Sustainable Business International Journal

DEZEMBRO DE 2012- ISSN 1807-5908

SUSTENTABILIDADE DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

Handerson Koerich,
handerson.koerich@gmail.com

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.*

Sustainable Business International Journal

DEZEMBRO DE 2012- ISSN 1807-5908

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*.

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 avalição. 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;

2 FUNDAMENTAÇÃO TEÓRICA

2.1 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*.

2.2 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 esta 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, 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.

2.3 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.

2.4 ICP BRASIL

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 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).

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.

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
1ª - Revisar a literatura e a legislação pertinente	Revisão Teórica + Análise Documental	Descritiva Exploratória Dedutivo	Análise documental Pesquisa bibliográfica Observação	Objetivo	"É"
2ª - Análise de casos à luz da teoria	Entrevistas abertas	Qualitativa Estudo de caso	Roteiro Observação	Objetivo + Subjetivo	"É" Versus "Deve ser"
3ª - Desenvolver modelo econômico-financeiro	Fundamentação teórica + objetivo + subjetivo	Avaliativo Indutivo	Modelagem de requisitos	Objetivo + Subjetivo	"Deve ser"
4ª - 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.

4 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 explicita, 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.

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 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.

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.

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.

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 esta 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.

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 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

gestão das atividades inerentes à AC é feita por três perfis distintos (ICP-BRASIL, 2010a), gerente de configuração, gerente de segurança e administrador do sistema.

Não existe uma quantidade mínima de pessoas exigidas nos DOC-ICPs, mas iremos assumir que são necessários no mínimo oito colaboradores: i) três gerentes; 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.

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 estimação 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.

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*.

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 centro, 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.

5 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.

5.1 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.

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%.

Descritivo	**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 2 - 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:

Descritivo	**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 3 - 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:

Descritivo	**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 4 - Comparativo do cenário atual AC sem hardware.
Fonte: Elaboração própria.

5.2 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.

Descritivo	**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 5 - Cenário proposto para AR e AC.
Fonte: Elaboração própria.

6 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 mais uma receita para a empresa, gera uma maior dificuldade em se tornar rentável a operação. A falta de uma estratégia ativa na capitação 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.

REFERÊNCIAS

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

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

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

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.

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.

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

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

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.

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.

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.

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