderna que impeça o autoritarismo setorial, dificultando os desvios e monitorando o desempenho. Assim sendo, nesse contexto, infere-se o entendimeto de que o rumo seguro está vinculado à confiança que deverá proporcionar resultados altamente desejáveis à gestão, desde que controlado e medido. Então, para as organizações, a criação de um modelo para avaliação do nível de confiança em gestão de TI possibilitará maior eficácia no alinhamento da mesma com a estratégia organizacional, além da diminuição do risco que tanto as ameaça, pois verificou-se que quanto mais confiança menos risco.

Prospectando todas estas potencialidades, verifica-se que o aprofundamento de pesquisa e estabelecimento de novas questões nas áreas de conhecimento relativo a governança e confiança, será relevante para a comunidade científica, por estimular a busca de novas fronteiras do conhecimento.

O Modelo apresenta algumas deficiências dentre as quais destaca-se que trabalha com informações objetivas e subjetivas e nesse último caso, respostas ao questionário, poderá sofrer distorções decorrentes de opiniões pessoais. Ressalta-se que a automatização dos processos envolvidos poderá atenuar esta tendência. Outro fator a ser descrito como uma deficiência é o fato do modelo ser dependente do compromisso e envolvimento dos gestores responsáveis pela TI, sem o que a sua aplicação será limitada a um exercício didático sem reflexo no desempenho da organização.

6.1. SUGESTÕES PARA PESQUISAS FUTURAS

De forma a seguir as tendências que no momento impregnam as áreas de pesquisa, e tendo em vista o poderoso chamamento da confiança e seu amplo aspecto de utilização, pesquisas poderão ser direcionadas, em área tecnológica e relacionadas à possibilidade de medição, abordando dentre outros, os seguintes campos:

a) Elaboração de modelo de confiança baseado em lógica Difusa, Redes Neurais ou um modelo híbrido Fuzzy-Neural

b) Medição da confiança em segurança da informação em aspectos preventivos e de detecção de problemas.

c) Controle da confiança em ambientes virtuais de ensino aprendizagem

7. REFERÊNCIAS

[1] Araújo, M.. Governança em Tecnologia da Informação. 2005. Disponível em http://www.issabrasil.org/artigos_0021.asp. Acesso em: 12 mar. 2006.

[2] Benzi D. M. ; Sousa JR, R. T. ; Bidan, C. ; Mé, L. Gerenciamento da Confiança na Tecnologia da Informação. *Anais do Séptima Conferencia Iberoamericana en Sistemas, Cibernética e Informática: CISCI*, Orlando.2008.

[3] Benzi, D. M. ; De Sousa Jr, R. T. Um Modelo de Confiança Aplicado aos Processos de Gestão da Tecnologia da Informação. *5th International Conference on Information Systems and Technology Management, V CONTECSI*, São Paulo, 2008.

[4] Benzi, D.M., De Sousa Jr, Rafael T., Bidan, C., Mé, L. Model for Trust Within Information Technology Management., *10th International Conference on Enterrise Information Systems, ICEIS* , Barcelona, 2008.

[5] Benzi, D.M., De Sousa Jr, Rafael T. Tratamento de Confiança Aplicado a Gestão de Tecnologia da Informação. *V Simpósio de Excelência em Gestão e Tecnologia, SEGET,* Resende – RJ, 2008..

[6] Benzi, D.M., De Sousa Jr, Rafael T.Medição da Confiança no Contexto dos Processos de Gestão da Tecnologia da Informação. *Revista Militar de Ciëncia e Tecnologia. V.*26, 2008.

[7] Bacharach, M, Gambetta, D. Trust in Signs. *MPIfG Discussion Paper*. Em 2000.http://www.mpi-fg-koeln.mpg.de/pu/mpifg_dp/dp05-8.pdf. Acesso em: 23 ago 2007.

[8] Barton T., Shenkir W., Walker P. *Making Enterprise Risk Management Pay Off and Enterprise Risk Management: Pulling It All Together*. The Institute of Internal Auditors Research Foundation, p.9-11. 2003. Em http://portal.acm.org/ Acesso em: 15 nov. 2007.

[9] Blomqvist, K. e Stahle, P. Trust in Technology Partnerships. *Trust in Knowledge Management Systems in Organizations*. Idea Group Publishing. USA., 173 - 199 2004. Em http://portal.acm.org/ Acesso em: 27 out. 2007.

[10] Burn, J.M.e Szeto, C. A Comparison of the Views of Business and IT Management on Success Factors for Strategic Alignment. Information & Management, V.37, p.197 - 216 .2000. Em http://portal.acm.org/citation.cfm?id=969799.969808. Em http://portal.acm.org/ Acesso em: 6 jun. 2005.

[11] Campomar, M. C. Do Uso de "Estudo de Caso" Em Pesquisas para Dissertações e Teses em Administração.*Revista de Administração, USP*, v. 26, n. 3, p. 95-97. 1991.

[12] Carbone, M. Carbone, M. N. and Sassone, V. A formal Model for Trust in Dynamic Networks.2003. Em http://www.di.inf.pucrio.br. Acesso em: 8 mai. 2005.

[13] Capra, L. Engineering Human Trust in Mobile System Collaborations. 2003.Em http://www-di.inf.puc-rio.br/~endler/courses/Mobile/Monografias/05/Guilherme-Mono.pdf. Acesso em: 2 abr. 2007.

[14] Couch, L.L., Jeffrey, A.M., & Jones, W.H. Measuring Level of Trust. *Journal of Personality Assessment*, V.67, P.305-323.1996.

[15] COBIT, Control Objectives, Management Guidelines Maturity Models. IT Governance Institute. 2005.

[16] COSO. Executive Summary, Enterprise Risk Management: Integrated Framework, The Comitee of Sponsoring Organizations. 2004.

[17] Davenport, E. e McLaughlin,L. Interpersonal Trust in Online Partnerships: The Challenge of Representation. Trust in Knowledge Management Systems in Organizations. Idea Group Publishing. USA. 2004. Em http://portal.acm.org. Acesso em: 17 set 2006.

[18] De Haes S., Van Grembergen W. IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. *38th Hawaii International Conference on System Sciences.* 2005.Em http://doi.ieeecomputersociety.org. Acesso em: 5 mai 2005.

[19] Dias, J. S. Confiança no Documento Eletrônico. Tese de Doutorado. Universidade Federal de Santa Catarina. 2004.

[20] Dodgson, M. Learning, Trust and Interfirm Technological Linkages: Some Theoretical Associations. London: Routledge, 1993.

[21] Domenico, S. M. R. e Macri, M. Administração geral, confiança e fidelização de clientes: um estudo em serviços aéreos.2005. Em http://www.ead.fea.usp.br/Semead/8semead/resultado/trabalhosPDF/267.pdf. Acesso em: 29 jul 2006.

[22] Duffy, J. IT/Business Alignment: Is it an Option or is it Mandatory? IDC Document.2003.Em http://archive.bitacenter.com/2003/proceedings/ bITa%20Report%20from%20IDC.pdf. Acesso em: 10 mar 2008.

[23] Falcone, R. e Castelfranchi, C.A Belief-Based Model of Trust. *Trust in Knowledge Management Systems in Organizations*. Idea Group Publishing. USA. 2004.

[24] Fukuyama, F. *Confiança: As Virtudes Sociais e a Criação da Prosperidade*. Rocco, Rio de Janeiro. 1996

[25] Gambetta, D. *Trust: Making and Breaking Cooperative Relations.* Oxford Blackwell.1988.

[26] Gambetta, Diego.Can We Trust Trust? *Trust: Making and Breaking Cooperative Relations, Electronic Edition*. University of Oxford, Department of Sociology chapter 13, P. 213-237.2000.

[27] Goffee, N., Kim, S. H. Greenpass: Decentralized, PKI-based Authorization for Wireless LANs. *3rd Annual Public Key Infrastructure Research and Development Workshop*, *NIST*. April 12-14, 2004. Publicação NISTIR 7122, 2004.

[28] Grandison, T., Sloman. M. *A Survey of Trust in Internet Applications*. IEEE Communications Surveys. 2000. http://www.comsoc.org/livepubs/surveys/public/2000/dec/index.html. Acesso em: 22 out 2007.

[29] Grandison, T. W. A. Trust Specification and Analysis for Internet Applications. PhD thesis. Imperial College of Science, Technology and Medicine University of London. 2003.Em http://citeseer.ist.psu.edu/grandison01trust.html. Acesso em: 11 nov 2006.

[30] Grassi, R.A.Em busca da noção evolucionária (neo-schumpeteriana) do auto-interesse dos agentes: uma contribuição a partir da literatura sobre cooperação interfirmas. *Revista Análise Econômica*. Faculdade de Ciências Econômicas, UFRGS. 2004.

[31] Harisalo, R. e Stenvall, J.Trust as Capital: The Foundation of Management. Trust in Knowledge Management Systems in Organizations. Idea Group Publishing. 2004. Em http://portal.acm.org. Acesso em: 3 set 2006.

[32] Harisalo, R. e Stenvall, J.Trust in Knowledge Management Systems in Organizations. Idea Group Publishing. Em http://portal.acm.org. Acesso em: 21 mai 2008.

[33] Henderson, J.C., & Venkatraman, N. Strategic Alignment: Leveraging Information Technology for Transforming Organizations. *IBM Systems Journal,* V. 32. 1993.

[34] Hoppen, N., Lapointe, L., Moreau, E. Avaliação de Artigos de Pesquisa em Sistemas de Informação: Proposta de um Guia. *ENANPAD*, 1997.

[35] Huotari, M.L. e Iivonen, M. Managing Knowledge-Based Organizations Through Trust. Trust in Knowledge Management Systems in Organizations. Idea Group Publishing, USA. 2004. Em http://portal.acm.org. Acesso em: 12 jub 2006.

[36] Iivonen, M. Trust Building as a Management Strategy. Trust in Knowledge Management Systems in Organizations. Idea Group Publishing. 2004. Em http://portal.acm.org. Acesso em: 16 ago 2007.

[37] Jones, S. TRUST-EC: Requirements for Trust and Confidence in E-Commerce. European Commission, Joint Research Centre. V. 43, P.81- 87 . 1999. http://portal.acm.org. Acesso em: 13 nov 2004.

[38] Keen, P. G. W., Balance. C., Chan. S., Schrump. S. Electronic Commerce Relationships: Trust by Design.Prentice-Hall.1999.Em http://portal.acm.org. Acesso em: 17 mar 2004.

[39] Luftman, J., & Brier, T. Achieving and Sustaining Business-IT Alignment. California Management Review, V.42, N.1, P. 109–122. 1999. Em http://www.emeraldinsight.com/Insight/ViewContentServlet?Filename=/published/emeraldfulltextarticle/pdf/1310110603_ref.html. Acesso em: 11 jul 2006.

[40] Lyons, B. e Mehta. J. Contracts, Opportunism and Trust: Self-Interest and Social Orientation. *Cambridge Journal of Economics*, V.l. 21. 1997.

[41] Manchala. D. W. Trust Metrics, Models and Protocols for Electronic Commerce Transactions. 1*8th International Conference on Distributed Computing Systems*. Holanda. Amsterdan.1998.

[42] Manchala. D. W. E-Commerce Trust Metrics and Models. *IEEE, Internet Computing*, P.36-44. 2000.

[43] Mandelli, A.Self-Organization and New Hierarchies in Complex Evolutionary Value Networks. Trust in Knowledge Management Systems in Organizations. Idea Group Publishing. 2004. Em http://portal.acm.org Acesso em: 10 set 2007.

[44] Mandelli, A. (2004). Exploring the Origins of New Transaction Costs in Connected Societies. Trust in Knowledge Management Systems in Organizations. Idea Group Publishing. 2004. Em http://portal.acm.org. Acesso em: 4 out 2006.

[45] McKnight, D. H. & Chervany, N. L. Trust Building Processes In Organizational Relationships. *Annual Meeting Decision Sciences Institute*, 2: 751-753., November 20-22, Boston, MA.1995.

[46] Marsh, Stephen Paul. Formalizing Trust as a Computational Concept, University of Stirling, Department of Computing Science and Mathematics.Doctorate Thesis. April 1994.

[47] Mayer. R. C., Davis. J. H., Schoorman. D. F. An Integration Model of Organizational Trust. Academy of Management. Academy of Management Review. Mississipi, V. 20, P.709-734.July 1995.

[48] Öörni, K., Kaleva, S., Hirvasniemi, S. e Kortelainem, T.Usability of Websites Contributing to Trust in E-commerce.Trust in Knowledge Management Systems in Organizations. Idea Group Publishing. 2004. Em http://portal.acm.org

[49] Pillatt. F. R. Um Modelo para o Tratamento de Confiança sobre Transações de e-Business. Dissertação de Mestrado. Universidade Federal de Campina Grande 2002. Em http://www.dsc.ufcg.edu.br/~copin/pessoas /alunos/htms/ FabioRobertoPillatt.htm. Acesso em: 17 set 2007.

[50] Pozzebon, M. Freitas, H. Pela Aplicabilidade – Com Maior Rigor Científico Dos Estudos De Caso Em Sistema De Informações. *ENANPAD*, 21, Rio das Pedras.2002.

[51] Riegelsberger, J. et al.The Mechanics of Trust: A Framework For Research and Design. *International Journal on Human-Computer Studies* V. 62, P. 381–422, 2005.

[52] Robinson, R., Jackson, E. Is Trust in Others Declining in America?: An Age-Period-Cohort Analysis. Social Science Research, V.30, P.117-145, 2001.

[53] Rodrigues, C. A. P.Governando as Surpresas. 2006. http://www.informationweek.com.br. Acesso em: 15 set 2007.

[54] Sambamurthy, V., Zmud R.W. Arrangements for Information Technology Governance: A Theory Of Multiple Contingencies. *MIS Quarterly,* V.. 23, n. 2, pp. 261-290. 1999.

[55] Santos, G. N. P.Um Modelo para o Gerenciamento de Confiança em Dispositivos Móveis. Rio de Janeiro. PUC, 2005. Em http://www.di.inf.pucrio.br/~endler/courses/Mobile/ Monografias/05/Guilherme-Mono.pdf.. Acesso em: 9 out 2006.

[56] Smaczny, T.Is an alignment between business and Information Technology the appropriate paradigm to manage IT in today's organizations? Management Decisions, V.39, N.10.2001.

[57] Sonnenwald, D. H. Managing Cognitive and Affective Trust in the Conceptual R&D Organization. Trust in Knowledge Management Systems in Organizations. Idea Group Publishing. USA.2004. Em http://portal.acm.org. Acesso em: 21 mar 2006.

[58] Van Grembergen, W.The Balanced Scorecard and IT Governance. *Information Systems Control Journal*, Volume 2.2000.

[59] Wang, Y.D., Emurian, H.H. (2005). An Overview of Online Trust: Concepts, Elements, and Implications. Computers in Human Behavior V. 21, P.. 105–125, 2005.

[60] Webb, B. P., Pollard C., Ridley, G.. Attempting to Define IT Governance: Wisdom or Folly? In: 39th Hawaii International Conference on System Sciences. . 2006. Disponível em http://doi.ieeecomputersociety.org. Acesso em: 11 nov 2007.

[61] Weill, P., Ross J. W. IT. Governance - How Top Performers Manage IT Decision Rights for Superior Results. São Paulo, Makron.Books do Brasil, 2006.

ANEXOS

ANEXO A – COLETA DE INFORMAÇÕES SOBRE OS PROCESSOS DE TI

Anexo A.1 – Planejamento

1. PLANEJAMENTO	

I. Em relação Plano Estratégico de TI, informar:		Nota
1.	O percentual dos objetivos de TI no plano estratégico de TI que sustentam o plano estratégico de negócio.	Selecione...
2.	O percentual dos projetos de TI no portfólio executivo de projeto de TI que pode ser diretamente traçado de volta para o plano tático de TI.	Selecione...
3.	O percentual de atraso entre a atualização do plano estratégico de TI e a atualização do plano tático de TI.	Selecione...

II. Em relação a Arquitetura da Informação, indicar:		Nota
1.	O percentual de elementos de dados redundantes/duplicados.	Selecione...
2.	O percentual de aplicações em desconformidade com a arquitetura da informação.	Selecione...
3.	A freqüência das atividades de validação dos dados.	Selecione...

III. Em relação a Direção da Tecnologia, indicar:		Nota
1.	Número de desvios do plano de infra-estrutura de tecnologia.	Selecione...
2.	Freqüência da revisão/atualização do plano de infra-estrutura de tecnologia.	Selecione...
3.	Número de plataformas de tecnologia por função dentro da empresa.	Selecione...

IV. Em relação aos Processos de TI, Organização e Relacionamento,informar:		Nota
1.	Percentual de funções com descrições de autoridades e posições documentadas.	Selecione...
2.	Número de unidades/processos de negócios não suportados pela TI da organização, mas que deveriam ser suportados, de acordo com a estratégia.	Selecione...

3.	Número de núcleos das atividades de TI fora da TI da organização que não são aprovados ou submetidos aos padrões organizacionais de TI.	Selecione...

V. Em relação ao Gerenciamento do Investimento de TI, apontar:		Nota
1.	Percentual da unidade de custo dos serviços de TI distribuídos reduzidos.	Selecione...
2.	Percentual de desvio do valor orçamentário comparado com o orçamento total.	Selecione...
3.	Percentual dos gastos com a TI expressos por indexadores de valor de negócios (por exemplo, vendas/serviços crescem devido ao aumento da conectividade)	

Anexo A.2 – Controle

2. CONTROLE	

VI. Em relação a Comunicar os Objetivos e a Direção do Gerenciamento		Nota
1.	Número de interrupção de negócio devido à falha de serviço de TI.	3
2.	Percentual de partes interessadas que entendem a estrutura de controle do negócio.	4
3.	Percentual das partes interessadas que em conformidade com a política.	5

VII. Controle os Recursos Humanos de TI, informar:		Nota
1.	Nível de satisfação das partes interessadas com as experiências e habilidades do pessoal de TI.	6
2.	Rotatividade de pessoal de TI na empresa.	10
3.	Percentual de pessoas certificadas de acordo com as necessidades de serviço.	1

VIII. Em relação ao Controle a Qualidade, apontar:		Nota
1.	Percentual das partes interessadas satisfeitas com a qualidade da TI (avaliado segundo a importância).	Selecione...
2.	Percentual de processos de TI formalmente revisados pela garantia de qualidade numa base periódica que atinja as metas e objetivos de qualidade e os objetivos como um todo.	Selecione...
3.	Percentual dos processos em fase de revisão de certificação de qualidade (QA).	Selecione...

IX. Em relação a Avaliação e Gerenciamento dos Riscos de TI, indicar:		Nota
1.	Percentual de objetivos de TI críticos contemplados pela avaliação de risco.	Selecione...
2.	Percentual dos riscos de TI críticos identificados pelos planos de ação desenvolvidos.	Selecione...
3.	Percentual dos planos de ação de controle de risco aprovado para implementação.	Selecione...

X. Em relação ao Controle os Projetos, apontar:	Nota

1.	Percentual de expectativas das reuniões de projetos das partes interessadas (sobre o tempo, sobre os requisitos das reuniões e orçamentos – pesados com base na importância).	Selecione...
2.	Percentual de recebimento de projetos revistos após sua implementação.	Selecione...
3.	Percentual de projetos que seguem os padrões e práticas de gerenciamento de projetos.	Selecione...

Anexo A.3 – Implementação

3. IMPLEMENTAÇÃO	

XI. Em relação a identificação das soluções automatizadas, indicar:		Nota
1.	Número de projetos onde os benefícios declarados não foram alcançados devido às presunções incorretas de viabilidade.	Selecione...
2.	Percentual de estudos de viabilidades interrompidos pelos seus respectivos proprietários de processo.	Selecione...
3.	Percentual de usuários satisfeitos com as funcionalidades apresentadas.	Selecione...

XII. Em relação a aquisição e manutenção de softwares de aplicação, apontar:		Nota
1.	Percentual do número de problemas de produção por aplicação causando visível inatividade.	Selecione...
2.	Porcentagem de usuários satisfeitos com a funcionalidade oferecida.	Selecione...

XIII. Em relação a aquisição e manutenção da infra-estrutura de Tecnologia, informar:		Nota
1.	Percentual de plataformas que estejam em alinhamento com a arquitetura de TI definida bem como os padrões tecnológicos.	Selecione...
2.	Número de processos de negócios críticos sustentados por infra-estrutura obsoleta (ou à deriva de ser).	Selecione...
3.	Número de componentes de infra-estrutura que não sejam mais suportáveis (ou que tendem a não ser suportadas num futuro próximo).	Selecione...

XIV. Em relação ao gerenciamento de mudanças, indicar:		Nota
1.	Percentual de desvios ou erros de dados causados por especificações imprecisas ou avaliação de impacto incompleta.	Selecione...
2.	Percentual de retrabalho de infra-estrutura ou aplicação causado por especificações de mudanças inadequadas.	Selecione...
3.	Percentual de mudanças que seguem os processos de controle de mudança formais.	Selecione...

XV. Em relação a instalação e validação das soluções e Mudanças, informar:		Nota
1.	Percentual de tempo improdutivo do aplicativo (inoperância) ou manutenção de dados causados por teste inadequado.	Selecione...
2.	Percentual de sistemas que atendam os benefícios esperados tais como os medidos pelo processo pós-implementação.	Selecione...

Anexo A.4 – Entrega

4. ENTREGA

XVI. Em relação a Definição do Gerenciamento dos Níveis de Serviço, indicar:		Nota
1.	Percentual das partes interessadas satisfeitas com os níveis de entrega de serviço acima do esperado.	Selecione...
2.	Percentual dos serviços prestados inexistentes no catálogo.	Selecione...
3.	Percentual de reuniões de revisão de SLA formal com os negócios por ano.	Selecione...

XVII. Em relação ao Gerenciamento dos Serviços de Terceirizados, indicar:		Nota
1.	Percentual de queixas de usuário devido aos serviços contratados.	Selecione...
2.	Percentual de fornecedores que atendam claramente os requisitos definidos e níveis de serviço.	Selecione...
3.	Percentual dos fornecedores sujeitos ao monitoramento.	Selecione...

XVIII. Em relação a Assegurar o Serviço Contínuo:		Nota
1.	Percentual de horas perdidas por usuários por mês devido inoperância de sistema (outages) não planejada.	Selecione...
2.	Percentual de processo de negócios críticos confiados à TI não contemplados no plano de continuidade de TI.	Selecione...

XIX. Em relação garantir a Segurança dos Sistemas, apontar:		Nota
1.	Percentual de reputação negativa dos incidentes de conhecimento público.	Selecione...
2.	Percentual de sistemas cujos requisitos de segurança não estão de acordo.	Selecione...
3.	Percentual de violações na distribuição dos deveres.	Selecione...

XX. Em relação fornecer Treinamento aos Usuários:		Nota
1.	Percentual de chamadas no centro de atendimento devido a falta de treinamento de usuário.	Selecione...
2.	Percentual de partes interessadas satisfeitas com o treinamento recebido.	Selecione...

3.	Percentual de Atraso no tempo entre a identificação da necessidade de treinamento e a sua respectiva efetivação.	Selecione...

Anexo A.5 – Suporte

5. SUPORTE	

XXI. Em relação ao Gerenciamento da Central de Serviço e Incidentes, indicar:		Nota
1.	Percentual da satisfação do usuário com a primeira instância do atendimento.	Selecione...
2.	Percentual de incidentes resolvidos dentro do período de tempo estipulado/aceitável.	Selecione...
3.	Percentual da taxa de desistência.	Selecione...

XXII.Em relação ao Gerenciamento da Configuração, informar:		Nota
1.	Percentual de questões de conformidade de negócio causadas pela configuração imprópria dos recursos.	Selecione...
2.	Percentual de desvios identificados entre o repositório de configuração e as configurações dos recursos atuais.	Selecione...
3.	Percentual de licenças adquiridas e não contabilizadas no rol do repositório.	Selecione...

XXIII.Em relação ao Gerencia os Problemas, indicar:		Nota
1.	Número de problemas recorrentes com impacto sobre os negócios.	Selecione...
2.	Percentual de problemas resolvidos dentro do período de tempo programado.	Selecione...
3.	Freqüência de registros ou atualizações de problemas existentes, com base na severidade do problema.	Selecione...

XXIV.Em relação ao Gerenciamento dos Dados, apontar:		Nota
1.	Percentual da satisfação do usuário com a disponibilidade dos dados.	Selecione...
2.	Percentual de incidentes onde os dados sensíveis foram restabelecidos com sucesso após a mídia ter sido disponibilizada.	Selecione...

XXV.Em relação ao Gerenciamento do Ambiente Físico, indicar:		Nota
1.	Percentual do tempo improdutivo conseqüente de incidentes	Selecione...

	no ambiente físico.	
2.	Percentual de incidentes devido às falhas ou violação do ambiente físico.	Selecione...
3.	Percentual da freqüência avaliação de risco físico e revisões.	Selecione...

Anexo A.6 – Monitoramento

6. MONITORAMENTO

XXVI.Em relação ao Gerenciamento das Operações, informar:		Nota
1.	Percentual do número de níveis de serviço impactados pelos incidentes operacionais.	Selecione...
2.	Percentual das horas de inoperância imprevistas dos sistemas causadas por incidentes operacionais.	Selecione...

XXVII.Em relação ao Monitoramento e Avaliação do Desempenho de TI, indicar:		Nota
1.	Percentual da satisfação das entidades de gerenciamento e governança com o relatório de desempenho.	Selecione...
2.	Percentual das ações de aperfeiçoamento segmentadas pelas atividades de monitoramento.	Selecione...
3.	Percentual de processos críticos monitorados.	Selecione...

XXVIII.Em relação ao Monitoramento e Avaliação do Controle Interno, informar:		Nota
1.	Percentual de falhas no controle principal.	Selecione...
2.	Percentual de iniciativas de melhoramento de controle.	Selecione...
3.	Percentual abrangente das auto-avaliações de controle.	Selecione...

XXIX.Em relação a Assegurar o Cumprimento das Normas Regulamentares,indicar:		Nota
1.	Percentual do custo da não conformidade com a TI, inclusive multas e penalidades.	Selecione...
2.	Percentual de Tempo médio de atraso entre a identificação das questões de conformidades externas.	Selecione...
3.	Percentual Freqüência das revisões de conformidades.	Selecione...

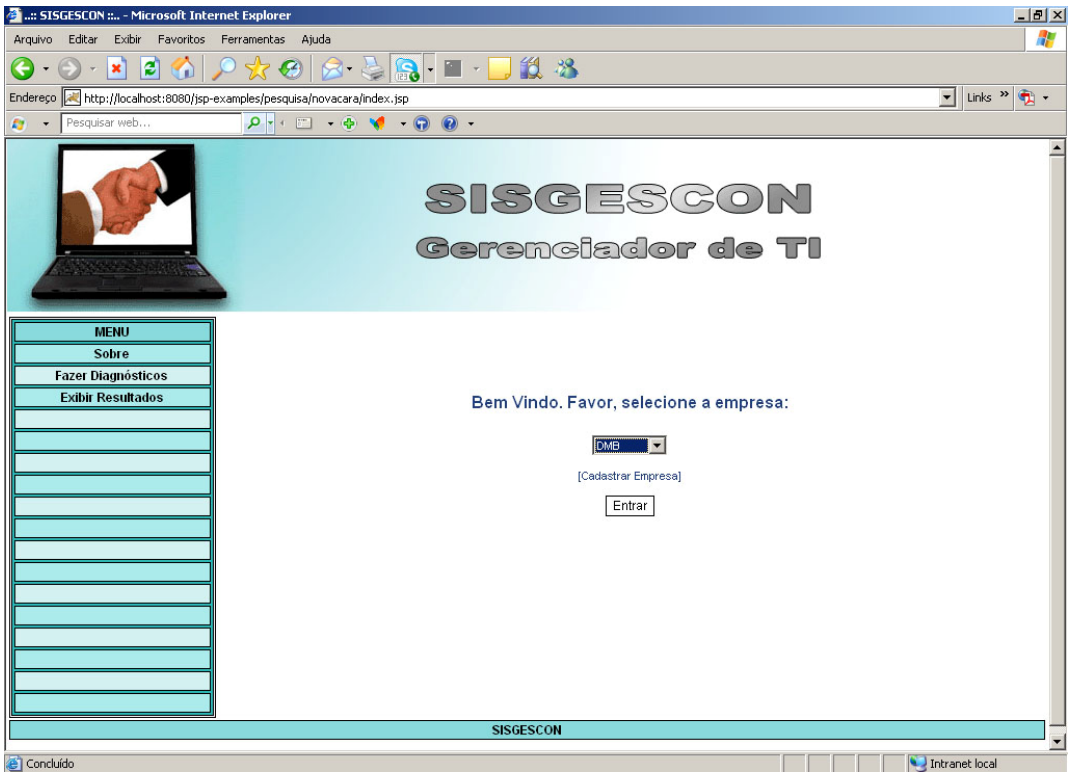
XXX.Em relação a fornecer Governança de TI, indicar:		Nota
1.	Percentual da freqüência dos relatórios da comissão sobre a TI às partes interessadas (inclusive maturidade).	Selecione...
2.	Percentual da freqüência dos relatórios da TI à comissão (inclusive maturidade).	Selecione...

3.	Percentual da freqüência das revisões independentes da conformidade da TI.	Selecione...

ANEXO B – SISTEMA GERENCIAMENTO DE TI BASEADO EM CONFIANÇA

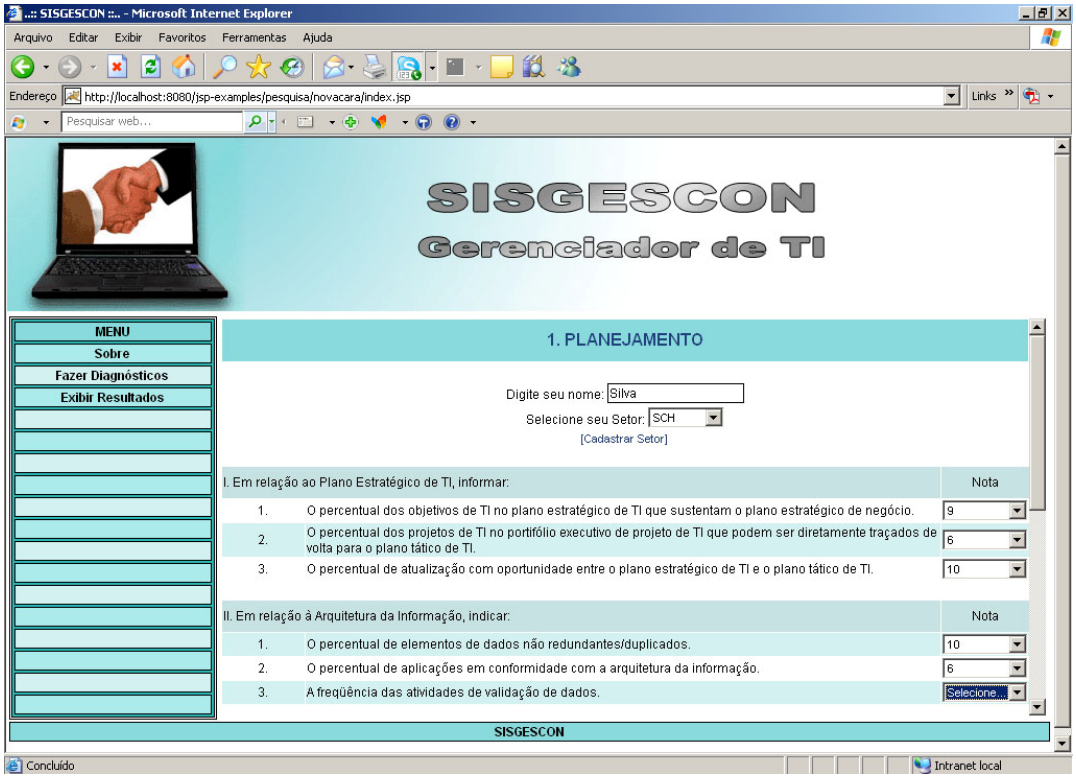
Anexo B.1 – Tela de Entrada

Esta tela possibilita o acesso ao sistema e iniciar a avaliação com o cadastramento da organização/empresa a ser avaliada.



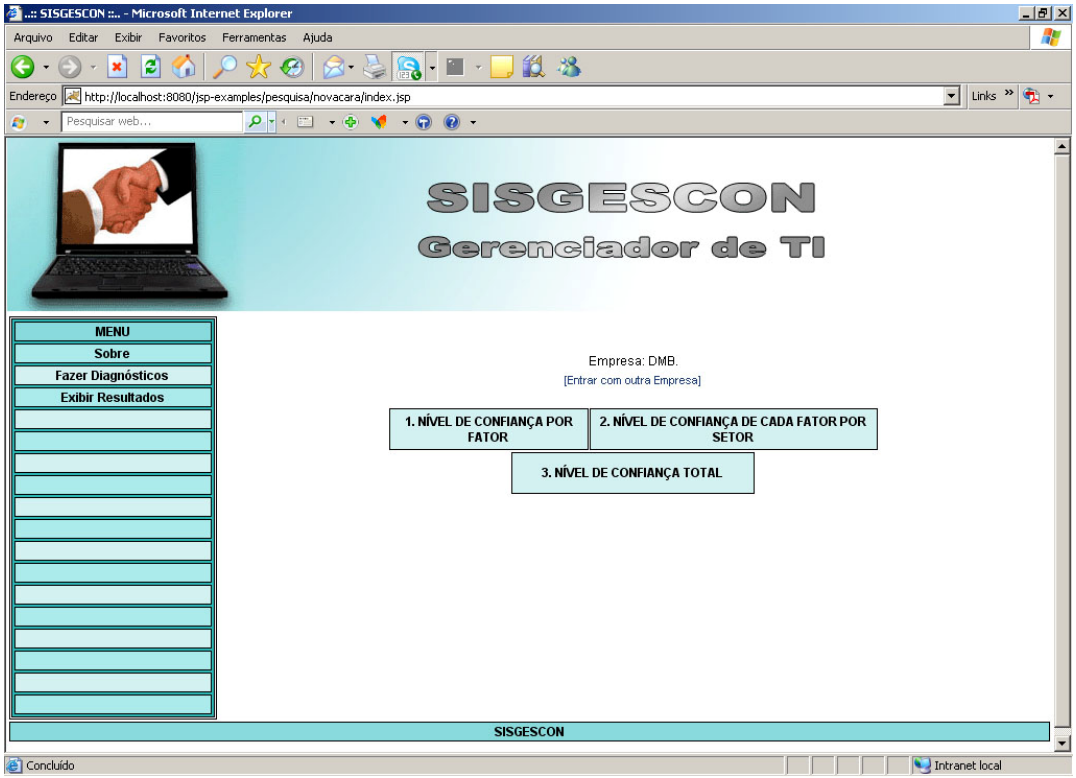
Anexo B.2 – Tela de Acesso à Pesquisa (questionário)

Esta tela possibilita acesso ao questionário, exibindo funcionalidades que permitem o cadastramento do gestor/usuário, seu setor, bem como a atribuição de valores de zero a dez em cada item avaliado.



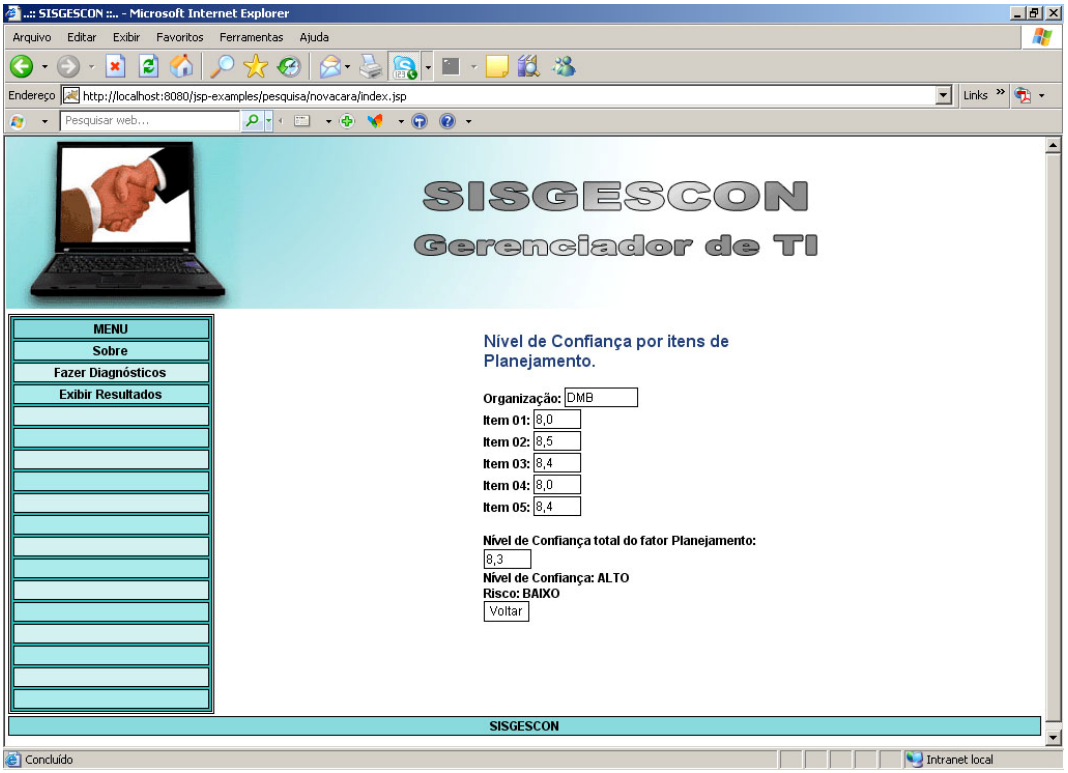
Anexo B.3 – Tela de Acesso aos Resultados

Após o processamento da avaliação da confiança, esta tela possibilita acesso aos resultados, mediante seleção de resultados totais por fator, resultados de cada fator por setor e resultado total.



Anexo B.4 – Tela de Acesso aos Resultados Totais por Fator

Após a seleção de resultados totais por fator na tela do Anexo B.3, os valores poderão ser acessados conforme mostra a figura abaixo, no caso, como exemplo, o fator Planejamento.

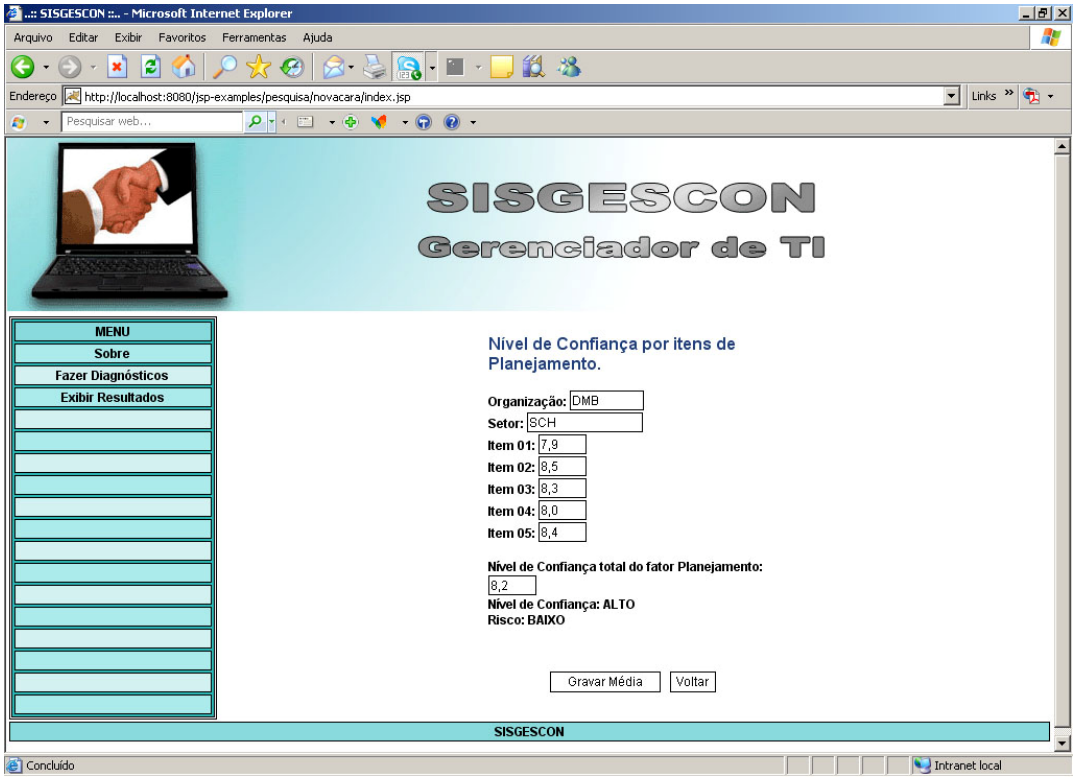


Anexo B.5 – Tela de Acesso aos Resultados de Cada Fator por Setor

Após a seleção de resultados de cada fator por setor na tela do Anexo B.3, os valores poderão ser acessados selecionando o fator Planejamento, Controle, Implementação, Entrega, Suporte ou Monitoramento.

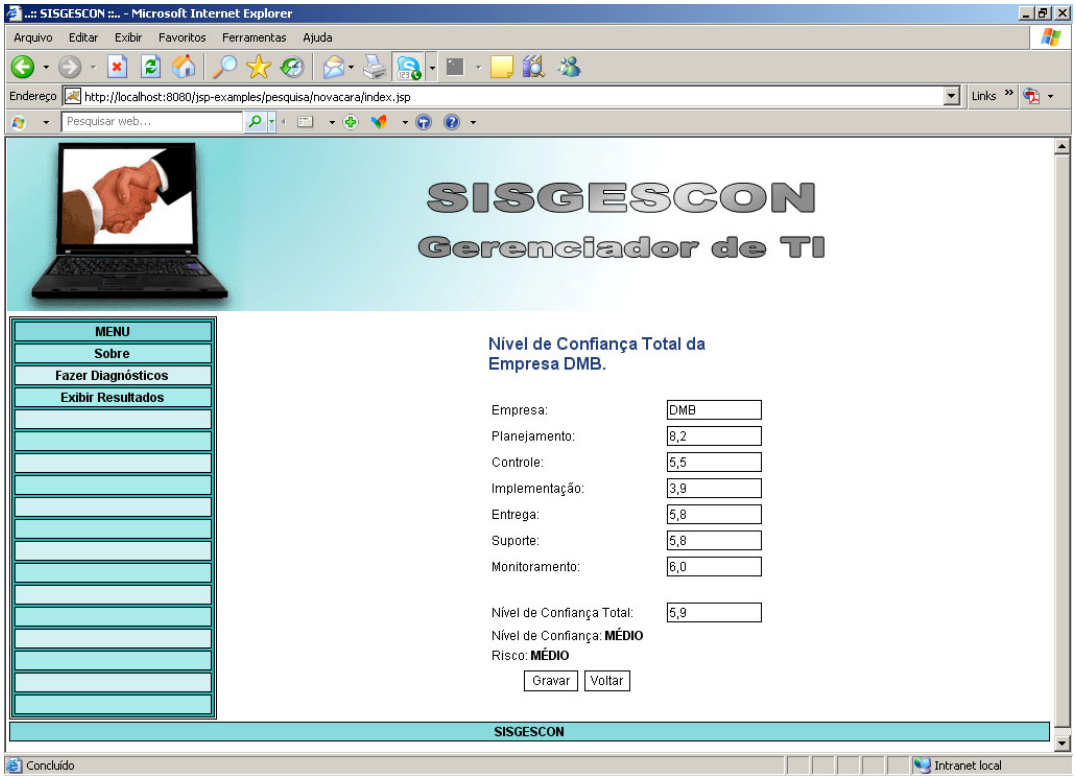
Anexo B.6 – Tela de Acesso aos Resultados de Cada Fator por Setor

Após a seleção de resultados de um fator na tela do Anexo B.5, neste caso como exemplo o fator planejamento do setor Subchefia, os valores poderão ser acessados conforme mostra a figura abaixo.



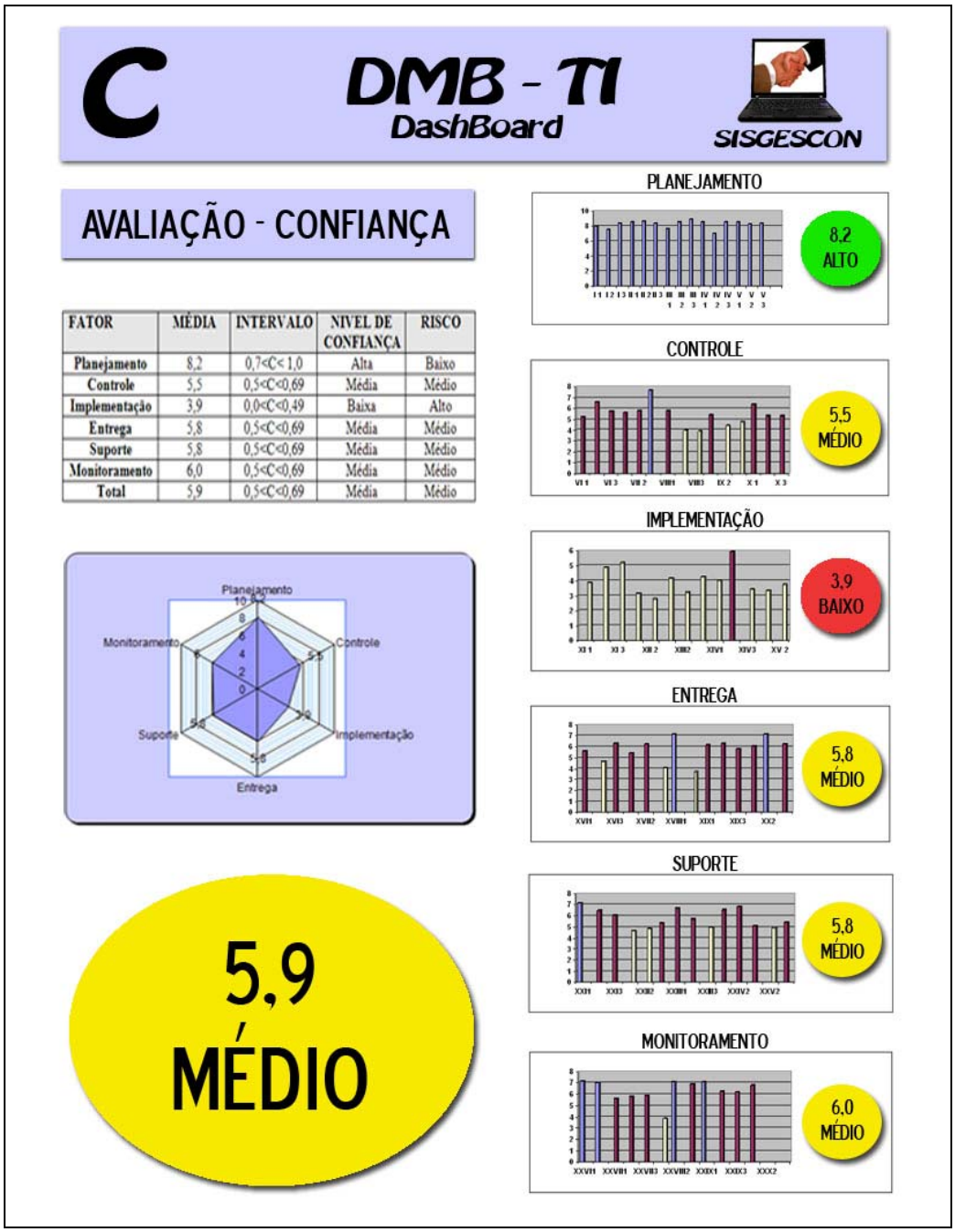
Anexo B.7 – Tela de Acesso ao Resultado Total

Após a seleção de resultado Total na tela do Anexo B.3, os valores poderão ser acessados conforme mostra a figura abaixo.



ANEXO C – PAINEL DE ACOMPANHAMENTO DA DMB

Para apoio à decisão e como um estímulo visual da situação da confiabilidade da TI o SISGESCON disponibiliza um Painel de Acompanhamento conforme mostrado abaixo.



FATOR	MÉDIA	INTERVALO	NIVEL DE CONFIANÇA	RISCO
Planejamento	8,2	0,7<C< 1,0	Alta	Baixo
Controle	5,5	0,5<C<0,69	Média	Médio
Implementação	3,9	0,0<C<0,49	Baixa	Alto
Entrega	5,8	0,5<C<0,69	Média	Médio
Suporte	5,8	0,5<C<0,69	Média	Médio
Monitoramento	6,0	0,5<C<0,69	Média	Médio
Total	5,9	0,5<C<0,69	Média	Médio

ANEXO D - PUBLICAÇÕES REALIZADAS DURANTE A PESQUISA DA TESE

1.	Benzi, D.M., De Sousa Jr, Rafael T.Medição da Confiança no Contexto dos Processos de Gestão da Tecnologia da Informação. *Revista Militar de Ciëncia e Tecnologia. V.*26, 2008.
2.	Benzi D. M. ; Sousa JR, R. T. ; Bidan, C. ; Mé, L. Gerenciamento da Confiança na Tecnologia da Informação. Anais do Séptima Conferencia Iberoamericana en Sistemas, Cibernética e Informática: CISCI, Orlando.2008.
3.	Benzi, D. M. ; de Sousa Jr, R. T. Um Modelo de Confiança Aplicado aos Processos de Gestão da Tecnologia da Informação. 5th International Conference on Information Systems and Technology Management, V CONTECSI, São Paulo, 2008.
4.	Benzi, D.M., de Sousa Jr, Rafael T., Bidan, C., Mé, L. Model for Trust Within Information Technology Management., 10th International Conference on Enterrise Information Systems, ICEIS , Barcelona, 2008.
5.	Benzi, D.M., de Sousa Jr, Rafael T. Tratamento de Confiança Aplicado a Gestão de Tecnologia da Informação. VI Simpósio de Excelência em Gestão e Tecnologia, SEGET, Resende – RJ, 2007.
6.	Benzi, D.M., de Sousa Jr, Rafael T. Governança de Tecnologia da Informação: Facilitadora na Estratégia Organizacional. V Simpósio de Excelência em Gestão e Tecnologia, SEGET, Resende – RJ, 2006