

HANDERSON KOERICH

**SUSTENTABILIDADE DA INFRAESTRUTURA DE CHAVES
PÚBLICAS BRASILEIRA**

Dissertação apresentada à Universidade
do Estado de Santa Catarina como
requisito para obtenção do título de
Mestre em Administração.

Orientador: Prof. Dr. Júlio da Silva Dias

**FLORIANÓPOLIS – SC
2012**

HANDERSON KOERICH

SUSTENTABILIDADE DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

Dissertação aprovada como requisito parcial para a obtenção do grau de Mestre em Administração, no curso de Mestrado Profissional em Administração, do Programa de Pós-Graduação em Administração da Universidade do Estado de Santa Catarina.

Banca Examinadora:

Orientador:

Prof. Dr. Júlio da Silva Dias
Universidade do Estado de Santa Catarina

Membro:

Prof. Dr. Carlos Roberto De Rolt
Universidade do Estado de Santa Catarina

Membro Externo:

Prof. Dr. Mário Antônio Ribeiro Dantas
Universidade Federal de Santa Catarina

Florianópolis – SC, 27/04/2012

À minha esposa, família e amigos, pelo apoio e
incentivo que tornaram possível este trabalho.

AGRADECIMENTO

À Deus, que meu deu saúde e condições para enfrentar com fé esta importante etapa de minha vida.

A minha esposa Hellen, pelo amor, companheirismo, paciência e atenção durante o desenvolvimento e conclusão deste trabalho.

Ao meu orientador Júlio da Silva Dias, pelos conhecimentos transmitidos e pela confiança depositada em minha capacidade de realizar este trabalho.

Ao professor Carlos Roberto De Rolt, pelos ensinamentos e suporte a realização deste trabalho.

Ao Manuel Matos e Patrícia Paiva, pelas valiosas sugestões dadas no desenvolvimento desta pesquisa.

À toda minha família, em especial a meus pais Ademir e Evanilda, pelo apoio, amor e dedicação e ao meu irmão Leonardo.

RESUMO

A Infraestrutura de Chaves Públicas do Brasil, instituída em agosto de 2001, é uma estrutura hierárquica e de confiança que viabiliza a emissão de certificados digitais para a identificação do cidadão e ou empresas quando efetuando transações no meio virtual. O principal objetivo da ICP-Brasil é o certificado digital, um documento eletrônico com validade jurídica, que garante a autenticidade, integridade, não repúdio e tempestividade do documento. Apesar da importância dos certificados digitais, da redução de custos e demais benefícios que este pode trazer, observa-se que até hoje não há uma utilização em larga escala do certificado digital. Sabe-se que a falta de acesso a tecnologia e custos envolvidos são problemas que fazem com que a situação se mantenha inalterada. As discussões até então existentes, são em relação à arquitetura e a operação técnica, com o objetivo de garantir a segurança e não sobre a sustentabilidade econômica e financeira em longo prazo da ICP-Brasil. Dessa forma pretendeu-se neste trabalho desenvolver um modelo que permita avaliar em diferentes cenários a estrutura operacional adequada para o funcionamento das entidades emissoras de certificados digitais em longo prazo. Esta pesquisa está embasada por uma abordagem teórico-empírica, na qual além da revisão da literatura e da legislação sobre o assunto, procura-se verificar a coerência com a realidade, através de um estudo de casos, para então desenvolver um modelo econômico-financeiro e avaliar cenários em busca da sustentabilidade econômico-financeira da ICP-Brasil. A pesquisa mostra que é possível termos um cenário sustentável, com redução dos preços praticados atualmente. Porém para observar a eficiência do modelo proposto seria necessário aplicá-lo num caso real.

PALAVRAS-CHAVE: Infraestrutura de Chaves Públicas. *Corporate Performance Management. Business Intelligence.*

ABSTRACT

The Brazilian Public-key Infrastructure (PKI), established in August 2001, is a hierarchical structure and confidence that enables the issuance of digital certificates for identification of citizens and or businesses when making transactions in the virtual environment. The main objective of the Brazilian PKI is the digital certificate, an electronic document with legal validity, which ensures the authenticity, integrity, non-repudiation and timeliness of the document. Despite the importance of digital certificates, the cost savings and other benefits it can bring, it is observed that even today there is not a large-scale use of the digital certificate. It is known that a lack of technology access and involved costs are problems that make the situation remains unchanged. The discussion heretofore, are in relation to architecture and technical operation, in order to ensure the security and not on the economic and financial sustainability in the long-term of the Brazilian PKI. Thus this work was intended to develop a model to assess different scenarios the operational structure suitable for the operation of the issuers of digital certificates in the long term. This research is based on a theoretical and empirical approach, in which besides the review of the literature and legislation on the subject, we try to check consistency with reality, through a case study, and then develop an economical and financial model and evaluate scenarios in search of economic and financial sustainability of the Brazilian PKI. The research shows that it is possible to have a sustainable scenario, with reduced current prices. But to observe the efficiency of the proposed model would be necessary to apply it to a real case.

KEYWORDS: Public-key Infrastructure. *Corporate Performance Management. Business Intelligence.*

LISTA DE ILUSTRAÇÕES

Figura 1 - Pirâmide hierárquica organizacional com níveis de gestão.	19
Figura 2 - Hiato de ação Figura 3 - Taxonomia das decisões.....	21 22
Figura 4 - O Processo de <i>Business Intelligence</i>	24
Figura 5 - A pirâmide da abstração.....	25
Figura 6 - Funcionalidades CPM.	27
Figura 7 - Atendimento aos Requisitos de Segurança.	29
Figura 8 - Esquema de criptografia simétrica.	30
Figura 9 - Esquema de criptografia assimétrica com sigilo de informação.....	31
Figura 10 - Esquema de criptografia assimétrica com autenticidade de informação.....	31
Figura 11 - Infraestrutura de Chaves Públicas	33
Figura 12 - Visão geral da estrutura da ICP-Brasil.....	34
Figura 13 - Estrutura da dimensão Conta.....	57
Figura 14 - Estrutura da dimensão Tempo.....	57
Figura 15 - Estrutura da dimensão Cenário.	58
Figura 16 - Estrutura da dimensão Entidade.	59
Figura 17 - Lista de Fórmulas 1.....	60
Figura 18 - Lista de Fórmulas 2.	60
Figura 19 - Lista de Formulários.....	62
Figura 20 - Formulário 01.01 – Premissas Gerais.	62
Figura 21 - Formulário 01.02 – Premissas Dias Úteis.	63
Figura 22 - Formulário 02.01 – Custos por AR.	63
Figura 23 - Formulário 02.02 – Custo Administrativos da AR.	64
Figura 24 - Formulário 02.03 – Custos AC.	64
Figura 25 - Formulário 02.04 – Custos Administrativos da AC.....	65
Figura 26 - Formulário 03.01 – Resultado.....	65
Figura 27 - Lista de Relatórios.....	66
Figura 28 - Relatório 01 – DRE Anual.	67
Figura 29 - Relatório 02 – DRE Comparativo Anual.	67
Figura 30 - Análise de Rentabilidade da AR.	68
Figura 31 - Análise de Rentabilidade da AC.	69
Figura 32 - Cenário AR atual com receita mínima	71
Figura 33 - Cenário AC atual sem hardware com 20 ARs vinculadas.	73

LISTA DE TABELAS

Tabela 1 - Estrutura metodológica da pesquisa	39
Tabela 2 - Custos fixos de um AR	47
Tabela 3 - Custos mensais de um AR	47
Tabela 4 - Custos esporádicos de um AR	48
Tabela 5 - Receitas máxima de uma AR.....	49
Tabela 6 - Custos fixos de um AC	53
Tabela 7 - Custos mensais de um AC	54
Tabela 8 - Custos esporádicos de um AC	54
Tabela 9 - Receitas da AC.....	55
Tabela 10 - Comparativo do cenário atual AR	71
Tabela 11 - Comparativo do cenário atual AC	72
Tabela 12 - Comparativo do cenário atual AC sem hardware.....	73
Tabela 13 - Cenário proposto para AR e AC	75

LISTA DE ABREVIATURAS

AC – Autoridade Certificadora

AC Raiz – Autoridade Certificadora Raiz

AR – Autoridade Registradora

BI – *Business Intelligence*

CG – Comitê Gestor

CNPJ – Cadastro Nacional de Pessoas Físicas

CPM – *Corporate Performance Management*

DW – *Data Warehouse*

ETL – *Extract, Transform and Load*

HSM – *Hardware Security Model*

ICP – Infraestrutura de Chaves Públicas

ICP Brasil – Infraestrutura de Chaves Públicas Brasileira

ITI – Instituto de Tecnologia da Informação

LL – Lucro Líquido

OLAP – *Online Analytical Processing*

PL – Patrimônio Líquido

PSS – Prestadores de Serviços de Suporte

RSPL – Retorno Sobre o Patrimônio Líquido

SAD – Sistema de Apoio à Decisão

TI – Tecnologia da Informação

TJLP – Taxa de Juros de Longo Prazo

SUMÁRIO

LISTA DE ILUSTRAÇÕES	7
LISTA DE TABELAS	8
LISTA DE ABREVIATURAS	9
1 INTRODUÇÃO	12
1.1 TEMA E PROBLEMA DE PESQUISA.....	12
1.2 OBJETIVOS DA PESQUISA.....	14
1.2.1 Objetivo Geral	14
1.2.2 Objetivos Específicos.....	14
1.3 JUSTIFICATIVA DA PESQUISA.....	14
1.4 ESTRUTURA DA DISSERTAÇÃO.....	15
2 FUNDAMENTAÇÃO TEÓRICA	17
2.1 GESTÃO ESTRATÉGICA.....	17
2.2 GESTÃO DA INFORMAÇÃO	18
2.3 PLANEJAMENTO E CONTROLE	19
2.4 SISTEMAS DE APOIO A DECISÃO.....	20
2.5 BUSINESS INTELLIGENCE	22
2.6 CORPORATE PERFORMANCE MANAGEMENT	25
2.7 DOCUMENTO ELETRÔNICO	27
2.8 CRIPTOGRAFIA.....	30
2.9 INFRAESTRUTURA DE CHAVES PÚBLICAS	32
2.10 ICP BRASIL	33
2.10.1 Comitê Gestor	34
2.10.2 Comitê Técnico	35
2.10.3 Autoridade Certificadora Raiz	35
2.10.4 Autoridade Certificadora.....	36
2.10.5 Autoridade de Registro	36
2.10.6 Prestador de Serviços de Suporte	36
2.10.7 Auditorias Independentes	37
2.10.8 Titulares de Certificados	37
2.10.9 Terceiras Partes	37

3 PROCEDIMENTOS METODOLÓGICOS	38
3.1 CARACTERIZAÇÃO DA PESQUISA	38
3.2 TÉCNICAS DE COLETA E ANÁLISE DE DADOS	39
3.3 LIMITAÇÕES DA PESQUISA.....	40
4 APRESENTAÇÃO, ANÁLISE E INTERPRETAÇÃO DOS DADOS.....	42
4.1 CUSTOS COMUNS AS ARS E ACS	43
4.2 CUSTOS DAS ARS.....	44
4.3 RECEITAS DAS ARS	48
4.4 CUSTOS DAS ACS	49
4.5 RECEITAS DAS ACS	55
5 APRESENTAÇÃO DO MODELO	56
5.1 FÓRMULAS DO MODELO	59
5.2 FORMULÁRIOS DO MODELO	61
5.3 RELATÓRIOS DO MODELO	66
5.4 ANÁLISES DE RENTABILIDADE DO MODELO	68
6 ANÁLISE DE CENÁRIOS	70
6.1 CONFIGURAÇÃO ATUAL	70
6.2 PROPOSTA DE SUSTENTABILIDADE.....	74
7 CONCLUSÕES.....	76
7.1 TRABALHOS FUTUROS.....	77
REFERÊNCIAS	79

1 INTRODUÇÃO

1.1 TEMA E PROBLEMA DE PESQUISA

Na era digital, o mundo ficou pequeno, as distâncias diminuíram e tudo ficou mais rápido e dinâmico. A tecnologia criou uma revolução social e econômica. As organizações, para continuarem competitivas, precisaram se adaptar a este novo ambiente, fazendo surgir uma economia baseada na tecnologia da informação denominada de economia digital (TAPSCOTT, 2006).

Na economia digital o uso do papel perdeu lugar para o documento eletrônico. No entanto, o uso do documento eletrônico ainda apresentava um grande problema, a falta de segurança. O papel possui atributos jurídicos essenciais, como autenticidade, integridade, tempestividade e o não repúdio. Assim, somente com o advento do certificado digital e da infraestrutura de chaves públicas (ICP), todos esses atributos jurídicos foram garantidos ao documento eletrônico.

A Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil) foi instituída em agosto de 2001 através da medida provisória 2200-2. A partir desta medida provisória foi operacionalizada a Autoridade Certificadora Raiz (AC Raiz) da ICP-Brasil e iniciado o processo de credenciamento de Autoridades Certificadoras (ACs) de segundo nível.

As aplicações dos certificados digitais são inúmeras, entre o quais se destacam a redução significativa do custo de envio de documentos de um estado para outro. Grandes sites de comércio eletrônicos podem substituir o velho usuário e senha, tendo o benefício do aumento da segurança. Os bancos também podem utilizar a assinatura digital no *home banking*, garantindo o não repúdio das operações e com isso reduzindo custos.

Até mesmo no aquecimento global, a assinatura digital tem importância. Em documento intitulado Acordo para o Desenvolvimento Sustentável, uma contribuição para a conferência Rio+20 que acontecerá em junho de 2012, foi destacado que a desmaterialização da produção pode ser feita com a troca do material em papel pelo documento eletrônico (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2011).

No entanto, observa-se que até hoje não há uma utilização em larga escala do certificado digital. Em maio de 2006, tínhamos cerca de 500 mil certificações digitais emitidas pela ICP-Brasil e a expectativa de se atingir um milhão (SERPRO, 2006). Contudo,

apenas em dezembro de 2010 a marca de um milhão de certificados, emitidos pela ICP-Brasil, foi atingida (CONFEDERAÇÃO NACIONAL DO COMÉRCIO, 2010).

Sabe-se que a falta de acesso a tecnologia e custos envolvidos são problemas que fazem com que a situação, de não utilização em massa dos certificados digitais, se mantenha inalterada. As discussões até então existentes, são em relação à arquitetura e a operação técnica, com o objetivo de garantir a segurança e não sobre a sustentabilidade econômica e financeira em longo prazo da ICP-Brasil.

Diante disto, pretendeu-se neste trabalho desenvolver um modelo que permita avaliar em diferentes cenários a estrutura operacional adequada para o funcionamento das entidades emissoras de certificados digitais em longo prazo.

A habilidade com que a organização coleta, organiza, analisa e implementa mudanças a partir de informações, integrando-as ao processo de melhoria contínua de suas atividades, que irá determinar a sua excelência. A formulação estratégica de qualquer negócio sempre é feita a partir das informações disponíveis e, portanto, nenhuma estratégia consegue ser melhor que a informação da qual é derivada (RESENDE, 2001). Dessa forma, a informação precisa e atualizada é essencial para as organizações sobreviverem no mercado atual, onde as mudanças ambientais são cada vez mais rápidas e o mercado mais acirrado (LÖNNQVIST e PIRTTIMÄKI, 2006).

Nesse conjunto, o uso da tecnologia da informação (TI) se torna fundamental para transformarmos os dados armazenados em vários locais, internos e externos a organização, em informação. Este processo é conhecido como *Business Intelligence* (BI), isto é, o processo de coletar, armazenar, acessar e analisar dados para auxiliar os usuários na tomada de decisões (WATSON, 2009).

Um sistema de apoio à decisão (SAD) corresponde a um aplicativo computacional que combinam dados e modelos matemáticos para ajudar a resolver os problemas complexos de tomada de decisão enfrentados na gestão das organizações (VERCELIS, 2009). O *Corporate Performance Management* (CPM), um instrumento de alavancagem do BI (COKINS, 2009), auxilia as organizações a traduzir suas estratégias e objetivos em planos, a monitorar o desempenho destes planos, a analisar as variações dos planos e a ajustar seus objetivos e ações em resposta as análises.

Assim, o modelo aqui desenvolvido utilizou uma ferramenta de CPM; tirando proveito de todos os benefícios tecnológicos, principalmente das funcionalidades de análise e criação de cenários, que são fundamentais na sua avaliação. Segundo Mintzberg et al (2000), “planejamento de cenários, o cenário, uma ferramenta no arsenal do estrategista, para citar

Poter (1985), baseia-se na suposição de que, se não se pode prever o futuro, especulando sobre uma variedade de futuros pode-se abrir a mente e, com sorte, chegar ao futuro correto”.

Tendo em vista a problemática apresentada, e considerando a importância em se conhecer os possíveis modelos de operação da ICP-Brasil que possam garantir a sua sustentabilidade e uso intensivo da certificação digital no Brasil, esta pesquisa se propôs a desenvolver o seguinte problema de pesquisa: Seria possível desenvolver um modelo para a ICP-Brasil que garanta sua sustentabilidade financeira e econômica em longo prazo?

1.2 OBJETIVOS DA PESQUISA

1.2.1 Objetivo Geral

O objetivo geral deste trabalho foi estruturar um modelo econômico-financeiro das entidades emissoras de certificados digitais para avaliar aspectos relacionados à sua sustentabilidade.

1.2.2 Objetivos Específicos

Dentro do escopo deste trabalho, apresentou os seguintes objetivos específicos:

- a) Mapear os requisitos para a operação de uma AC, incluindo as ARs vinculadas, com o objetivo de emissão de certificados digitais em larga escala;
- b) Desenvolver um modelo econômico-financeiro da AC e da AR utilizando uma ferramenta de CPM;
- c) Avaliar os possíveis cenários buscando a situação onde os recursos existentes são otimizados e a população seja mais bem atendida;

1.3 JUSTIFICATIVA DA PESQUISA

A relação entre os usuários e prestadores de serviços públicos e privados pode ser realizada através da internet. Nesta situação o uso de certificados digitais é necessário para identificação das partes envolvidas e garantir requisitos de segurança tais como autenticidade, integridade, tempestividade e não repúdio.

Como exemplos de instituições públicas que permitem o uso de certificação digital no processo de prestação de serviços têm-se a Receita Federal, a Prefeitura Municipal de Florianópolis e diversos Tribunais de Justiça.

Atualmente, o uso do certificado digital é limitado pela falta de disseminação da tecnologia e também pelo investimento inicial que é considerado elevado para pessoas físicas.

As discussões até então existentes, no meio acadêmico, da ICP-Brasil são em relação à arquitetura e a operação técnica, com o objetivo de garantir a segurança e não sobre a sustentabilidade econômica e financeira em longo prazo da ICP-Brasil. No entanto a saúde financeira das instituições, que compõem a ICP-Brasil, também está diretamente relacionada a segurança, a quanto a instituição poderá investir em atualizações tecnológicas visando a manutenção ou ao aumento da segurança.

O presente estudo é importante por procurar um modelo que permita determinar a melhor estrutura possível, que consiga emitir certificados digitais de forma eficiente a um custo aceitável para os usuários finais.

1.4 ESTRUTURA DA DISSERTAÇÃO

Quando à sua estrutura, este trabalho está dividido em sete capítulos da seguinte forma:

O primeiro capítulo apresenta o tema e o problema que orientaram o desenvolvimento da pesquisa, o objetivo geral e os objetivos específicos, e a justificativa da pesquisa.

O segundo capítulo apresenta a fundamentação teórica para a pesquisa. Este capítulo inicia-se com a gestão estratégica e sua importância, depois descreve a gestão da informação e sua evolução, para entrar na importância do planejamento e controle financeiro e orçamentário, apresenta as ferramentas tecnológicas para apoio a tomada de decisão: BI e CPM. Em seguida é apresentado o documento eletrônico e a criptografia que propicia a utilização deste. Por último é descrito a estrutura da ICP-Brasil, objeto de estudo deste trabalho.

No terceiro capítulo estão apresentados os procedimentos metodológicos da pesquisa, incluindo a caracterização, as técnicas de coleta de dados e as limitações encontradas durante a pesquisa.

No quarto capítulo são apresentados os dados coletados e inicia-se a categorização e análise destes por grupos: custos comuns as ARs e ACs, custos das ARs, receitas das ARs, custos da AC e receita da AC.

O quinto capítulo apresenta o modelo criado utilizando-se as ferramentas tecnológicas, CPM. O capítulo é subdivido para apresentar as formulas de cálculo, formulários de entrada de dados, relatórios para análises e interfaces para análise de rentabilidade.

No sexto capítulo é apresentado em detalhes o cenário criado com a configuração atual das ARs e AC. Por último é apresentado o cenário proposto para a sustentabilidade econômica da AC e ARs.

No sétimo capítulo estão as considerações finais do estudo e as conclusões. Ainda neste capítulo são feitas recomendações para futuras pesquisas.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 GESTÃO ESTRATÉGICA

O que é estratégia? Não existe uma única definição universalmente aceita, segundo Mintzberg e Quinn (2001), estratégia é o padrão ou plano que integra as principais metas, políticas e sequência de ações de uma organização em um todo coerente. Já, para JOHNSON et al (2007) a estratégia é a direção e o escopo de uma organização em longo prazo, que obtém vantagem em um ambiente em mudança através de sua configuração de recursos e competências com o objetivo de atender às expectativas dos *stakeholders*, enquanto que para Mintzberg et al (2000) não optam por oferecer uma única definição e sim baseadas nos 5 Ps (Plano, Padrão, Posição, Perspectiva e Pretexto).

O aumento na complexidade das organizações associado à aceleração do ritmo das mudanças tem exigido cada vez mais dos gestores. A capacidade de formular e implementar estratégias que possibilitem superar os desafios de mercado, para que sejam atingidos os seus objetivos de curto, médio e longo prazo são características essenciais aos gestores. Diante de tal cenário, o planejamento estratégico surge como uma valiosa ferramenta de auxílio à alta administração.

O planejamento estratégico formal é um processo explícito e permanente de organização, que dispõe de um número de componentes, tais como o estabelecimento de metas e a geração e avaliação de estratégias (BOYD, 1991). Segundo Hitt et al (2003), o processo de gestão estratégica é representado pelos compromissos, decisões e ações necessárias para que uma empresa alcance a competitividade estratégica e aufera retornos superiores à média.

Já Jordan et al (2008), definem o planejamento estratégico como um sistema composto pelas seguintes fases: (i) Informação: a análise que conduz ao conhecimento de ameaças e oportunidades do meio ambiente e aos pontos fortes e fracos da empresa em face desse meio. (ii) Formulação de alternativas estratégicas: identificar estratégias alternativas para solucionar os problemas ou aproveitar as oportunidades. (iii) Avaliação das alternativas, através de estudos sobre as consequências de cada uma das alternativas. (iv) Decisão: escolha de uma das alternativas que venha a ser considerada mais interessante para o objetivo almejado.

Os benefícios do planejamento estratégico, conforme descrito na literatura (GREENLEY, 1986; JOHNSON e SCHOLES, 2002; KOUFOPOLOUS e MORGAN, 1994),

pode ser resumido como: para reforçar a coordenação; para o controle através da revisão de desempenho e progresso rumo aos objetivos; para identificar e explorar oportunidades futuras; para melhorar a comunicação interna entre o pessoal; para incentivar o pessoal a uma atitude favorável à mudança; para melhorar o desempenho social de empresas.

Dessa forma, a gestão estratégica norteia o processo contínuo e interativo da organização com o seu ambiente. Ainda este almeja atingir a eficácia da empresa sem a colocar em risco, de forma a garantir a sua estabilidade num ambiente onde ser competitivo é condição *sine qua non* para a sua continuidade a longo prazo.

2.2 GESTÃO DA INFORMAÇÃO

Segundo Cautela e Polioni (1982), "A informação é considerada como o ingrediente básico do qual dependem os processos de decisão". Resende (2001) enfatiza que nenhuma estratégia consegue ser melhor que a informação da qual é derivada. Desse fato surge à necessidade e a importância da gestão da informação para as organizações.

Davenport (1998) define Gestão da Informação como um conjunto de atividades estruturadas que englobam como as empresas definem, obtêm, distribuem e usam a informação. A definição consiste na identificação das necessidades e exigências de informações (MCGEE e PRUSAK, 1994). Com as necessidades definidas se começa a obtenção da informação, através da busca, classificação, formatação e estruturação das informações. A etapa de distribuição está relacionada às formas de comunicação e compartilhamento utilizadas. Na última etapa, a do uso da informação, se tem a interpretação e utilização dessa informação (DAVENPORT, 1998).

Para a organização ter a Gestão da Informação de forma eficaz, é necessário um conjunto de políticas coerentes que possibilitem o fornecimento de informação relevante, com qualidade, precisão, transmitida para o local certo, no tempo correto, a um custo apropriado e facilidade de acesso para os utilizadores autorizados (REIS, 19993).

A informação gerida pode vir de três níveis: estratégico, tático e operacional. No nível estratégico temos os objetivos, recursos e políticas de longa duração; no nível tático está a execução dos planos e objetivos do nível estratégico; no nível operacional monitoram-se e executam-se as atividades diárias da organização. Dessa forma, à medida que descemos na pirâmide hierárquica organizacional a especificidade aumenta, enquanto que no nível mais alto os problemas são mais gerais, mais correlacionados a estratégia da organização como um todo (ANTHONY, 1965).

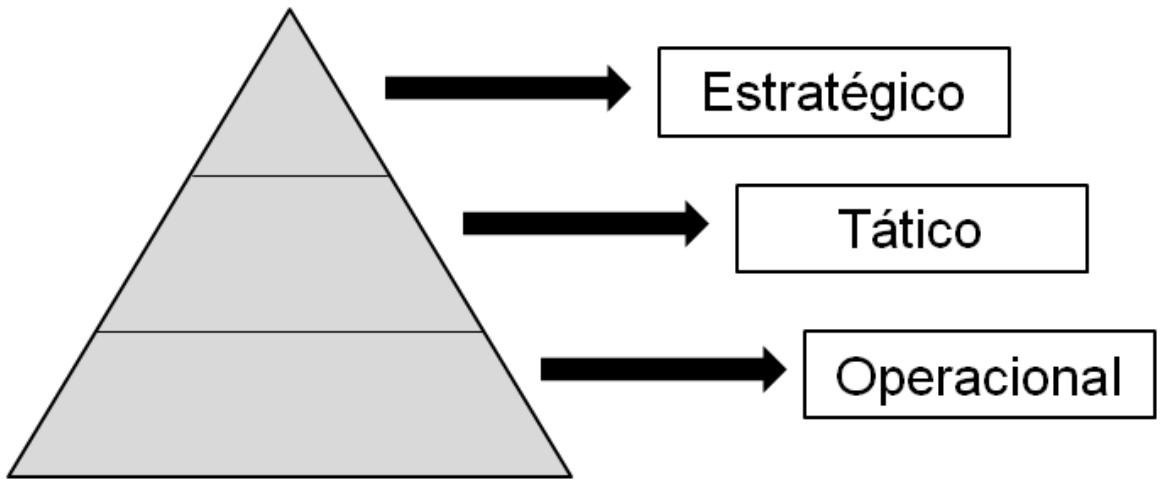


Figura 1 - Pirâmide hierárquica organizacional com níveis de gestão.
Fonte: domínio público

2.3 PLANEJAMENTO E CONTROLE

As novas condições econômicas globais estão levando as empresas a se tornarem mais cautelosas com o futuro. Os administradores das organizações buscam cada vez mais instrumentos flexíveis de previsão do desempenho corporativo, de maneira que se possa assegurar a continuidade do negócio. Neste contexto, o processo de planejamento e controle corporativo se destaca por permitir mensurar se as metas estabelecidas para o crescimento de uma empresa atingem resultados satisfatórios.

A organização corresponde a um conjunto de recursos econômicos, sociais e humanos, que podem ser vistos como um sistema aberto e direcionado para a execução das suas funções. A missão do controle de gestão é zelar pela continuidade da empresa, assegurando a otimização do resultado (CAGGIO e FIGUEIREDO, 2004).

Segundo Jordan et al (2008), o planejamento estratégico é orientado para o exterior procurando adaptar a empresa ao seu ambiente a longo prazo; enquanto que o controle de gestão procura a coordenação e o empenho dos responsáveis operacionais para alcançarem os objetivos definidos a curto prazo no âmbito dos mercados, dos produtos e dos meios atualmente existentes.

Para Jiambalvo (2001), o planejamento é uma atividade fundamental que envolve todas as organizações. Um plano financeiro comunica as metas aos empregados e especifica os recursos necessários para atingi-las. Além disso, fornece uma base para a avaliação do desempenho empresa.

O orçamento, o principal produto do planejamento financeiro, é uma ferramenta importante para o controle e o planejamento das empresas, é um plano que abrange todos os processos de um determinado período de tempo e resulta em um plano financeiro (ANTHONY, 2008; LUNKES, 2007). A elaboração do orçamento, segundo ANTHONY (2008) tem quatro propostas principais: (i) ajustar o planejamento estratégico; (ii) coordenar as várias áreas da empresa; (iii) estabelecer responsabilidades e (iv) gerar comprometimento de desempenho.

Este é considerado um dos processos mais relevantes numa solução de CPM, sendo a tradução operacional da estratégia de uma organização em termos de custos e receitas previstas; é desenhado para alocar os recursos de uma companhia e permite aos gestores avaliar o seu desempenho no decorrer de um período (ROUX, 2004).

2.4 SISTEMAS DE APOIO A DECISÃO

Um sistema de apoio à decisão (SAD) corresponde a um aplicativo baseado em computação interativa que combinam dados e modelos matemáticos para ajudar a resolver os problemas complexos de tomada de decisão enfrentados na gestão das organizações. (VERCELIS, 2009).

Segundo Jordam et al, esses sistemas consideram que as decisões devem ser tomadas sempre que possível sobre acontecimentos e com o passar do tempo à informação vai perdendo relevância. Quanto mais antiga a informação, menor sua relevância.

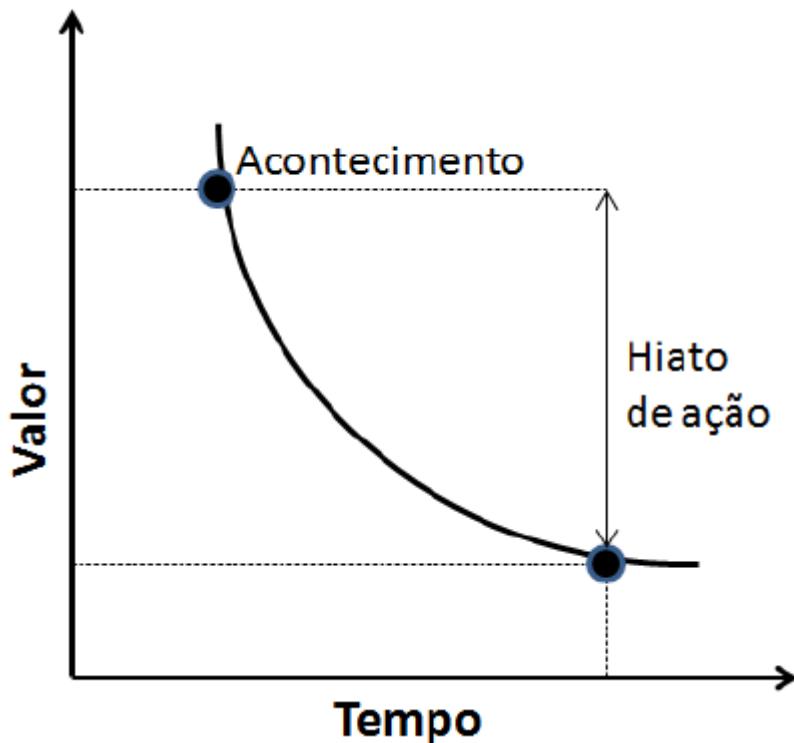


Figura 2 - Hiato de ação

Fonte: JORDAN, NEVER, RODRIGUES, 2008.

Um modelo SAD é a tentativa de representar a realidade por meio de equações matemáticas, premissas, regras e restrições impostas pelas condições da realidade que se tenta reproduzir (LAPONI, 2004). Esses modelos são compostos basicamente por três componentes: entradas, dados disponíveis; saídas, dados resultantes; fórmulas matemáticas que atendam às regras de negócio.

Vercelis (2009) classifica as decisões de acordo com sua natureza como: estruturada, que contem uma rígida estrutura e permita a criação de um algoritmo, pode ser descrito passo a passo em detalhes; semiestruturada, quando algumas fases não são estruturadas; não estruturada, as fases de concepção, inteligência e escolha são não estruturadas.

Assim como Anthony (1965), Vercelis (2009) também usa os três níveis da pirâmide hierárquica organizacional (figura 3) para classificar o escopo das decisões, em estratégica, tática e operacional. Dessa forma, temos a taxonomia das decisões usando as duas dimensões, natureza e escopo, da seguinte forma:



Figura 3 - Taxonomia das decisões.

Fonte: VERCELIS, 2009.

A nova geração de SAD conta com novas tecnologias, como o *Data Warehouse* (DW) e *Online Analytical Processing* (OLAP). Tais conceitos têm sido unificados e substituídos por BI.

2.5 BUSINESS INTELLIGENCE

O uso da tecnologia da informação (TI) se tornou fundamental para transformarmos os dados armazenados em vários locais, internos e externos a organização, em informação. Este processo é conhecido como *Business Intelligence* (BI), isto é, o processo de coletar, armazenar, acessar e analisar dados para auxiliar os usuários na tomada de decisões (WATSON, 2009).

Nos últimos cinco anos, BI é uma das maiores prioridades para os diretores de TI e quase todas as 5000 maiores organizações mundiais a utilizam (GARTNER GROUP, 2010). As ferramentas de BI estão evoluindo rapidamente, mas por outro lado as organizações estão lidando cada vez mais com um mercado mais acirrado, onde a quantidade de informação é maior a cada dia e em um formato não estruturado. A necessidade de integrar as informações

das mais diversas fontes de dados como e-mail, áudio, vídeo e outros formatos de documentos é quase que vital para as organizações continuarem competitivas atualmente (GREENGARD, 2010).

Pode parecer surpreendente, mas muitos gestores frequentemente encontram dificuldade em obter informações simples como o nível do estoque, evolução de vendas, histórico de um cliente e assim por diante. Inclusive algumas pessoas chaves levam horas senão dias para obter essas informações. Isso acontece porque essas informações ficam espalhadas em vários sistemas internos da empresa, como sistema contábil, sistema de faturamento, CRM e assim por diante. Então para se conseguir uma determinada informação às vezes é necessário cruzar dados dessas diversas fontes de dados e isso não é uma tarefa para um usuário comum, o que causa a dificuldade em conseguir a informação (HOCEVAR e JAKLIC, 2010).

Neste contexto, a organização é rica em dados, e o maior desafio é transformar esses dados em informação útil (CARVER e RITACCO, 2006). Como os dados estão espalhados em vários sistemas em diferentes departamentos da organização, é preciso envolver várias pessoas para consolidar os dados e conseguir extrair a informação necessária. Nesse momento a área de TI é envolvida para auxiliar o processo, mas ainda assim essa tarefa demanda tempo, justificando a demora em obter as respostas das perguntas simples.

Com o mercado cada vez mais competitivo, obter as respostas em tempo real se torna uma necessidade, e dai surge o BI. O termo BI foi primeiramente usado como um nome comum para descrever “conceitos e metodologias para melhorar a tomada de decisões usando fatos e informações dos sistemas de suporte” em 1989 por Howard Dresner (POWER, 2007).

O BI não é composto de apenas uma aplicação ou de apenas um sistema e sim de um conjunto de sistemas que trabalham em conjunto. De um ponto de vista de arquitetura um sistema de BI é composto dos seguintes componentes (HOCEVAR e JAKLIC, 2010):

- a) Vários bancos de dados operacionais, onde os sistemas das empresas armazenam seus dados e de onde o BI deve extrair as informações;
- b) Ferramenta de ETL (*Extract, Transform and Load*) para extrair os dados das diversas fontes de dados, transformar esses dados em informações e carregar nos armazém de dados (*Data Warehouse*);
- c) Armazém de dados (*Data Warehouse*), onde todas as informações são salvas de forma centralizada e num formato mais amigável e performático para responder as perguntas dos gestores;

- d) Ferramentas para acesso e análise de dados, são as ferramentas que permitem os usuários finais de forma fácil explorar e analisar seus dados.

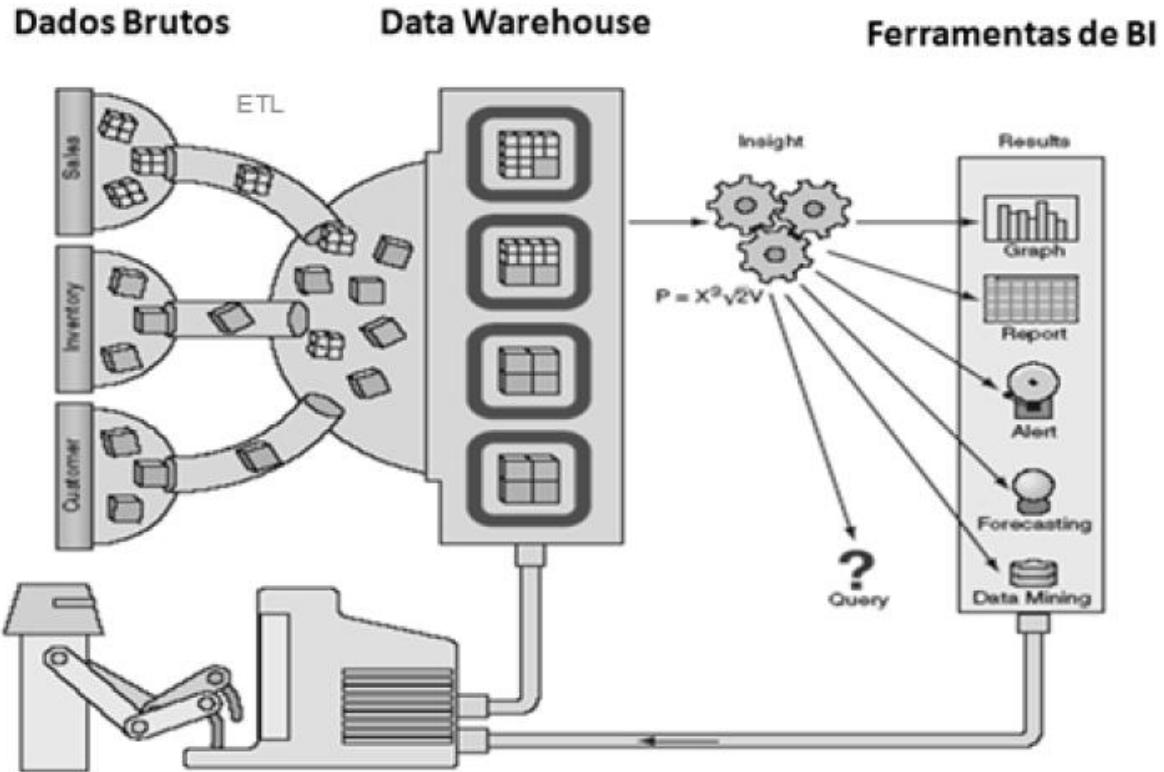


Figura 4 - O Processo de *Business Intelligence*.

Fonte: TURBAN *et al*, 2003.

Assim, o objetivo final do BI se baseia numa pirâmide de abstração que se relaciona com as formas como conseguimos as informações e a capacidade de fornecer acesso a esse ativo de conhecimento. A capacidade para explorar eficazmente a informação alicerça-se numa evolução da estrutura hierárquica da gestão da informação até a gestão do conhecimento (LOSHIN, 2003).

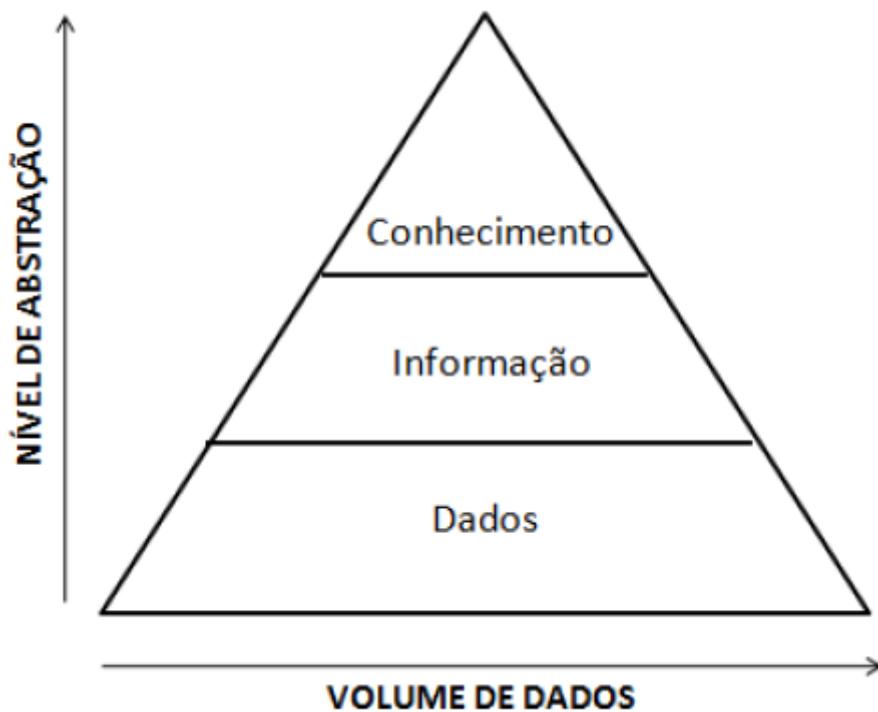


Figura 5 - A pirâmide da abstração.

Fonte: ZENKNER, 2011, p. 25

2.6 CORPORATE PERFORMANCE MANAGEMENT

Corporate Performance Management (CPM) pode ser considerado como a próxima geração, ou o último componente, do BI. Esta é a fase seguinte na evolução dos sistemas de apoio à decisão e dos sistemas de informação empresarial. Cokins (2009) classifica o CPM como um instrumento de alavancagem do BI. Sezões et al (2006), consideram que o CPM visa integrar e automatizar a composição, o cálculo, a consolidação e disseminação dos dados financeiros e operacionais.

O Gartner Group (2011), através do *Magic Quadrant for Corporate Performance Management Suites*, descreve CPM como ferramentas que contenham as seguintes funcionalidades:

- *Budget, Plan & Forecast* (BP&F) – permitem o desenvolvimento de orçamentos, planos e previsões, de curto e longo prazo. A principal funcionalidade é o motor para criação de modelos financeiros integrado com os demonstrativos de lucros e perdas, balanço patrimonial e fluxo de caixa. Também deve possuir funcionalidades de workflow para o controle do

processo de aprovação e revisão orçamentária. Permitir a utilização de modelos matemáticos, estatísticos complexos para as projeções.

- *Activity-based costing* (ABC) – aplicações que determinam a alocação de custos por atividade; forneçam recursos de modelagem para permitir aos usuários analisarem o impacto sobre a rentabilidade de custos e estratégias de diferentes alocações de recursos.
- Planejamento Estratégico – aplicações que deem suporte ao planejamento estratégico, modelagem e monitoramento para melhorar o desempenho corporativo, acelerando a tomada de decisão e facilitando a colaboração. Aqui estão inclusas metodologias como *balanced scorecard* (BSC) e a criação de *dashboards*.
- Consolidação Financeira e Fechamento – permitem a reconciliação, consolidação, resumo e agregação financeira de dados seguindo diferentes padrões e regulamentações contábeis (IFRS, por exemplo).
- Relatórios Financeiros, de Gestão e Divulgação – funcionalidades para a geração de relatórios seguindo os padrões e especificidades financeiras (US-GAAP, IFRS, XBRL, etc).

Diante desse contexto, conclui-se que o CPM é uma abordagem holística, a qual permite a integração e a utilização de BI, gestão de processos, gestão de serviços e gestão de desempenho corporativo para alcançar uma visão única e completa da organização. Não apenas olhando os dados históricos com as funcionalidades de BI, mas também projetando o futuro com as funcionalidades preditivas do CPM.

Devido à experiência prévia do autor com a ferramenta *Sysphera Enterprise Suite*, uma ferramenta de CPM; os motores de cálculos, semelhantes a uma planilha Excel, que permite a análise preditiva; somado as funcionalidades de análise, como os relatórios com facilidades na exploração de dados (funcionalidades de BI); são as principais características que justificam a utilização desta ferramenta na construção deste trabalho.

Na figura 6 temos descrito todas as funcionalidades principais da ferramenta *Sysphera Enterprise Suite*.

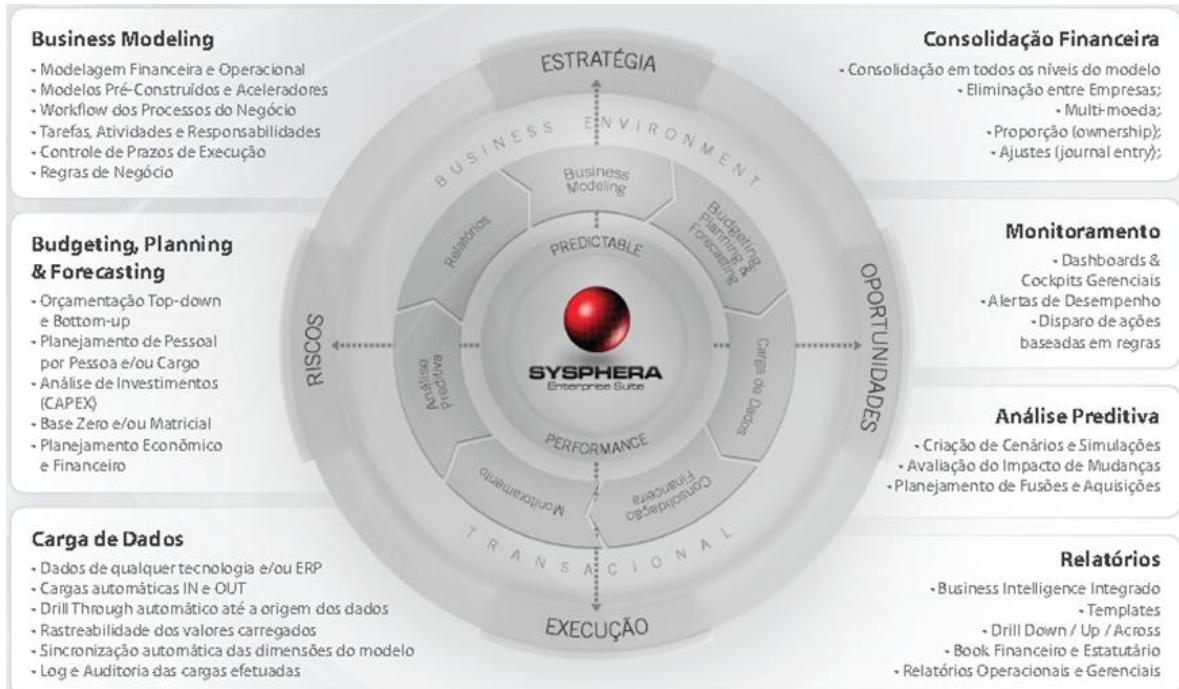


Figura 6 - Funcionalidades CPM.

Fonte: SYSPHERA, 2011.

2.7 DOCUMENTO ELETRÔNICO

A evolução da tecnologia da informação permitiu o armazenamento de informação em meios magnéticos e ópticos, criando a independência de substratos físicos, o chamado documento eletrônico. O ambiente cada vez mais competitivo e dinâmico do mercado fez com que a aceitação do documento eletrônico fosse rapidamente aceita. As vantagens deste são inúmeras, como: a redução do custo de armazenamento e transmissão, velocidade de transmissão, velocidade na busca de informação, entre outros (DIAS, 2003).

O documento eletrônico se apresenta como uma sequência de bits que pode ser visualizada com suporte computacional (SCHEIBELHOFER, 2001), através de ferramentas adequadas para traduzir os bits em informação legível ao ser humano.

No entanto, essa separação do meio físico da informação e da forma de armazenamento e visualização geram desvantagens em relação ao papel. Abaixo estão listados alguns dos requisitos que o documento eletrônico precisa ter para se manter tão confiável quanto o papel, segundo Dias (2004) e Costa (2010):

- Autenticidade – permitir a identificação do autor do documento. No documento em papel é possível se reconhecer a caligrafia do autor, o que no documento eletrônico não é possível sem a utilização de técnicas adicionais;

- Integridade – garantir que o documento é original, não tenha sido alterado por uma terceira parte depois da sua criação. Não havendo uma ligação entre o conteúdo e o meio físico, não é possível o atendimento deste requisito;
- Não repúdio – não permitir que o autor do documento não assuma sua autoria. Deve ser possível além de a autenticidade garantir que quem está ligada ao documento eletrônico realmente foi à pessoa que o criou;
- Tempestividade – identificar a data e hora exatas da criação do documento. Para isso é necessário uma marcação de tempo por uma terceira entidade, para garantir a existência do documento naquela data e hora;

Além dos requisitos citados acima, ainda existe um último requisito bastante importante, garantir o sigilo das informações. Ter a segurança que as informações que trafegam na rede ou são armazenadas estejam cifradas, não possam ser lidas por pessoas não autorizadas, e possam ser decifradas sempre que necessário para as pessoas autorizadas.

Com a obtenção de todos estes requisitos (Figura 7), o documento eletrônico se torna confiável para uso das organizações em transações internas e comerciais, com respaldo jurídico. Assim, desfrutando de todos os benefícios do documento eletrônico com a mesma segurança do documento em papel.

Requisitos	Documento em Papel	Documento Eletrônico
Autenticidade	Assinatura manuscrita atrelada a um substrato físico contendo as informações que se deseja transmitir ou expressar concordância.	Assinatura eletrônica ou digital, que dependem dos requisitos irrefutabilidade e irretratabilidade.
Integridade	O documento não deve ter seu conteúdo e formato alterados, sendo qualquer tentativa de fraude identificada. É garantida através da integridade do substrato físico para os documentos em papel.	A integridade de documentos eletrônicos é garantida através do uso de funções resumo criptográficas.
Tempestividade	Requisito relacionado com o estabelecimento de referência temporal, criando evidências da existência do documento em determinado instante do tempo. Terceiras Partes Confiáveis como Cartórios garantem este requisito para documentos em papel.	Terceiras Partes Confiáveis como Autoridades de Datação garantem este requisito para documentos eletrônicos.
Sigilo	O conteúdo do documento deve ser mantido oculto até que a ocorrência de determinado evento. Documentos como propostas comerciais em licitações ou testamentos não devem ter seu conteúdo revelado até que eventos apropriados ocorram. Uma forma de atendimento deste requisito para documentos em papel é o uso de envelopes lacrados mantidos por entidades confiáveis.	Cifragem do documento.
Privacidade	Classificação dos documentos aos quais o acesso é restrito.	Cifragem com a chave pública, utilizando algoritmo RSA, de uma entidade comprova que somente esta entidade tem acesso à informação, sendo a divulgação prova da quebra de privacidade.
Irrefutabilidade	Requisito no qual o autor de um documento não pode negar a autoria do mesmo. Obtida através da assinatura manuscrita.	Uso da chave privada expressa consentimento por parte do assinante.
Irretratabilidade	Requisito no qual o autor de um documento não pode negar os termos contidos no documento. Atendido pela assinatura manuscrita que expressa a aprovação do conteúdo visualizado diretamente.	Uso de plataforma confiável garante o acesso ao conteúdo, sendo a assinatura digital responsável pela expressão da concordância.
Disponibilidade	O aspecto segurança está ligado ao armazenamento seguro do documento. O aspecto funcionalidade está relacionado à forma de acesso ao documento ou cópia autenticada.	O aspecto segurança está relacionado com o armazenamento seguro e controle de acesso. O aspecto funcionalidade é relacionado ao uso plataforma computacional com recursos suficientes para acesso ao documento local ou remotamente.
Anonimato	O uso de documentos impressos sem assinaturas garante o atendimento deste requisito.	O uso de redes de misturadores garante o anonimato no envio.
Auditoria	A auditoria com relação ao acesso aos documentos não é facilmente obtida sendo necessário mecanismos externos para o controle de acesso. Uma entidade depende de recursos próprios para armazenar dados sobre documentos ou assinaturas geradas anteriormente.	A auditoria com relação ao controle de acesso pode ser obtida através de aplicativos apropriados ou então fornecida pelos sistemas operacionais, parte componente das plataformas computacionais utilizadas.

Figura 7 - Atendimento aos Requisitos de Segurança.

Fonte: DIAS, 2004, p. 37

2.8 CRIPTOGRAFIA

Criptografia é a escrita oculta (do grego *kryptós*, oculto, e *graphos*, escrita), isto é, escrever de forma codificada, permitindo apenas com que o remetente e o destinatário possam ler a mensagem original.

O processo de codificar uma informação se chama cifragem e o processo inverso decifragem. Estes se utilizam de algoritmos matemáticos para modificar as informações. O algoritmo se utiliza de uma chave, um segredo conhecido apenas pelas partes envolvidas para modificar a informação, transformando esta num texto cifrado ilegível para todos. Para decifrar a informação é necessária novamente a mesma chave, assim permitindo voltar à mensagem original.

A criptografia pode ser de dois tipos: simétrica, quando a chave utilizada para cifrar e decifrar são exatamente as mesmas; e assimétrica, quando a chave utilizada para cifrar for diferente da utilizada para decifrar.



Figura 8 - Esquema de criptografia simétrica.
Fonte: O QUE É CERTIFICADO DIGITAL, p. 2

Apesar de a criptografia simétrica ser mais eficiente, consumir menos recursos tecnológicos, ela possui um grande problema: como compartilhar uma mesma chave de forma segura? Sem que nenhuma pessoa indevida a descubra? Por isso atualmente é mais utilizado a criptografia assimétrica, que contém uma chave pública (compartilhada com todos) e uma chave privada (somente seu dono deve possuir). Tudo que for cifrado com a chave privada pode ser decifrado com a respectiva chave pública e vice e versa.

Dessa forma, se desejarmos mandar uma informação sigilosa para Beto, basta cifrarmos a mensagem com sua chave pública e teremos a garantia de que somente o Beto, com sua chave privada, poderá decifrar a mensagem.

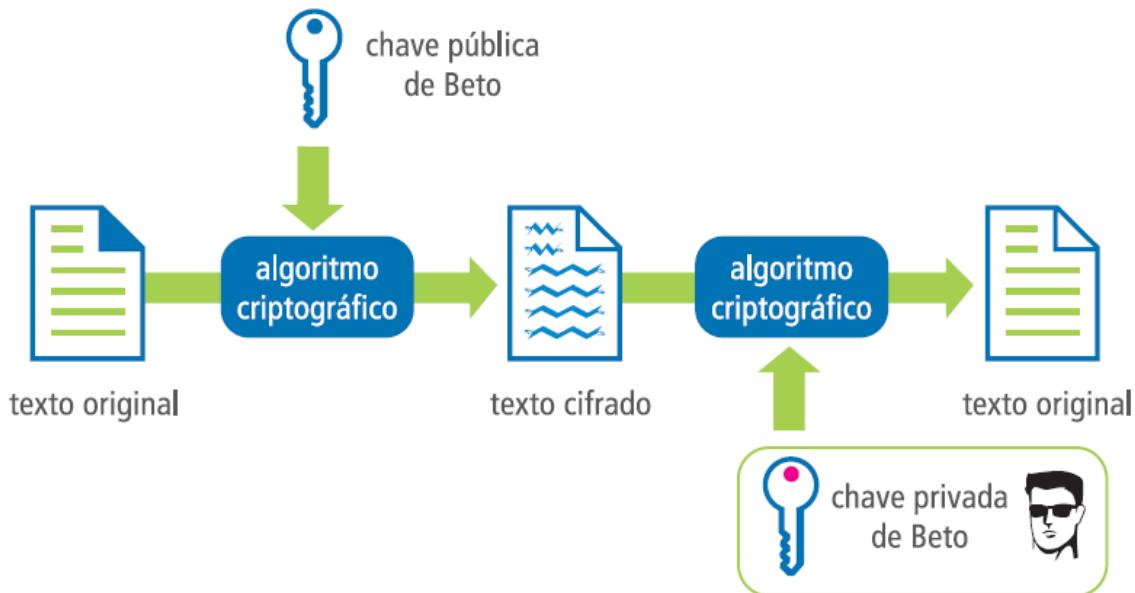


Figura 9 - Esquema de criptografia assimétrica com sigilo de informação.

Fonte: O QUE É CERTIFICADO DIGITAL, p. 4

Por outro lado, se Beto desejar mandar uma mensagem pública, em que todos possam ler e ter certeza de sua autenticidade; basta que Beto crie com sua chave privada. Assim todos que possuírem sua chave pública de Beto poderão ler a mensagem e ter certeza que foi Beto que a escreveu.

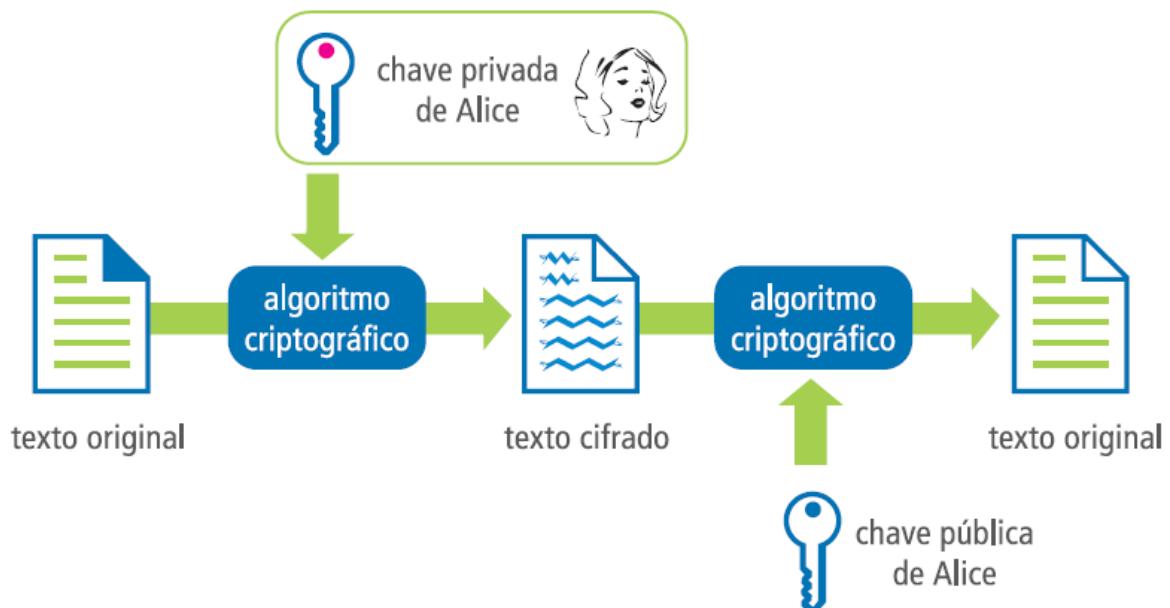


Figura 10 - Esquema de criptografia assimétrica com autenticidade de informação.

Fonte: O QUE É CERTIFICADO DIGITAL, p. 5

Um dos únicos, pontos fracos da criptografia assimétrica é garantir a autenticidade das chaves públicas. Como ter certeza que a chave pública é realmente de uma determinada

pessoa? Para isso, Loren Kohnfelder (1978) propôs uma solução adicionando uma terceira entidade confiável, denominada de Autoridade Certificadora. Esta entidade garante o relacionamento entre a chave pública e o seu proprietário.

2.9 INFRAESTRUTURA DE CHAVES PÚBLICAS

A infraestrutura de chaves públicas (ICP) foi introduzida para prover um incremento no nível de confiança na troca de informações na internet, combatendo o aumento da insegurança na internet. Uma ICP é composta por *hardware*, *software*, pessoas, políticas e procedimentos necessários para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais (TOORANI e SHIRAZI, 2008).

Uma das entidades da ICP é a autoridade certificadora (AC), que utiliza o conceito de terceira parte confiável, e tem como objetivo relacionar a chave pública com seu respectivo usuário. A identidade do usuário deve ser única e estabelecida através do registro deste, que é de responsabilidade da autoridade de registro (AR). O processo de registro garante que a chave pública é relacionada ao indivíduo sem possibilidade de repúdio.

Outra das atribuições da AC é manter um repositório com todos os certificados digitais válidos emitidos e a lista dos certificados digitais revogados. Dessa forma sempre que necessário é possível checar se um determinado documento digital assinado é válido, garantindo a autenticidade e o não repúdio.

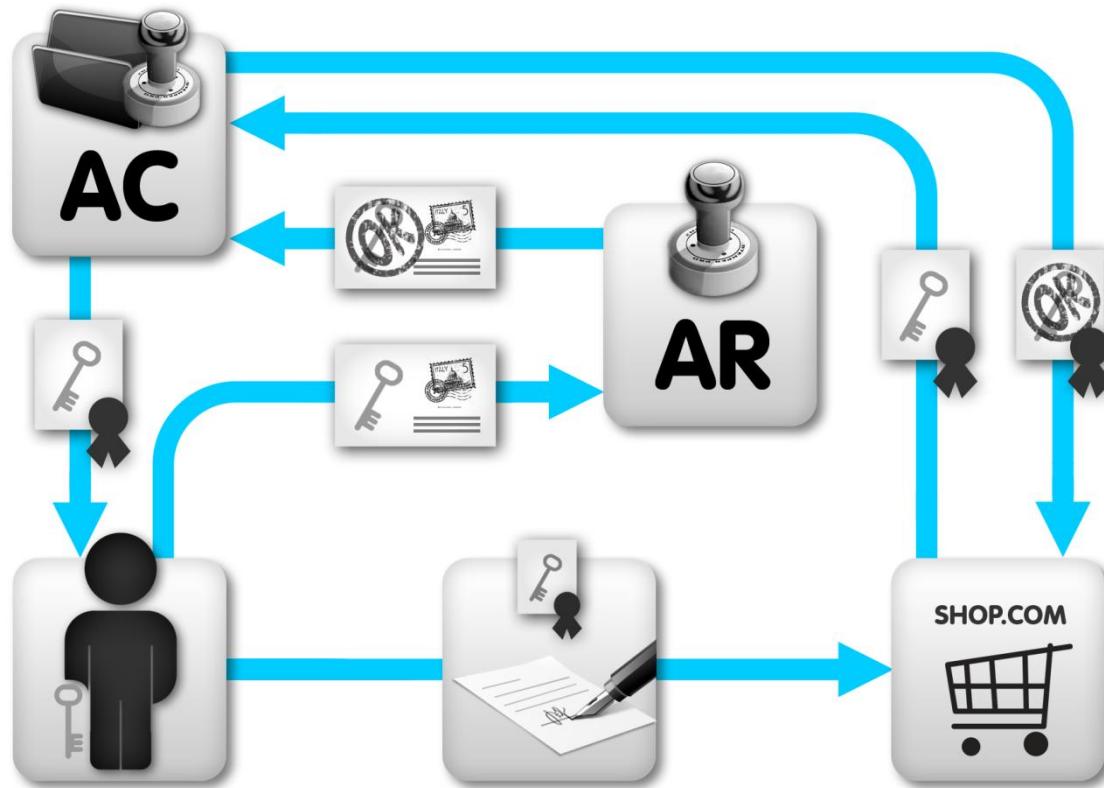


Figura 11 - Infraestrutura de Chaves Pùblicas

Fonte: produção do próprio autor

2.10 ICP BRASIL

A Infraestrutura de Chaves Pùblicas do Brasil (ICP-Brasil) foi instituída em agosto de 2001 através da medida provisória 2200-2. A partir desta medida provisória foi operacionalizado o Comitê Gestor (CG), a AC Raiz da ICP-Brasil e iniciado o processo de credenciamento de Autoridades Certificadoras de segundo nível. O Governo Federal, ao criar a ICP-Brasil, teve o intuito de aumentar a segurança nas transações eletrônicas e incentivar a utilização da Internet para negócios (RIBEIRO *et al.*, 2004).

A partir dessa medida foram elaboradas as Resoluções do Comitê Gestor da ICP-Brasil, que passaram a reger as atividades das entidades integrantes da ICP-Brasil. Estas regulamentações estão disponíveis no site www.iti.gov.br.

O Instituto Nacional de Tecnologia da Informação (ITI), uma autarquia federal vinculada à Casa Civil da Presidência da República, é o responsável por manter a ICP-Brasil. Outra de suas atribuições, é coordenar o Comitê Técnico de Implementação do Software Livre no Governo Federal, que compete estimular projetos de pesquisa científica e de

desenvolvimento tecnológico voltados à ampliação da cidadania digital. A principal linha deste é a popularização da certificação digital e a inclusão digital (COSTA, 2010).

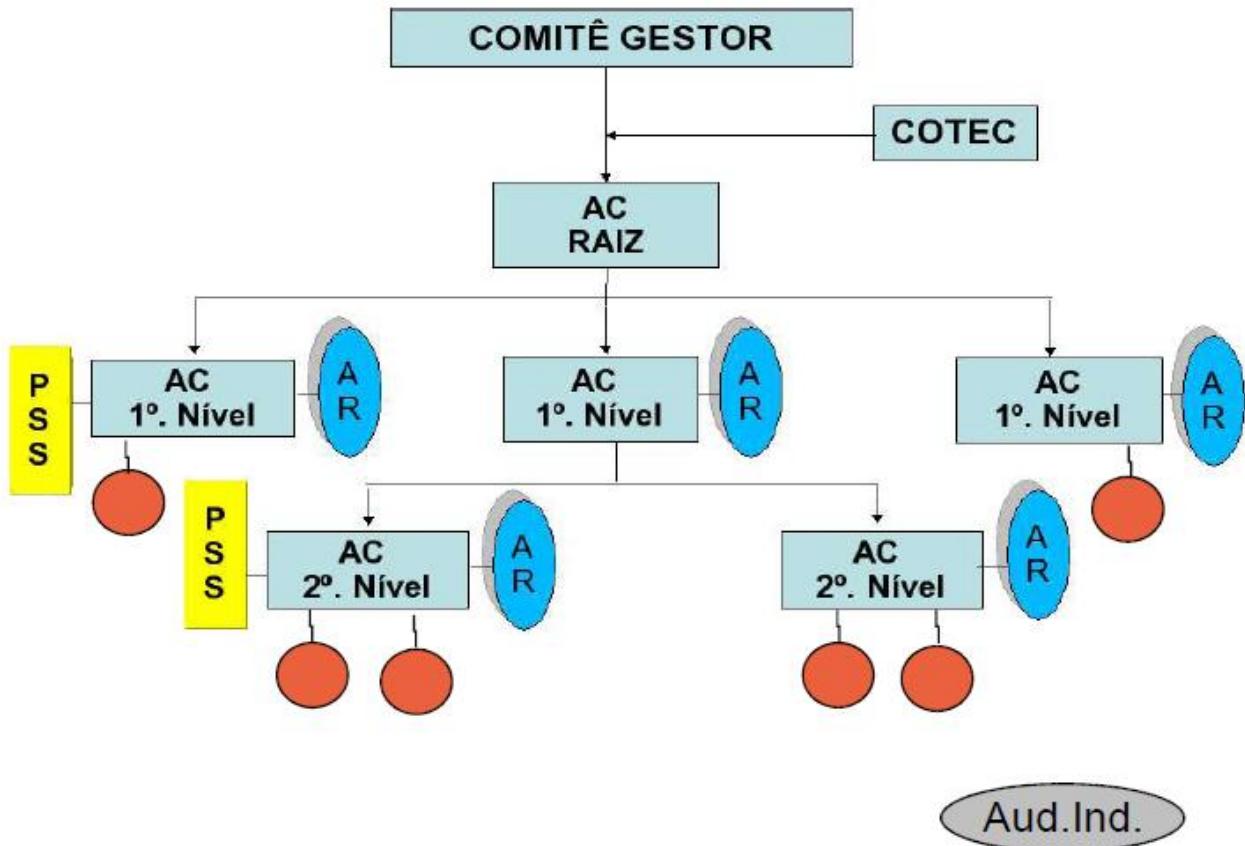


Figura 12 - Visão geral da estrutura da ICP-Brasil.

Fonte: RIBEIRO *et al*, 2004, p. 6

A ICP-Brasil é formada por várias entidades, sendo elas: o Comitê Gestor (CG), o Comitê Técnico (COTEC), a Autoridade Certificadora Raiz (AC-Raiz), as Autoridades Certificadoras (AC), as Autoridades Registradoras (AR), os Prestadores de Serviços de Suporte (PSS), os Auditores Independentes, Titulares de Certificados e Terceiras Partes. A seguir estão explicados o que são e as funções de cada uma destas entidades.

2.10.1 Comitê Gestor

Segundo Costa (2010), o CG possui as seguintes funções:

- Coordena a implantação e o funcionamento da ICP-Brasil;
- Estabelece a política, os critérios e as normas para credenciamento das AC, AR e demais PSS em todos os níveis da cadeia de certificação;

- Estabelece diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das ARs;
- Define níveis da cadeia de certificação;
- Atualiza, ajusta e revisa os procedimentos e as práticas estabelecidas para a ICP-Brasil;
- Garante a compatibilidade da ICP-Brasil e promove a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança;
- Estabelece a política de certificação e as regras operacionais da AC Raiz;
- Homologa, audita e fiscaliza a AC Raiz e os seus prestadores de serviço;
- Aprovam políticas de certificados, práticas de certificação e regras operacionais;
- Credencia e autoriza o funcionamento das AC e das ARs;
- Autoriza a AC Raiz a emitir o correspondente certificado;
- Identifica e avalia as políticas de ICP externas;
- Negocia e aprova acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional;
- Certifica, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais;
- Pode delegar atribuições à AC Raiz.

2.10.2 Comitê Técnico

O Comitê Técnico é responsável por prestar suporte técnico e assistência ao CG sobre suas decisões e análises (RIBEIRO *et al*, 2004).

2.10.3 Autoridade Certificadora Raiz

A AC Raiz, segundo Ribeiro *et al* (2004) e Costa (2010), é a primeira autoridade da cadeia de certificação da ICP-Brasil, e possui as seguintes funções:

- Executa as políticas de certificados e normas técnicas e operacionais aprovadas pelo CG;

- Emite, expede, distribui, revoga e gerencia os certificados das AC de nível imediatamente subsequente ao seu;
- Gerencia a lista de certificados revogados;
- Executa atividades de fiscalização e auditoria das AC e das ARs e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo CG da ICP-Brasil;
- Participa de tratativas para celebração de convênios e políticas de certificação internacionais.

2.10.4 Autoridade Certificadora

As ACs são credenciadas pela AC-Raiz para emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular. Suas principais funções de acordo com Costa (2010) são:

- Emitir, expedir, distribuir, revogar e gerenciar os certificados;
- Colocá-los à disposição dos usuários as listas de certificados revogados e outras informações pertinentes;
- Manter o registro de suas operações.

2.10.5 Autoridade de Registro

As ARs são operacionalmente vinculadas à uma determinada AC, sendo suas funções: identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros das suas operações (RIBEIRO *et al*, 2004).

2.10.6 Prestador de Serviços de Suporte

Os Prestadores de Serviços de Suporte são empresas contratadas por uma AC ou AR para realizar uma ou mais das atividades abaixo (RIBEIRO *et al*, 2004):

- Disponibilizar infraestrutura física e lógica;
- Disponibilizar recursos humanos especializados.

2.10.7 Auditorias Independentes

As Auditorias Independentes, autorizadas pela AC-Raiz da ICP-Brasil, são contratadas pelas AC para realizar auditorias operacionais em entidades a elas subordinadas (RIBEIRO *et al*, 2004).

2.10.8 Titulares de Certificados

Os Titulares de Certificados são pessoas físicas ou jurídicas, que podem ser titulares dos certificados digitais emitidos por uma das AC integrantes da ICP-Brasil (RIBEIRO *et al*, 2004).

2.10.9 Terceiras Partes

As Terceiras Partes são a parte que confia no teor, na validade e na aplicabilidade do certificado digital emitido por uma das AC integrantes da ICP-Brasil (RIBEIRO *et al*, 2004).

3 PROCEDIMENTOS METODOLÓGICOS

Como visto anteriormente o objetivo deste estudo é estruturar um modelo econômico-financeiro para avaliar a sustentabilidade das ACs e ARs vinculadas. Dessa forma, resultando em um modelo multidimensional criado dentro de uma ferramenta de CPM, permitindo a análise de cenários em busca do modelo econômico-financeiro mais sustentável.

3.1 CARACTERIZAÇÃO DA PESQUISA

Esta pesquisa está embasada por uma abordagem teórico-empírica, na qual além da revisão da literatura e da legislação sobre o assunto, procura-se verificar a coerência com a realidade, para conceber um conjunto de informações que possuam contribuições práticas para o problema em questão.

A pesquisa se caracterizou como de abordagem qualitativa, já que busca estruturar um modelo econômico-financeiro para avaliar a sustentabilidade da ICP-Brasil. Para Richardson (1999) a abordagem é qualitativa quando a investigação não é baseada em dados quantificáveis, mas sim na coleta e organização de dados que fornecessem informações suficientes para a construção de um modelo.

Segundo, Neves (1996, p. 1) faz parte da pesquisa qualitativa a obtenção de dados descritivos mediante contato direto e interativo do pesquisador com a situação objeto do estudo. O mesmo autor afirma que nas pesquisas qualitativas é frequente que o pesquisador procure entender os fenômenos, segundo a perspectiva da situação estudada e a partir disso situe sua interpretação dos fenômenos abordados.

No que diz respeito à sua natureza, esta pesquisa é considerada como aplicada e prática, já que ela tem como principal finalidade gerar soluções potenciais para os problemas humanos (ROESCH, 1999), sendo que neste caso específico, tem a finalidade de construir um modelo que permita determinar a melhor composição econômico-financeira possível para a emissão de certificados digitais de forma eficiente e a um custo aceitável para os usuários finais.

3.2 TÉCNICAS DE COLETA E ANÁLISE DE DADOS

A pesquisa configura-se metodologicamente em quatro etapas apresentadas na tabela 1, a partir do qual se pode ter uma visão geral de todas as características do conjunto de metodologias que foi adotado:

Etapas	Técnica	Abordagem ou Método	Instrumentos	Características	Dimensão
1 ^a - Revisar a literatura e a legislação pertinente	Revisão Teórica + Análise Documental	Descritiva Exploratória Dedutivo	Análise documental Pesquisa bibliográfica Observação	Objetivo	“É”
2 ^a - Análise de casos à luz da teoria	Entrevistas abertas	Qualitativa Estudo de caso	Roteiro Observação	Objetivo + Subjetivo	“É” Versus “Deve ser”
3 ^a - Desenvolver modelo econômico-financeiro	Fundamentação teórica + objetivo + subjetivo	Avaliativo Indutivo	Modelagem de requisitos	Objetivo + Subjetivo	“Deve ser”
4 ^a - Avaliar cenários em busca da sustentabilidade	Fundamentação teórica + objetivo + subjetivo	Descritiva Avaliativo Comparativa	Análise de cenários Estado da arte	Objetivo + Subjetivo	“Deve ser”

Tabela 1 - Estrutura metodológica da pesquisa.

Fonte: Elaboração própria, com base em Amboni, 1997; Bertero, 2006.

O trabalho em sua primeira fase é exploratório e descritivo, buscando identificar os requisitos operacionais de uma AC e suas ARs vinculadas. Isso se dará tanto através de uma análise documental como observação e pesquisa bibliográfica.

Posteriormente para confrontar os dados encontrados com a prática foi feito um estudo de casos. Para isso foi estudado uma ARs na cidade de Florianópolis, uma AR de pequeno porte, que tem como atividade fim a prestação de serviços e o desenvolvimento de ferramentas e hardware para a segurança de dados. Nesta AR a emissão de certificados digitais tinha como objetivo aproveitar o espaço físico e o conhecimento, já existente, em certificados digitais.

Além dos dados obtidos desta AR, foram feitas duas entrevistas em profundidade com um gestor integrante da ICP-Brasil, o qual possui fluência nas normas e conhece o dia a dia de diversas ARs e ACs no Brasil. Ainda com o objetivo de se aprofundar ainda mais no objeto de estudo, foi feito uma terceira entrevista com uma consultora da ICP-Brasil e gestora de uma AC com alcance a nível nacional.

Com o objetivo de se ter uma visão do usuário final do certificado digital, o autor adquiriu um e-CPF com o *e-token*. A solicitação do certificado foi feita on-line e a emissão foi

feita através de uma visita a empresa do autor. A emissora do certificado digital é uma empresa de grande com atendimento nacional, sua indicação veio do banco Itaú.

Na sequência foi elaborado um modelo multidimensional financeiro-econômico em uma ferramenta de COM, *Sysphera Enterprise Suite*. Para isto além de levar em conta a teoria e a legislação encontrada, foi confrontado com a realidade de algumas organizações através dos dados dos estudos de casos descrito acima.

Por último, o modelo foi avaliado em possíveis cenários buscando a situação ideal e permitindo a sua comparação com a situação atual, mostrando aos gestores o potencial de modelos alternativos.

O presente trabalho de pesquisa também se distingue pela dimensão do ‘é’ e do ‘deve ser’, de forma semelhante a Bertero (2006) e a Amboni (1997). Conforme Amboni (1997) a dimensão do ‘é’ apresenta como característica essencial a precisão e a objetividade, retratando as circunstâncias atuais na etapa exploratória. Essa etapa consiste na expressão do conhecimento racional, ela é informativa e objetiva.

Dessa forma, a pesquisa busca combinar aspectos da dimensão objetiva, de como as ACs e ARs são atualmente e na sequência realiza-se uma apreciação acerca do assunto (dimensão subjetiva) configurando uma etapa avaliativa de como eles poderiam ser aperfeiçoados (dimensão do ‘deve ser’). Assim através deste estudo é possível avaliar e identificar o modelo econômico-financeiro ideal para a operação das ACs e ARs no Brasil.

3.3 LIMITAÇÕES DA PESQUISA

A literatura sobre a ICP-Brasil e pesquisas neste campo são escassas. A documentação oficial da ICP-Brasil, em alguns pontos, é bastante subjetiva e a interação com o objeto de pesquisa confirmou esse fato. O principal objetivo da ICP-Brasil é garantir a segurança, o sigilo e a integridade de seus dados, com isso em mente as auditorias e fiscalizações traduzem a subjetividade em bom senso. No entanto, isso gera maior dificuldade em identificar os custos envolvidos.

A estrutura da ICP-Brasil envolve muita segurança e controle. Dessa forma, o acesso a ela é difícil; ainda mais o acesso a sua parte financeira, pois isso revela estratégias sigilosas da organização em questão. Assim o acesso ao objeto de estudo foi bastante difícil, alguns custos foram identificados apenas na cidade de Florianópolis e outros na cidade de São

Paulo, não sendo estatisticamente possível extrapolarmos os resultados desta pesquisa para outros lugares.

O tempo disponível para se estudar uma organização tão complexa como a ICP-Brasil é curto, quanto mais para apresentar um modelo ideal para analisar a sustentabilidade econômico-financeira.

O mercado de certificados digitais não fez parte deste estudo, o limite do volume de emissões foi ponderado por características físicas (limite de hardware e de pessoal). O impacto de ações de marketing para suportar o aumento do volume de emissões também não foi considerado neste estudo.

4 APRESENTAÇÃO, ANÁLISE E INTERPRETAÇÃO DOS DADOS

A ICP-Brasil é regida por diversas normativas ou resoluções, que orientam as entidades envolvidas na emissão de certificados digitais. De forma a facilitar o estudo e a compreensão destas normas, a ICP-Brasil organizou os documentos principais (DOC-ICP), que trazem as diretrizes gerais sobre os diversos assuntos normatizados. Cada DOC-ICP corresponde a uma resolução vigente, uma versão resumida da publicada no Diário Oficial da União.

Os custos presentes nas AC e AR foram identificados através de oito documentos de normas principais. Nestes documentos as obrigações, responsabilidades, procedimentos e controles foram demonstrando os custos envolvidos nas atividades de emissão de certificados digitais. Em algumas situações as normas impõem os custos de forma explícita, como citando tarifas e número mínimo de colaboradores, mas em outras situações o custo fica subjetivo, onde somente com a prática, o dia a dia de uma entidade, é possível identificarmos o verdadeiro custo. Para isso foram feitas visitas a algumas ARs, conversas informais com alguns gestores e prestadores de serviços tanto de ARs como de ACs.

Os oito documentos utilizados para identificarmos os custos foram:

- DOC-ICP-01 - Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil - v.4.1 (ICP-BRASIL, 2010a);
- DOC-ICP-02 - Política de Segurança da ICP-Brasil - v.3.0 (ICP-BRASIL, 2008a);
- DOC-ICP-03 - Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil - v.4.5 (ICP-BRASIL, 2010b);
- DOC-ICP-03.01 - Características Mínimas de Segurança para as AR da ICP-Brasil - v.1.4 (ICP-BRASIL, 2010c);
- DOC-ICP-05 - Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil - v.3.5 (ICP-BRASIL, 2010d);
- DOC-ICP-06 - Política Tarifária da Autoridade Certificadora Raiz da ICP-Brasil - v.3.0 (ICP-BRASIL, 2008b);
- DOC-ICP-08 - Critérios e Procedimentos para Auditoria das Entidades Integrantes da ICP-Brasil - v.4.0 (ICP-BRASIL, 2009);

- DOC-ICP-09 - Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP-Brasil - v.3.0 (ICP-BRASIL, 2008c);

A análise dos custos para buscar o equilíbrio econômico-financeiro foi feito focando nas duas principais entidades da ICP-Brasil, as ARs e ACs. Dessa forma, buscou-se identificar todos os custos e receitas destas entidades, como se fossem empresas separadas e independentes.

4.1 CUSTOS COMUNS AS ARS E ACS

No DOC-ICP-02 (ICP-BRASIL, 2008a) são estabelecidas as diretrizes de segurança que deverão ser adotadas por todas as entidades participantes da ICP-Brasil, incluindo então as ARs e ACs. O principal objetivo dessas diretrizes são garantir um nível de segurança mínimo para a ICP-Brasil e suas entidades, consequentemente essas normas acabam tendo um impacto direto nos custos.

Os requisitos de segurança são bastante abrangentes, desde regras gerais até regras mais específicas passando pelo âmbito humano, físico, lógico e de recursos criptográficos. As regras gerais impõem o gerenciamento de riscos e a criação, revisão e testes de um plano de continuidade do negócio uma vez por ano. Na prática isso acarreta mais procedimentos administrativos para um gestor, que de tempos em tempos deve se reunir com sua equipe para analisar, planejar e testar esses planos.

No âmbito humano, de segurança de pessoal, as necessidades são para a proteção dos ativos das entidades participantes da ICP-Brasil. Regras que impõe um processo de admissão mais criterioso, com uma série de procedimentos visando um maior controle e previsibilidade das ações dos envolvidos.

A segurança do ambiente físico também é um ponto bastante importante, impondo a necessidade de sistemas de vigilância, controle de acesso, detecção de intrusão e até o monitoramento das áreas onde ocorrem processos críticos.

Os requisitos de ambiente lógico impõem uma série de regras para acesso a sistemas, controle de usuário e senha, auditoria de logs, rotinas de backup, combate a vírus, entre outros. Os recursos criptográficos são imposições para utilização de *softwares* e *hardwares* homologados pela ICP-Brasil. Por ultimo, temos a imposição de auditorias e fiscalizações periódicas, que também ajudam a aumentar a percepção de confiança da comunidade de

usuários, dado que estes visam verificar a capacidade das entidades em atender aos requisitos da ICP-Brasil.

Todas essas regras, aqui resumidas, se encontram no DOC-ICP-02 (ICP-BRASIL, 2008a). Estas acarretam claramente em custos maiores de infraestrutura e manutenção destes processos. Seguir todas essas regras do ambiente humano, físico, lógico e de requisitos criptográficos geram um esforço maior, exigindo um custo operacional e administrativo maior. No entanto, é difícil mensurarmos isto sem uma visão mais prática, por isso no detalhamento de ARs e ACs iremos utilizar essa visão para quantificarmos o impacto nos custos destes requisitos.

4.2 CUSTOS DAS ARS

Inicialmente a AR precisa fazer o seu credenciamento na ICP-Brasil. Para isso ela precisa atender aos requisitos econômico-financeiros estabelecidos, além dos requisitos jurídicos e fiscais. A boa situação econômico-financeira é considerada aos candidatos que (ICP-BRASIL, 2010b):

- a) Possuírem um Retorno Sobre o Patrimônio Líquido (RSPL) igual ou superior à da Taxa de Juros de Longo Prazo (TJLP) média no último exercício social;
- b) Caso se tenha um prejuízo no último exercício social, o candidato poderá efetuar o cálculo da média dos cinco últimos anos;
- c) Caso o resultado no item “a” e “b” sejam menor que o TJPL, mas forem maiores do que zero, o candidato deverá comprovar que possui Patrimônio Líquido (PL) igual ou superior a R\$ 100.000,00 reais;
- d) Caso a empresa tenha sido criada a menos de um ano e não seja elegível, a candidata deverá apresentar um seguro de responsabilidade civil e operacional no valor mínimo de R\$ 100.000,00 reais;

A RSPL é calculada dividindo o Lucro Líquido do exercício (LL) pela média do PL inicial mais o PL final do período.

A AC pode cobrar da AR uma taxa de credenciamento, esta taxa pode ser de R\$15.000,00 até R\$40.000,00 reais. Vamos considerar um valor de R\$15.000,00 reais, que foi o menor valor encontrado no mercado.

Ainda em relação ao credenciamento é exigido ter sede administrativa, instalações operacionais e recursos de segurança física e lógica compatíveis com a atividade de registro

(ICP-BRASIL, 2010b). Essas exigências são verificadas via auditoria pré-operacional e operacional, no caso específico da AR podem ser feitas por uma empresa de auditoria independente credenciada junto ao ITI (ICP-BRASIL, 2009). O custo desta auditoria é em média de R\$3.500,00 reais por ano, podendo variar bastante por região e empresa de auditoria.

A fiscalização da AR pode ser feita semestralmente, em outro prazo sugerido pela auditoria, por denúncia feita por usuário, ou por constatação de ameaça à confiabilidade da ICP-Brasil (ICP-BRASIL, 2008c). Quem realiza os processos de fiscalização são os fiscais da AC Raiz, este processo não tem custos para a AR.

Para a execução das atividades inerentes à AR, existem os agentes de registro, pessoa responsável pela validação e verificação da solicitação de certificados (ICP-BRASIL, 2010c). Nos DOC-ICPs não é exigido uma quantidade mínima de agentes de registro, mas para manter um nível adequado de segurança consideramos dois agentes de registro como o número mínimo. Dessa forma, uma única pessoa não conseguirá emitir um certificado, sempre teremos a dupla verificação feita por duas pessoas para uma maior segurança.

Os agentes de registro precisam ser treinados no momento de sua contratação, este treinamento precisa conter uma carga horária mínima de 16 horas, sobre os seguintes temas (ICP-BRASIL, 2010c):

- Princípios e mecanismos de segurança da AR;
- Sistema de certificação em uso na AC;
- Procedimentos de recuperação de desastres e de continuidade do negócio;
- Reconhecimento de assinaturas digitais e validade dos documentos apresentados;
- Outros assuntos relativos á atividade sob sua responsabilidade;

Anualmente os agentes de registro devem ser avaliados, de forma com que seja detectado a necessidade de atualização técnica e de segurança (ICP-BRASIL, 2010c). Apesar de não exigido nos DOC-ICPs algumas ACs exigem um treinamento de atualização anual sem custos. O custo do treinamento inicial para os agentes de registro é em média de R\$ 300,00 reais.

Além dos agentes de registro, uma AR precisa do responsável pela instalação técnica ou posto provisório. Este responsável deverá garantir a segurança física, lógica, de rede e da informação. Outras atividades administrativas, comuns a toda e qualquer empresa, também podem ser feitas por este mesmo responsável.

Com isso concluímos que uma AR precisa no mínimo de três pessoas para o seu funcionamento. Sendo que em média esses profissionais terão um salário médio de R\$2.500,00 reais mais encargos.

As instalações físicas de uma AR podem ser dedicado ou compartilhado com outras atividades da organização. Em ambos os casos é necessário (ICP-BRASIL, 2010c):

- Equipamentos de prevenção de incêndio;
- Armário ou gabinete com chave;
- Circuitos elétricos com *no-break* para os equipamentos de processamento de dados;
- Circuitos elétricos e lógicos deverão ser protegidos por tubulação adequada.

No caso das ARs com ambiente dedicado, temos as seguintes exigências (ICP-BRASIL, 2010c):

- Controle de acesso ao ambiente;
- Porta única de entrada, com fechadura tetra;
- Paredes que previnam o acesso não autorizado;
- Iluminação de emergência;
- No caso de possuir janelas ou qualquer abertura para o ambiente exterior, essas devem ser lacradas ou gradeadas, para impedir o acesso externo.

Para as ARs com ambiente compartilhado, temos as seguintes exigências (ICP-BRASIL, 2010c):

- Vigilância ostensiva ou monitoramento por circuito fechado de TV, no ambiente da AR;
- Controle de acesso ao prédio ou ao ambiente onde se encontra a AR;

Em relação ao custo do espaço físico, no caso do ambiente dedicado seria necessária uma sala com no mínimo trinta metros quadrados, resultando num aluguel mínimo de R\$1.200,00 reais mensais. No caso do ambiente compartilhado este valor pode ser menor ou até mesmo nulo, pois outras atividades da organização que se utilizam do mesmo espaço físico podem ser suficientes para pagar os custos de aluguel.

Abaixo (tabela 2) segue os custos fixos médios iniciais de uma AR:

Descriutivo	Valor
Dois computadores	R\$6.000,00
Impressora multi-funcional	R\$1.200,00
Dois certificados digitais e-CPF com <i>smart-card</i>	R\$730,00
Três mesas	R\$1.575,00
Seis cadeiras	R\$1.020,00
Duas estantes	R\$2.489,00
No-break	R\$1.108,00
Treinamento inicial de dois agentes de registro	R\$600,00
Taxa de credenciamento na AC	R\$15.000,00
Total	R\$29.722,00

Tabela 2 - Custos fixos de um AR.

Fonte: Elaboração própria.

Abaixo (tabela 3) seguem os custos mensais médio de uma AR:

Descriutivo	Valor
Aluguel de sala comercial	R\$1.100,00
Software para emissão de certificado digital	R\$400,00
Limpeza do escritório	R\$200,00
Energia elétrica	R\$300,00
Telefone e Internet	R\$200,00
Salário com encargos e benefícios do responsável técnico	R\$4.000,00
Salário com encargos e benefícios dos dois agentes de registro	R\$7.655,56
Contador	R\$500,00
Total	R\$14.355,56

Tabela 3 - Custos mensais de um AR.

Fonte: Elaboração própria.

Abaixo (tabela 4) seguem os custos mensais esporádicos médios de uma AR:

Descriutivo	Valor
Auditoria (a cada 12 meses)	R\$3.500,00
Total	R\$3.500,00

Tabela 4 - Custos esporádicos de um AR.

Fonte: Elaboração própria.

Além dos custos citados acima ainda temos os impostos, que devidos as características de micro empresa de uma AR iremos considerar uma alíquota média de 15,15% sobre o faturamento bruto.

4.3 RECEITAS DAS ARS

As receitas de uma AR são concentradas basicamente na emissão de diferentes tipos de certificados digitais e na venda de hardware para armazenar estes certificados digitais. Os certificados digitais mais vendidos são o e-CPF e o e-CNPJ, pois são geralmente os mais exigidos para várias finalidades.

O prazo de duração desses certificados também pode variar, mas o com validade de três anos é o que possui um melhor custo benefício. Um e-CNPJ para três anos custa R\$245,00 reais enquanto que para um ano custa R\$165,00 reais, mais do que o dobro se considerarmos que a primeira opção custa R\$82,00 reais por ano.

O hardware pode variar de tipo e marca, os mais ofertados são o *eToken* (funciona como um *pen-drive*) e o *smartcard* (com ou sem a leitora inclusa). O preço do *eToken* e do *smartcard* com a leitora é equivalente, na faixa de R\$200,00 reais.

No caso do certificado digital a AR ganha uma comissão sobre o valor de venda, de aproximadamente trinta por cento. Para o hardware a AR também pode ganhar apenas uma comissão sobre a venda deste, de aproximadamente vinte por cento; ou ela pode buscar no mercado outra forma mais barata para adquirir o hardware, assim aumentando seu percentual de comissão. Com uma pesquisa rápida pode-se encontrar no Brasil o *eToken* por R\$50,00 reais e no exterior por \$10 dólares, isto é, deve ser bastante viável para a AR fazer uma importação direta ou mesmo procurar outras opções de fornecedores para o hardware.

No modelo para avaliar a sustentabilidade econômico-financeira iremos simplificar assumindo que todas as vendas irão incluir hardware e um certificado com validade de três

anos a um preço médio de R\$205,00 reais. Como o e-CPF custa R\$165,00 reais e o e-CNPJ custa R\$245,00 reais assumimos uma proporção de venda equivalente, chegando a um preço médio de R\$205,00 reais mais o hardware de R\$200,00 reais. A comissão que usaremos por padrão será de trinta por centro sobre o *software* e de vinte por centro sobre o hardware, como se a AR opta-se apenas por revender todos os *hardwares* fornecidos pela AC que ele está vinculado.

Outra variável importante relacionada à receita é o volume de vendas. Cada agente de registro tem capacidade de atender a um usuário a cada quarenta e cinco minutos, sendo trinta minutos para atendimento do cliente e mais quinze minutos para outros procedimentos sem a presença do cliente. Conforme citado anteriormente, para termos um maior nível de segurança sempre serão necessários termos dois agentes de registro para a emissão de cada certificado, assim sempre que um agente atender o usuário, o segundo agente deverá fazer os demais procedimentos. Garantindo assim que nunca um único agente de registro poderá emitir um certificado digital.

Com isso temos um volume total por agente de 224 emissões de certificados digitais por mês, totalizando uma capacidade de 448 emissões mensais para os dois agentes de registro.

Na tabela 5 está representado o resumo das receitas de uma AR com dois agentes de registro utilizando sua capacidade máxima, que será dificilmente alcançada, mas exploraremos mais disso nas análises de cenários:

Descriutivo	Valor Unitário	Valor Total
Número de emissões de certificados digitais	224	448
Comissão de emissão de certificado digital (30%)	R\$61,50	R\$27.552,00
Comissão de hardware (20%)	R\$40,00	R\$17.920,00
Total		R\$45.472,00

Tabela 5 - Receitas máxima de uma AR.

Fonte: Elaboração própria.

4.4 CUSTOS DAS ACS

Da mesma forma que a AR a AC também precisa fazer o seu credenciamento na ICP-Brasil. Para isso ela precisa atender aos requisitos econômico-financeiros estabelecidos, além

dos requisitos jurídicos e fiscais. A boa situação econômico-financeira é considerada aos candidatos que (ICP-BRASIL, 2010b):

- a) Possuírem um RSPL igual ou superior à da TJLP média no ultimo exercício social;
- b) Caso se tenha um prejuízo no último exercício social, o candidato poderá efetuar o cálculo da média dos cinco últimos anos;
- c) Caso o resultado no item “a” e “b” sejam menor que o TJPL, mas forem maiores do que zero, o candidato deverá comprovar que possui PL igual ou superior a R\$2.500.000,00 reais para AC de primeiro nível e igual ou superior a R\$1.000.000,00 reais para AC de segundo nível;
- d) Caso a empresa tenha sido criada a menos de um ano e não seja elegível, se candidata a:
 - AC de primeiro nível: possuir patrimônio líquido de R\$2.500.000,00 reais e deverá apresentar fiança bancária no valor do seu capital social integralizado;
 - AC subsequente: possuir patrimônio líquido de R\$1.000.000,00 reais e deverá apresentar fiança bancária no valor do seu capital social integralizado

A AC Raiz irá cobrar uma tarifa para a emissão do primeiro certificado da AC, no seu credenciamento de R\$500.000,00 reais. Para emissões posteriores ao primeiro certificado digital da AC a taxa muda para R\$100.000,00 reais (ICP-BRASIL, 2008b).

Ainda em relação ao credenciamento é exigido ter sede administrativa, instalações operacionais e recursos de segurança física e lógica, inclusive sala-cofre, compatíveis com a atividade de certificação (ICP-BRASIL, 2010b). Essas exigências são verificadas via auditoria pré-operacional, que acontece uma única vez antes da AC iniciar suas atividades, e operacional (ICP-BRASIL, 2009). O custo destas auditorias é estimado em média de R\$50.000,00 reais por ano.

A auditoria operacional em específico pode ser compartilhada quando a AC utiliza um prestador de serviços para a parte física. Dessa forma como a parte física do prestador de serviços é compartilhada entre várias ACs, a auditoria acontece uma única vez e o seu custo é compartilhado entre todas as ACs que utilizam-se desta infraestrutura. No escopo deste trabalho consideramos que a AC não irá utilizar-se de prestadores de serviços para a parte de infraestrutura, assim tendo que absorver todo o custo de auditoria de forma individual.

A fiscalização da AC, assim como a da AR, pode ser feita semestralmente, em outro prazo sugerido pela auditoria, por denúncia feita por usuário, ou por constatação de ameaça à confiabilidade da ICP-Brasil (ICP-BRASIL, 2008c). Quem realiza os processos de fiscalização são os fiscais da AC Raiz, este processo não tem custos para a AC.

A gestão das atividades inerentes à AC é feita por três perfis distintos (ICP-BRASIL, 2010a):

- Gerente de Configuração – responsável pela configuração e manutenção do hardware e software da AC;
- Gerente de Segurança – gerenciamento dos operadores da AC Raiz, implementação das políticas de segurança, verificação dos registros de auditoria e verificação do cumprimento da declaração de práticas de certificação;
- Administrador do Sistema – gerenciamento dos processos de iniciação dos usuários internos; emissão, expedição distribuição, revogação e gerenciamento de certificados; distribuição de cartões ou *token*, quando necessário;

Não existe uma quantidade mínima de pessoas exigidas nos DOC-ICPs, mas iremos assumir que são necessários no mínimo oito colaboradores: i) três gerentes como citado acima; ii) dois operadores para as atividades do dia a dia da AC; iii) um administrador para as atividades financeiras e administrativas da AC; iv) um gerente de recursos humanos para o controle de pessoal; v) um gerente comercial e de marketing para conseguir novas ARs vinculadas.

O treinamento de todo o pessoal da AC envolvido diretamente nas atividades de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá receber treinamento documentado e suficiente para os seguintes temas (ICP-BRASIL, 2010d):

- Princípios e mecanismos de segurança da AC;
- Sistema de certificação em uso na AC;
- Procedimentos de recuperação de desastres e de continuidade do negócio;
- Reconhecimento de assinaturas e validade dos documentos apresentados;
- Outros assuntos relativos a atividade sob sua responsabilidade;

A reciclagem técnica destas pessoas envolvidas nas atividades principais da AC deve ser constante, de forma a manter atualizado sobre eventuais mudanças tecnológicas (ICP-BRASIL, 2010d). O custo inicial deste treinamento é de R\$1.500,00 reais por pessoa, como temos cinco pessoas operacionais teremos um custo total de R\$7.500,00 reais. Iremos estimar

que o custo para eventuais atualizações tecnológicas seja de R\$500,00 reais por pessoa anualmente, totalizando em R\$2.500,00 reais.

O espaço físico de uma AC precisa ser composto de uma sala-cofre, que gira em torno de cinco milhões de reais a sua construção, mais uma parte administrativa que pode ser um anexo a sala-cofre, ou mesmo ficar em separado. Neste trabalho vamos considerar que a parte administrativa gera um aluguel de R\$22.000,00 reais e que o custo de manutenção da sala-cofre; incluindo seu seguro e manutenções como: de ar condicionado, equipamento anti-incêncio, entre outros; é de R\$50.000,00 reais por mês.

Além da sala cofre é necessária a aquisição de um Hardware Security Module (HSM) para a emissão de certificados digitais, mais um servidor onde iremos rodar um software para a gestão e controle das emissões de certificados digitais. Ainda a estimativa dos custos de uma sala cofre demonstrou-se bastante complexa, já que são poucas as empresas que prestam esse tipo de serviço e nenhuma quer divulgar seus preços. Em conversa com pessoas da área, chegou-se a uma estimativa de um custo total de três a quatro milhões de reais, então neste trabalho iremos considerar um custo a maior de cinco milhões de reais. Neste custo já estamos incluindo a HSM, que deve ter um custo aproximado de R\$150.000,00 reais, mais dois servidores com software, um sendo backup para eventual falha do primeiro, que devem ter um custo unitário de R\$30.000,00 reais incluindo o software necessário, e um relógio atómico.

O credenciamento de uma de uma AR gera um custo administrativo, que é cobrado da AR via a taxa de credenciamento. Dessa forma iremos considerar a inexistência deste custo, pois é pago pela AR.

Outro custo envolvido é o do hardware, conforme citado nas receitas da AR, o custo do hardware pode variar muito. Neste trabalho consideramos um custo de R\$40,00 reais por *eToken*.

Abaixo (tabela 6) segue os custos fixos médios iniciais de uma AC:

Descriutivo	Valor
Sete computadores	R\$21.000,00
Sala-cofre completa com HSM, servidor e software para gestão e emissão de certificados digitais	R\$5.000.000,00
Impressora multi-funcional	R\$1.200,00
Sete certificados digitais e-CPF com <i>smart-card</i>	R\$2.555,00
Sete mesas	R\$3.675,00
Quatorze cadeiras	R\$2.380,00
Quatro estantes	R\$4.978,00
No-break	R\$3.324,00
Treinamento inicial de cinco pessoas	R\$7.500,00
Primeira emissão de certificado	R\$500.000,00
Auditória pré-operacional	R\$50.000,00
Total	R\$5.596.612,00

Tabela 6 - Custos fixos de um AC.

Fonte: Elaboração própria.

Na tabela 7 estão representados os custos mensais médio de uma AC:

Descriutivo	Valor
Aluguel de sala para parte administrativa	R\$22.000,00
Custo de manutenção da sala-cofre (incluindo seguro)	R\$50.000,00
Manutenção de Software para emissão de certificado digital	R\$2.000,00
Limpeza do escritório	R\$2000,00
Energia elétrica	R\$1.500,00
Telefone e Internet	R\$1.000,00
Salário com encargos e benefícios dos três gerentes, dois operadores e um comercial	R\$32.695,56
Salário com encargos e benefícios dos gerentes de RH e administrativo	R\$10.000,00
Contador	R\$1.500,00
Serviços jurídicos	R\$3.500,00
Despesas com publicidade e propaganda	R\$15.000,00
Despesas com softwares	R\$2.000,00
Total	R\$143.195,56

Tabela 7 - Custos mensais de um AC.

Fonte: Elaboração própria.

Abaixo (tabela 8) seguem os custos mensais esporádicos médio de uma AC:

Descriutivo	Valor
Auditória (a cada 12 meses)	R\$50.000,00
Atualização tecnológica de cinco pessoas	R\$2.500,00
Total	R\$52.500,00

Tabela 8 - Custos esporádicos de um AC.

Fonte: Elaboração própria.

Além dos custos citados acima ainda temos os impostos, que devidos as características da AC iremos considerar uma alíquota média de cinco por cento sobre o faturamento bruto, referentes ao ISS, PIS e COFINS. Ainda sobre o resultado bruto da empresa iremos aplicar uma alíquota de trinta e quatro por cento, referentes ao imposto de renda e a contribuição social.

4.5 RECEITAS DAS ACS

As receitas da AC são basicamente quatro: i) a de emissão de certificados, a qual ela fica com setenta por centro do valor; ii) a do hardware vendido, o qual ela fica com vinte por centro do valor, pois consideramos que quarenta por centro é o custo de aquisição deste; iii) taxa de credenciamento da AR; iv) taxa de software para a AR.

As ponderações feitas na AR em relação aos tipos, valores e volumes dos certificados digitais são mantidos exatamente os mesmos na AC. A única diferença é que em baixo de uma AC podemos ter várias ARs, assim temos um multiplicador ainda maior sobre o volume de emissões de certificados digitais. A única limitação de volume da AC é de hardware, a HSM utilizada para gerar as assinaturas digitais tem capacidade de 500 mil requisições de assinatura por segundo. Isso significa que teríamos que ter mais do que 1.350 ARs credenciadas, com dois agentes cada, para gerar um volume superior a 500 mil requisições por segundo, um volume muito acima da realidade de uma AC, hoje em dia.

A quantidade de ARs credenciadas na AC vai depender do seu esforço comercial em credenciar o maior número possível de ARs e divulgar os seus serviços e de suas ARs assim auxiliando as ARs na obtenção de clientes.

Como estimamos que o custo de credenciamento de uma AR seria igual a taxa de credenciamento, neste momento também iremos desconsiderar esta receita, pois o custo e a receita devem se eliminar.

Abaixo (tabela 9) segue o resumo das receitas de uma AC com dez ARs credenciadas, emitindo cada uma 220 certificados por dia útil (adicionamos o custo do hardware para não distorcermos tanto a análise):

Descriutivo	Valor Unitário	Valor Total
Número de ARs credenciadas		10
Número de emissões de certificados digitais	220 por AR	2200
Comissão de emissão de certificado digital (70%)	R\$143,50	R\$351.700,00
Comissão de hardware (80%)	R\$160,00	R\$352.000,00
Custo do hardware	R\$40,00	-R\$88.000,00
Receita de software	R\$400,00	R\$4.000,00
Total		R\$619.700,00

Tabela 9 - Receitas da AC.

Fonte: Elaboração própria.

5 APRESENTAÇÃO DO MODELO

De forma a facilitar a análise dos dados levantados foi criado um modelo multidimensional dentro da ferramenta de CPM *Sysphera Enterprise Suite*. O modelo foi criado de forma a permitir a entrada de todos os custos, despesas e receitas para planejarmos uma AR e uma AC com suas várias ARs credenciadas.

O modelo foi criado com quatro dimensões:

- Conta – possui um plano de contas com premissas, criado para atender uma AR e uma AC (Figura 13);
- Tempo – nesta dimensão temos a abertura temporal, isto é, cinco anos abertos mês a mês (Figura 14);
- Cenário – esta dimensão permite criarmos vários cenários e versões dos dados, para depois podermos comparar um com o outro (Figura 15);
- Entidade – nas entidades abrimos as duas empresas, uma para a AR e outra para a AC (Figura 16);

Na figura 13 tem-se uma visão do plano de contas, como se fosse um demonstrativo de resultados das ARs e ACs.

The screenshot shows the SYSPHERA Enterprise Suite 2.5 Administration interface. The main title bar reads "http://localhost/mestrado/WebForm/Administration/Mem1" and "Administração dos Membros". The top menu includes "Modelagem", "Usuários", "Processos", "Data-Entry", "Carga de Dados", "Análise", "Relatórios", and "Dashboard". A dropdown menu "Administrador" is set to "Sustentabilidade". The left sidebar has a "Hierarquia" dropdown set to "Conta". The main panel displays a tree view under "Membros" labeled "Nome" with various financial categories like "Demonstrativo de resultados", "Resultado líquido", "Resultado antes dos impostos", "Resultado bruto", "Despesas gerais e administrativas", "IR e CSLL", "Resultado líquido acumulado", "Premissas", and "Qtd. dias úteis". To the right, a "Propriedades" panel shows settings for "Identificador" (47), "Tipo de Conta" (Receita), "Função de Agregação" (Soma), "Tipo de Dado" (Moeda), and "Tipo de Agregação" (+). Other properties include "Descrição", "Conta Dividendo", "Conta Divisor", "Lista" (Nenhum), "Nível", "Formatação Resumo" (Nenhum), and "Mostrar Relatório" (Sim).

Figura 13 - Estrutura da dimensão Conta.

Fonte: SYSPHERA, 2011.

Na figura 14 temos a estrutura temporal, isto é, a abertura em meses, trimestres e anos do modelo. Todas as simulações foram feitas numa janela de cinco anos.

The screenshot shows the SYSPHERA Enterprise Suite 2.5 Administration interface. The main title bar reads "http://localhost/mestrado/WebForm/Administration/Mem1" and "Administração dos Membros". The top menu includes "Modelagem", "Usuários", "Processos", "Data-Entry", "Carga de Dados", "Análise", "Relatórios", and "Dashboard". A dropdown menu "Administrador" is set to "Sustentabilidade". The left sidebar has a "Hierarquia" dropdown set to "Tempo". The main panel displays a tree view under "Membros" labeled "Nome" with time periods from 2012 to 2016, categorized by quarters (1T, 2T, 3T, 4T) and months (Janeiro, Fevereiro, Março, etc.). To the right, a "Propriedades" panel shows settings for "Identificador" (1), "Ano" (2012), "Mês" (20121Janeiro), "Mês - Não Único" (Janeiro), "Trimestre" (20121T), and "Trimestre - Não Único" (1T).

Figura 14 - Estrutura da dimensão Tempo.

Fonte: SYSPHERA, 2011.

Na figura 15 temos os vários cenários criados, ou seja, versões, simulações criadas.

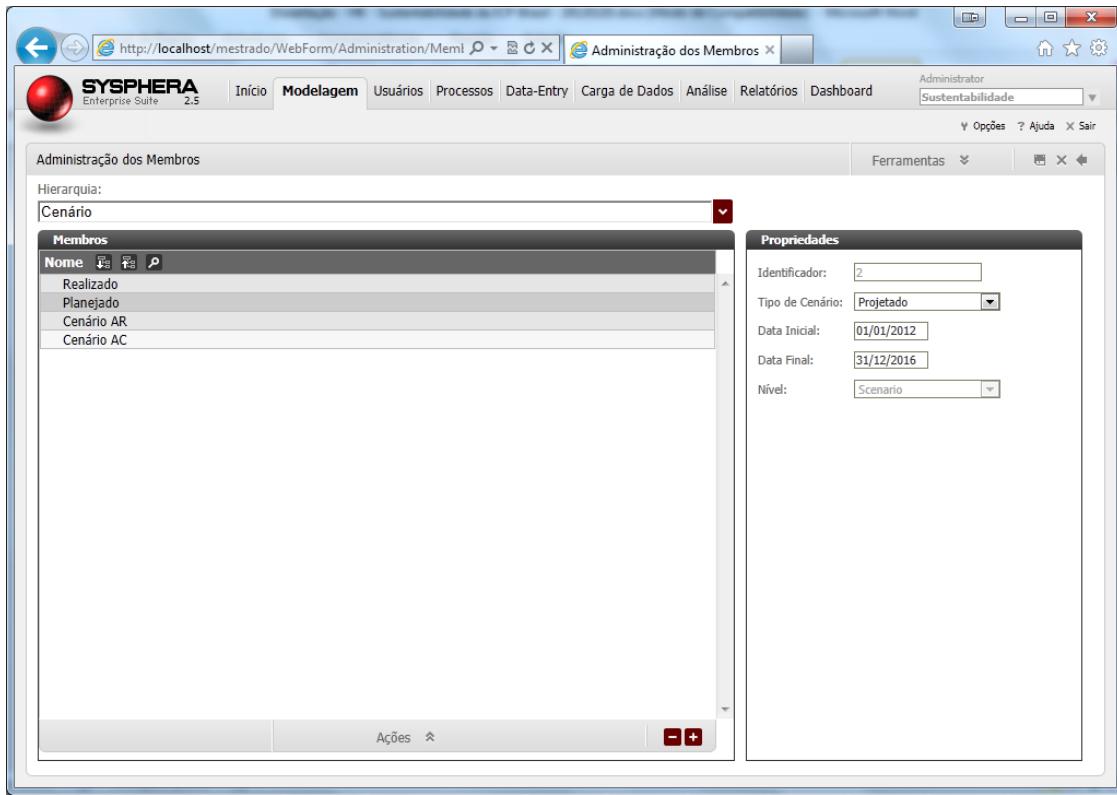


Figura 15 - Estrutura da dimensão Cenário.

Fonte: SYSPHERA, 2011.

Na figura 16 temos as entidades ou empresas do modelo, neste caso a AC e as ARs.

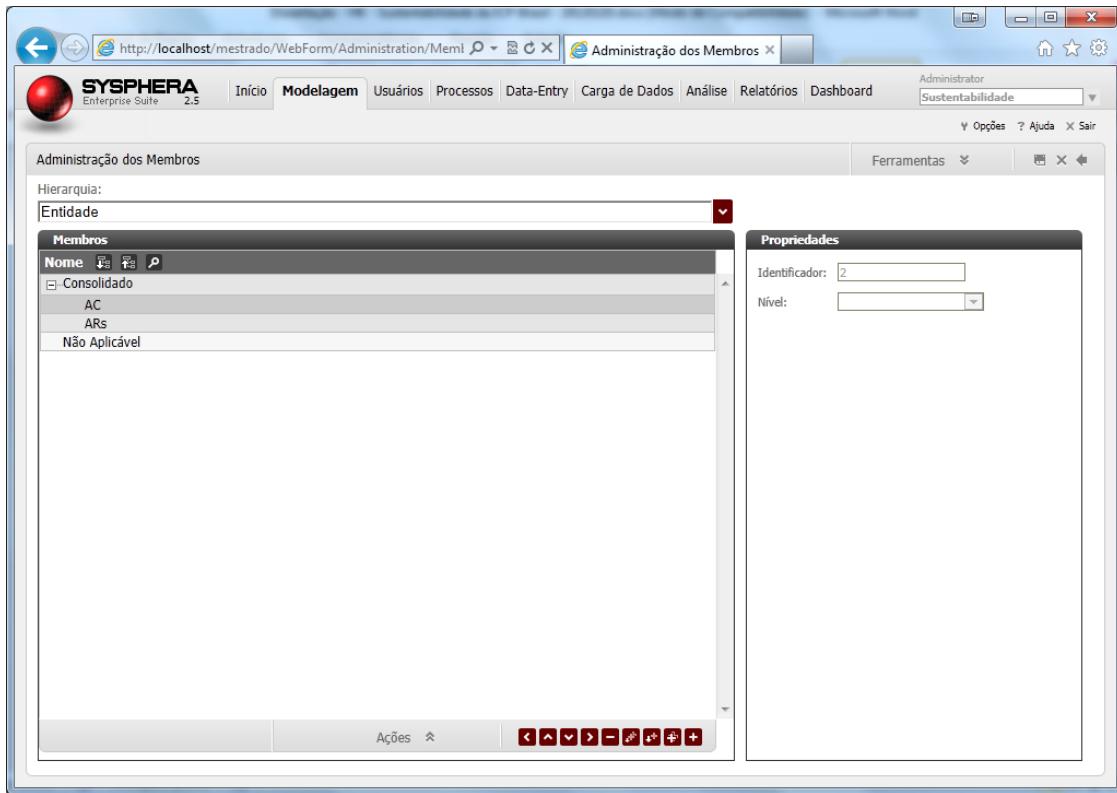


Figura 16 - Estrutura da dimensão Entidade.

Fonte: SYSPHERA, 2011.

5.1 FÓRMULAS DO MODELO

Assim como numa planilha Excel, dentro do Sysphera temos a opção de criar fórmulas, regras de cálculo para projetarmos os valores. Por exemplo, uma vez entrado o valor da receita e o percentual de impostos, temos como calcular o valor dos impostos multiplicando um pelo outro ($\text{Imposto} = \text{Receita} * \% \text{ Imposto}$).

Essas fórmulas que dão inteligência ao modelo e permitem com que ao trocarmos o valor de uma premissa, como a quantidade de certificados vendidos por ARs, imediatamente seja possível ver o impacto no resultado líquido da empresa.

Na figura 17 e 18 temos a lista completa de cálculos do modelo.



Figura 17 - Lista de Fórmulas 1.

Fonte: SYSPHERA, 2011.

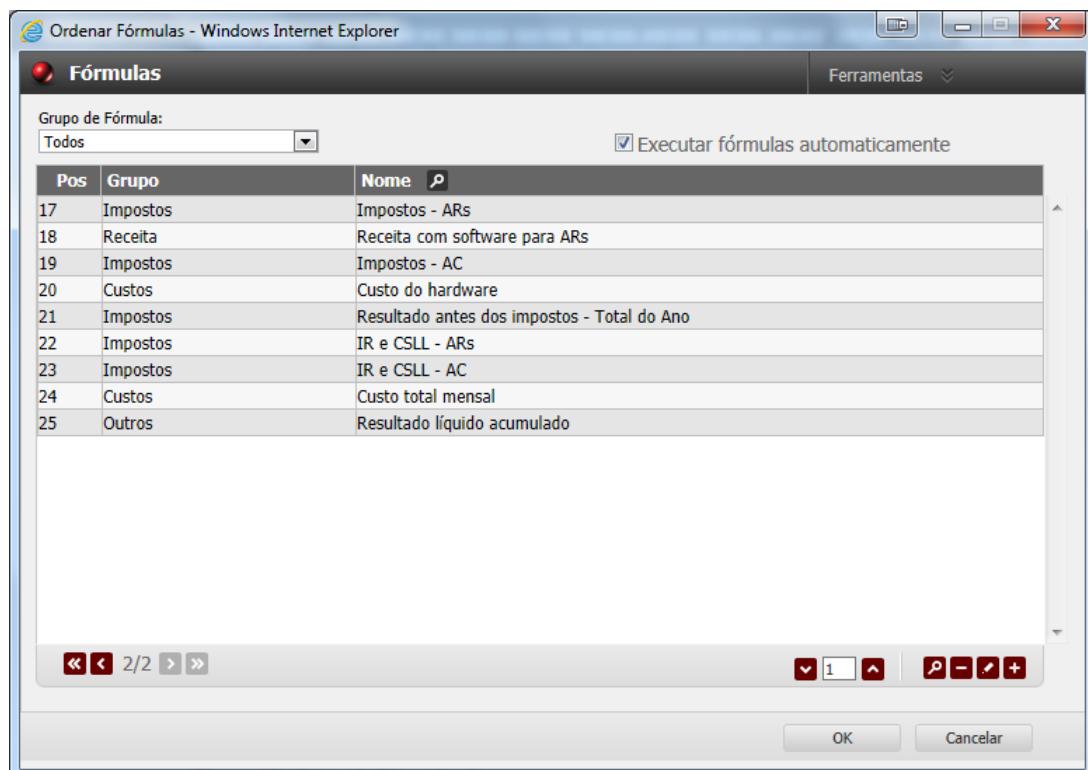


Figura 18 - Lista de Fórmulas 2.

Fonte: SYSPHERA, 2011.

5.2 FORMULÁRIOS DO MODELO

A entrada de dados no modelo pode ser feito via formulários, estes são interfaces parecidas a uma planilha Excel que o usuário pode usar para digitar os valores desejados, como percentual de impostos, volume de vendas, entre outros.

No modelo de sustentabilidade da ICP-Brasil foram criados os formulários listados abaixo (Figura 19):

- 01.01 – Premissas Gerais – onde é feito o cadastro da maioria das premissas, como quantidade de ARs, quantidade de emissões de certificados por dia, percentuais de impostos, entre outros (Figura 20);
- 01.02 – Premissas Dias Úteis – neste formulário que é digitado a quantidade de dias úteis por mês, utilizado no cálculo da quantidade de emissões de certificados (Figura 21);
- 02.01 – Custos por AR – aqui são digitados os custos operacionais por AR (Figura 22);
- 02.02 – Custos Administrativos da AR – neste formulário é digitado os custos administrativos da AR (Figura 23);
- 02.03 – Custos AC – onde são digitados os custos operacionais da AC (Figura 24);
- 02.04 – Custos Administrativos da AC – neste formulário é digitado os custos administrativos da AC (Figura 25);
- 03.01 – Resultado – é um formulário de visualização, que permite vermos o demonstrativo de resultados por AR e AC (Figura 26);

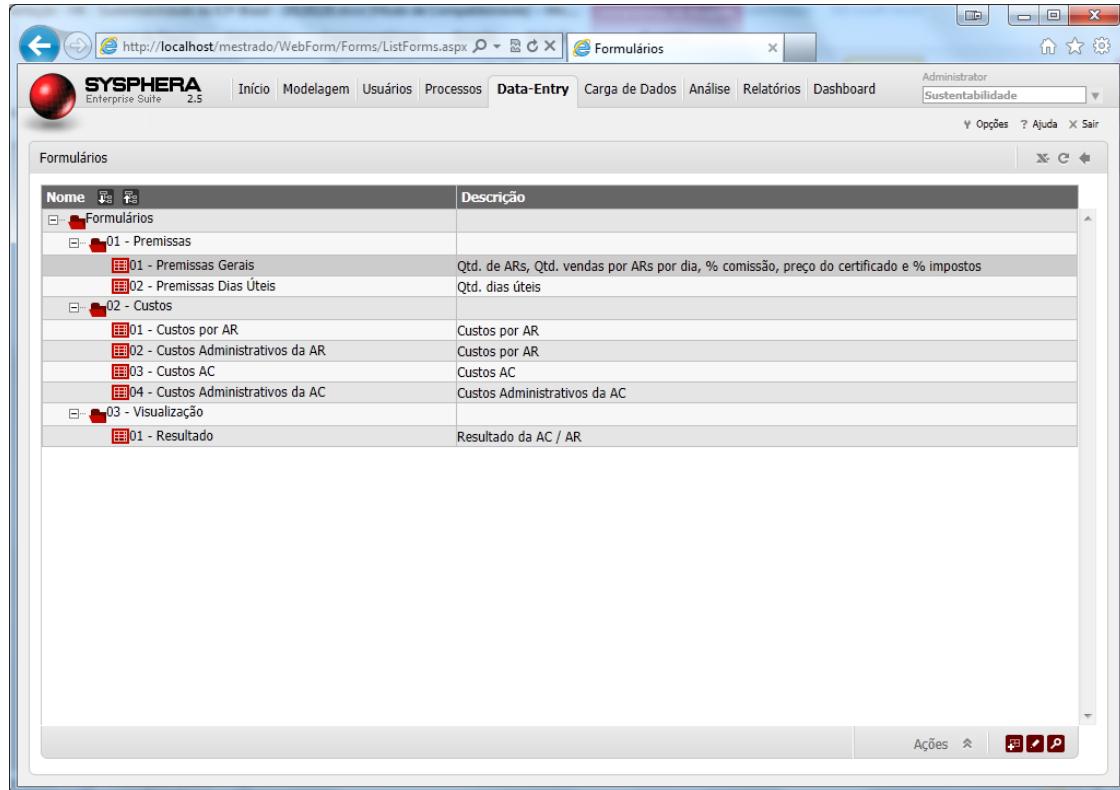


Figura 19 - Lista de Formulários.

Fonte: SYSPHERA, 2011.

Descrição	Valor
Qtd. de ARs	10,00
Qtd. vendas por ARs por dia	10,00
Qtd. vendas por mês	2.200,00
% Comissão AR com certificado	30,00%
% Comissão AR com hardware	20,00%
Preço do certificado	205,00
Preço do hardware	200,00
% Impostos de Vendas AR	6,15%
% Impostos de Vendas AC	5,00%
% IR e CS AR	9,00%
% IR e CS AC	34,00%
Comissão AR com certificado	61,50
Comissão AC com certificado	143,50
Comissão AR com hardware	40,00

Figura 20 - Formulário 01.01 – Premissas Gerais.

Fonte: SYSPHERA, 2011.

02 - Premissas Dias Úteis

Processar Páginas: Planejado 2012

	Janeiro	Fevereiro	Março	Abril	<th>Junho</th> <th>Julho</th> <th>Agosto</th> <th>Setembro</th> <th>Outubro</th>	Junho	Julho	Agosto	Setembro	Outubro
Qtd. dias úteis	22,00	19,00	22,00	20,00	22,00	20,00	22,00	23,00	19,00	22

Figura 21 - Formulário 01.02 – Premissas Dias Úteis.

Fonte: SYSPHERA, 2011.

01 - Custos por AR

Processar Páginas: Planejado

	Janeiro	Fevereiro	Março	Abril	<th>Junho</th> <th>Julho</th> <th>Agos</th>	Junho	Julho	Agos
Treinamento	600,00							
Aluguel de escritório	800,00	800,00	800,00	800,00	800,00	800,00	800,00	
Condomínio, IPTU e outras taxas de escritório	300,00	300,00	300,00	300,00	300,00	300,00	300,00	
Limpeza do escritório	200,00	200,00	200,00	200,00	200,00	200,00	200,00	
Energia elétrica	300,00	300,00	300,00	300,00	300,00	300,00	300,00	
Telefone e internet	200,00	200,00	200,00	200,00	200,00	200,00	200,00	
<input checked="" type="checkbox"/> Custo com escritório	1.800,00	1.800,00	1.800,00	1.800,00	1.800,00	1.800,00	1.800,00	
Software	400,00	400,00	400,00	400,00	400,00	400,00	400,00	
Equipamentos e computadores	9.038,00							
Outros custos operacionais	5.084,00							
Custo de credenciamento da AR	15.000,00							
Auditória da AR	3.500,00							

Figura 22 - Formulário 02.01 – Custos por AR.

Fonte: SYSPHERA, 2011.

Figura 23 - Formulário 02.02 – Custo Administrativos da AR.

Fonte: SYSPHERA, 2011.

Figura 24 - Formulário 02.03 – Custos AC.

Fonte: SYSPHERA, 2011.

	Janeiro	Fevereiro	Março	Abril	<th>Junho</th> <th>Julho</th> <th>Agosto</th> <th>S</th>	Junho	Julho	Agosto	S
Administrativo e financeiro	6.500,00	6.500,00	6.500,00	6.500,00	6.500,00	6.500,00	6.500,00	6.500,00	
Jurídico	3.500,00	3.500,00	3.500,00	3.500,00	3.500,00	3.500,00	3.500,00	3.500,00	
Recursos humanos	5.000,00	5.000,00	5.000,00	5.000,00	5.000,00	5.000,00	5.000,00	5.000,00	
<input checked="" type="checkbox"/> Pessoal e serviços de terceiros	15.000,00	15.000,00	15.000,00	15.000,00	15.000,00	15.000,00	15.000,00	15.000,00	
Envios e transportes									
Seguros									
Limpeza									
<input checked="" type="checkbox"/> Utilidades e serviços									
Publicidade e propaganda	15.000,00	15.000,00	15.000,00	15.000,00	15.000,00	15.000,00	15.000,00	15.000,00	
Outras despesas									
<input checked="" type="checkbox"/> Despesas gerais e administrativas	30.000,00	30.000,00	30.000,00	30.000,00	30.000,00	30.000,00	30.000,00	30.000,00	

Figura 25 - Formulário 02.04 – Custos Administrativos da AC.

Fonte: SYSPHERA, 2011.

	Janeiro	Fevereiro	Março	Abril	Maio	Junho	Julho
Receita com emissão de certificados	315.700,00	272.650,00	315.700,00	287.000,00	315.700,00	287.000,00	315.700,00
Receita com credenciamento de ARs	150.000,00						
Receita com venda de hardware	352.000,00	304.000,00	352.000,00	320.000,00	352.000,00	320.000,00	352.000,00
Receita com software para ARs	4.000,00	4.000,00	4.000,00	4.000,00	4.000,00	4.000,00	4.000,00
<input checked="" type="checkbox"/> Receita operacional bruta	821.700,00	580.650,00	671.700,00	611.000,00	671.700,00	611.000,00	671.700,00
Impostos	41.085,00	29.032,50	33.585,00	30.550,00	33.585,00	30.550,00	30.550,00
<input checked="" type="checkbox"/> Receita operacional líquida	780.615,00	551.617,50	638.115,00	580.450,00	638.115,00	580.450,00	638.115,00
Salário	23.000,00	23.000,00	23.000,00	23.000,00	23.000,00	23.000,00	23.000,00
INSS (20%)	4.600,00	4.600,00	4.600,00	4.600,00	4.600,00	4.600,00	4.600,00
FGTS (8%)	1.840,00	1.840,00	1.840,00	1.840,00	1.840,00	1.840,00	1.840,00
Benefícios	700,00	700,00	700,00	700,00	700,00	700,00	700,00
Férias	638,89	638,89	638,89	638,89	638,89	638,89	638,89
Décimo terceiro salário	1.916,67	1.916,67	1.916,67	1.916,67	1.916,67	1.916,67	1.916,67
<input checked="" type="checkbox"/> Salário e encargos	32.695,56	32.695,56	32.695,56	32.695,56	32.695,56	32.695,56	32.695,56
Treinamento	7.500,00						

Figura 26 - Formulário 03.01 – Resultado.

Fonte: SYSPHERA, 2011.

5.3 RELATÓRIOS DO MODELO

A análise dos dados de forma mais detalhada pode ser feita através dos relatórios. Para isso foram criados os relatórios abaixo (Figura 27):

- 01 – DRE Anual – neste relatório é possível analisar em detalhes o demonstrativo de resultado de uma das entidades (AR ou AC) mês a mês (Figura 28);
- 02 – DRE Comparativo Anual – este relatório permite a análise comparativa do demonstrativo de resultados de dois cenários (Figura 29);

Nome	Descrição
01. DRE Anual	Visualização do DRE Anual no formato Resumido
02. DRE Comparativo Anual	Visualização do DRE Comparativo Anual no formato Resumido

Figura 27 - Lista de Relatórios.
Fonte: SYSPHERA, 2011.

DRE Anual - Resumido (AC)
Planejado - 2012

	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Receita com emissão de certificados	315.700	272.650	315.700	287.000	315.700	287.000	315.700	330.050	272.650	315.700	287.000	287.000
Receita com credenciamento de ARs	150.000	0	0	0	0	0	0	0	0	0	0	0
Receita com venda de hardware	352.000	304.000	352.000	320.000	352.000	320.000	352.000	368.000	304.000	352.000	320.000	320.000
Receita com software para ARs	4.000	4.000	4.000	4.000	4.000	4.000	4.000	4.000	4.000	4.000	4.000	4.000
Receita operacional bruta	821.700	580.650	671.700	611.000	671.700	611.000	671.700	702.050	580.650	671.700	611.000	611.000
Impostos	41.085	29.033	33.585	30.550	33.585	30.550	33.585	35.103	29.033	33.585	30.550	30.550
Receita operacional líquida	780.615	551.618	638.115	580.450	638.115	580.450	638.115	666.948	551.618	638.115	580.450	580.450
Salário e encargos	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696
Treinamento	7.500	0	0	0	0	0	0	0	0	0	0	0
Custo com pessoal	40.196	32.696										
Aluguel de escritório	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000
Condomínio, IPTU e outras taxas de escritório	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000
Limpeza do escritório	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000
Energia elétrica	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500
Telefone e internet	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
Custo com escritório	26.500	26.500	26.500	26.500	26.500	26.500	26.500	26.500	26.500	26.500	26.500	26.500
Manutenção da sala cofre	0	50.000	50.000	50.000	50.000	50.000	50.000	50.000	50.000	50.000	50.000	50.000
Custo inicial sala cofre	5.000.000	0	0	0	0	0	0	0	0	0	0	0
Sala cofre	5.000.000	50.000										
Primeira emissão de certificado	500.000	0	0	0	0	0	0	0	0	0	0	0
Auditória pré-operacional ou operacional	50.000	0	0	0	0	0	0	0	0	0	0	0
Custos com certificados	550.000	0										

Figura 28 - Relatório 01 – DRE Anual.

Fonte: SYSPHERA, 2011.

DRE Comparativo Anual - Resumido (AC)
Planejado x Cenário AC - 2012

	Janeiro			Fevereiro			Março		
	Planejado	Cenário AC	% Var	Planejado	Cenário AC	% Var	Planejado	Cenário AC	% Var
Receita com emissão de certificados	315.700	254.100	-19,51%	272.650	219.450	-19,51%	315.700	254.100	-19,51%
Receita com credenciamento de ARs	150.000	150.000	0,00%						0,0
Receita com venda de hardware	352.000	352.000	0,00%	304.000	304.000	0,00%	352.000	352.000	0,0
Receita com software para ARs	4.000	4.000	0,00%		4.000	0,00%	4.000	4.000	0,0
Receita operacional bruta	821.700	760.100	-7,50%	580.650	527.450	-9,16%	671.700	610.100	-9,1
Impostos	41.085	38.005	-7,50%	29.033	26.373	-9,16%	33.585	30.505	-9,
Receita operacional líquida	780.615	722.095	-7,50%	551.618	501.078	-9,16%	638.115	579.595	-9,1
Salário e encargos	32.696	6.264	-80,84%	32.696	6.264	-80,84%	32.696	6.264	-80,8
Treinamento	7.500	0	-100,00%						0,0
Custo com pessoal	40.196	6.264	-84,42%	32.696	6.264	-80,84%	32.696	6.264	-80,8
Aluguel de escritório	20.000	2.000	-90,00%	20.000	2.000	-90,00%	20.000	2.000	-90,0
Condomínio, IPTU e outras taxas de escritório	2.000	500	-75,00%	2.000	500	-75,00%	2.000	500	-75,0
Limpeza do escritório	2.000	300	-85,00%	2.000	300	-85,00%	2.000	300	-85,0
Energia elétrica	1.500	500	-66,67%	1.500	500	-66,67%	1.500	500	-66,6
Telefone e internet	1.000	500	-50,00%	1.000	500	-50,00%	1.000	500	-50,0
Custo com escritório	26.500	3.800	-85,66%	26.500	3.800	-85,66%	26.500	3.800	-85,6
Manutenção da sala cofre			0,00%	50.000	50.000	0,00%	50.000	50.000	0,0
Custo inicial sala cofre	5.000.000	5.000.000	0,00%						0,0
Sala cofre	5.000.000	5.000.000	0,00%	50.000	50.000	0,00%	50.000	50.000	0,0
Primeira emissão de certificado	500.000	500.000	0,00%						0,0
Auditória pré-operacional ou operacional	50.000	50.000	0,00%						0,0
Custos com certificados	550.000	550.000	0,00%						0,0

Figura 29 - Relatório 02 – DRE Comparativo Anual.

Fonte: SYSPHERA, 2011.

5.4 ANÁLISES DE RENTABILIDADE DO MODELO

Uma das melhores funcionalidades da ferramenta Sysphera é a análise de rentabilidade. Com esta funcionalidade é possível customizarmos telas do sistema com as premissas que queremos alterar e com as contas às quais queremos analisar o impacto.

Dessa forma foi possível criarmos duas telas de análise de rentabilidade:

- Análise AR – podemos alterar a quantidade de vendas por AR por dia, o preço do certificado, o preço do hardware e imediatamente vermos o impacto na receita operacional bruta, no resultado bruto e no resultado líquido (Figura 30);
- Análise AC – podemos alterar a quantidade de ARs a AC possui, o preço do certificado, o preço do hardware e imediatamente vermos o impacto na receita operacional bruta, no resultado bruto e no resultado líquido (Figura 31);

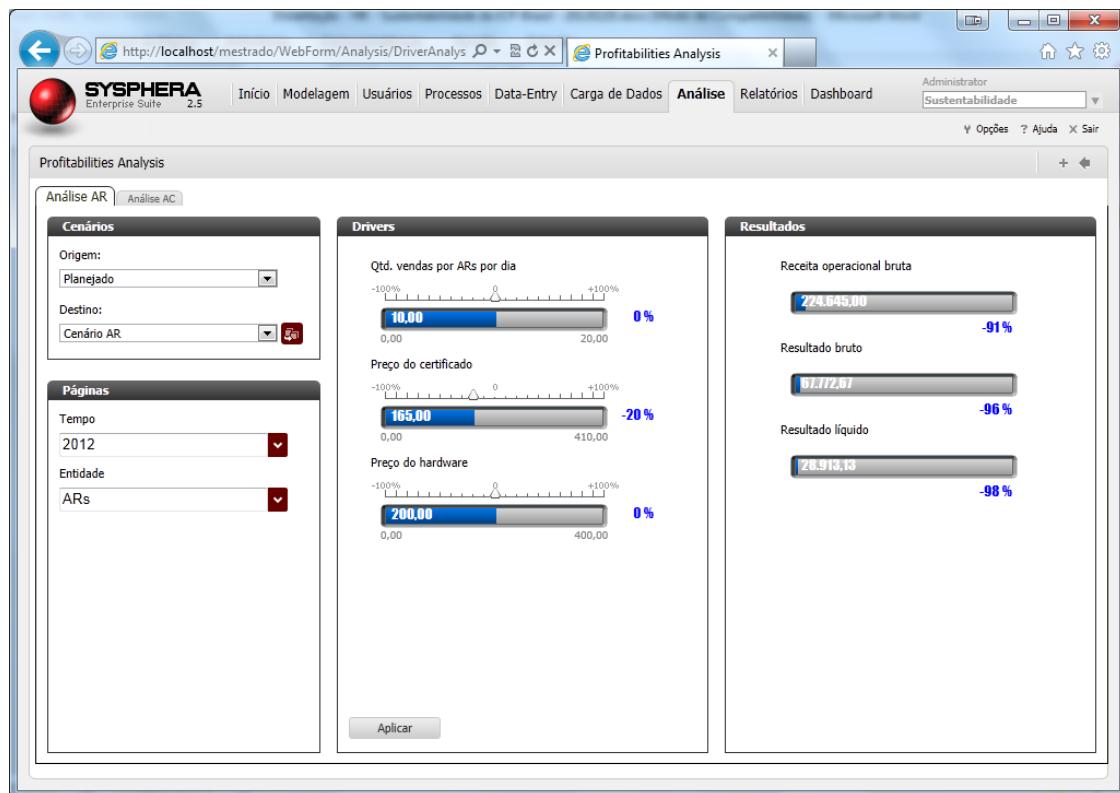


Figura 30 - Análise de Rentabilidade da AR.

Fonte: SYSPHERA, 2011.

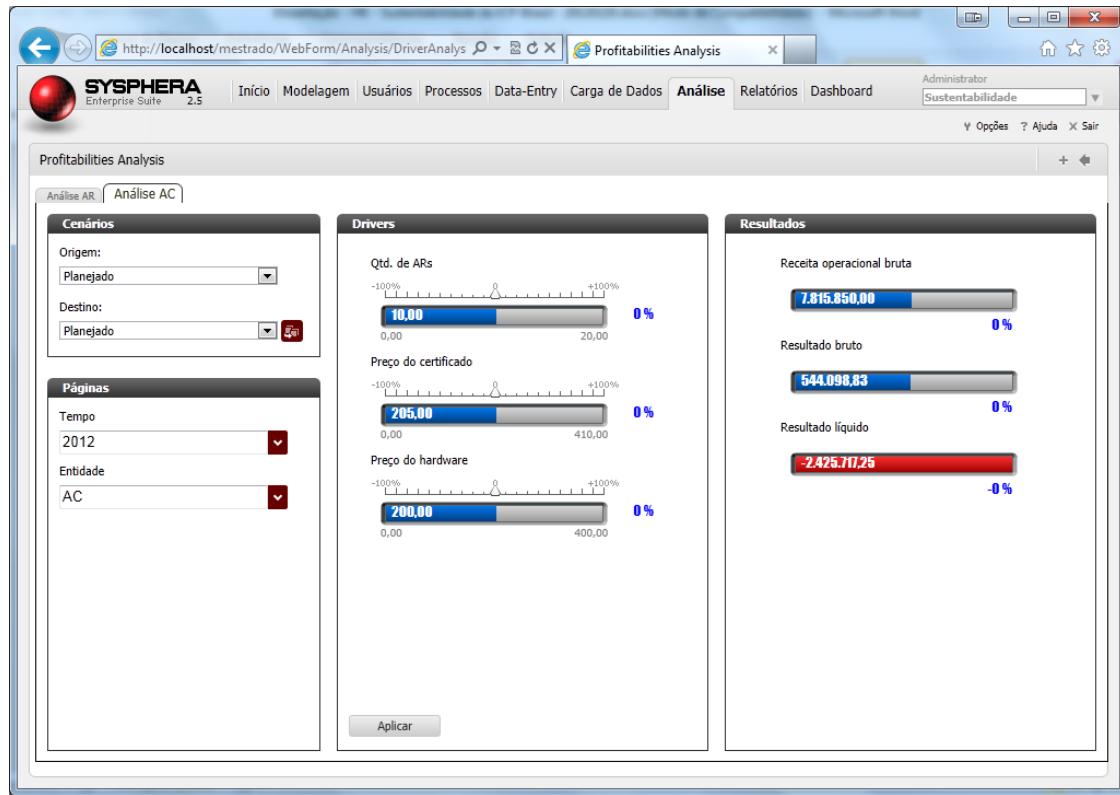


Figura 31 - Análise de Rentabilidade da AC.

Fonte: SYSPHERA, 2011.

6 ANÁLISE DE CENÁRIOS

Com o objetivo de identificarmos o melhor modelo para a sustentabilidade econômico-financeira de uma AC e de uma AR, criamos três cenários: i) Configuração atual; ii) Ajustes no preço e no volume de emissões; iii) Ajustes nas comissões da AC e AR.

Nos três cenários desenvolvidos foi considerado a AR e a AC como empresas independentes, sendo que a AR apenas estará credenciada a AC, mas como uma empresa, um CNPJ diferente.

O detalhamento do volume de vendas e o credenciamento das ARs a ACs no tempo não foi objeto deste estudo. Dessa forma, foi feito a simplificação de trabalhar com valores médios, isto é, não consideramos que a quantidade de emissões de certificados por dia vai crescer a medida que a AR fica conhecida no mercado, apenas considerou-se que temos uma emissão de X certificados por dia desde o dia um da empresa. Essa premissa deve gerar uma distorção nos primeiros meses de vida da empresa, mas como o objetivo deste estudo é analisar a sustentabilidade financeira de longo prazo isso não irá afetar as conclusões deste trabalho.

6.1 CONFIGURAÇÃO ATUAL

O primeiro cenário analisado é o estado atual das ARs e ACs, onde o principal objetivo foi encontrar o ponto de equilíbrio financeiro, isto é, conseguir com que a entidade de lucro e pague todo o investimento inicial em menos de cinco anos respeitando as sua configurações atuais encontradas.

Para isso criou-se inicialmente um cenário exclusivo para analisar a AR isoladamente. Neste cenário foram considerados todos os custos de uma AR com dois agentes, e buscou-se a receita mínima para que a AR se pagasse. Com o volume de oito emissões diárias, em média 176 emissões mensais, foi possível encontrar o ponto de equilíbrio da AR. Mensalmente a AR irá gerar um lucro líquido de R\$112,50 a R\$2.886,40 reais, essas variação acontecem devido às despesas esporádicas e a quantidade de dias úteis de cada mês que varia.

Desta forma a AR irá pagar o seu investimento inicial no vigésimo terceiro mês de operação e no final de cinco anos teria acumulado um lucro de R\$43.527,55 reais, já considerando o pagamento do capital inicial investido. Como o investimento inicial foi de R\$47.577,55 reais tivemos um retorno de 91% em cinco anos.

DRE Anual - Resumido (ARs)

AR Atual - 2012



	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez	2012
Receita com emissão de certificados	10.824	9.348	10.824	9.840	10.824	9.840	10.824	11.316	9.348	10.824	9.840	9.840	123.492
Receita com venda de hardware	7.040	6.080	7.040	6.400	7.040	6.400	7.040	7.360	6.080	7.040	6.400	6.400	80.320
Receita operacional bruta	17.864	15.428	17.864	16.240	17.864	16.240	17.864	18.676	15.428	17.864	16.240	16.240	203.812
Impostos	1.099	949	1.099	999	1.099	999	1.099	1.149	949	1.099	999	999	12.534
Receita operacional líquida	16.765	14.479	16.765	15.241	16.765	15.241	16.765	17.527	14.479	16.765	15.241	15.241	191.278
Salário e encargos	7.656	7.656	7.656	7.656	7.656	7.656	7.656	7.656	7.656	7.656	7.656	7.656	91.867
Treinamento	600	0	0	0	0	0	0	0	0	0	0	0	600
Custo com pessoal	8.256	7.656	92.467										
Aluguel de escritório	800	800	800	800	800	800	800	800	800	800	800	800	9.600
Condomínio, IPTU e outras taxas de escritório	300	300	300	300	300	300	300	300	300	300	300	300	3.600
Limpeza do escritório	200	200	200	200	200	200	200	200	200	200	200	200	2.400
Energia elétrica	300	300	300	300	300	300	300	300	300	300	300	300	3.600
Telefone e internet	200	200	200	200	200	200	200	200	200	200	200	200	2.400
Custo com escritório	1.800	21.600											
Auditória da AR	3.500	0	0	0	0	0	0	0	0	0	0	0	3.500
Custos com certificados	3.500	0	3.500										
Software	400	400	400	400	400	400	400	400	400	400	400	400	4.800
Equipamentos e computadores	9.038	0	0	0	0	0	0	0	0	0	0	0	9.038
Outros custos operacionais	5.084	0	0	0	0	0	0	0	0	0	0	0	5.084
Custo de credenciamento da AR	15.000	0	0	0	0	0	0	0	0	0	0	0	15.000
Custos operacionais	43.078	9.856	151.489										
Resultado bruto	-26.312	4.624	6.910	5.386	6.910	5.386	6.910	7.672	4.624	6.910	5.386	5.386	39.789
Pessoal e serviços de terceiros	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	54.000
Despesas gerais e administrativas	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	4.500	54.000
Resultado antes dos impostos	-30.812	124	2.410	886	2.410	886	2.410	3.172	124	2.410	886	886	-14.211
IR e CSLL	-2.773	11	217	80	217	80	217	285	11	217	80	80	-1.279
Resultado líquido	-28.039	112	2.193	806	2.193	806	2.193	2.886	112	2.193	806	806	-12.932
Resultado líquido acumulado	-28.039	-27.927	-25.734	-24.928	-22.735	-21.929	-19.736	-16.849	-16.737	-14.544	-13.738	-12.932	-12.932
Custo total mensal	47.578	14.356	14.356	14.356	14.356	14.356	14.356	14.356	14.356	14.356	14.356	14.356	205.489

Figura 32 - Cenário AR atual com receita mínima

Fonte: SYSPHERA, 2011.

Caso fosse considerado o volume máximo para dois agentes, de dez emissões por dia, resultaria num resultado líquido de R\$3.406,51 a R\$6.007,05 reais por mês e no sétimo mês se pagaria o valor investido. No final de cinco anos encontrar-se-ia um retorno sobre o capital investido de 549%.

Descriutivo	8 Emissões/Dia	10 Emissões/Dias
Resultado líquido mensal médio	R\$ 1.212,99	R\$4.836,11
Meses para pagar o investimento	23	7
Lucro líquido acumulado total	R\$43.527,55	R\$261.105,78
Investimento inicial	R\$47.577,55	R\$47.577,55
% de retorno total	91%	549%
% de retorno médio mensal	3%	10%

Tabela 10 - Comparativo do cenário atual AR.

Fonte: Elaboração própria.

Neste caso fica claro a importância da AR investir em melhor captar seu cliente. A grande maioria das ARs existentes são empresas com outros objetivos fins, que apenas

aproveitam o seu espaço físico, recursos e conhecimento para ter uma segunda receita; como por exemplo, os cartórios que prestam serviço de AR.

As ARs são em sua maioria passivas, no máximo criam parcerias com instituições como escritórios de contabilidade e advocacia, para que estes direcionem seus clientes a medida que o governo exija a utilização de certificados digitais.

No entanto, foram encontrados alguns casos atípicos positivos, onde a AR instiga e fomenta seus clientes a utilizarem os certificados digitais, mostrando os benefícios destes, dando inicialmente com custo zero alguns certificados digitais, de forma a provar ao cliente os benefícios do certificado digital. Mais tarde esse cliente vendo os benefícios começa a se utilizar do certificado digital e cria assim uma parceira com a AR, demandando um volume muito maior de emissões de certificado digital.

Num segundo momento, foi criado o cenário atual da AC. Neste caso foi considerado que as ARs teriam as mesmas características do cenário atual da AR, um volume mínimo de oito emissões diárias de certificados digitais. Assim partiu-se do pior cenário, com a menor quantidade de emissões por AR.

Neste cenário foi necessário um mínimo de sete ARs vinculadas a AC, um número bastante conservador, para que se obtivesse o retorno de todo o investimento em menos de cinco anos. Abaixo (tabela 11) segue o resultado do cenário atual da AC variando a quantidade de ARs vinculadas de sete, dez e vinte:

Descriptivo	7 ARs	10 ARs	20 ARs
Resultado líquido mensal mínimo	R\$105.356,38	R\$196.248,78	R\$484.311,11
Meses para pagar o investimento	52	25	9
Lucro líquido acumulado total	R\$836.815,50	R\$6.331.722,37	R\$23.688.267,68
Investimento inicial	R\$5.737.087,56	R\$5.758.207,56	R\$5.828.607,55
% de retorno total	15%	110%	406%
% de retorno médio mensal	2%	3%	8%

Tabela 11 - Comparativo do cenário atual AC.

Fonte: Elaboração própria.

No caso da AC conclui-se que com uma quantidade mínima de ARs vinculadas a AC tem um lucro considerável. Isto se deve ao fato de assumirmos que todo o hardware é comprado junto a AC e não adquirido de outro fornecedor, pois a receita mensal de hardware é em média de quarenta e seis (46) por cento do total da receita.

Como a atividade fim da AC deveria ser a venda de certificados digitais e neste cenário as ARs provavelmente não comprariam o hardware da AC e sim de outro fornecedor, iremos estimar que a AC não tenha nenhuma receita referente a venda de hardware. Abaixo segue a mesma análise da AC sem considerar a receita de hardware:

Descriptivo	7 ARs	10 ARs	20 ARs
Resultado líquido mensal mínimo	R\$10.570,52	R\$60.840,40	R\$228.406,67
Meses para pagar o investimento	Não se paga	Não se paga	20
Lucro líquido acumulado total	-R\$4.893.534,57	-R\$1.854.492,03	R\$8.275.649,81
Investimento inicial	R\$5.687.807,56	R\$5.687.807,56	R\$5.687.807,56
% de retorno total	Não aplica	Não aplica	145%
% de retorno médio mensal	Não aplica	Não aplica	4%

Tabela 12 - Comparativo do cenário atual AC sem hardware.

Fonte: Elaboração própria.

DRE Anual - Resumido (AC)

Planejado - 2012



	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez	2012	
Receita com emissão de certificados	505.120	436.240	505.120	459.200	505.120	459.200	505.120	528.080	436.240	505.120	459.200	459.200	5.762.960	
Receita com software para ARs	8.000	8.000	8.000	8.000	8.000	8.000	8.000	8.000	8.000	8.000	8.000	8.000	96.000	
Receita operacional bruta	513.120	444.240	513.120	467.200	513.120	467.200	513.120	536.080	444.240	513.120	467.200	467.200	5.858.960	
Impostos	25.656	22.212	25.656	23.360	25.656	23.360	25.656	26.804	22.212	25.656	23.360	23.360	292.948	
Receita operacional líquida	487.464	422.028	487.464	443.840	487.464	443.840	487.464	509.276	422.028	487.464	443.840	443.840	5.566.012	
Salário e encargos	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	32.696	392.347	
Treinamento	7.500	0	0	0	0	0	0	0	0	0	0	0	7.500	
Custo com pessoal	40.196	32.696	399.847											
Aluguel de escritório	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	20.000	240.000	
Condomínio, IPTU e outras taxas de escritório	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	24.000	
Limpeza do escritório	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	24.000	
Energia elétrica	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	1.500	18.000	
Telefone e internet	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	12.000	
Custo com escritório	26.500	318.000												
Manutenção da sala cofre	0	50.000	50.000	50.000	50.000	50.000	50.000	50.000	50.000	50.000	50.000	50.000	550.000	
Custo inicial sala cofre	5.000.000	0	0	0	0	0	0	0	0	0	0	0	5.000.000	
Sala cofre	5.000.000	50.000	5.550.000											
Primeira emissão de certificado	500.000	0	0	0	0	0	0	0	0	0	0	0	500.000	
Auditória pré-operacional ou operacional	50.000	0	0	0	0	0	0	0	0	0	0	0	50.000	
Custos com certificados	550.000	0	550.000											
Software	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	2.000	24.000	
Equipamentos e computadores	28.079	0	0	0	0	0	0	0	0	0	0	0	28.079	
Outros custos operacionais	11.033	0	0	0	0	0	0	0	0	0	0	0	11.033	
Custos operacionais	5.657.808	111.196	6.880.959											
Resultado bruto	-5.170.344	310.832	376.268	332.644	376.268	332.644	376.268	398.080	310.832	376.268	332.644	332.644	-1.314.947	
Pessoal e serviços de terceiros	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	180.000	
Publicidade e propaganda	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	15.000	180.000	
Despesas gerais e administrativas	30.000	30.000	30.000	30.000	30.000	30.000	30.000	30.000	30.000	30.000	30.000	30.000	360.000	
Resultado antes dos impostos	-5.200.344	280.832	346.268	302.644	346.268	302.644	346.268	368.080	280.832	346.268	302.644	302.644	-1.674.947	
Resultado líquido	-5.200.344	280.832	346.268	302.644	346.268	302.644	346.268	368.080	280.832	346.268	302.644	302.644	-1.674.947	
Resultado líquido acumulado	-5.200.344	-4.919.511	-4.573.243	-4.270.598	-3.924.330	-3.621.685	-3.275.417	-2.907.336	-2.626.504	-2.280.236	-1.977.591	-1.674.947	-1.674.947	
Custo total mensal	5.687.808	141.196	141.196	141.196	141.196	141.196	141.196	141.196	141.196	141.196	141.196	141.196	7.240.959	

Figura 33 - Cenário AC atual sem hardware com 20 ARs vinculadas.

Fonte: SYSPHERA, 2011.

6.2 PROPOSTA DE SUSTENTABILIDADE

Um dos objetivos deste trabalho é avaliar os possíveis cenários, buscando a situação onde os recursos existentes são otimizados e a população seja melhor atendida, gerando um custo menor e mais aceitável para os usuários finais.

Então primeiramente visando um aumento da utilização dos certificados digitais, partiu-se da premissa de reduzirmos o preço médio aqui considerado até então de R\$205,00 reais (média do e-CPF que custa R\$165,00 reais e do e-CNPJ que custa R\$245,00 reais) para R\$120,00 reais, uma redução de quarenta e um (41) por cento no custo médio do certificado digital. Com isso consideramos um aumento nas vendas dos certificados digitais de oito (8) emissões diárias para dez (10) emissões diárias devido à redução do preço.

No preço do hardware foi identificada uma margem muito grande, pois foi encontrado em alguns fornecedores o *hardware* avulso a um custo de R\$50,00 reais, enquanto que o preço praticado para os usuário finais é de R\$200,00 reais. Em algumas pesquisas na internet foi possível encontrar o mesmo *hardware* num lote de quinhentas (500) unidades por dez (10) dólares, então assumimos que se a AC fizer uma compra em maior escala seria possível chegar a um custo de vinte (20) reais.

Como vimos em algumas ARs uma das formas delas maximizarem o seu retorno é fazendo a importação direta do hardware, em vez de adquirir com a AC que paga uma comissão de apenas vinte (20) por cento. Uma forma de evitarmos isso seria dividirmos o lucro do *hardware* entre a AC e a AR, dessa forma a AC irá fazer a compra em maior escala, conseguindo um custo unitário muito menor que se a AR tentar fazer a importação direta, desmotivando essa prática. Com isso poderíamos colocar um preço final no *hardware* de cem (100) reais, sendo 20% o custo, 40% margem para a AC e outros 40% margem para a AR, totalizando os 100% por cento do *hardware*.

Finalmente, é proposto um ajuste na comissão de venda das ARs, passando de 30% para 40%, assim dando um maior equilíbrio na operação.

Com essas alterações propostas conseguiu-se uma redução total do preço médio do certificado digital com *hardware* de R\$405,00 reais para R\$220,00 reais, uma redução de 46%. Mesmo assim o retorno mensal do investimento total da AC se manteve próximo dos 4% e o da AR em 5%, que seriam valores bastante atrativos.

Caso a AR busque mais clientes, sendo mais proativa, facilmente conseguirá melhorar ainda mais o retorno sobre o investimento, pois aumentando o volume de emissões diárias só

necessitaria a contratação de novos agentes, assim diluindo os demais custos fixos e com isso melhorando ainda mais o seu retorno sobre o investimento.

Da mesma forma a AC buscando mais ARs para credenciar, será traduzido num retorno financeiro imediato. No caso da AC os custos não precisam aumentar para isso, sua estrutura comporta um aumento considerável de ARs vinculadas sem grandes aumentos dos custos, gerando um retorno maior e mais atrativo para a AC. Isto também é um dos motivos que as ACs devem se preocupar com as ARs, deixar o negócio da AR mais atrativo é benéfico para a AC também. Dados apresentados na tabela 13.

Descriptivo	AR	AC
Quantidade de ARs	1	20
Quantidade média de emissões por mês	220	4400
Resultado líquido mensal mínimo	R\$2.426,65	R\$217.344,29
Meses para pagar o investimento	7	22
Lucro líquido acumulado total	R\$116.410,90	R\$261.105,78
Investimento inicial	R\$47.577,55	R\$7.606.865,33
% de retorno total	245%	132%
% de retorno médio mensal	5%	4%

Tabela 13 - Cenário proposto para AR e AC.

Fonte: Elaboração própria.

7 CONCLUSÕES

As tecnologias da informação e da comunicação estão cada vez mais presentes em todo tipo de relacionamento. Nas relações sociais, comerciais, diplomáticas, educacionais, empresariais, governamentais, políticas, em todo tipo de relação que envolva troca de informações.

A utilização do certificado digital para garantir a segurança da informação trocada; garantindo a autenticidade, integridade, não repúdio e tempestividade; não é mais questionada. Atualmente a questão é quando de fato existira o uso em massa desta tecnologia, pois seus benefícios são claros, partindo da redução de custos, aumento da segurança e velocidade na troca de informação.

Ainda não existem estudos sobre a sustentabilidade econômica e financeira da ICP-Brasil, as discussões até então existentes, são em relação à arquitetura e a operação técnica, com o objetivo de garantir a segurança.

No entanto, durante o desenvolvimento deste trabalho, foram constadas situações onde a dificuldade em obter um negócio sustentável, de certa forma incentiva o relaxamento das medidas de segurança, com o objetivo de reduzir custos e com a consequência do aumento da possibilidade de fraudes.

Dessa forma, a saúde financeira de todas as instituições pertencentes a ICP-Brasil, deve fazer parte dos estudos e discussões, com o intuito de garantir a segurança e sustentabilidade de longo prazo da ICP-Brasil.

A configuração atual da maioria das ARs, onde a sua atividade fim não é a emissão de certificados digitais, onde a emissão de certificados digitais é apenas uma receita para a empresa, gera uma maior dificuldade em se tornar rentável a operação. A falta de uma estratégia ativa na captação de novos clientes tornam estas ARs passivas, na busca de novos clientes. Nestes casos a sustentabilidade financeira é mais difícil de ser atingida.

Por outro lado, existem exemplos de ARs onde isso foi vencido pela pró-atividade, pela criatividade do gestor. Encontraram-se casos onde alguns cartórios instruíram e incentivaram seus melhores clientes a utilizarem o certificado digital. Conseguiram mostrar para estes clientes as vantagens do certificado digital e com isso abriram um novo mercado. Deixaram de ser passivas, apenas aguardando que novos clientes batam em suas portas, para serem ativas na busca de novos clientes.

A variável mais importante para tornar a AR sustentável economicamente é a quantidade de clientes, a quantidade de emissões por dia. Relatasse que se forem feitos mais

investimentos, por parte de todas as entidades da ICP-Brasil no sentido de divulgar e difundir o uso do certificado digital, a sustentabilidade não só da AR, mas de toda a ICP-Brasil será garantida.

Neste sentido, de garantir a sustentabilidade e incentivar a utilização em massa dos certificados digitais, foi proposto neste trabalho um cenário sustentável, onde o valor final do certificado digital, incluindo o hardware, foi reduzido em 46%. Mesmo com essa redução considerável do preço foi possível manter a operação da AR e da AC rentáveis, com taxas de retorno muito acima dos padrões de mercado.

No cenário proposto neste trabalho, a AC precisaria reduzir o preço do certificado digital, reduzir o preço do *hardware*, aumentar o comissionamento do certificado digital, aumentar o comissionamento do *hardware* de forma a desmotivar a aquisição de outro fornecedor e criar campanhas para incentivar e divulgar a utilização do certificado digital. Em contra partida a AR deveria aumentar o volume de vendas, ser mais criativa na busca de novos clientes e sempre adquirir o *hardware* via AC.

Por último, a criação do modelo utilizando-se uma ferramenta de CPM, foi bastante benéfica, pois permite o aproveitamento de todos os benefícios tecnológicos, principalmente para a criação e análise dos mais diversos cenários.

7.1 TRABALHOS FUTUROS

A pesquisa deste trabalho se baseou apenas na AC e AR, não levando em conta as demais entidades envolvidas na ICP Brasil. Durante esta pesquisa, observou-se casos onde o compartilhamento de recursos, através de prestadores de serviços foi a solução encontrada por algumas ACs, para mitigar seu custo inicial e mensal. Então para melhorar o modelo proposto seria interessante termos uma visão mais completa, considerando todas as entidades existentes na ICP Brasil e incluir essas alternativas permitidas pela ICP-Brasil.

A projeção de receita partiu da capacidade operacional e não do mercado, isto é, um complemento a este trabalho seria fazer uma estudo focado no potencial do mercado de certificados digitais no Brasil.

Pesquisas de marketing, buscando estudar as melhores alternativas para divulgar, instruir e incentivar o uso do certificado digital seria complementar a este o trabalho e de grande valia para o desenvolvimento da ICP-Brasil.

Por fim, a melhor maneira de observar a eficiência do modelo proposto seria aplicá-lo num caso real, utilizando o modelo aqui proposto para se fazer o planejamento econômico-financeiro de uma AC com suas ARs vinculadas. Dessa forma, acompanhando o planejado com o realizado na prática, geraria novos dados para se analisar e fazer uma melhoria contínua no modelo, de forma a tornar a ICP-Brasil cada vez mais sustentável.

REFERÊNCIAS

AMBONI, Nério. **O Caso da cecrisa s.a.: uma aprendizagem que deu certo.** Tese de Doutorado, EPS - UFSC -. Florianópolis: 1997

ANTHONY, R; **Planning and Control Systems: A Framework for Analysis.** Cambridge, MA: Harvard University Press, 1965.

ANTHONY, Robert; GOVINDARAJAN, Vijay. **Sistemas de controle gerencial.** São Paulo: McGraw-Hill, 2008.

BERTERO, Carlos Osmar. **Ensino e pesquisa em administração.** São Paulo: Thomson Learning, 2006.

BOYD, B. **Strategic planning and financial performance: a meta analysis review.** Journal of Management Studies, 1991.

BRASIL. **Medida Provisória 2.200-2.** Medida Provisória que instituí a ICP-Brasil.

CAGGIANO, P. C.; FIGUEIREDO, S. **Controladoria: Teoria e Prática** (3.^a ed.). São Paulo: Atlas, 2006.

CARVER, A.; RITACCO, M. The Business Value of Business Intelligence. A Framework for Measuring the Benefits of Business Intelligence. **Business Objects.** 2006.

CAUTELA, A. L.; POLIONI, F. G. F. **Sistemas de informação.** São Paulo: Livros científicos e técnicos, 1982.

COKINS, G. **Performance Management: Integrating Strategy, Execution, Methodologies, Risks and Analytics.** Hoboken: John Wiley & Sons, Inc, 2009.

CONFEDERAÇÃO NACIONAL DO COMÉRCIO. **Mais de um milhão de certificados digitais já foram emitidos.** Disponível em: <<http://www.cnc.org.br/noticias/mais-de-um-milhao-de-certificados-digitais-ja-foram-emitidos>>. Acesso em: 4 dezembro 2011.

COSTA, F. A. **Modernização dos processos de auditoria e fiscalização da ICP Brasil.** 2010. 290 p. Dissertação (Mestrado em Administração) – Programa de Pós Graduação em Administração, Universidade do Estado de Santa Catarina, Florianópolis, 2010.

DIAS, J. da S. **Confiança no Documento Eletrônico**. 2004. 141 p. Tese (Doutorado em Engenharia de Produção e Sistemas) – Programa de Pós Graduação em Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, 2004.

GARTNER GROUP. Gartner Magic Quadrant for Business Intelligence 2010. 2010. Disponível em: <http://www.businessintelligence.info/docs/estudios/Gartner-Magic-Quadrant-for-Business-Intelligence-platforms-2010-T1.pdf>. Acesso em 21/03/2011.

GARTNER GROUP. Gartner Magic Quadrant for Business Intelligence 2011. 2011. Disponível em: <https://resource.microstrategy.com/ResourceCenter/collateral.aspx?rid=12822>. Acesso em 21/03/2011.

GARTNER GROUP. Gartner Says Social Network Analysis Can Help Enterprises Achieve a Pattern-Based Strategy™ that Leverages Relationship Information. 2009. Disponível em: <http://www.gartner.com/it/page.jsp?id=1239913>. Acesso em 21/03/2011.

GARTNER GROUP. Magic Quadrant for Corporate Performance Management Suites. 2011. Disponível em: <http://www.gartner.com/technology/media-products/reprints/oracle/article187/article187.html>. Acesso em 26/12/2011.

GREENGARD S. Business Intelligence & Analytics: Optimizing Your Enterprise. **Baseline**. 2010, p.18-23.

GREENLEY, E. **Does strategic planning improve company performance?**. Long Range Planning, 1986.

HANSEN, Derek; SHNEIDERMAN, Ben; SMITH, Marc A. **Analyzing Social Media Networks with NodeXL: Insights from a Connected World**. Morgan Kaufmann, 2010.

Hitt, M. A., Ireland, R. D., & Hoskisson, R. E.. **Administração Estratégica**. São Paulo: Thomson, 2003.

HOCEVAR B.; JAKLIC J.. Assessing Benefits of Business Intelligence Systems - A Case Study. **Management**. 2010, v. 15, p. 87-119.

ICP-BRASIL. **Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil**: DOC-ICP-01 v.4.1. 2010. Disponível em:

<<http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/docip4.pdf>>. Acesso em: 4 dezembro 2011.

_____. **Política de Segurança da ICP-Brasil:** DOC-ICP-02 v.3.0. 2008. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-02_-_v._3.0.pdf>. Acesso em: 4 dezembro 2011.

_____. **Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil:** DOC-ICP-03 v.4.5. 2010. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC_ICP_03.pdf>. Acesso em: 4 dezembro 2011.

_____. **Características Mínimas de Segurança para as AR da ICP-Brasil:** DOC-ICP-03.01 v.1.4. 2010. Disponível em: <<http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-03.01.pdf>>. Acesso em: 4 dezembro 2011.

_____. **Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil:** DOC-ICP-05 v.3.5. 2010. Disponível em: <<http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-05.pdf>>. Acesso em: 4 dezembro 2011.

_____. **Política Tarifária da Autoridade Certificadora Raiz da ICP-Brasil:** DOC-ICP-06 v.3.0. 2008. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-06_-_v._3.0.pdf>. Acesso em: 4 dezembro 2011.

_____. **Critérios e Procedimentos para Auditoria das Entidades Integrantes da ICP-Brasil:** DOC-ICP-08 v.4.0. 2009. Disponível em: <<http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-08.pdf>>. Acesso em: 4 dezembro 2011.

_____. **Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP-Brasil:** DOC-ICP-09 v.3.0. 2008. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-09_-_v._3.0.pdf>. Acesso em: 4 dezembro 2011.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Desmaterialização de processos integra pauta da Rio+20. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Noticias/PressRelease2011Oct13_211303>. Acesso em: 4 dezembro 2011.

JIAMBALVO, James. **Contabilidade Gerencial**. Tradução Tatiana Carneiro Quírico. Rio de Janeiro: LTC – Livros técnicos e Científicos Editora S.A., 2002.

JOHNSON, G.; SCHOLES, K. **Exploring Corporate Strategy**. Harlow: Financial Times Prentice Hall, 2002.

JOHNSON, Gerry; SCHOLES, Kevan; WHITTINGTON, Richard. **Explorando a estratégia corporativa: textos e casos**. Porto Alegre: Bookman, 2007.

JORDAN, H.; NEVES, J. C.; RODRIGUES, J. A. **O Controlo de Gestão** (8.^a ed.). Lisboa: Áreas, 2008.

KEMPE, D.; KLEINBERG, J.; TARDOS, E. Influential nodes in a diffusion model for social networks. **Proceedings...** Lisboa, 2005.

KOHNFELDER, L. **Towards a practical public-key cryptosystem**. MIT laboratory for Computer Systems. Master thesis, 1978.

KOUFOPOULOS, D.; MORGAN, N. **Competitive pressures force Greek entrepreneurs to plan**. Long Range Planning, 1994.

LAPPONI, J. C. **Modelagem Financeira com Excel**. Rio de Janeiro: Campus, 2004.

LÖNNQVIST, A.; PIRTTIMÄKI, V.. The Measurement of Business Intelligence. **Information Systems Management Journal**. 2006, p. 32-40.

LOSHIN, D. **Business Intelligence: The Savvy Manager's Guide**. São Francisco: Morgan Kaufmann, 2003.

LUNKES, Rogério João. **Contabilidade gerencial: um enfoque na tomada de decisão**. Florianópolis: Visual Books, 2007.

MINTZBERG, Henry; AHLSTRAND, Bruce; LAMPEL, Joseph. **Safari de estratégia: um roteiro pela selva do planejamento estratégico**. Porto Alegre: Bookman, 2000.

MINTZBERG, Henry; QUINN, James Brian. **O processo da estratégia**. Porto Alegre: Bookman, 2001.

NEVES, José Luis: Pesquisa qualitativa: características, usos e possibilidades. **Caderno de pesquisas em administração.** v.1, nº 3, 2º sem., São Paulo, 1996

O QUE É CERTIFICAÇÃO DIGITAL. [on line] Disponível em:
<<http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>> Acesso em 27 dez. 2011.

POWER, D.J. A Brief History of Decision Support Systems. 2007. Disponível em:
<http://dssresources.com/history/dsshistory.html>. Acesso em 07/11/2010.

RECUERO, Raquel. **Redes sociais na internet.** Porto Alegre: Sulina, 2009. Coleção Cibercultura.

REIS, Carlos; **Planeamento Estratégico de Sistemas de informação.** Lisboa: Presença, 1993.

RIBEIRO, A. M. et al. **A Infraestrutura de Chaves Públicas Brasileira e suas Bases para a Auditoria em Segurança da Informação.** Diretoria de Auditoria, Fiscalização e Normalização, Instituto Nacional de Tecnologia da Informação, Brasília, 2004.

RICHARDSON, R. J. **Pesquisa social:** métodos e técnicas. São Paulo: Atlas, 1999

ROESCH, S. M. A. **Projetos de Estágio e de Pesquisa em Administração.** 2ª ed. São Paulo: Atlas, 1999.

ROUX, D. S. **Best Practice in Corporate Performance Management** (Master's Thesis in Business Management, unpublished). Johannesburg: Faculty of Economic and Management Sciences, Rand Afrikaans University, University of Johannesburg, 2004.

SCHEIBELHOFER, K. **Signing XML Documents and the Concept of “What You See Is What You Sign”.** 2001. 118 p. Dissertação (Master's Thesis in Telematics) - Institute for Applied Information Processing and Communications, Graz University of Technology, Austria, 2001.

SERPRO. **ICP-Brasil é padrão de qualidade**, folha de Pernambuco, Informática. Disponível em: <http://www.serpro.gov.br/noticias-antigas/noticias-2004/20040714_03>. Acesso em: 4 dezembro 2011.

SERPRO. Número de certificados digitais deve chegar a 1 milhão em 2006, Wnews, Larissa Januário. Disponível em: <http://www.serpro.gov.br/noticias-antigas/noticias-2006/20060509_01>. Acesso em: 4 dezembro 2011.

SEZÕES, C.; OLIVEIRA, J.; BAPTISTA, M. **Business Intelligence**. Porto: Princípia, 2006.
TAPSCOT, D., WILLIAMS,A. **Wikinomics: como a colaboração em massa pode mudar o seu negócio**. Rio de Janeiro: Nova Fronteira, 2007.

TOORANI, M.; SHIRAZI, A.A.B. **LPKI - A Lightweight Public Key Infrastructure for the Mobile Environments**. 11th IEEE International Conference on Communication Systems (IEEE ICCS'08), p.162-166, Guangzhou, China, Nov. 2008.

TURBAN, E; RAINER JR; R. K; POTTER, R. E. **Administração de Tecnologia da Informação**. Rio de Janeiro: Elsevier, 2003.

VERCELLIS, C. **Business Intelligence: Data Mining and Optimization for Decision Making**. John Wiley & Sons, 2009.

WATSON H. Tutorial: Business Intelligence -- Past, Present, and Future. **Communications of AIS**. 2009, p. 487-510.

WELLMAN B.; SALAFF J.; DIMITROVA D.; GARTON L.; GULIA M.;
HAYTHORNTHWAITE C. Computer Networks as Social Networks: Collaborative Work, Telework, and Virtual Community. **Annual Review of Sociology**. 1996, v. 22 p. 213

ZENKNER, Alberto. **O Uso dos Sistemas de Informação no Apoio ao Planeamento e Controlo Corporativo**. Lisboa, 2011. f. Dissertação.