Um modelo para a implementação de contratos eletrônicos válidos

Telmo De Cesaro Júnior[1]
Roberto dos Santos Rabello[1]

Resumo: Este artigo tem como objetivo apresentar um modelo de implementação para um módulo de geração de contratos eletrônicos válidos. Pelo fato de não existir uma regulamentação específica sobre essa modalidade de contratação no Brasil, este estudo irá buscar na atual legislação um enquadramento para a contração eletrônica. A partir dessa fundamentação, unida com a regulamentação da certificação digital e do avanço da biometria, será possível garantir a integridade e a autoria dos contratos eletrônicos, requisitos fundamentais para a obtenção da validade. Nesse sentido, este artigo irá elucidar os recursos computacionais necessários pra tal.

Palavras-chave: Biometria. Certificado digital. Contratos eletrônicos.

Abstract: *This meta-paper has as goal to present an implementation model for a module to generate electronic contracts valid. Because there isn't a specific regulation on this type of hiring in Brazil, this study will search in the current legislation guidelines for electronic hiring. For this reason, joint with the regulation of digital certification and advancement of biometrics, it will be possible to ensure the integrity and authorship of electronic contracts, which are fundamental requirements for obtaining valid. Accordingly, the model will present the resources computational for achieving this goal.*

Keywords: *Biometrics. Digital certificate. Electronics contracts.*

1 Introdução

Atualmente, a convergência de dados para o meio eletrônico é entendida como uma necessidade, pois a relação custo/benefício é extremamente positiva, trazendo inúmeras vantagens para os seus usuários e/ou envolvidos. Uma das principais razões para tal mudança é a facilidade no tráfego de dados no meio digital. Segundo a maioria dos estudiosos em análise prospectiva, essa tendência vem comprovar a atual transformação de sociedade industrial para a pós-industrial e informacional.

Seguindo essa ideia, com o aprimoramento tecnológico, alinhada com a atual legislação, tornou possível a migração de documentos físicos, como contratos tradicionais feitos em papel, para documentos eletrônicos, mantendo a sua validade legal. Atualmente, não são muitos os estudos que exemplificam a utilização de técnicas computacionais, como os certificados digitais e a biometria por impressão digital, bem como na verificação da legalidade na contratação eletrônica.

Diante dessa constatação, motivou-se a elaboração dessa pesquisa, cujo objetivo principal é apresentar um modelo de implementação para um módulo de geração de contratos eletrônicos válidos e contribuir na disseminação do conhecimento, no que se refere à utilização de recursos computacionais em prol da contratação eletrônica.

Os próximos dois itens apresentarão o enquadramento para contratos eletrônicos, o carimbo do tempo, a assinatura digital e a manifestação da vontade pela biometria. No item quatro será proposto um modelo de

[1] Curso de Ciência da Computação, UPF, Campus 1 - BR 285 - Passo Fundo (RS) - Brasil
{decesarojunior@yahoo.com.br,rabello@upf.br}

http://dx.doi.org/10.5335/rbca.2012.2061

implementação, elucidando os recursos computacionais para a geração de contratos eletrônicos válidos. Por fim, são apresentadas as considerações finais.

2 Contratos eletrônicos

A internet, considerada como um dos principais meios de comunicação da atualidade, trouxe consigo a possibilidade da realização de diversos negócios por meio do computador. Com isso surgiram os denominados "documentos eletrônicos", os quais, em síntese, são aqueles emanados da celebração de um negócio jurídico por intermédio do meio digital. Atualmente, os contratos eletrônicos representam um fator de extrema importância em termos de crescimento e evolução da internet. Para enriquecer o assunto, vale subsidiar-se em Albertin [1], quando explica que

> a internet e seus serviços básicos, tais como correio eletrônico e WWW, têm criado um novo espaço para a realização de negócios. Esse novo ambiente tem fornecido para os agentes econômicos – tanto para empresas como indivíduos - canais alternativos para trocar informações, comunicar, distribuir diferentes tipos de produtos e serviços e iniciar transações comerciais.

No entanto, mesmo com todo o desenvolvimento tecnológico na área da informática, grande parte dos usuários da internet limita-se somente às relações de consumo no mundo real. Isso se deve ao fato de que a sociedade entende a internet como um meio inseguro, o que causa receio na maioria dos usuários em contratar eletronicamente [2].

2.1 Elementares de contratos eletrônicos

Os contratos eletrônicos podem ser conceituados como negócios jurídicos bilaterais, que se utilizam de computadores e outros tipos de aparelhos eletrônicos, como, por exemplo, telefone celular, iPhone ou tablet, conectados à internet, por meio de um provedor de acesso, a fim de se instrumentalizar e firmar o vínculo contratual, gerando, assim, uma nova modalidade de contratação, denominada contratação eletrônica.

Buscando o necessário auxílio na doutrina sobre o assunto, no intuito de conceitualizar a contratação eletrônica, é possível entender que, segundo Slanz [3], "O contrato eletrônico, portanto, nada mais é do que um contrato tradicional celebrado em meio eletrônico, ou seja, através de redes de computadores – é aquele celebrado por meio de programas de computador ou aparelhos com tais programas".

Ainda sobre esse importante conceito, Barbagalo [4] assim se manifesta: "[...] definimos como contratos eletrônicos os acordos entre duas ou mais pessoas para, entre si, constituírem, modificarem ou extinguirem um vínculo jurídico, de natureza patrimonial, expressando suas respectivas declarações de vontade por computadores interligados entre si."

É possível afirmar que o contrato eletrônico não é uma nova modalidade no âmbito da teoria geral dos contratos, mas uma forma de contratação que facilita a relação dos contratantes. A diferença para os demais contratos está na sua formação, onde a execução e/ou elaboração é promovida na internet.

Nesse tipo de contratação é dispensado em parte a intervenção humana, no que tange ao contato pessoal entre os contratantes. Esse diferencial, visto como uma vantagem em relação ao método tradicional, tem recebido diversos questionamentos quanto à ausência de vontade no momento da celebração dos contratos eletrônicos, que podem ser considerados apenas como uma espécie de documento eletrônico. De acordo com Barbagalo [4]:

> O contrato eletrônico é caracterizado por empregar meio eletrônico para sua celebração. Apresenta quanto à capacidade, objeto, causa e efeitos as mesmas regras a serem aplicadas aos contatos celebrados por meio físico.
>
> [...]
>
> A contratação eletrônica é aquela que se realiza mediante a utilização de algum elemento eletrônico, e se este tem ou pode ter uma incidência real e direta sobre a formação da vontade ou do desenrolar da interpretação futura do acordo.

[...]

O contrato eletrônico, por sua vez, é o negócio jurídico bilateral que resulta do encontro de duas declarações de vontade e é celebrado por meio da transmissão eletrônica de dados.

Diante dessas citações, é possível afirmar que a manifestação da vontade pode se verificar de qualquer maneira inequívoca, de modo que o meio eletrônico é hábil à formação do vínculo contratual, desde que se consiga identificar o agente.

Para que seja possível identificar os agentes envolvidos na formação do vínculo contratual, se faz necessário analisar sua técnica de formação. Sobre essa questão, Santos [5] estabelece a seguinte distinção entre "contratos concluídos por computador e contratos executados por computador". Essa tese afirma que, no primeiro caso, o computador intervém na formação da vontade e/ou na instrumentalização do contrato, sendo possível servir como meio de prova. No segundo caso, o computador funciona meramente como meio de comunicação entre as partes contratantes, pois o acordo de vontades já se encontra estabelecido.

Por fim, é válido ressaltar a diferença entre contrato eletrônico e contrato informático, pois, segundo Santos [5], contratos eletrônicos são "os negócios jurídicos que utilizam o computador como mecanismo responsável pela formação e instrumentalização do vínculo contratual...", ao tempo que os contratos informáticos têm por finalidade bens e/ou serviços na área da informática.

2.2 Classificação dos contratos eletrônicos

Para determinar o momento e o local onde a contratação é celebrada, é necessário classificar os contratos eletrônicos. Haja vista que não existe uma regulamentação sobre o tema na legislação brasileira, faz-se necessário buscar na literatura um modelo de classificação que melhor represente os principais tipos de contratos. Existem diversas classificações acerca dos contratos eletrônicos baseadas na forma como o computador é utilizado para a celebração do contrato, ou do modo em que o este é firmado na internet.

A classificação utilizada neste estudo será a de Santos e Rossi[6], compactuada por Barbagalo [4] e Biago Júnior [7]. A sua escolha justifica-se por ser a mais abrangente entre as inúmeras outras classificações existentes e por ser frequentemente adotada em estudos afins. É baseada na forma de comunicação realizada por meio da internet. Segundo esses autores, os contratos eletrônicos podem ser classificados em três espécies:

1. Contratos eletrônicos intersistêmicos, também denominados como "contratação em rede fechada": nessa modalidade de contrato todo conteúdo é previamente acordado entre as partes e estas passam suas vontades para o computador conectado à internet. Assim, a utilização do computador não interfere na formação do consentimento das partes. Um exemplo de aplicação desse tipo de contratação é a troca eletrônica de dados, ou EDI (*eletronic data interchange*: intercâmbio eletrônico de dados).
2. Contratos eletrônicos interpessoais: nesse tipo de contrato, as partes obrigatoriamente dependerão da utilização dos computadores conectados à internet para a formação do vínculo contratual, pois a manifestação da vontade ocorre a partir da comunicação entre estes. Isso pode ocorrer de forma simultânea ou não, o que caracterizará a contratação entre presentes ou entre ausentes. Como exemplo, pode-se citar a utilização de ambientes ou softwares que proporcionam diálogos na internet, tais como Windows Live Messenger (MSN), Skype e E-mail.
3. Contratos eletrônicos interativos: essa modalidade é a mais utilizada atualmente na aquisição de produtos e serviços na internet. A relação contratual ocorre entre a interação de uma pessoa com um sistema aplicativo previamente programado. Os contratos de "adesão" ou "condições gerais dos contratos" são exemplos desse tipo de contratação. O CDC, no art. 54, traz a seguinte regulamentação sobre essa modalidade: "É aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo." Assim, não caberá, em momento algum, a discussão ou negociação preliminar nesse tipo contratual.

2.3 Legislação brasileira e os contratos eletrônicos

Antes de iniciar esta subseção, é primordial informar que o CC brasileiro não apresenta disposições específicas quanto à contratação eletrônica; não há sequer um capítulo específico nesse diploma legal que trate

exclusivamente das questões que permeiam o meio virtual. No entanto, algumas disposições são aplicadas diretamente às questões jurídicas que envolvem a questão da internet; isso se dá de forma positiva e amplia os mecanismos legais de proteção neste novo meio [8].

Os contratos eletrônicos trazem alguns questionamentos em decorrência das regras advindas do CC. Dentre as questões que merecem enfoque, citam-se a força probatória dos contratos entre ausentes, a vinculação existente entre as partes, o momento em que o contrato eletrônico passará a valer e o momento em que é considerada aceita a proposta e a retratação [2].

Na questão da segurança da informação, é preciso destacar que cabe ao administrador, seja diretor, gerente, chefe de segurança (CSO: Chief Security Officer), a responsabilidade pelos sistemas informáticos, a manutenção de ações preventivas, reparação de danos e obrigação legal de bloquear as vulnerabilidades existentes nos sistemas eletrônicos, bem como processar judicialmente os responsáveis por invasões, fraudes, entre outros ilícitos ocorridos em meio virtual, conforme o disposto no CC brasileiro (Direito da empresa – Livro II – Parte Especial).

Torna-se pertinente salientar que questões como a boa-fé, a função social do contrato, os usos e os costumes dispostos no CC trazem sustentação a essa nova forma de contratação. Sobre o assunto, Blum [8] acredita que

> significa dizer que houve uma preocupação em garantir a manifestação de vontade por qualquer meio, especialmente no eletrônico, já incorporado à nossa tradição tecnológica e que pode ser equiparado a contratação via telefone, nas situações em que efetivamente ocorra a transação "ao vivo", configurando-se uma contratação entre presentes, como preceitua o Livro I, Das Obrigações (Parte Especial).

A prova eletrônica, de fundamental importância para a obtenção do reconhecimento legal nesse tipo de contratação, pode ser criada com a inclusão de uma assinatura digital, que visa garantir a integridade do documento eletrônico. Esse mecanismo será detalhado no item 3.3.2.

A presença das partes é uma questão a ser ressaltada, visto que também existirá na contratação por meio da internet. Exemplo disso é a utilização de softwares de trocas de mensagens instantâneas, como Windows Live Messenger (MSN) e o Skype. Segundo Pinheiro [9], um simples "ok" no MSN poderá ser considerado como uma manifestação válida de vontade, obrigando as partes contratantes. No caso da utilização do e-mail, cuja forma de transmissão das mensagens é assíncrona, não bastará apenas o envio do e-mail: este terá de ser aberto pelo destinatário.

Por fim, em relação à forma da contratação, assunto que foi abordado anteriormente, é possível afirmar que não havendo previsão de forma, como o caso dos contratos de compra e venda de imóvel, qualquer contrato comercial ou de prestação de serviço poderá ser realizado por meio eletrônico.

2.3.1 Assinatura digital no Brasil

Na internet, para que se possa comprovar a autoria de um determinado documento eletrônico, é necessário anexar uma assinatura digital. A criação dessa assinatura consiste na geração de um resumo do documento original, também conhecido como *hash* e a sua criptografia. A regulamentação da assinatura digital e da criptografia no Brasil foi editada em 29 de dezembro de 1998, por meio do decreto nº. 2.910, emitido pelo então presidente da República Fernando Henrique Cardoso. A partir desse decreto estabeleceram-se as normas para proteção e garantia de documentos, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa, entre outras providências.

Com a regulamentação e utilização da assinatura digital, tornou-se possível comprovar legalmente e tecnicamente a vinculação da criação ou concordância de um documento eletrônico com uma pessoa física ou jurídica. Além disso, a assinatura digital oferece um nível considerável de segurança nas relações contratuais firmadas via internet, pois informa o autor sobre a assinatura e se o documento foi adulterado; se esta última hipótese vier a ocorrer, a assinatura digital também será adulterada.

Contribuição importante sobre essa questão vem ser obtida em Brasil, quando a mesma afirma que

> [...] a assinatura digital ou assinatura eletrônica, diferentemente da assinatura real, se modifica a cada arquivo transformado em documento e seu autor não poderá repeti-la como faz com as assinaturas apostas nos documentos reais.
>
> [...]
>
> Assinatura é ato pessoal, físico e intrasferível. Dado codificado digital é uma seqüência de bits, representativos de um fato, registrados em um programa de computador [10].

O certificado digital, além de personificar o cidadão na internet, garante, por força da legislação atual, validade jurídica aos atos praticados com seu uso. É uma ferramenta que permite que aplicações, como comércio eletrônico, assinatura de contratos, operações bancárias, órgãos governamentais, entre outras, sejam realizadas com segurança jurídica e identificação inequívoca das partes envolvidas [11].

Atualmente, é possível afirmar que a utilização do certificado digital e, consequentemente, dos documentos eletrônicos assinados digitalmente vem crescendo rapidamente. Esse crescimento se deve ao fato de que as instituições públicas, como a Receita Federal[2] e o Poder Judiciário,[3] contribuíram de forma significativa na disseminação desse recurso computacional no Brasil, com a implantação de projetos de informatização de documentos fiscais e jurídicos. O tipo mais comum para certificados digitais no âmbito da ICP é o X.509, proveniente do padrão ITU-T X.509. Esse tipo foi desenvolvido para ser utilizado em serviços da Web, como e-mail e assinatura de documentos XML.

2.3.2 Carimbo do tempo

Para ter validade, a assinatura digital precisa estar ligada a um certificado digital válido. Como os certificados digitais possuem validades predefinidas, no momento que são gerados, é necessária uma referência temporal para determinar se a assinatura foi produzida enquanto o certificado era válido.

O carimbo do tempo foi regulamentado pelo decreto nº 4.264, de 10 de junho de 2002, o qual reafirmou a competência do Observatório Nacional na geração e disseminação da hora legal brasileira. Portanto, o carimbo ou selo do tempo é o recurso computacional que possibilita a obtenção da hora legal brasileira, de forma segura, autêntica e auditável. O órgão responsável pela infraestrutura para a emissão de carimbos do tempo é a Autoridade de Carimbo do Tempo Brasileira de Registros (ACTBR).

3 Manifestação da vontade pela biometria

A biometria é o uso automatizado de características fisiológicas ou comportamentais dos seres humanos para identificar a sua identidade. Entre os atributos físicos comumente utilizados, tem-se a impressão digital dos dedos, o reconhecimento do rosto, da retina, da íris e o mapeamento de vasos sanguíneos. No que se refere ao comportamento, tem-se o reconhecimento de tom de voz, ritmo de digitação e análise grafotécnica. Em síntese, a biometria é a ciência que estuda a medida dos seres vivos.

A utilização das características físicas para identificar um indivíduo do outro não é algo novo, pois é utilizada pelo homem desde os primórdios. O método biométrico que apresenta maior exatidão é o teste de DNA, o qual já é aceito pelo Judiciário, apesar de não ser totalmente seguro. É possível afirmar que em todos os métodos biométricos existe uma margem de erro, que deve ser levada em consideração.

A assinatura autógrafa, que também é um tipo de reconhecimento biométrico, considerando as características únicas de traço, pressão e velocidade, pode ser substituída por outras formas de autenticação. Sobre essa importante afirmação Therrien e Tronco [12] assim se manifestam:

[2] A Receita Federal, através da instrução normativa SRF nº 222, de 11 de outubro de 2002, instituiu o "Serviço interativo de atendimento virtual", denominado abreviadamente de "Receita 222", cujo acesso somente se efetiva com a utilização dos certificados digitais "e-CPF", "e-CNPJ". A instrução normativa nº 482, de 21 de dezembro de 2004, tornou obrigatória a entrega da Declaração de débitos e créditos tributários (DCTF) mediante certificação digital.

[3] O Poder Judiciário conta com a Autoridade Certificadora do Sistema Justiça Federal (AC-JUS), uma autoridade certificadora (AC) de nível intermediário na ICP-Brasil (AC-Raiz), a primeira autoridade certificadora do Poder Judiciário mundial.

> Existem diversos meios de autenticação, sendo o mais conhecido e ainda utilizado, a assinatura autógrafa, em que de próprio punho, o indivíduo posta sinal identificador exclusivo seu. Este meio, na verdade, também é um método de natureza biométrica, que pode ser realizado de forma manual ou automático.

Nos contratos eletrônicos, há manifestação da vontade por parte da contratante, que também poderia ser realizada por meio de uma assinatura digital, torna-se mais viável financeiramente se for realizada através de um método biométrico automático. Para comprovar tal afirmação, pode-se tomar como exemplo o custo de um leitor biométrico ótico de impressões digitais em comparação com um certificado digital, os quais são equivalentes. Neste caso não seria necessário exigir da parte contratante um certificado digital para a manifestação da vontade, bastando apenas a utilização do leitor biométrico, que poderia ser utilizado inúmeras vezes e também para outros fins.

O método biométrico, tomado como referência para este estudo, será a autenticação pela impressão digital. A captura dessa característica física é realizada por meio de um leitor de impressões digitais, que pode ser óptico ou capacitivo. As informações colhidas são únicas, não sendo possível ter duas pessoas com a mesma impressão digital, exceto em caso de fraude. Tal mecanismo biométrico é o mais utilizado atualmente em aplicações comerciais, financeiras e hospitalares, em virtude da relevante vantagem na relação custo/benefício e da facilidade de implantação.

Atualmente, com a evolução dos algoritmos de reconhecimento de impressões digitais, bem como a disponibilidade de leitores biométricos capacitivos rolados, que permitem capturar uma grande quantidade de informações da impressão digital, é possível afirmar que esse tipo de biometria apresenta índices de confiabilidade superiores à assinatura autografada. Essa afirmação pode ser comprovada na crescente adoção da biometria, por parte da iniciativa pública[4] e privada,[5] as quais encontraram na biometria um mecanismo eficiente para a redução de fraudes em seus processos.

3.1 Aspectos legais da utilização da biometria

Na legislação brasileira não há lei específica sobre a biometria, contudo está associada diretamente aos conceitos de intimidade, privacidade e imagem do usuário. Sobre essa questão, é sabido que a Constituição da República Federativa do Brasil de 1988, em seu título II, capítulo I, que versa sobre os Direitos e deveres individuais e coletivos, em seu artigo 5º, inciso X, traz a seguinte cláusula:

> Art. 5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e os estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes [...].
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação.

Com base nessa cláusula, é possível afirmar que a Constituição visa proteger o segredo da vida privada do indivíduo e a sua liberdade para exercê-la sem a interferência de terceiros. Para Silva, esses direitos são ameaçados pela investigação de acontecimentos relacionados à vida pessoal e familiar do indivíduo, bem como a divulgação ao público, ou ao menos a um determinado número de pessoas, desses acontecimentos [13]. Nesse sentido, não seria um equívoco afirmar que o segredo da vida privada é ameaçado também por investigações e divulgações ilegítimas, por aparelhos como máquinas fotográficas, gravadores de voz e dados.

Portanto, a coleta de dados biométricos recai sobre o direito à privacidade. Para minimizar a possibilidade de violação desse direito, faz-se necessário que a referida coleta com guarda dos dados biométricos em algum banco de dados seja realizada após a autorização do indivíduo proprietário da característica captada.

[4] Eleições 2008: votação com urnas biométricas transcorre normalmente. Disponível em: <http://idgnow.uol.com.br/internet/2008/10/05/eleicao-2008-votacao-com-urnas-biometricas-transcorre-normalmente/>. Acesso em: jan. 2011.

[5] Biometria no vestibular da Unicamp previne fraudes. Disponível em: <http://www.unicamp.br/unicamp/divulgacao/2007/05/22/biometria-no-vestibular-da-unicamp-previne-fraudes >. Acesso em: jan. 2011.

4 Um modelo de implementação para contratos eletrônicos

Para alcançar o principal objetivo desse estudo, esta sessão irá apresentar um modelo de implementação para um módulo de geração de contratos eletrônicos válidos. Segundo a classificação dos contratos eletrônicos apresentada neste estudo, o tipo de contrato que será gerado por esse modelo será o interativo.

Esse modelo tem como premissa básica a conformidade com os requisitos técnico-legais, tais como preservação de provas e mitigação de riscos relacionados à violação dos diretos autorais, de integridade e de repúdio, que foram levantados nas sessões anteriores desta obra. Para um melhor entendimento, a explanação será dividida em cinco partes: visão geral, detalhamento, validação técnica, aspectos financeiros e requisitos de segurança.

A primeira parte apresentará uma visão geral sobre os componentes que compõem o modelo. Os recursos tecnológicos empregados em cada componente serão detalhados e justificados. Nas partes sequentes será apresentado o detalhamento técnico que exemplificará uma forma de implementação do modelo. Sua validação técnica será verificada por meio da apresentação de um protótipo.

4.1 Visão geral sobre o modelo

Como pode ser visto na Figura 1, para a celebração do contrato eletrônico será necessária a união dos seguintes dados: cláusulas contratuais, impressão digital dos envolvidos, carimbo do tempo e assinatura digital.

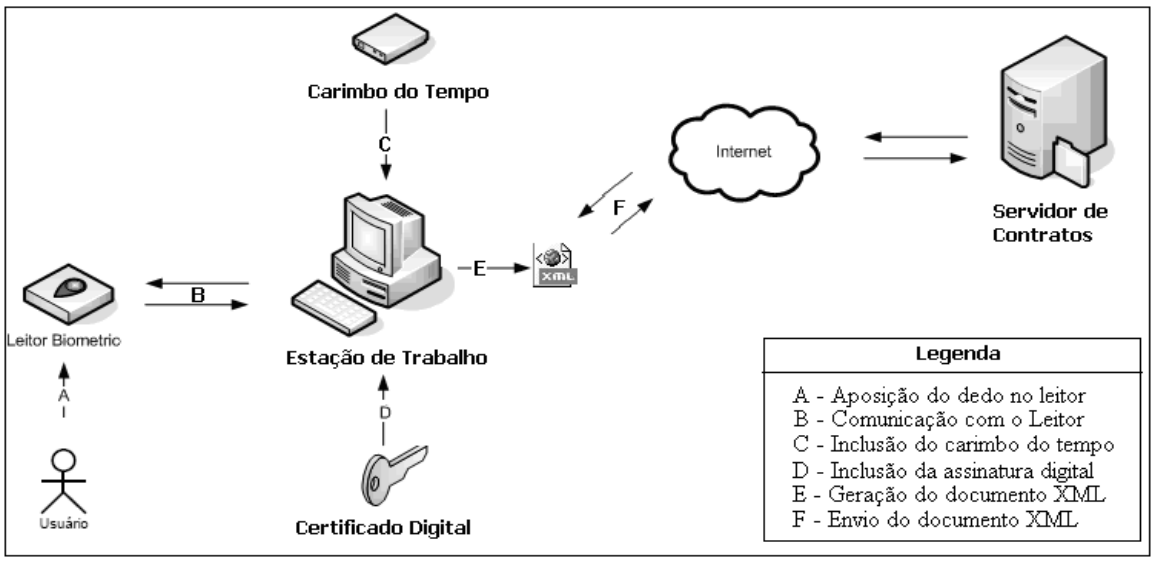

Figura 1: Visão geral do modelo

A biometria por impressão digital é usada para que os envolvidos possam manifestar a sua vontade em contratar por meio da aposição das digitais dos seus dedos em um leitor biométrico. Outros métodos biométricos também poderiam ser utilizados, como, por exemplo, a autenticação facial ou a combinação de duas ou mais formas para minimizar os riscos de fraudes.

Para afastar qualquer discussão sobre a possibilidade de violação do direito de imagem, o proprietário da característica captada deverá autorizar tal procedimento por meio da aceitação de um termo. Esse termo deverá esclarecer a finalidade da captura, a sua utilização e o seu armazenamento. Após o indivíduo aceitar o termo, declarando que tem ciência e concordância com as informações ali presentes, a captura poderá ser realizada de fato.

As cláusulas contratuais, que representam a proposta contratual, são armazenadas no formato XML. Esse formato, amplamente conhecido no meio técnico, organiza os dados por intermédio de marcadores, também conhecidos como *tags*, o que facilita a leitura e a assinatura digital por sistemas informáticos.

O carimbo do tempo é o mecanismo responsável pela comprovação do momento em que o contrato foi estabelecido. A referência temporal, conhecida como selo do horário, é obtida pela utilização de um serviço de Time-Stamping reconhecido pela ACT BR, disponível na internet. O selo do horário gerado pelo serviço é incorporado no documento XML.

O certificado digital será o mecanismo que garantirá a integridade do documento. O certificado ilustrado na Figura 1 é o da parte contratada, não sendo necessário o contratante dispor também de um certificado. Assim, após a união das cláusulas contratuais, dados biométricos, selo do horário e assinatura digital, o documento XML é enviado para ser gravado no servidor de contratos.

4.2 Detalhamento da implementação do modelo

A implementação do modelo dar-se-á pela codificação de componentes de software e pela utilização do leitor de impressões digitais. Seguindo o padrão de arquitetura de software Model-View-Controller (MVC), o qual visa separar o desenvolvimento em três camadas lógicas, permitindo o desenvolvimento, teste e manutenção de forma separada, os componentes de software elencados nesse modelo são: camada de modelo ou lógica da aplicação (M): componente biométrico, componente de assinatura e componente de persistência; camada de controle (C): componente controlador; camada de apresentação ou visualização (V): componente de interface.

O diagrama da Figura 2 é o UML de Implantação. Neste é possível observar os componentes de software e hardware, bem como sua interligação.

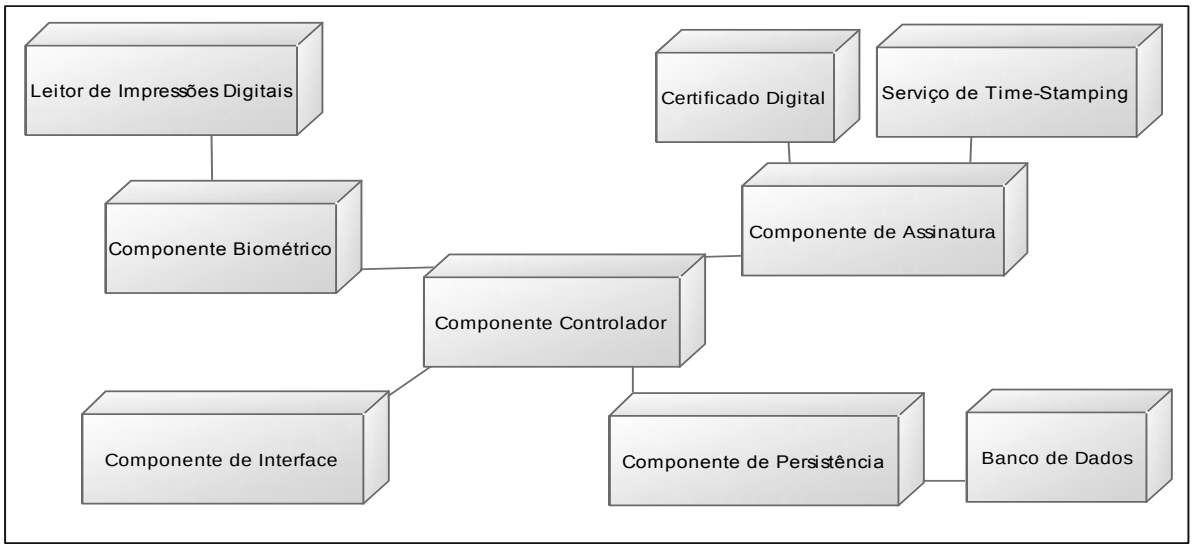

Figura 2: Diagrama UML de implantação

Como pode ser visto na Figura 2, o controlador é o componente que faz a interligação entre os demais, atuando como um distribuidor de tarefas. É responsável pela sincronização dos dados gerados e enviados pelos outros componentes. Para facilitar a sua codificação é aconselhável a utilização de um framework ou algum padrão de codificação. Entre os frameworks para a linguagem Java podem ser citados o JavaServer Faces (JSF)[6] e o Struts. Para a linguagem CSharp tem-se a prática Business Logic Layer (BLL).

O componente biométrico é responsável pela geração dos dados biométricos. Atualmente existem kits de desenvolvimento de software (SDK), interfaces de programação de aplicações (API) ou simplesmente bibliotecas disponíveis na internet para a interação com os principais leitores biométricos do mercado. Um exemplo disso é o SDK OTW[7] da empresa DigitalPersona. Por meio desse kit é possível criar um componente para capturar a impressão digital e, posteriormente, gerar um template biométrico em diferentes linguagens de programação, como, por exemplo, Java, Visual Basic, CSharp e C++.

[6]Maiores informações: <http://www.oracle.com/technetwork/java/javaee/javaserverfaces-139869.html>.
[7]Disponível em: <http://www.digitalpersona.com/biometrics/overview/>

O componente de assinatura realiza a geração da assinatura digital e a obtenção do carimbo do tempo. Na linguagem Java existe um pacote de classes chamado "javax.xml.crypto", que oferece métodos para a criação e validação de assinaturas em documentos XML. O carimbo do tempo pode ser obtido por meio da utilização de um serviço de Time-Stamping, disponível na internet, exemplo: Sistema de Carimbo do Tempo Bry Sct.[8] Esse recurso pode ser acessado através de uma aplicação Java com a biblioteca Axis2,[9] criada pela fundação Apache.

O componente de interface pode ser implementado com a utilização de uma biblioteca ou framework para a camada de apresentação, o que possibilita padronizar e agilizar a codificação. Na linguagem Java existem diversos recursos disponíveis para tal finalidade, como, por exemplo, a Java Server Pages (JSP), Java Standard Tag Library (JSTL), ou os frameworks Velocity e ICEFaces.

A codificação do componente de persistência pode ser realizada através de frameworks que realiza o mapeamento objeto-relacional. Essa ferramenta facilita o mapeamento dos atributos entre uma base de dados relacionais e o modelo de objetos de uma aplicação, mediante o uso de arquivos XML ou notações para estabelecer essa relação. Na plataforma de desenvolvimento .Net tem-se o framework NHibernate e o ADO.NET Entity. Para a linguagem Java, o principal framework para essa finalidade é o Hibernate. Em razão do considerável ganho de produtividade, reutilização de recursos e confiabilidade, a utilização de um framework para a persistência dos dados é imprescindível no desenvolvimento de qualquer software para fins comerciais.

4.3 Validação técnica do modelo de implementação

A validação técnica do modelo de implementação será demonstrada através de um protótipo. Esse software é uma aplicação web, cuja única funcionalidade é gerar um documento XML, que representa o contrato eletrônico interativo. Esse protótipo, denominado PGCE (Protótipo de geração de contratos eletrônicos), exemplificará a utilização de alguns dos recursos computacionais que foram citados anteriormente, bem como as demais ferramentas utilizadas para sua codificação.

As ferramentas computacionais utilizadas para o desenvolvimento foram a linguagem de programação Java, o framework Java Server Faces (JCF), o SDK OTW, o leitor biométrico de impressões digitais DigitalPersona U.are.U 4500, o pacote de criptografia "javax.xml.crypto", um certificado digital autoassinado no padrão X.509, o serviço de carimbo de tempo e-Timestamp[10] disponibilizado pela empresa DigiStamp e o ambiente de desenvolvimento NetBeans. Esses recursos foram escolhidos por não ser necessário adquirir licença de uso, exceto o caso do leitor biométrico.

O diagrama UML de atividades ilustrado na Figura 3 demonstra o processo de geração contrato eletrônico no formato XML. Tal processo inicia-se com a apresentação do termo de autorização da captura dos dados biométricos. Assim que todos os envolvidos concordarem com o termo, a captura das impressões digitais é iniciada. Aconselha-se o cadastro de, no mínimo, dois dedos por indivíduo para que se tenha uma margem de segurança em casos de lesões, acidentes ou ressecamento da pele do dedo.

[8]Maiores informações: < http://www.bry.com.br/index.php?class=solucoes&page=carimbo>.
[9]Maiores informações: < http://axis.apache.org/axis2/java/core/>.
[10] Maiores informações em: < http://www.digistamp.com/toolkitDoc/Java/index.htm>.

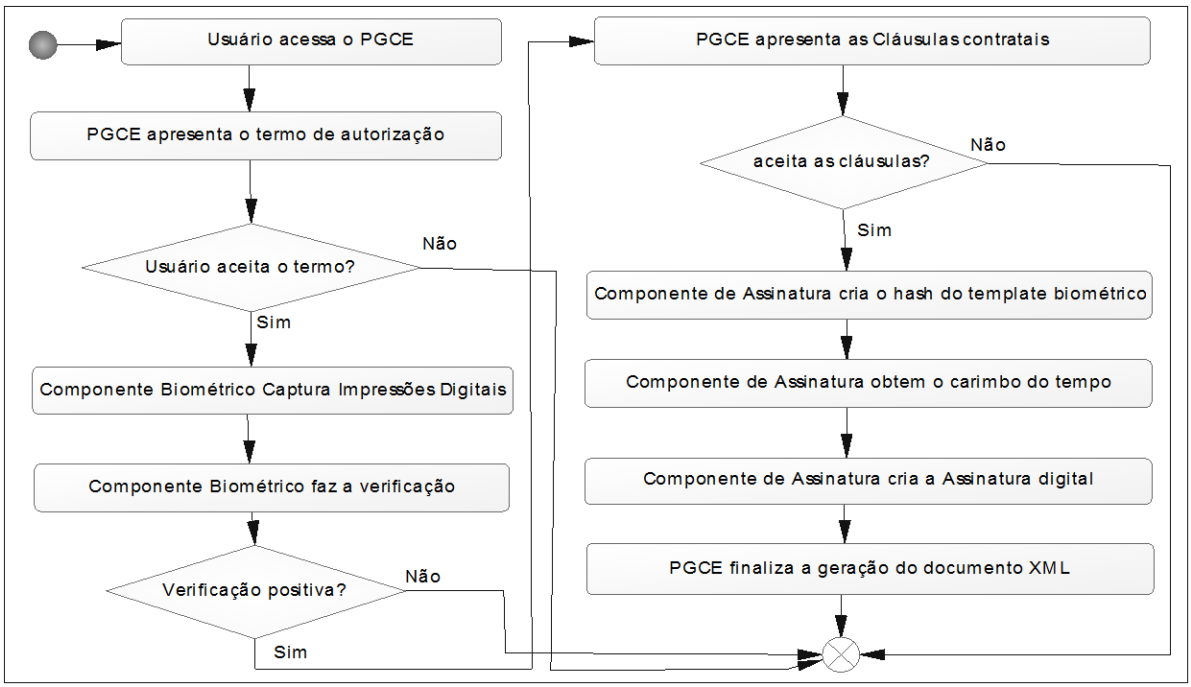

Figura 3: Diagrama UML de atividades – celebração do contrato

Na sequência, o PGCE realiza a autenticação biométrica através do componente biométrico, que por sua vez interage com o leitor. Caso a verificação seja positiva, as cláusulas contratuais são apresentadas. Com a aceitação das cláusulas, esse mesmo componente irá gerar o resumo (hash) dos templates biométricos e inseri-los em um documento XML. A Figura 4 apresenta a tela de captura das impressões digitais.

Figura 4: Coleta das impressões digitais

Por fim, o controlador aciona o componente de assinatura para a adição do carimbo do tempo e assinatura digital, utilizando o serviço de Time-Stamping e o certificado digital autoassinado, respectivamente. O contrato eletrônico, representado pelo documento XML, conterá as seguintes informações quando finalizado: cláusulas contratuais, hash do(s) template(s) biométricos, carimbo do tempo e a assinatura digital.

A finalização do processo dar-se-á com apresentação do documento XML finalizado, como pode ser visto na Figura 5. Para facilitar a identificação do contrato e para fins de fiscalização, além das informações citadas anteriormente, é importante que o documento contenha o número ou protocolo do contrato, uma referência ao identificador interno do dado biométrico, o número do certificado e o nome da autoridade certificadora. A Figura 5 apresenta a interface gráfica do PGCE, nela é possível o documento XML que representa o contrato eletrônico.

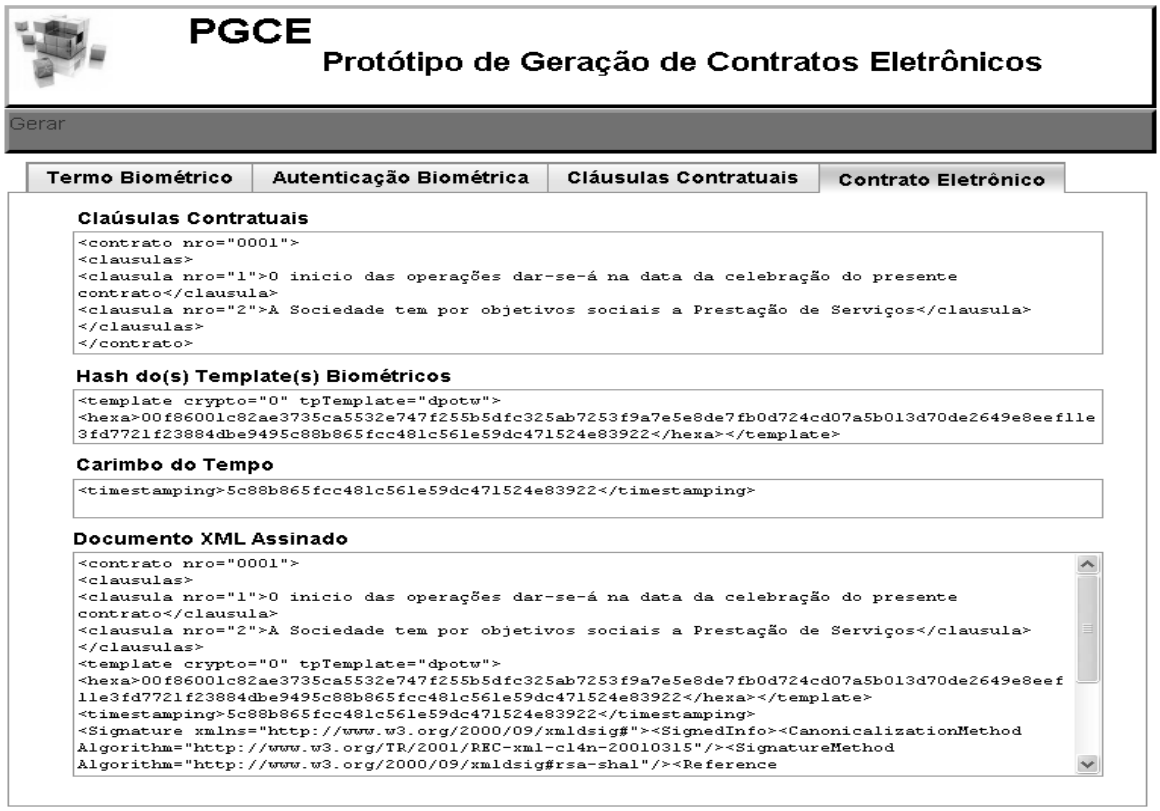

Figura 5: Tela de geração do contrato eletrônico através do PGCE

Por meio da apresentação do protótipo PGCE foi possível demonstrar a viabilidade técnica da implementação do modelo. Vale ressaltar que esse software exemplificou apenas a celebração do contrato eletrônico através da criação de um documento XML. Os processos de cadastro biométrico, utilização do certificado digital válido e persistência dos dados são funcionalidades que deverão ser codificadas para dar prosseguimento na evolução do protótipo, a fim de torná-lo uma aplicação comercial.

4.4 Requisitos básicos de segurança

O gerenciamento dos dados biométricos, realizado pelo componente biométrico, deve ser aderente a alguma norma de segurança que provém meios de assegurar que o processo de especificação, implementação e avaliação, foi conduzido de maneira rigorosa e padronizada. Desse modo, indica-se a adequação à norma ISO 19092:2008 e à ISO/TR 17994, que é um modelo de segurança aplicável a sistemas financeiros.

Ainda sobre a questão legal, o arquivamento dos dados biométricos deverá conter controles de confidencialidade, a fim de garantir que esses dados não sejam utilizados indevidamente. Um exemplo de controle de confidencialidade é a implantação de uma política de acesso ao banco de dados, a qual regulamenta quem poderá ter acesso, o que poderá ser acessado, alterações dos dados e sanções em caso de descumprimento das regras. Para atender as exigências contidas no CDC, no que dizem respeito a cadastros de clientes, os dados

biométricos deverão ser eliminados tão logo seja encerrada a relação entre as partes e o prazo de discussão contratual.

4.5 Aspectos financeiros relacionados ao modelo

Em virtude da informatização dos serviços governamentais, como a nota fiscal eletrônica e o registro de identidade civil (RIC), qualquer pessoa, seja física ou jurídica, terá de dispor de um certificado digital. Esse mesmo certificado poderá ser utilizado na assinatura de contratos eletrônicos [14].

Quanto às vantagens na utilização da contratação eletrônica, é possível afirmar que haverá uma significativa redução nos custos relacionados à impressão e logística, pois não será necessário imprimir cópia do contrato para que as partes possam inserir a assinatura autografada. Outra vantagem é a redução do tempo de geração do contrato e a facilidade de arquivamento, visto que no meio digital esses processos podem ser facilmente executados com custos relativamente baixos.

5 Considerações finais

A presente pesquisa abordou, inicialmente, as noções elementares sobre os contratos eletrônicos. A partir desse estudo, apresentou-se o enquadramento dos contratos eletrônicos. Por fim, para alcançar o principal objetivo desse estudo, foram apresentados um modelo de implementação e um protótipo para geração de contratos eletrônicos válidos.

A declaração da vontade, requisito fundamental para a celebração de um contrato, é realizada através da biometria por impressão digital. Procedimento que pode ser considerado válido para tal finalidade, uma vez que a assinatura autografada é um mecanismo de autenticação biométrica menos eficiente que a impressão digital. Para afastar os riscos relacionados à violação dos direitos de imagem e privacidade, o indivíduo deve concordar com o fornecimento dos dados biométricos pela aceitação de um termo.

Para garantir a integridade do documento eletrônico, o modelo em tela apresentou a utilização do certificado digital que garante a integridade do documento eletrônico. Para que se possa comprovar o momento exato em que o contrato foi celebrado, o modelo indica a utilização de um carimbo do tempo.

Com base nesses fundamentos é possível concluir que contratos comerciais ou de prestação de serviço, firmados no meio eletrônico, têm validade legal, desde que seja possível comprovar a manifestação da vontade das partes, isto é, da prova de autoria e integridade do documento eletrônico. Nesse sentido, o modelo de implementação exemplifica a utilização de recursos computacionais necessários para atender às exigências da lei e demonstrar a sua viabilidade técnica através de um protótipo.

Como já mencionado, atualmente existe certa resistência na adoção da contratação eletrônica, por não haver uma legislação específica para essa forma de contratação, pela insegurança que o meio virtual traz consigo e pela dificuldade na implementação e escolha dos requisitos computacionais. Portanto, também é possível afirmar que esta obra trouxe relevante contribuição teórica no que se refere à contratação eletrônica e à sua implementação.

Referências

[1] ALBERTIN, Alberto Luiz. *Comércio eletrônico*: modelo, aspectos e contribuições de sua aplicação, 4ed. São Paulo: Atlas, 2002. p. 45.

[2] SOUZA, Vinicius Roberto Prioli de. *Contratos eletrônicos & validade da assinatura digital*. Curitiba: Juruá Editora, 2009. p. 22, 82.

[3] GLANZ, Semy. Internet e contrato eletrônico. *Revista dos Tribunais*. São Paulo: Revista dos Tribunais, ano 87, v. 757, p. 72, 1998.

[4] BARBAGALO, Érica Brandini. *Contratos eletrônicos*: contratos formados por meio de redes de computadores - peculiaridades jurídicas da formação do vínculo. São Paulo: Saraiva, 2001. p. 37-38, 51-58.

[5] SANTOS, Manoel J. Pereira dos. Contratos eletrônicos. In: ROVER, Aires José (Org.). *Direito, sociedade e informática*: limites e perspectivas da vida digital. Florianópolis: Boiteux, 2000. p. 196-197, 105.

[6] SANTOS, Manoel J. Pereira dos; ROSSI, Mariza Delapieve. Aspectos legais do comércio eletrônico: contratos de adesão. *Revista de Direito do Consumidor*, São Paulo: Revista dos Tribunais, ano 9, n. 36, p. 129, 2004.

[7] BOIAGO JÚNIOR, José Wilson. *Contratação eletrônica*: aspectos jurídicos. Curitiba: Juruá, 2005. p. 87-94.

[8] BLUM, Renato Opice. O novo Código Civil e a internet. *Jus Navigandi*, Teresina, ano 8, n. 63, 1º. mar. 2003. Disponível em: <http://jus.com.br/revista/texto/3882>. Acesso em: 1º. abr. 2011.

[9] PINHEIRO, Patrícia Peck. *Direito digital*. 2ed. São Paulo: Saraiva, 2008. p. 72.

[10] BRASIL, Ângela Bittencourt. Assinatura digital não é assinatura formal. *Jus Navigandi*, 2000. Disponível em: <http://jus.com.br/revista/texto/1783/assinatura-digital-nao-e-assinatura-formal>. Acesso em: 12 mar. 2011.

[11] ACBR, Autoridade Certificadora Brasileira de Registros, 2011. Disponível em: <http://www.acbr.org.br/>. Acesso em: 02 abr. 2011.

[12] THERRIEN, Cristiano; TRONCO, Marlise. Biometria e identificação civil: aspectos técnicos e questões jurídicas. *Diálogo Jurídico*, 2006. p. 30.

[13] SILVA, Jose Afonso. *Curso de direito constitucional positivo*, 10. ed. São Paulo: Malheiros Editores, 1995. p. 204.

[14] REGISTRO DE IDENTIDADE CIVIL. Conheça o RIC. Disponível em: <http://portal.mj.gov.br/portal/ric/conhecao-o-ric>. Acesso em: 15 mar. 2011.

[15] RAUBER, Jaime José; SOARES, Márcio. *Apresentação de trabalhos científicos*: normas e orientações práticas. 3. ed. Passo Fundo: UPF, 2005.