Universidade Federal da Bahia

Fundação Faculdade de Direito

Curso de Pós-graduação em Direito Tributário Estadual

O USO DA INTERNET PELA SECRETARIA DA FAZENDA DO ESTADO DA BAHIA

ASPECTOS LEGAIS E DE SEGURANÇA

Alexandre Alcantara da Silva

Monografia apresentada à Fundação Faculdade de Direito da Universidade Federal da Bahia, como exigência parcial para obtenção do título de especialista em Direito Tributário Estadual, sob a orientação do Prof. Dr. Helcônio de Souza Almeida.

Salvador

Dezembro - 2001

Comissão Examinadora

_____

_____

_____

_____

_____

_____

Dedico esta monografia

À Jane, minha grande amiga e esposa, e aos pequenos Matheus, Lucas e Alexandre, pelas demonstrações de paciência, durante os momentos de elaboração deste trabalho.

Agradecimentos

Ao meu orientador, Profº Dr. HELCÔNIO DE SOUZA ALMEIDA, por ter me encorajado neste tema, e pelas contribuições ao trabalho.

Aos colegas da Secretaria da Fazenda do Estado da Bahia (SEFAZ-Ba.), que ao tomarem conhecimento do tema que escolhemos tornaram-se grande colaboradores enviando importantes contribuições.

Aos técnicos das Diretorias de Tributação, Diretoria de Tecnologia da Informação e Diretoria de Atendimento da SEFAZ-Ba, que prontamente se colocaram a disposição para debater as idéias e fornecer as informações solicitadas.

A Deus, por estar presente em todos os momentos, inclusive os mais difíceis de minha vida.

Internet no es simplemente una tecnología, sino que es la forma de organización dela nueva economía y de la nueva sociedad. Se puede decir que esta sociedad sin Internet es como la era industrial sin electricidad."

Manuel Castells

SUMÁRIO

RESUMO

A presente monografia traz o estudo do uso da Internet pela Secretaria da Fazenda do Estado da Bahia, no momento em que ela foi eleita como ferramenta prioritária no relacionamento com seus contribuintes. O foco principal do trabalho é o estudo da validade jurídica dos documentos eletrônicos produzidos neste relacionamento, inclusive os aspectos de segurança envolvidos. Trabalha-se, inicialmente, com os conceitos básicos sobre o que é a Internet, seu surgimento, funcionamento e problemáticas. Procede-se, em seguida, ao estudo dos aspectos relacionados à sua regulamentação, validade jurídica dos documentos eletrônicos e da assinatura digital, para em seguida fazer um levantamento da sua aplicabilidade nas administrações tributárias. Por último, analisa-se o uso desta ferramenta pela Secretaria da Fazenda do Estado da Bahia, detalhando seus aspectos históricos, serviços oferecidos, e apresentando algumas sugestões para contornar os principais problemas que entendemos existir no seu uso pela administração tributária baiana.

LISTA DE FIGURAS

INTRODUÇÃO

Nesta monografia abordaremos o uso da Internet pela Secretaria de Fazenda do Estado da Bahia (SEFAZ-Ba), no momento em que foi eleita a Internet como ferramenta prioritária de relacionamento com seus contribuintes, enfocando a validade jurídica dos documentos eletrônicos dela resultantes, inclusive os aspectos de segurança envolvidos. A Internet vem se revelando, a cada dia, como um veículo que permite tanto ao fisco como ao contribuinte minimizarem os custos. Para o contribuinte, a Internet reduziu de maneira significativa esses custos, pois possibilitou uma simplificação no cumprimento das obrigações tributárias acessórias, evitando as consultas desnecessárias às repartições fiscais. No Estado da Bahia, para alguns contribuintes, o deslocamento à repartições da Secretaria da Fazenda Estadual implica em até 300 quilômetros.

Com efeito, a partir desta relação fisco-contribuinte, via Internet, alguns aspectos no que diz respeito à obrigatoriedade de uso dessa ferramenta de relacionamento serão considerados, haja vista que os contribuintes são obrigados, em algumas situações, a se relacionarem exclusivamente pela Internet enquanto que em outras, facultativamente. Esta situação merece alguma atenção à medida que, nem todos os municípios brasileiros, e aí se inserem os baianos, não possuem provedores de acesso à grande rede de computadores. Destacamos ainda o fato em que boa parcela dos contribuintes não possui microcomputador, dado a sua capacidade econômica, delegando a tarefa a terceiros contratados, numa forma de repasse virtual de competência. Essa problemática será aprofundada no Capítulo VI.

Para que se chegue ao entendimento da real importância da Internet em nossos dias, no segundo capítulo faremos um levantamento histórico do seu surgimento, sob uma ótica eminentemente técnica, não aprofundada. Procura-se avaliar a utilidade e legalidade das operações efetuadas, não o seu funcionamento.

Abordaremos ainda os principais problemas pelos quais atravessa a rede mundial de computadores, no que diz respeito aos aspectos de segurança, sigilo, consistência na transmissão e armazenamento de dados, e a certificação dos usuários na rede.

No terceiro capítulo estaremos estudando o surgimento do documento eletrônico e correspondente assinatura digital, demonstrando as principais diferenças existentes em relação aos do papel.

O quarto capítulo será destinado à síntese da regulamentação da Internet em nosso país, onde listaremos os principais conceitos da legislação em vigor e os principais Projetos de Lei em andamento no Congresso Nacional. Veremos ainda alguns aspectos importantes na Lei Modelo da Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL) no que se refere ao uso desta tecnologia e suas implicações de segurança e legalidade. Ao concluí-lo, abordaremos os aspectos relacionados à validade jurídica dos documentos eletrônicos e da assinatura digital.

O capítulo seguinte é dedicado ao estudo do uso da Internet pelas Administrações Tributárias, onde destacaremos as sugestões apresentadas pelo Banco Interamericano de Desenvolvimento (BID) no sentido de que estas administrações utilizem a tecnologia da informação como forma de alavancar a arrecadação e obterem um efetivo controle sobres suas ações, utilizando para isto a Internet como solução tecnológica. Em seguida veremos o alcance do uso da Internet no Brasil nas várias esferas de governo, em especial pelas Administrações Tributárias estaduais, a partir de sugestões e análises divulgadas pela UCP/PNAFE (Unidade de Coordenação do Programa Nacional de Apoio à Administração Fiscal para os Estados Brasileiros).

Finalmente, no último capítulo analisaremos de forma minuciosa, a utilização da Internet pela SEFAZ-Ba, mostrando o histórico da sua implementação serviços oferecidos. Assim como os problemas e algumas sugestões que atenuariam os efeitos decorrentes, levando-se em consideração os mecanismos de segurança que deverão estar sujeitos os que optarem por esta forma de relacionamento.

CAPÍTULO I

A METODOLOGIA DA PESQUISA

1.1. Objetivos

Partimos do princípio de que a popularização da Internet é algo incontestável, estando muitos dos seus conceitos já absorvidos pela grande maioria da população economicamente ativa. Ela é uma das grandes ferramentas de geração de riquezas em nossa economia cada vez mais globalizada, bem como uma forma de gestão pelas mais diversas esferas governamentais, este trabalho dá um enfoque apenas crítico a esta realidade, avaliando-a, especificamente, quanto ao seu uso pelas Administrações Tributárias Estaduais, em especial pela Secretaria da Fazenda do Estado da Bahia (SEFAZ-Ba).

1.2. Objetivos Específicos

Para a realização dessa pesquisa, estabelecemos alguns pontos que precisam ser entendidos, que foram:

1. O que é a Internet.
   a) Levantamento de problemas;
   b) A normatização;
   c) A validade jurídica dos documentos eletrônicos;
2. O uso da Internet pelas Administrações Tributárias Estaduais
3. O uso da Internet pela SEFAZ-Ba

1.3. Metodologia da Pesquisa

As abordagens deste trabalho foram baseadas na legislação vigente, onde o estudo do uso da Internet pela SEFAZ-Ba deu todo o contorno ao enfoque. Para tanto, navegamos insistentemente no site da Administração Tributária baiana, procurando explorá-lo, ao máximo, no sentido de perceber os reais serviços oferecidos, comparando-os com os de outras unidades da Federação, e se estão inseridos nos modelos apresentados pelo Banco Interamericano de Desenvolvimento (BID), o maior financiador dos programas de modernização das administrações tributárias.

Foram feitas ainda entrevistas com os técnicos das Diretorias de Tributação, Diretoria de Tecnologia da Informação e Diretoria de Atendimento da SEFAZ-Ba.

A partir desses elementos e da análise do farto material produzido pela mídia, tanto impresso quanto virtual, é que foi possível chegar à elaboração do presente trabalho.

Convém destacar que este estudo foi finalizado na primeira quinzena de novembro de 2001, de modo que as referências feitas à legislação e projetos legislativos, em curso, são contemporâneas ao momento.

CAPÍTULO II

ASPECTOS TÉCNICOS DA INTERNET

2.1. A Internet

2.1.1. Conceito

Internet é o nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o "software" e os dados nele contidos.. Esta comunicação ou conexão é feita através de linhas telefônicas, cabos ou satélites, utilizando-se para tanto os chamados Provedores de Serviço de Conexão à Internet (PSCI), cujo serviço prestado constitui-se [1]:

- dos equipamentos necessários aos processos de roteamento, armazenamento e encaminhamento de informações, e dos "software" e "hardware" necessários para o provedor implementar os protocolos da Internet, gerenciar e administrar o serviço;
- das rotinas para administração de conexões à Internet (senhas, endereços e domínios Internet);
- dos "softwares" dispostos pelo PSCI - aplicativos (correio eletrônico, acesso a computadores remotos, transferência de arquivos, acesso à banco de dados, a diretórios, e a outros correlatos), mecanismos de controle e segurança, e outros;
- dos arquivos de dados, cadastros e outras informações dispostas pelo PSCI;
- do "hardware" necessário para o provedor ofertar, manter, gerenciar e administrar os "softwares" e os arquivos especificados nas letras "b", “c" e "d" deste subitem;
- outros "hardwares" e "softwares" específicos, utilizados pelo PSCI.

Além dos provedores de acesso, temos os de informação, que tem o papel de coletar, manter e organizar informações de caráter geral ou particular e disponibilizá-las para acesso através da Internet, a exemplo dos jornais, revistas, universidades, órgãos governamentais, empresas comerciais, dentre outros.

A popularização da Internet deu-se pela possibilidade de disponibilizar essa grande quantidade de informações a um custo bastante acessível. Atualmente, temos alguns provedores de acesso gratuito, ficando o usuário apenas com o custo da ligação telefônica, e

em alguns casos, nem esse custo é repassado. Através dela, também é possível fazer compras, ler livros, ouvir músicas, "assistir aulas", movimentar conta bancária, efetuar troca de e-mail e de arquivos magnéticos, só para citar os mais populares.

A Internet é também chamada de rede mundial de computadores, ou simplesmente *Web* (do inglês, teia), também significa abreviatura de World Wide Web (www – teia de alcance global), derivando assim o significado de Internet como Rede Mundial de Computadores.

A Internet é um meio de comunicação bastante complexo, conseguindo mesclar tudo o que existe nos meios convencionais, ou sejam, texto, imagem, dados de áudio e vídeo, com a possibilidade de armazenamento ilimitado de praticamente tudo o que por ela trafega.

CASTELLS (1999: 375) após refletir sobre a arquitetura de funcionamento dessa rede de computadores e a universalidade da linguagem digital, chega à conclusão de que é praticamente impossível exercer controle ou censura sobre Internet. O autor chega ao ponto de afirmar que "*o único modo de controlar a rede é não fazer parte dela, e esse é um preço alto a ser pago por qualquer instituição ou organização*".

2.1.2. Origem

A vasta bibliografia disponível sobre o assunto, informa-nos que a Internet surgiu de uma demanda militar americana, que, em meio à Guerra Fria, necessitava de uma rede de comunicação entre os principais centros militares de comando e que pudesse sobreviver a um possível ataque nuclear, interligando-os ainda aos grandes centros de pesquisa e universidades.

A primeira conexão bem sucedida ocorreu em 1969, sob a direção da ARPA (Advanced Research Projects Agency), razão pela qual na época, a Internet (inter = interligada + net= rede/malha) era conhecida como Arpanet (ARPA + net, onde NET = rede ou malha em inglês).

Até o início da década de 80, o uso da Internet estava basicamente restrito aos seus propósitos originários. Mas, com a popularização dos microcomputadores, essa tecnologia veio a se espalhar em função do baixo controle no meio acadêmico, dando oportunidade de surgimento dos primeiros provedores privados de conexão.

---

[1] Conforme Norma 004/95, baixada através da Portaria nº 148 de 31/05/1995 do Ministério das Comunicações.

O uso inicial da Internet nessa fase resumia-se à transmissão de arquivos, através de um rudimentar serviço de FTP, e correio eletrônico, porém sem a interface gráfica e amigável como temos hoje. Esta interface amigável só veio surgir por volta de 1991 em Genebra (Suíça), no Laboratório Europeu de Estudo de Partículas Físicas (Conseil Europeen pour la Recherche Nuclcleaire - CERN), que desenvolveu sistemas que viabilizavam a transmissão de imagens, som e vídeo pela rede, dentro dos atuais padrões World Wide Web.

Desde então, não houve grandes mudanças na interface gráfica da Internet, a inovação chegou com a incorporação de novas linguagens de construção e edição de páginas, e acesso interativo a bancos de dados.

Com a celeridade do aumento de novos usuários, a Internet consolida-se definitivamente. A demanda é equivalente à incorporação de novas tecnologias, que, de certa forma, barateiam o acesso à rede.

2.1.3. O surgimento da Internet no Brasil

O ponto de partida na Internet brasileira foi dado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), que para atender aos clamores de seus estudantes bolsistas que voltavam dos cursos de doutorado nos Estados Unidos, desejavam manter o mesmo nível de comunicação com colegas e instituições de ensino onde estudavam. Através do uso da Internet fizeram os primeiros contatos

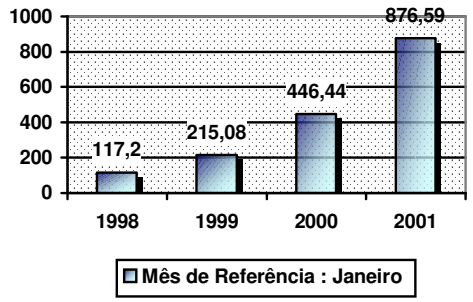
Em 1988, já se formavam no Brasil alguns embriões independentes de redes, interligando grandes universidades e centros de pesquisa de vários estados brasileiros (Rio de Janeiro, São Paulo e Porto Alegre) aos Estados Unidos. Em setembro daquele ano, surge a Rede Nacional de Pesquisa (RNP), criada sob a coordenação do Ministério da Ciência e Tecnologia, formado por representantes do CNPq, pela Financiadora de Estudos e Projetos (FINEP), e pelas Fundações de Amparo à Pesquisa dos Estado de São Paulo, Rio de Janeiro Rio Grande do Sul. O Objetivo de criação da RNP foi o de integrar esses esforços e coordenar uma iniciativa nacional em redes no âmbito acadêmico. Dessa forma, a RNP funcionou como primeira espinha dorsal (backbone) a interligar instituições educacionais[2].

[2] Conforme histórico constante no site da RNP. [Internet] http://www.rnp.br/rnp/rnp-historico.html [Capturado em 30.Nov.2001]

Porém, o grande impulso para a Internet brasileira ocorreu com a realização do mega evento Ecológico Internacional de 1992, a *ECO-92*, no Rio de Janeiro, onde o Instituto Brasileiro de Análises Sociais e Econômicas (Ibase), através de parceria com instituições ligadas à americana *Associação para o Progresso das Comunicações* (APC), instalou modernos equipamentos, tornando-se assim a primeira instituição não-governamental brasileira a conectar a incipiente rede brasileira à Internet mundial, porém apenas dentro do âmbito da chamada Rede Rio. A partir de 1995, a Embratel passou a oferecer acesso aos demais Estados brasileiros, democratizando o acesso à rede mundial, que até então, restrita ao Rio de Janeiro (Rede Rio), tinha alguns poucos usuários espalhados pelo Brasil, via BBS, os quais mantinham conexões regulares com o Ibase.

Com a criação do Comitê Gestor da Internet do Brasil em maio de 1995, a Internet encontrou o apoio que necessitava para se instalar como ferramenta, não apenas acadêmica, mas também comercial. Atualmente a Fapesp atua como braço forte do Comitê Gestor, com a competência para realizar as atividades de registro de nomes de domínio, distribuição de endereços IPs e sua manutenção na rede[3]. Como resultado, o Brasil está em 11º lugar no *ranking* mundial no número de Host, sendo que nas Américas está em posição de destaque, ocupando o terceiro lugar, após os Estados Unidos e Canadá. O Brasil tem experimentado uma ampliação significativa no número de *hosts* nos últimos anos.

Gráfico 1 - Evolução do número de host no Brasil (em mil)



Fonte : Comitê Gestor da Internet Brasil

2.2. Como funciona a Internet

Com a popularização da Internet, alguns chavões se popularizaram entre os seus usuários, popularmente chamados de "*internautas*". Entre estes, um dos mais utilizados é "estar

[3] Conforme Resolução nº 2 de 15/04/1998, do Comitê Gestor Internet do Brasil

conectado", que tem dois significados. Primeiramente, "estar conectado" significa ter uma conta aberta em um provedor de acesso; em segundo lugar, a utilização de um microcomputador, dotado de um software de discagem, que, através de um *modem* e de uma linha telefônica comum o interliga ao computador do provedor, e este, aos demais microcomputadores conectados à Internet, através dos backbones. Ter essa "conta" implica em ter um "endereço eletrônico", que funciona de forma similar ao endereço postal tradicional.

Essa conexão só é possível porque, tanto os provedores quanto os usuários utilizam os mesmos protocolos de comunicação, que nada mais são do que um conjunto de normas e regras, que funcionam como uma espécie de linguagem única entre os computadores conectados, compatibilizando a comunicação entre eles, independente dos softwares que estejam sendo utilizados. Essa capacidade de entendimento entre diversos computadores é conhecida como "capacidade de interoperabilidade" COMER (1998: 4).

Uma descrição técnica do funcionamento da Internet, a partir do conceito de protocolo é apresentada pela mestra em Direito e técnica em eletrônica Érica Barbagalo (BARBAGALO, 2001: 33 a 35):

> *Para que os computadores possam comunicar-se pela Internet, a linguagem comum utilizada é o protocolo TCP/IP. O protocolo TCP/IP é formado por dois componentes: o TCP, Transmission Control Protocol, protocolo de controle de transmissão, e o IP, Internet Protocol, protocolo Internet.*
>
> *Na Internet as informações são divididas em "pacotes" e enviadas por meios físicos de comunicação, sendo que os pacotes de vários usuários podem ser transmitidos simultaneamente, a compartilhar o meio de transmissão. Se um dos circuitos que compõem o meio de comunicação utilizado estiver inoperante ou congestionado, o pacote de informações é redirecionado a outro canal por meio do roteador. (...) Como os pacotes de informação podem trafegar por diferentes canais, cada um deles contém, além dos dados do remetente, um cabeçalho, que especifica as funções de controle e o endereço de destino. Assim, ao alcançar o destino, os pacotes são organizados na seqüência correta até que se complete a transmissão da mensagem original.*
>
> *Os provedores de acesso à internet recebem números de identificação (...) chamados de endereços IP, Internet Protocol. Para a conexão de um usuário à Internet, o provedor atribui-lhe um dos endereços de IP que dispõe. Essa atribuição de endereço de IP fica, assim, registrada nos sistemas do provedor de acesso durante todo o tempo em que o usuário permanecer conectado à rede. Esse número acompanha a trajetória que o usuário traça na rede, possibilitando ao provedor de acesso identificar o momento em que o usuário se conectou e desconectou.*

Os usuários da Internet têm acesso a uma gama de serviços, sendo que os mais difundidos são: Correio Eletrônico (e-mail); World Wide Web (WWW ou W3); FTP (File Transfer Protocol) e Telnet.

2.3. Segurança na Internet

A facilidade de uso e a grande quantidade de serviços e informações ofertadas, foram determinantes para a popularização da Internet, e, como subproduto desta massificação, vimos surgir uma variedade de problemas, dentre os quais, destacamos os relacionados à segurança dos dados que por ela trafegam.

Quando se fala de segurança na Internet logo vem à tona personagens até então inexistentes - os chamados hackers e crackers. Preliminarmente, faz-se necessário distinguir o que seja hackers e crackers, pois não são a mesma espécie de pessoas. A diferença entre eles reside na intenção de seus atos, apesar de se assemelharem aos métodos utilizados para invadirem a privacidades dos internautas. Os hackers são pessoas interessadas em testar e recondicionar qualquer tipo de sistema operacional, possuindo alto grau de conhecimento nesses sistemas e em linguagens de programação, buscando sempre mais conhecimento. Muitas vezes, compartilhando gratuitamente o que descobrem e sem terem a intenção de destruir arquivos e sistemas. Por sua vez, os crackers são indivíduos que utilizam esses mesmos conhecimentos, para comprometer a segurança da rede, incluindo, entre suas práticas, os acessos não autorizados, espionagem e danos a qualquer tipo de sistemas e base de dados. Os crackers são também conhecidos como cibercriminosos (GOMES, 2000: 19 a 31), e estão entre os principais disseminadores de vírus de computador.

Diante dessa fragilidade da rede, destacamos que os princípios básicos de segurança seriam a confidencialidade, integridade e disponibilidade de informações, redução dos riscos de vazamentos, fraudes, erros, uso indevido, sabotagens e roubo de informações. As empresas têm aderido, como fator ponderável de prioridade, a segurança de informação.

Uma das questões que mais tem movimentado o meio jurídico diz respeito à integridade das mensagens que circulam via e-mail, pois este aspecto ligado à segurança, tem feito com que uma simples mensagem enviada via e-mail não seja aceita como meio de prova, em razão da possibilidade de alteração de tais documentos sem deixar vestígios. Deve ficar claro que muitas vezes a integridade das informações trafegadas na *Web* podem sofrer modificações, não apenas por parte de agentes mal intencionados, a exemplo dos crackers. Uma simples

interferência elétrica no momento da gravação ou transmissão, pode alterar o conteúdo de documentos transmitidos (GRECO, 2000: 21 a 27).

Para se contornar essa problemática de segurança, a solução bem mais aceita atualmente é a utilização de sistemas de criptografia de chave pública, através da adoção de assinatura digital, também denominada *Public Key Infrastructure* (PKI – Infra Estrutura de Chave Pública). Esta PKI está baseada em um sistema de confiança, onde duas partes confiam mutuamente em uma *Autoridade Certificadora* (AC) para verificar e confirmar a identidade de ambas.

Atualmente é o método disponível mais confiável por oferecer proteção contra as ameaças que surgem quando do envio e armazenamento de informações, e merecerá atenção especial nos tópicos seguintes, onde traremos maiores detalhes dessa tecnologia.

2.4. Aspectos de Segurança na Transmissão de dados via Internet

Ao analisarmos os aspectos de segurança de um *site* devemos ater-nos não apenas na invasão propriamente dita, no qual os seus conteúdos podem ser modificados, destruídos, ou até mesmo acessados por pessoas não autorizadas. Sem sombra de dúvida, esse é um aspecto bastante relevante.

Nesse estudo, o nosso foco será dirigido aos aspectos que envolvem autenticação, sigilo e integridade dos usuários, por estarem intimamente ligados ao aspecto de validade dos documentos eletrônicos, assunto que estaremos abordando adiante.

2.4.1. Autenticação do usuário

A certeza quanto à identificação de quem está do outro lado da conexão, e se realmente é seguro manter um relacionamento com ele a ponto de enviarmos, ou dele obtermos informações, é um fator que não pode deixar de merecer atenção especial. Esse aspecto é crucial para todo *site* que esteja se propondo a prestar serviços, tidos como confidenciais. A identificação positiva do usuário é a única forma de garantir a privacidade e, por conseqüência direta, o sigilo.

Para sanar esses problemas, muitos *sites* possuem serviço de identificação, através do uso de senhas ou sistema de identificação com chave pública. A solução tecnológica de menor custo e mais utilizada é a adoção de senhas. Porém, não é a mais segura, haja vista a facilidade de se

obter a senha durante as operações de relacionamento, através de ações bastante sofisticadas, perpetradas por cibercriminosos, que invadem os computadores das respectivas empresas usuárias para "roubar" os arquivos de registro de senhas. Isso ocorre porque os custo para instalação de equipamentos e sistemas que protegem esses dados o tornam proibitivo para a maioria das empresas. A alternativa menos onerosa e mais segura é a utilização do sistema de certificação digital de chave pública, pois além de se autenticar o usuário e o próprio *site* acessado, a operação pode passar pelo crivo de empresas certificadoras, que têm condições de arcar com os custos de segurança.

A realidade é que apenas algumas empresas, geralmente instituições financeiras e grandes corporações e uma pequena parcela dos órgãos públicos já utilizam os serviços de certificação digital para dar garantia aos usuários. É uma garantia de mão única (uma vez que o inverso não é verdadeiro), pois nem os sites governamentais nem as instituições privadas têm a certeza de que estão se relacionando com quem se identifica. Isto só seria possível se os correspondentes, sejam eles pessoas físicas ou jurídicas, também obtivessem o seu próprio certificado digital, o que representaria um custo adicional, que os usuários nem sempre estão dispostos a arcarem.

Para entendermos a importância do uso dessa certificação ou autenticação dos usuários, faremos algumas considerações sobre essa tecnologia. Por tudo já exposto, percebemos que um dos "calcanhares de Aquiles" na Internet é saber que a pessoa com a qual você está se relacionando na Web é realmente quem ela diz ser. Como assegurar? Isso só é possível através do uso da tecnologia denominada "certificação eletrônica" ou simplesmente "autenticação" – uma espécie de serviço de reconhecimento de firma - amplamente utilizado no mundo não virtual, com a ação dos tabeliões.

Na Internet, esta certificação é feita atualmente através da intermediação de *autoridades certificadoras*, as quais, em sua maioria, são entidades privadas que utilizam tecnologia de criptografia. O uso dessa tecnologia baseia-se em quatro conceitos :

- **Não repudiação** – este recurso garante que a pessoa que utilize uma certificação digital, para, por exemplo, assinar um documento, não poderá negar sua autoria ou conteúdo enviado, sendo este o aspecto que mais guarda similaridade com a assinatura manuscrita.

- **Autenticação de remetente** - é o processo que permite a um usuário certificar-se de que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive, provar perante um juiz tal veracidade.
- **Autenticação do destinatário** - consiste em provar se a mensagem enviada foi fielmente recebida pelo destinatário.
- **Autenticação de atualidade** - consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas.

O funcionamento deste sistema de autenticação será detalhadamente abordado no Capítulo III, onde estaremos estudando o documento e assinatura eletrônica.

2.4.2. Sigilo

Sigilo ou confidencialidade na Internet é uma questão que tem sido encarada como algo relativo, apesar da sua gravidade, na medida em que terceiros podem ter acesso ao conteúdo que transita pela rede de computadores, sem que as partes comunicantes percebam. Um exemplo claro disto é a possibilidade de leitura de conteúdos pelo provedor de acesso tanto das mensagens oriundas de terceiros para seus clientes e vice-versa, sem que as partes se dêem conta do ocorrido.

Uma polêmica tem sido levantada, quanto ao sigilo previsto no inciso XII do artigo 5º da CF-88. Este sigilo abrangeria as mensagens que trafegam pela Internet, uma vez que o texto constitucional volta-se especificamente para as correspondências, comunicações telegráficas, de dados e das comunicações telefônicas? Há de se ter em mente que a intenção do legislador constitucional visa a garantia de confidencialidade na troca de informações entre as partes, e, no caso das mensagens eletrônicas, as mesmas se enquadrariam perfeitamente em qualquer categoria destas mensagens. Aliado a isto, a própria CF-88 no inciso X do mesmo artigo 5º fala da garantia da inviolabilidade da intimidade das pessoas. Então, a partir do momento em que um terceiro tem condições de acessar dados que trafegam pela *Web*, sem o consentimento ou conhecimento das partes, fica evidente a necessidade da utilização de uma solução tecnológica capaz de neutralizar esta investida.

Ocorrendo uma situação em que não se consiga evitar que os dados sejam acessados, o invasor da privacidade deverá se defrontar, então, com dados que lhe seja ininteligível. Neste aspecto, o uso da tecnologia de criptografia garante a confidencialidade das informações. Para isso, utilizam-se programas específicos, os quais, mediante o uso de senhas, permitem que apenas os destinatários das mensagens e de dados tenham acesso ao seu conteúdo.

Dessa forma, o detentor de um Certificado Digital poderá distribuir sua Chave Pública para quem desejar, sem comprometer a integridade do Certificado em si, já que manterá em boa guarda a Chave Privada. Portanto, qualquer pessoa que possua uma Chave Pública de uma outra, poderá enviar uma mensagem criptografada com a certeza de que somente o destinatário, detentor da Chave Privada, conseguirá decifrar o seu conteúdo.

2.4.3. Integridade

Vencido a barreira da autenticidade e da quebra de sigilo ou confidencialidade, adentra-se em outra seara não menos problemática: a garantia de que os dados enviados chegarão de forma íntegra ao destino, com a garantia de que não foram adulterados, nem com a inclusão, alteração ou exclusão de informações enviadas originalmente.

A corrupção de dados é possível porque, antes de chegar ao seu destino, eles trafegam por diversos nós na rede de computadores que compõe a Internet. Nesses nós (gateway) os dados podem ser capturados, correndo o risco de serem adulterados, com inclusões, modificações ou exclusão de conteúdo, e no destino, o receptor entenderá que o conteúdo foi enviado pelo remetente, sem que ambos dêem-se conta da adulteração perpetrada. Esta seria uma corrupção voluntária de dados.

Porém, existe ainda a possibilidade de uma corrupção involuntária, quando no tráfego desses dados, algum fator externo provoque a alteração do conteúdo, como por exemplo, uma oscilação na corrente elétrica ou a ação de um vírus.

O uso da tecnologia de criptografia assimétrica, associado ao uso de assinatura digital, garante não só a integridade dos dados, mas também a autenticação do emissor/receptor e o sigilo de cada pacote de dados que esteja trafegando pela Internet, conforme detalharemos no do terceiro capítulo.

2.4.4. Armazenamento

O armazenamento é outro fator de risco na Internet, pois os provedores de acesso geralmente catalogam dados dos seus clientes. Acontece que, mesmo expostos a invasores de rede os dados não correm o risco de serem danificados, mas copiados e, posteriormente acessadas as informações dos proprietários. Esse tem sido um dos maiores temores na atualidade, pois o trabalho é feito com bastante calma, sem o risco de ter o arquivo ou dados, sob exame,

excluído pelo proprietário ou administrador da rede. Até que ponto os backups de dados efetuados pelos provedores estão protegendo os proprietários de dados que podem a qualquer momento excluir um arquivo por não mais achá-lo interessante ou necessário. Em determinado momento ele poderia ser surpreendido com a divulgação de uma idéia que ele não mais sustenta, e ver-se envolvido em embaraçosas situações ou embates jurídicos. O armazenamento de informações é realmente um ponto crítico e atualmente sem solução tecnológica satisfatória. A situação se torna mais delicada quando vista sob o prisma da confidencialidade dos dados fiscais de contribuintes, armazenados pelas administrações tributárias.

As conseqüências desse ponto crítico na utilização da Internet, já estão previstas no Projeto de Lei nº 84/99 (de autoria do Deputado Luiz Piauhylino de Mello Monteiro), que, entre outras disposições, prevê sanções para os seguintes crimes: danos a dados ou programa de computador; apagar, destruir, modificar ou inutilizar os dados de forma não autorizada; acesso indevido ou não autorizado; alteração de senha ou de mecanismos de acesso; obtenção indevida ou não autorizada de dado ou instrução de computador; violação de segredo armazenado em meios eletrônicos; criação, desenvolvimento ou inserção de dados ou programa nocivo; veiculação de pornografia.

Um detalhe bastante importante é que na hora de capitular as sanções, o projeto prevê que será considerada de maior gravidade os crimes cometidos contra o poder púbico, ou que visem a obtenção de lucros.

2.5. Novas tecnologias de segurança - Biometria

Além da utilização da criptografia e assinatura eletrônica, outras tecnologias estão surgindo. São os métodos de identificação biométrica, a partir do reconhecimento de voz, da impressão digital e até a identificação pela leitura da íris.

Essas tecnologias porém, ainda não estão sendo utilizadas pelas Administrações Tributárias, em função dos altos custos com aquisição de equipamentos que teriam que ser arcados pelos contribuintes e demais interessado no relacionamento virtual via Internet.

2.5.1. Reconhecimento de voz

Esta tecnologia já está sendo utilizada para obtenção de vários serviços, em especial os acessados via telefone. Em recente matéria sobre tecnologia da informação a Gazeta Mercantil[4] menciona essa possibilidade de - através do uso de uma linha telefônica, fixa ou celular- navegar através de um novo tipo de portal, desenvolvido para facilitar e popularizar o acesso a *Web* e a bases de dados em geral. Esse portal é conhecido como *portal de voz*, cujo sistema utiliza a tecnologia de reconhecimento da fala para oferecer uma interface mais amigável com o computador. Na mesma matéria, informa que o Bradesco já está utilizando em caráter experimental na cidade de São Paulo, um serviço tecnológico denominado *Fone Fácil*, que permite ao cliente ter acesso a uma variedade de serviços.

2.5.2 Leitura de impressão digital

Recurso que consiste na adaptação de um mouse especial com microprocessador e scanner, onde o usuário deve apoiar o polegar. O scanner captura a impressão digital e o microprocessador converte a imagem em fórmula matemática, de caráter individual, ou seja, corresponde a uma única pessoa. Essa tecnologia origina-se de pesquisas desenvolvidas pela agência secreta da extinta União Soviética (KGB). No Brasil já estão sendo desenvolvidas soluções para uso no comércio eletrônico e nos Home-Banking (BRAGA, 2000).

No âmbito do judiciário, o Supremo Tribunal Federal começou a utilizar internamente, a partir de fevereiro deste ano, o reconhecimento da impressão digital para viabilizar o acesso a informações judiciais sigilosas.[5]

2.5.3 Identificação da íris

Método que consiste em um processo composto de várias etapas: localização e posição do olho; captura da imagem; processamento, codificação e gravação do padrão da íris. Esse padrão será gravado em um banco de dados, permitindo a identificação do usuário em apenas um segundo[6].

---

[4] VOZ comanda a Navegação – Reconhecimento de fala permite interface amigável com computador. Gazeta Mercantil, Caderno Tecnologia da Informação. 17/04/2001. p. 12

[5] SUPREMO Tribunal Federal coloca biometria a serviço da segurança. In : Boletim eletrônico PC World de 22/08/2001. [Internet] http://pcworld.terra.com.br/pcw/update/4522.html [Capturado em 06.Set.2001]

[6] LG anuncia novo sistema de segurança baseado na íris humana. Boletim eletrônico PC World de 10/09/2001. [Internet] http://pcworld.terra.com.br/pcw/update/4740.html [Capturado em 11.Set.2001]

A identificação da íris humana, apesar de estar sendo utilizada basicamente para identificação presencial, poderá ser armazenada em um banco de dados para utilização na Internet, através do uso de micro-câmeras adaptadas ao computador do usuário.

CAPÍTULO III

DOCUMENTO E ASSINATURA ELETRÔNICA

Vivemos em um momento da história onde os tradicionais conceitos de documento e assinaturas são colocadas à prova, quando já não mais precisamos sair de casa para, por exemplo, utilizar serviços bancários, comprar, assistir filmes, celebrar contratos ou pagar impostos, bastando para isto acessar a Internet - esta grande fomentadora das relações não presenciais. A polêmica e o debate se instalaram com o surgimento dos documentos eletrônicos, onde a assinatura – antes manuscrita – passou a ser digital. O consagrado "documento em papel" não é mais viável, e em certas situações até impossível nessa emaranhada rede de serviços.

3.1. O documento eletrônico

Faz-se necessário uma reflexão sobre os atuais conceitos a respeito dos documentos, pois como bem observou Marco Aurélio Greco, algumas diferenças "saltam aos olhos" quando comparamos os documentos pertencentes ao mundo dos átomos com os pertencentes do mundo dos *bits*. Greco faz algumas considerações sobre os conceitos de meio e mensagem, destacando três diferenças entre esses dois tipos de documentos (GRECO, 2000: 26 e 27):

> ***Primeira**: No mundo dos átomos, tendo em vista a fusão que existe entre meio e mensagem, uma alteração na mensagem deixa rastro no meio físico. É a rasura, o borrão, a diferença tipográfica etc. que torna possível submeter o objeto a um exame de autenticidade considerando a grafia, o tipo e a idade da tinta, as qualidades do papel etc. Além disso, as características do meio podem ser comparadas com as características da mensagem para aferir sua adequação. Por exemplo, a incompatibilidade entre meio (tipo de papel) e mensagem (caracteres impressos) que pode ser um modo de demonstrar tratar-se de uma moeda falsa etc. Ou então, num exemplo caricato, seria o caso de um documento que alguém diz ser do século XIX, mas que está grafado com tinta de uma caneta esferográfica.*
>
> *Por outro lado, no mundo dos bits, como o referencial é apenas a mensagem e esta corresponde àquela imensa série de zeros e uns, a reprodução, com exatidão, da seqüência de bits conduz à reprodução do mesmo resultado final. Bits são bits. Não há bits falsos. Impulsos elétricos são meros impulsos elétricos. Quem conseguir copiar aquela determinada seqüência de bits fará uma cópia exatamente igual ao produto original.*
>
> ***Segunda**: Esta característica é particularmente importante em se tratando da autenticidade dos documentos eletrônicos e operações realizadas por meio de computadores. No mundo dos átomos é possível realizar uma comparação estática da*

> *mensagem superposta ao meio físico, para aferir sua autenticidade. Assim, é possível examinar as assinaturas, reconhecer firmas, examinar o tipo de tinta, o papel utilizado etc.*
>
> *No mundo dos bits, como a entidade é formada por simples dígitos binários e como a reprodução da mesma seqüência de bits implica obter exatamente o mesmo resultado, sem possibilidade de distinguir o verdadeiro do falso, a comparação não pode ser estática (o produto em si), mas deve ser dinâmica, no sentido de que o exame da autenticidade ou falsidade é feito em função da analise do processo de produção do documento ou de emissão da mensagem (horário, local do emissor, tempo de emissão, tamanho do arquivo, data em que foi criado etc.). Ou seja, não basta ter acesso ao resultado final; é preciso conhecer seu processo de produção.*
>
> ***Terceira**: A terceira característica está ligada à transmissão do documento ao destinatário. No mundo dos átomos a transmissão ao destinatário se dá pelo transporte físico; é a entrega pessoal, o correio etc. No mundo dos bits, como o documento é formado pelo (ou a partir do) conjunto de dígitos, seu transporte pode se dar por inúmeros meios físicos como a linha telefônica, a fibra óptica e outros que os avanços da tecnologia podem vir a desenvolver.*
>
> *Como se verifica, há profundas diferenças entre as características do mundo dos átomos cotejado com o mundo dos bits. Imensos são os reflexos na criação de novas entidades, bem como na conformação de entidades tradicionalmente conhecidas no dia a dia.*

O documento eletrônico não se encaixa nos tradicionais conceitos de documento, em especial no seu aspecto material (meio). Porém, por ter em si a capacidade de registrar um fato (mensagem), pode ser entendido como tal, pois o seu conteúdo pode ser facilmente revelado através do uso de softwares específicos, trazendo a lume a expressão da vontade de quem o criou. Entre os mais populares documentos eletrônicos destacamos as mensagens de correio eletrônico (*e-mail*), porém, temos uma grande variedade de transações eletrônicas produzindo documentos virtuais.

Como vimos até aqui, a questão que até então tem sido levantada reside no fato de que em todo nosso ordenamento jurídico, antes do advento da Internet, quando se mencionava "documento", deduzia-se algo concreto, geralmente em papel. E quando se falava em "assinatura" referia-se a uma marca manual grafada no papel. Isto mudou sistematicamente com o advento da Internet.

A validade jurídica dos documentos eletrônicos será assunto abordado no tópico 4.3 de forma mais aprofundada.

3.2. A assinatura digital

O documento eletrônico pode ser estudado com referência aos aspectos ligados à sua integridade, autenticidade e autoria, conforme foi abordado no capítulo anterior, pois como qualquer outro, ele está passível de ser assinado, autenticado e ter sua firma reconhecida, como no mundo dos átomos.

Primeiramente, vale mencionar que "assinatura" é uma marca individual feita com finalidades declarativa - identifica o autor; declaratória - afirma a autoria do conteúdo do documento pela pessoa nela identificada; e probatória - garante a autenticidade do documento (QUEIRÓZ, 2000: p.398). Estas finalidades trazem por sua vez outros significados muito importantes: intenção (compromisso com o texto); afirmação (transação consumada); evidência (vinculação do signatário ao documento); e cerimônia (significado e conseqüências legais). Assim, aposto uma assinatura em um documento qualquer, este se reveste da natureza de prova documental, cuja autenticidade, para que produza os devidos efeitos legais, será reconhecida por ato de um tabelião que declarará que a mesma confere com outra escrita em sua presença (art. 369 do CPC, e art. 7º, inciso IV da Lei nº 8.935/94).

Quando uma assinatura é aposta fisicamente em um documento, autograficamente, tem-se garantido naquele momento a perenidade e a integridade do conteúdo, pois estão ligados ao papel de uma maneira praticamente indissolúvel e relativamente difícil de fraudar (QUEIRÓZ, 2000: p.399).

A assinatura eletrônica, ou simplesmente assinatura digital, é um método que se propõe a garantir que determinada mensagem não será alterada durante o seu trajeto de transmissão ao destinatário, bem como identificar seu autor.

Uma assinatura eletrônica se equivaleria a uma assinatura escrita autograficamente? No entendimento do mestre Régis Queiroz, "para que um sistema de assinatura digital tenha a mesma força que a assinatura autográfica é preciso que, à sua maneira, ele também preencha os requisitos que garantam a identidade, a integridade e a perenidade do conteúdo" (QUEIRÓZ, 2000: p.399). Dentro desta linha de raciocínio, para MARCACINI (1998), a partir do momento em que a evolução da informática possibilitou o surgimento da "assinatura eletrônica", que permite ao seu usuário gerar um sinal distintivo único e exclusivo, o Direito não lhe poderá negar o mesmo significado e eficácia jurídica atribuída a uma assinatura manual.

É consenso entre os especialistas na área de segurança digital que a melhor maneira de se atingir segurança na utilização de assinaturas digitais é fazer uso da certificação digital baseado em criptografia assimétrica, onde se utiliza um par de chaves - sendo uma pública e outra privada. A chave pública é colocada disponível para uso de qualquer pessoa, e se destina descriptografar informações e confirmar a veracidade das assinaturas digitais agregadas no final do documento e mensagem de correio eletrônico, ou para criptografar informações destinadas ao titular da respectiva chave. Por outro lado, a chave privada ou privativa deverá ser mantida em segredo por seu titular, para criar a sua assinatura digital.

O funcionamento da assinatura digital ocorre através dos algoritmos de autenticação, ou seja, efetua-se um processo lógico-matemático sobre a mensagem, levantando-se assim uma determinada expressão que será utilizada como assinatura. A mensagem é acompanhada de uma assinatura digital, que é baseada na chave privada do remetente em conjunto com o próprio conteúdo da mensagem. Ao chegar ao destino, a assinatura é verificada, utilizando-se uma chave pública que pertence ao remetente. Caso se confirme a assinatura digital do remetente a mensagem é considerada autêntica, bem como a integridade da mesma. O receptor da mensagem poderá enviar, em retorno, uma mensagem cifrada com a chave pública do remetente que, com sua chave privada, conseguirá verificar ou mesmo decifrar o conteúdo sem a menor dificuldade (VOLPI, 2001: 37). (vide Apêndice – Funcionamento do sistema de assinatura digital baseado em criptografia assimétrica)

A segurança no uso de Certificados Digitais está intimamente relacionada com o sigilo que o detentor da Chave Privada mantém em relação a sua senha. Caso alguém tenha acesso ao Certificado Digital de uma pessoa, não poderá utilizá-la, a menos que saiba a senha de acesso. Sendo assim, a manutenção de uma Chave Privada em um computador, sem que a mesma esteja devidamente protegida por uma senha, equivaleria em deixar em uma gaveta sem chave um talonário de cheques assinados em branco.

3.3. A produção de documentos eletrônicos e o uso de assinatura digital no Brasil

No Brasil, já é comum a utilização de senhas em alguns setores da economia. Dentre os maiores usuários destacamos as instituições bancárias que disponibilizam para seus clientes os caixas eletrônicos (através do uso de cartões magnéticos combinado com o uso de senha) ou

serviços via Internet (simplesmente através da combinação de senhas), onde se suprimiu o uso do cheque e demais documentos de débito/crédito e, por conseguinte a assinatura manuscrita.

Recentemente, o Banco do Brasil configurou-se como a primeira instituição financeira da América Latina a adotar os serviços de certificação digital nas operações com seus correntistas pela Internet, distribuindo gratuitamente entre seus correntista certificados digitais. O projeto do banco abrange desde a Internet e home-banking até o correio eletrônico da instituição financeira, adquirindo cerca de 800 mil certificados digitais para distribuição entre correntistas e funcionários[7].

Por outro lado, o setor público está também entre os maiores usuários do meio eletrônico para se relacionar com a sociedade. Nos capítulos seguintes estaremos abordando os aspectos relacionados à validade jurídica da assinatura eletrônica no Brasil, e o uso da Internet como meio de relacionamento entre as administrações tributárias estaduais e os contribuintes.

[7] Certificação Digital protege clientes do BB. Gazeta Mercantil, Caderno Tecnologia da Informação. 17/04/2001. p. 03

CAPÍTULO IV

VALIDADE JURÍDICA DOS DOCUMENTOS E ASSINATURAS ELETRÔNICAS

O ordenamento jurídico precisa contar neste momento de transição – do documento físico para o virtual – com uma legislação que consolide esta nova forma de relacionamento, sem abrir mão dos pressupostos de segurança, autenticidade, integridade e confidencialidade. Um dos grandes problemas é a morosidade do legislativo, que tem atrasado a votação dos vários projetos que versam sobre a matéria. O poder executivo, procurando agilizar esse processo, baixou uma Medida Provisória sobre o assunto, já que o governo é um dos grandes usuários da Internet e por conseqüência, o grande gerador e receptor de documentos eletrônicos.

4.1. Regulamentação da Internet

4.1.1. Legislação em vigor

O marco inicial da regulamentação da Internet brasileira ocorreu em 31 de maio de 1995 com a edição de duas Portarias Interministeriais, do Ministério da Ciência e Tecnologia (MCT) e Ministério das comunicações (MC):

> **Portaria MCT/MC nº 147/95** - Criou o Comitê Gestor INTERNET do Brasil, que tem entre outras, as seguintes atribuições:
>
> - acompanhar o provimento de serviços Internet no país;
> - recomendar padrões, procedimentos técnicos e operacionais e código de ética de uso, para todos os serviços Internet no Brasil;
> - coordenar a atribuição de endereços IP (*Internet Protocol*) e o registro de nomes de domínio
> - coletar, organizar e disseminar informações sobre o serviço Internet no Brasil
>
> **Portaria MC nº 148/95 -** Esta portaria veio a regulamentar os aspectos técnicos, com a instituição da Norma nº 004/95, que trata do uso de meios da rede pública de telecomunicações para acesso à Internet.

Procurando viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira, foi instituído através do Decreto nº 3.295 de 15/12/1999 o Programa Sociedade da

Informação (SocInfo), sob a responsabilidade do MCT. Através desse programa, o Governo Federal pretende integrar, coordenar e fomentar ações para a utilização de tecnologias de informação e comunicação, de forma a contribuir para que a economia do país tenha condições de competir no mercado global e, ao mesmo tempo, contribuir para a inclusão social de todos os brasileiros na nova sociedade. Estão previstos investimentos na ordem de R$ 3,4 bilhões até 2003.[8] Para a implementação do Programa SocInfo, foi disponibilizado, desde setembro de 2000, no site do referido programa, o *Livro Verde*, documento que contém as metas e conjunto de ações do Governo a serem observadas na sua implementação, constituindo-se em uma súmula de possíveis aplicações de Tecnologias da Informação, trazendo ainda a descrição do conjunto de ações a serem adotadas.[9]

Para estabelecer a Política de Segurança da Informação nos Órgãos e entidades da Administração Pública Federal, foi editado o Decreto nº 3.505 de 13 de junho de 2000, cujos principais objetivos destacamos:

- Dotar os Órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais, que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;
- Eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;
- Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação.

Atropelando os projetos de Lei em andamento no Congresso Nacional, foi editada em 28/06/2001 a Medida Provisória nº 2.200, instituindo a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), tendo sido reeditada duas vezes, por ter encontrado uma grande reação da sociedade através da OAB e também do próprio legislativo que percebeu alguns equívocos na primeira edição. Com essas reedições, o Executivo mostrou estar desprovido de argumentos que justificassem a urgência na edição dessa Medida Provisória, afirmando que o caminho a ser seguido teria sido a ampla discussão dos projetos já em tramitação no Congresso Nacional.

---

[8] BRASIL – Ministério da Ciência e tecnologia - Programa Sociedade da Informação. [Internet] http://www.socinfo.org.br [Capturado em 20.Abr.2001]

[9] BRASIL, Ministério da Ciência e Tecnologia – Livro Verde. [Internet] http://www.socinfo.org.br/livro_verde [Capturado em 26.Abr.2001]

A Medida Provisória, em sua edição original, entrava em conflito com alguns pontos dos principais projetos de Lei em andamento no Congresso, pois vinculava a validade jurídica do documento eletrônico no credenciamento das empresas certificadoras a um órgão governamental - o que poderia criar um grande cartório eletrônico. Outro ponto polêmico previsto na redação original, porém retirada na primeira reedição, foi o poder que o gestor da ICP-Brasil teria para emitir, expedir, distribuir, revogar e gerenciar os certificados, com total acesso, não somente às chaves públicas, mas também às privadas. Com esse amplo acesso o Governo teria condições de não só assinar documentos em nome dos cidadãos, como ter também acesso a qualquer conteúdo sigiloso de mensagens trocadas entre qualquer cidadão ou empresa.

A segunda reedição desta Medida, ocorrida em 24/08/2001, trouxe, como principal alteração a transformação do Instituto de Tecnologia da Informação (ITI) em uma Autarquia Federal, vinculada ao Ministério da Ciência e Tecnologia, que passa a desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz) da ICP-Brasil. Já existe a possibilidade desta Medida Provisória sofrer mais uma reedição, a fim de transferir a competência do ITI para o Serpro, já que esta autarquia é que atualmente dispõe de infra-estrutura física e tecnológica necessária para exercer as funções de AC-Raiz.

A premissa básica da MP 2.200/01 estabelece que as certificações realizadas por entidades não vinculadas à ICP-Brasil poderão continuar sendo feitas. Nessa condição, ao certificar determinado documento, as entidades o atestam quanto à sua autenticidade e integridade, de modo semelhante a uma testemunha. Porém, se forem efetuadas por entidade certificadora vinculada ao sistema ICP-Brasil, os documentos por ela certificados gozarão de uma presunção de autenticidade derivada da lei. Desta forma, as operações e transações feitas com ou sem certificação, efetuada por entidades certificadoras não vinculadas, mantém a validade relativa que lhes é garantida nos respectivos contratos e nas leis civis e comerciais do país e continuarão a tê-la[10].

Além da regulamentação, faz-se necessário que as empresas de software façam os devidos ajustes, através da inserção da chave-raiz da ICP-Brasil em seus produtos, como por exemplo, os sistemas operacionais, navegadores, programas de correio eletrônico, entre outros. Os especialistas de empresas certificadoras privadas avaliam que este novo modelo de

---

[10] Instalação pelo governo da Infra-Estrura de chaves públicas brasileira. In: Presidência da República. [Internet] http://www.planalto.gov.br/ccivil_03/revista/Rev_26/notícia.htm [Capturado em 29.Nov.2001]

certificação digital demandará, pelo menos, três anos para ser absorvido pelas grandes empresas de software[11]. Sendo assim, para entenderem o par de chaves criptográficas assimétricas da IPC-Brasil, os softwares de navegação na Internet e os programa de correio eletrônico deverão ser adaptados para interagir com estas novas chaves. É uma barreira tecnológica a ser vencida.

Desta forma, através do Decreto nº 3.996 de 31/10/2001, o governo deixou claro que, para prestar serviços de certificação digital no âmbito da Administração Pública Federal, as empresas privadas deverão estar de conformidade com os padrões adotados pela ICP-Brasil, determinando ainda que, a tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais, far-se-á mediante certificação disponibilizada por Autoridade Certificadora integrante da ICP-Brasil.

No último dia 30 de novembro, foi gerado o par de chaves criptográficas assimétricas e o respectivo certificado digital da Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas do Brasil (AC Raiz da ICP-Brasil), nas instalações do SERPRO, no Rio de Janeiro, em sala cofre destinada, exclusivamente, a este evento. A partir de então, a AC Raiz da ICP-Brasil poderá emitir certificados para Autoridades Certificadoras (AC) que desejarem integrar à ICP-Brasil[12].

Uma lista completa e atualizada contendo toda a legislação relacionada, não apenas com a Internet, mas com tudo o que diz respeito à informática e automação, pode ser encontrada no site do Ministério da Ciência e Tecnologia (http://www.mct.gov.br/legis/info.htm) , inclusive com acesso à íntegra de cada texto legal (Medidas Provisórias; Leis; Decretos; Portarias Ministeriais; Portarias; Outros Atos e Pareceres).

4.1.2. Projetos de regulamentação em tramitação no Congresso Nacional

Podemos observar que o Brasil começa a construir um regime jurídico capaz de proteger os usuários e instituições interligadas à essa poderosa rede de informações.

---

[11] Microsoft já discute integração da ICP-Brasil. Boletim eletrônico PCWORLD de 01/11/2001. [Internet] http://pcworld.terra.com.br/pcw/update/5312.html [Capturado em 06.Nov.2001]

[12] Gerado Certificado da AC Raiz da ICP-Brasil. In: Site Oficial da ICP-Brasil [Internet] http://www.icpbrasil.gov.br/certificado.htm [Capturado em 02/12/2001]

No Congresso Nacional encontram-se em tramitação vários projetos voltados, não só para a regulamentação da Internet, mais principalmente para a segurança das relações levadas a efeitos, via utilização da *Web*.

O principal Projeto de Lei em tramitação é o PLC nº 4.906/01 de autoria do deputado Júlio Semeghini, o qual é um substitutivo ao PLC nº 1.483/99 (de autoria do Deputado Dr. Hélio). Este último incorporava dois outros PL, ou seja, PLC nº 1.589/99 (de autoria do Deputado Luciano Pizzato) e PLS nº 672/99, apresentado pelo Senador Lúcio Alcantara.

Este Projeto de Lei nº 4.906/01, conforme dito acima, é um novo substitutivo apresentado pelo deputado Júlio Semeghini, ao PLC nº 1.589/99, e dispõe sobre o valor probante do documento eletrônico e da assinatura digital; regula a certificação digital; institui normas para as transações de comércio eletrônico e dá outras providências. O projeto já foi aprovado em 26/09/2001 pela Comissão Especial do Comércio Eletrônico, trazendo basicamente as linhas mestras constantes no projeto anterior.

Os pontos discordantes em relação ao constante na Medida Provisória que instituiu a ICP-Brasil, são os seguintes:

- As empresas certificadoras privadas não são obrigadas a submeter-se a ICP-Brasil para obter a validade jurídica dos documentos por ela certificados;
- Cria a possibilidade de que outras Autoridades Certificadoras Raiz possam atuar no mercado. Na Medida Provisória esta função é privativa de uma autarquia Federal.

O que ainda permanece uma incógnita é o futuro da MP nº 2.200/01 caso o PLC Nº 4.906/01 venha a ser aprovado nos dois plenários do Congresso, já que estes dois pontos são divergentes em relação à Medida Provisória.

Uma coisa é certa. Não há mais dúvidas de que existe uma cultura favorável nas três esferas de governo quanto a utilização de assinatura digital, via autoridades certificadoras, no sentido de dar validade jurídica aos documentos eletrônicos.

4.2. A Lei Modelo da UNCITRAL

A Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL) elaborou um modelo de Anteprojeto de Lei sobre Regulamentação do Comércio Eletrônico. O objetivo é servir de referencial aos países-membros da ONU, e nela se buscou a possibilidade

de tornar-se uniforme a legislação internacional sobre o comércio eletrônico. Este modelo foi aprovado em Assembléia Geral de 16/12/1996, através da Resolução nº 51/162. Ao anteprojeto foi anexado um Guia para incorporação da Lei Modelo ao direito interno de cada país, oferecendo, dentre outras orientações ao legislador, um conjunto de regras aceitáveis no âmbito internacional.

A principal linha dessa diretiva é que ela foi elaborada dentro do princípio da neutralidade tecnológica, onde a lei interna de cada país deve ultrapassar qualquer conceito tecnológico em voga.

No Brasil os Projetos de Lei em tramitação no Congresso Nacional já trazem os conceitos desse modelo da UNCITRAL

4.3. Documentos eletrônicos produzidos na Internet e sua validade jurídica

Antes de adentrarmos na questão da validade jurídica dos documentos eletrônicos, analisaremos a definição legal e doutrinária sobre "documento" e sua importância para o mundo jurídico.

O Código Civil (art. 136, III) assinala que documento público ou particular é todo aquele que faz prova de um ato jurídico qualquer. Depreende-se dessa norma baseado na doutrina, que "documento é a coisa que representa um fato", e que uma vez conservado, poderá ser utilizado para comprová-lo no futuro.

Esse entendimento já é consagrado através de Moacyr Amaral dos Santos, quando, nos ensina que a palavra documento é de origem latina – *documentum* – cuja raiz é o verbo "doceo", que significa ensinar, mostrar, indicar; portanto é, a idéia de que "documento" expressa a natureza de "representatividade" de um fato, associado à idéia de "prova", quando nos voltamos ao estudo dos processos.

Para o mestre Moacyr Amaral, quando analisado sob a ótica de "prova", documento "*é a coisa representativa de um fato e destinada a fixá-lo de modo permanente e idôneo, reproduzindo-o em juízo*" (SANTOS, 1977: p. 338). Discorrendo sobre o verbete "documento", De Plácido e Silva expõe que "*...documento é uma representação material destinada a reproduzir, com idoneidade, uma certa manifestação do pensamento, como se fora uma voz fixada permanentemente no papel escrito, que o indica. É, pois, a prova*

material e literal da relação jurídica instituída entre duas ou mais pessoas decorrente de convenção ou contrato." (SILVA, 1999). O Professor Paulo de Barros Carvalho acrescenta ainda que é indispensável para um documento ser eficaz como meio de prova, estar "*subscrito pelo autor, além do que, naturalmente, assuma foros de autenticidade*" (CARVALHO, 1998: p.109)

Partindo-se então para documento como algo inerente à prova forense, ressaltamos que o Código de Processo Civil preceitua em seu art. 332 que todos os meios legais, bem como os moralmente legítimos, ainda que nele não especificados, são hábeis para provar a verdade dos fatos. Daí surge a necessidade de qualificar os documentos eletrônicos como uma dessas possibilidades de prova, já que eles trazem em si, os mesmos elementos da prova pertencente ao mundo dos átomos, como bem definiu GRECO (vide tópico 3.1 deste estudo).

Feitas essas considerações iniciais sobre a natureza jurídica dos documentos, podemos então definir que documento eletrônico é todo aquele elaborado mediante processamento eletrônico de dados, podendo ser expresso através de texto, imagem ou som, representado por um arquivo magnético, cujo objetivo será também representar um fato, podendo ser utilizado como prova forense.

Diante disso, alguns aspectos devem ser considerados para avaliar se determinado documento eletrônico pode ser aceito ou não como prova de um fato.

A partir do momento em que o uso de criptografia assimétrica aliada à assinatura digital permite que um determinado documento eletrônico permaneça inalterável desde a sua criação e a ele possamos atribuir autoria, então podemos caracteriza-lo como válido para o mundo jurídico.

MARCACINI (1998) apresenta algumas considerações bastante interessantes sobre certas características peculiares aos documentos eletrônicos:

> *Se documento, em sentido lato, é o registro de um fato, o documento físico é o registro de um fato inscrito em meio físico e a ele inseparavelmente ligado.*
>
> *Já o documento eletrônico, como dito acima, não se prende ao meio físico em que está gravado, possuindo autonomia em relação a ele. O documento eletrônico é, então, uma seqüência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de um fato. Da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito,*

> *como também pode ser um desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato e que esteja armazenado em um arquivo digital.*
>
> *Dado o fato de que o documento eletrônico pode ser copiado infinitas vezes, mantendo-se exatamente igual à matriz, é impossível falar-se em original e cópia, ou em número de vias do documento eletrônico. Toda "cópia" do documento eletrônico terá sempre as mesmas características do "original" e, por isso, deve ser assim considerada. É o caso de dizermos que não existe um original e não existem cópias nem vias do documento eletrônico, enquanto ele for mantido nesta forma.*
>
> *Se pensarmos, porém, que um documento eletrônico pode ser reproduzido em meio físico, e vice-versa, neste caso é possível falar-se em original e cópia. (...) Neste caso, o papel é a cópia e o arquivo eletrônico com assinatura criptográfica é o original.*

Para melhor entendimento das particularidades que envolvem o documento e a assinatura digital elaboramos o demonstrativo a seguir, fazendo a comparação com o documento e a assinatura manual:

Tabela 1 – Comparativo entre o Documento/Assinatura Digital x Manual

DOCUMENTO/ASSINATURA DIGITAL	DOCUMENTO/ASSINATURA MANUAL
Por ser resultante de um processo de criptografia assimétrica, cada assinatura é única. O que implica em seqüência de bits diferentes para cada assinatura aposta em um documento eletrônico.	Devem ser sempre iguais, pois representam a exata marca gráfica do seu titular. Dessa forma, o titular repetirá, ou melhor, grafará sempre da mesma forma em cada documento que assinar.
A regulamentação para os serviços de validação de assinatura eletrônica ainda está incipiente. Os atuais serviços são utilizados de forma privada, sem a devida fé pública.	Já existe uma sólida regulamentação para os serviços notariais de reconhecimento de firma, dando a eles a devida fé pública (art. 236 CF e Lei nº 8.935/94).
Gravada e armazenada em arquivo magnético.	Manuscrita, ou autográfica.
Podem ser facilmente duplicados, ficando impossível aplicar os consagrados conceitos de original e cópia. As cópias de qualquer documento/assinatura digital são arquivos magnéticos, apresentando, portanto a mesma seqüência de bits.	Documentos em papel são assinados à caneta, e sua reprodução (fotocópia, fax, etc.) não dá à cópia a mesma essência, mas poderá a ela ser atribuído uma autenticação de que confere com o original apresentado (art. 6º da Lei nº 8.935/94).
É transferível, podendo ser de alguma forma utilizada por outrem, já que para assinar basta apenas conhecer as senhas relacionadas à chave privada. Caso o titular faça conhecer a terceiros sua chave privada, a assinatura gerada a partir de então será atribuída a ele próprio.	É intransferível, não pode ser grafada por terceiros, pois através de perícias grafotécnicas é possível determinar se foi assinada ou não por seu titular.
Para que uma pessoa assine em seu nome, o titular fornecerá a senha vinculada a sua chave privada. Não há limite para o uso dessa chave por terceiros; uma vez revelada	Para assinar em nome de uma pessoa, o terceiro necessita de uma procuração em papel, devidamente registrada em cartório, sendo que nela deve constar os limites da

a senha da chave privada, é impossível determinar se determinada assinatura digital foi aposta pelo titular ou por terceiros.	representatividade que lhe é atribuída. É possível saber que determinado ato foi praticado pelo procurador.
Impessoal - A chave pública é fornecida por terceiro (Autoridade Certificadora). É esta combinação de seqüências matemáticas que irá identificar que a assinatura foi feita pelo titular. Não cabe ao titular da chave determinar que forma terá a sua assinatura digital.	Pessoal - Sua forma é determinada pela manifestação do intelecto do titular que a grafa no papel com algo que lhe é inerente. A marca representativa da assinatura é criada pelo titular sem a ingerência de terceiros.

Como a tecnologia disponível permite que determinado documento eletrônico seja autenticado, ou melhor, certificado digitalmente, podemos concluir que não há nenhum óbice para aceitarmos como prova admissíveis quaisquer documentos eletrônicos, desde que acompanhado da correspondente certificação digital.

A Certificação Digital, oferecida atualmente pelas empresas especializadas, já atende aos requisitos previstos nos projetos de Lei em andamento, bem como na MP nº 2.2200.

Na situação atual, caso as administrações tributárias venham adotar o uso de entidades certificadoras privadas nas suas relações com os contribuintes estará, apenas produzindo provas de eficácia restrita ao âmbito administrativo.

Sendo assim, as administrações tributárias devem buscar, no âmbito estadual, a convalidação do uso da Certificação Digital, a exemplo do Governo Federal, que recentemente editou o Decreto n.º 3.996/2001, conforme já comentado no tópico 4.1.1.

CAPÍTULO V

O USO DA INTERNET PELAS ADMINISTRAÇÕES TRIBUTÁRIAS

A Internet vem demonstrando que é a tecnologia que oferece melhores condições para aperfeiçoar a relação fisco-contribuinte, uma vez que permite a obtenção de informações de maneira confiável, rápida, com baixo custo, podendo ser estendido este relacionamento aos contadores e instituições financeiras, estas últimas no sentido de otimizar o sistema de arrecadação.

No âmbito Federal, o uso intensivo que se faz da Internet, pode ser observado através do site Rede Governo (http://www.redegoverno.gov.br/), que funciona como um mega portal que facilita a busca e acesso a mais de 4.200 sites de órgão federais, através de mais 11 mil links, disponibilizando, através de 30 grandes grupos temáticos. (FERNANDES e AFONSO, 2001: p.41). O Portal da Rede Governo reúne mais de 1.400 serviços, representando 72% de todos os prestados pelo Governo Federal: 49% são informativos e apenas 19% possuem interatividade[13].

Já na esfera municipal os serviços têm se mostrados mais tímidos no que diz respeito à quantidade de sites em relação à quantidade total de municípios. Em levantamento efetuado por técnicos do BNDES, apenas 358 municípios brasileiros, com mais de 200 mil habitantes, oferecendo alguma espécie de serviços e informações, porém poucos prestam serviços em tempo real (FERNANDES e AFONSO, 2001: p.49).

O nosso enfoque é sobre o uso da Internet pelas administrações tributárias estaduais. O ponto de partida para este estudo foi os principais documentos produzidos pelo BID e pelos técnicos do PNAFE (Programa Nacional de Apoio à Administração Fiscal para os Estados Brasileiros).

5.1. O Uso da Internet pelas Administrações Tributárias Estaduais Brasileiras – Modelo BID /PNAFE

Com o objetivo de viabilizar a modernização das administrações fiscais do Distrito Federal e demais Estados brasileiros, em seus aspectos de gestão tributária e financeira, o BID aprovou

[13] **E-Gov economizou R$ 500 milhões em um ano** – Boletim Eletrônico Computerworld de 30/10/2001. [Internet] http://www.computerworld.com.br/templ_textos/noticias.asp?id=15762 [Capturado em 30.Nov.2001]

em dezembro de 1996 um empréstimo de US$ 500 milhões. Foi então criado o PNAFE, cuja supervisão, integração e coordenação são exercidas pela Secretaria Executiva do Ministério da Fazenda, através da Unidade de Coordenação do PNAFE (UCP)[14]. O objetivo do PNAFE é assegurar o fortalecimento e modernização das administrações fiscais dos Estados e Distrito Federal, de forma que assumam, em definitivo, a parcela que lhes cabe de instrumentos da eficácia do Sistema Fiscal brasileiro, assegurando, por outro lado racionalidade e transparência no manejo dos recursos públicos por parte dos Estados e Distrito Federal.

Para auxiliar as administrações tributárias estaduais a UCP/PNAFE e o BID têm divulgado vários documentos e notas técnicas, no sentido de subsidiar as estratégias de ação na implementação de soluções nas áreas tributária e fiscal. Os principais trabalhos voltados para a administração tributária serão abordados a seguir.

5.1.1. Atendimento ao Contribuinte e o Cumprimento Voluntário das Obrigações Tributárias - Junho/1998 [15]

Quando as administrações tributárias fazem uso adequado de tecnologias para se relacionarem com os contribuintes, especificamente através do uso da Internet, acabam por criar uma predisposição ao cumprimento voluntário de suas obrigações.

São apresentadas ferramentas que podem ser utilizadas para servir de veículo na oferta de serviços aos contribuintes, sendo mencionados os quiosques eletrônicos, resposta audível (Voice Response/Call Center), auto-atendimento, correio, fax, postos avançados, central de atendimento telefônico e Internet.

Para exemplificar o uso da Internet, o documento apresenta o caso da Secretaria da Receita Federal (SRF), que criou o seu site em outubro/1996. Em 1999 foram disponibilizados para download os programas de IRPF e IRPJ, sendo que, naquele mesmo ano, 500 mil declarações foram entregues via Internet, sendo já disponibilizadas ainda a consulta às restituições.

---

[14] Conforme site da UCP/PNAFE. [Internet] http://www.fazenda.gov.br/ucp/pnafe/ [Capturado em 16.Nov.2001]

[15] GUSMÃO, Bráulio. **Atendimento ao Contribuinte e o Cumprimento Voluntário das Obrigações Tributárias.** Brasília: UCP/PNAFE, 1998. [Internet] http://www.esaf.fazenda.gov.br/cst/arquivos/atend-01.doc [Capturado em 16.Nov.2001]

Esse caso da SRF é típico do sucesso da Internet pelas administrações tributárias, pois, de acordo com o secretário da SRF, Everardo Maciel, 92% dos contribuintes do IR já entregam suas declarações via Internet no ano de 2001.[16]

5.1.2. Modelo de Prestação de Serviços aos Contribuintes por meio de Internet - abril/1999 [17]

Neste modelo, a Internet é apresentada como a tecnologia que oferece melhores perspectivas para melhorar o processo da gestão tributária, com a possibilidade de revolucionar duas áreas críticas para uma Administração Tributária eficaz: a obtenção de informação tributária confiável e o melhor relacionamento com o seu cliente, o contribuinte. O objetivo é oferecer às Unidades da Federação, uma referência para a elaboração dos seus próprios modelos. O documento apresenta ainda um Marco de Referência para sites de administrações tributárias na *Web*, no que diz respeito aos serviços a serem oferecidos.

Esse Marco de Referência tem o objetivo de servir de parâmetro para as administrações tributárias em relação aos avanços na implementação de serviços. Para tanto, é proposta uma classificação em quatro níveis: presença, prospecção, integração e transformação.

- **Presença** – Neste estágio ficará os sites que apenas disponibilizem informações meramente institucionais, podendo nesse nível serem disponibilizados textos legais, sem mecanismos de buscas textuais;
- **Prospecção** – Além dos serviços disponibilizados no estágio anterior, são acrescentados os serviços em que o visitante possa interagir com a administração, porém, sem o uso de senhas. É possível efetuar buscas textuais, inclusive na base de dados de legislação;
- **Integração** – Neste estágio o usuário poderá dispor de uma interação maior, efetuando a entrega de declarações, obtendo arquivos de programas para download, e acessar dados confidenciais através do uso de senhas.
- **Transformação** – Para estar classificada neste estágio, as Administrações Tributárias deverão ter passado por uma reestruturação, tanto na área de tecnologia quanto nos seus processos. A característica dos serviços e informações disponibilizadas está intimamente relacionada com a interação que a Administração terá com outras instituições (Juntas Comerciais; Receita Federal; Conselhos Regionais de Contabilidade, dentre outros).

---

[16] Internet tem aprovação quase total dos contribuintes brasileiros. Boletim eletrônico PCWorld, 01/10/2001. [Internet] http://pcworld.terra.com.br/pcw/update/4980.html [Capturado em 02.Out.2001]

[17] FERREIRA, Antonio Sergio Seco. **Modelo de Prestação de Serviços aos Contribuintes por meio da Internet.** Brasília: UCP/PNAFE, 1999. [Internet] http://www.esaf.fazenda.gov.br/cst/arquivos/Modelo-Serviços-Internet-V1.pdf [Capturado em 16/11/2001]

Figura 1 – Marco de Referência para "sites" WEB da Administração Tributária

Fonte : Antonio Seco - Modelo de Prestação de Serviços aos Contribuintes por meio da Internet – UCP/PNAFE, 1998

O documento ainda lista 40 serviços que potencialmente poderiam ser disponibilizados nos sites das Administrações Tributárias, agrupados em sete grandes grupos; Legislação; Cadastro; Declarações, AIDF; Conta Fiscal; IPVA; e Serviços Diversos. Após listar os serviços é feita uma breve descrição de cada um dos serviços, seguido das "Informações Requeridas" e "Dicas de Implementação" para cada um deles.

5.1.3. Tecnología de la Información Aplicada a la Administración Tributaria - 2ª Edição-Março/2000 [18]

A segunda edição deste documento merece atenção especial porque traz um capítulo dedicado especialmente à utilização da Internet pelas Administrações Tributárias. O documento foi elaborado com o objetivo de fornecer uma atualização quanto aos temas relativos a aplicação da tecnologia da informação, através da exposição de experiências praticadas por diversas Administrações ao longo dos últimos anos, através do uso dos avanços tecnológicos.

---

[18] FERREIRA, Antonio Sergio Seco. **Tecnología de la Información Aplicada a la Administración Tributaria. Best Practice Paper, 2ª Edición.** In: BID – Banco Interamericano de Desarrollo. Brasília, 2000. [Internet] http://www.iadb.org/int/fiscal/documents/pdf/bpp_tiat2_esp.pdf [Capturado em 06.Nov.2001]

No capítulo dedicado a aplicação da tecnologia Internet, é feita uma abordagem através de sugestões de serviços que potencialmente poderiam ser disponibilizados na Web, agrupando-os principalmente em: Legislação; Cadastro; Declarações, Documentos Fiscais; Pagamentos; e Conta Corrente Fiscal.

Pelo modelo proposto, esses serviços, devem estar sujeitos a restrições de acesso, que poderiam ser assim distribuídas:

Tabela 2 – Demonstrativo da classificação das restrições de acesso a sites de Administrações Tributárias

TIPOS DE ACESSO	CARACTERÍSTICA	EXEMPLOS DE SERVIÇOS
PÚBLICOS	Serviços de domínio público	• Consultas à legislação • Agendas • Jurisprudências
LIMITADOS	Associados aos serviços que requeiram que o contribuinte possua algum dado específico que identifique a informação solicitada	• Serviços que guardam informações confidenciais de determinado contribuinte, para os quais deverá ser previamente identificado e autenticado
PRIVADOS	Serviços que guardam informações confidenciais de determinado contribuinte, para o qual ele deverá ser previamente identificado e autenticado	• Consulta à conta-corrente fiscal; • Alterações cadastrais; • Consulta ao cadastro.

Outro aspecto tratado é a questão de restrições legais para a implementação de serviços na Web. De acordo com o documento, algumas administrações tributárias precisariam modificar seus regulamentos para adequá-los a essa nova ferramenta, citando como exemplo os *"... procedimientos tributarios que requieran la firma del contribuyente para su formalización, ya que todavía la institución no dispone de instrumentos legales para aceptar "firmas electrónicas" (contraseñas, certificados digitales, etc.)"* Chama-se atenção para possíveis demandas judiciais, quando expõe que *"otro aspecto a ser discutido sería saber si la seguridad ofrecida por el sistema informático es considerada insuficiente para determinados servicios, pudiendo incentivar al contribuyente a entrar con acciones en la justicia para invalidar transacciones realizadas o a su vez dejar todo el servicio bajo sospecha"* (FERREIRA, 2000, p. 82).

Porém, o que mais chama a atenção neste capítulo é a preocupação com os requisitos de segurança nestas transações, a ponto do documento sugerir detalhes de como deveriam ser

feitas as validações no momento de entrega de declarações, assim como a melhor forma de utilização de serviços de identificação digital através do uso de PKI, ou seja, a utilização de infra-estrutura de chaves públicas.

Para fazer uso dessa tecnologia de autenticação de documentos eletrônicos por meio de certificados digitais, é sugerido que as Administrações Tributárias optem por três alternativas, conforme quadro apresentado no documento (FERREIRA, 2000, p. 89 – tradução livre do autor):

Tabela 3 – Comparativo entre diversas soluções para implantação de uma PKI

	VANTAGENS	DESVANTAGENS
Criar sua própria PKI	• Confiabilidade • Controle sobre os recursos	• Alto custo de implantação e manutenção • Certificado válido apenas para a Administração Tributária • Não faz parte da atividade fim da Administração Tributária •
Estimular a criação de uma PKI em nível de governo	• Confiabilidade • Repartir custos • Certificado válido para todo o governo	• Dependência de outras entidades para sua implantação
Utilizar PKI privada	• Custo zero para a Administração Tributária • Utilização de entidade especializada	• Confiabilidade • Custo maior para o contribuinte

5.1.4. Governo Eletrônico e as Administrações Tributárias Brasileiras : Segundo Benchmark - Setembro/2001 [19]

Visando subsidiar as Administrações Tributárias, a UCP/PNAFE já divulgou dois relatórios onde faz a avaliação e *benchmark* dos serviços já oferecidos pelas Administrações Tributárias estaduais, a partir do *Modelo de Serviços aos Contribuintes por Meio de Internet* (vide tópico 5.1.2 acima). O primeiro *benchmark* foi divulgado em agosto de 2000, e o último em setembro/2001.

[19] FERREIRA, Antonio Sergio Seco. **Governo Eletrônico e as Administrações Tributárias Estaduais Brasileiras: Segundo Benchmark** In: UCP/PNAFE. Brasília: Set/2001 [Internet] http://www.esaf.fazenda.gov.br/cst/arquivos/e-fisco&Benchmark-2.pdf [Capturado em 16.Nov.2001]

Neste último relatório ficou demonstrado que alguns fatores contribuíram para o avanço dos serviços oferecidos pelas Administrações Tributárias. O primeiro fator é a alta taxa de crescimento do uso da Internet no Brasil, e em segundo lugar o fato de que o ICMS, principal imposto estadual, estar relacionado a contribuintes Pessoas Jurídicas, cujo relacionamento deste com a Administração Tributária é efetuado através de contadores, que são uma classe profissional com grande disponibilidade de acesso á Internet, já que também acessam a Web para fins de relacionamento com a Receita Federal e Previdência Social.

O relatório apresenta uma tabela contendo a classificação dos *sites* das 27 Administrações Tributárias, apresentado o estágio em que cada um deles se enquadram dentro do Marco de Referência (FERREIRA, 2001, p. 5):

Tabela 4 – Inserção das Administrações Tributárias no Marco de Referência – Setembro/2001

ESTÁGIO	Unidades da Federação
1 – Presença	Roraima
2 – Prospecção	Acre, Alagoas, Amapá, espírito santo, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Pará, Paraíba, Piauí. Rio de Janeiro, Rondônia, Sergipe, Tocantins Total: 15
3 – Integração	Amazonas, Ceará, Distrito Federal, Mato Grosso, Paraná, Pernambuco, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina Total: 9
4– Transformação	São Paulo, Bahia Total: 2

No caso específico do site da Administração Tributária baiana, apenas 07 dos 40 serviços indicados no Modelo de Prestação de Serviço ainda não foram implementados integralmente, conforme segue:

> **Legislação :** Verbetes Tributários ou Afins
>
> **Conta Fiscal :** Extrato de Débito, Emissão de Certidão de Regularidade, Solicitação de Parcelamento de Débitos; e Notificação de Irregularidade e/ou Consulta;
>
> **Serviços Diversos** : Cálculo para pagamento de Débitos Atrasados; Opinião do Fisco sobre Temas Polêmicos;

Desses sete serviços, quatro estão em fase de homologação, e em breve estarão sendo disponibilizados para os contribuintes baianos, e os demais, provavelmente, não serão implementados de acordo com a Diretoria de Atendimento da SEFAZ-Ba.

CAPÍTULO VI

O USO DA INTERNET PELA SECRETARIA DA FAZENDA DO ESTADO DA BAHIA

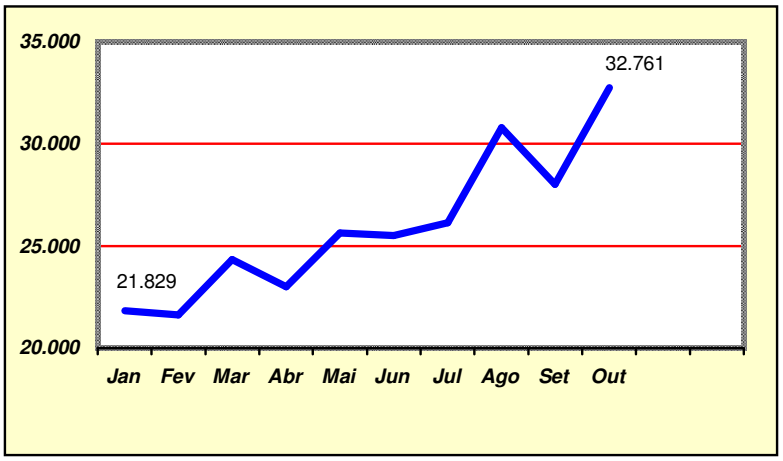
6.1. Histórico

A Internet passou a ser um meio de relacionamento entre a SEFAZ-Ba e os seus contribuintes a partir de 1997, quando foi disponibilizada a primeira versão de seu site (http://www.sefaz.ba.gov.br). Inicialmente o site oferecia apenas informações institucionais, possibilidade de envio de correio eletrônico, acesso aos textos legais e endereços das repartições fazendárias, sendo gradativamente agregados novos serviços.

No início de 2001 foi disponibilizado no site da SEFAZ-Ba o resultado do *Projeto Sefaz 100% Internet*. O projeto tem como escopo a disponibilização de todos os serviços até então prestado aos contribuintes nas repartições fazendárias, criando assim uma unidade fazendária digital, onde o atendimento ao contribuinte adquire novos contornos, com a redução da burocracia, proporcionando acesso fácil, rápido e seguro em serviços e informações.

O número de visitantes ao site durante o ano de 2001 cresceu de forma bastante acelerada desde a disponibilização dos serviços do programa 100% Internet , conforme se pode observar no gráfico a seguir:

Gráfico 2 - Evolução do número de visitantes ao Site da SEFAZ-Ba em 2001 (em mil)



Fonte : SGF/DTI/GEDES – Gerência de Desenvolvimento de Sistemas e Administração de Dados/Coordenação GEDES - Web

Para alguns serviços, o acesso dos contribuintes, estabelecimentos gráficos e contadores só são permitidos com identificação através do uso de senhas. A obtenção de senhas foi normatizada através da Portaria n.º 582, de 29 de dezembro de 2000. A indicação dos serviços que depende de senha para serem acessados, consta no Anexo 2 - Demonstrativo dos Serviços Oferecidos no Site da SEFAZ-Ba.

Além do uso de senha para acessar alguns serviços, foi criada uma outra classificação de acesso, denominado de "acesso restrito". Nesse tipo de acesso, além da senha, o usuário - geralmente contribuintes e contadores - é informado, através de um sistema de autenticação, de que ele está acessando o site da SEFAZ-Ba, já que esta utiliza um Certificado Digital em seu servidor de rede, obtido junto a uma empresa que presta serviço de Certificação Digital.

Outra garantia de segurança é também a utilização de um Certificado Digital para Software. Este tipo de certificado garante, para o contribuinte e contador, que todos os programas copiados do site foram desenvolvidos pela SEFAZ-Ba. Além disso, os softwares estão providos da Chave Pública da Sefaz, que criptografa todos os arquivos de dados com as informações econômico-fiscais que são transmitidas pelos contribuintes. Dessa forma, tanto a Sefaz quanto o contribuinte, tem a garantia de que os dados serão transmitidos de forma íntegra e sigilosa.

6.2. Serviços oferecidos aos contribuintes

A lista de serviços oferecidos pelo programa 100% Internet está coerente com as sugestões feitas pelo BID, estando disponibilizados mais de 70 serviços, distribuídos em 14 grupos, conforme discriminado no Anexo 2 - Demonstrativo dos Serviços Oferecidos no Site da SEFAZ-Ba.

6.3. Problemáticas levantadas na utilização da Internet pela SEFAZ-Ba

A partir dos pontos abordados nesse estudo, pudemos constatar que a SEFAZ-Ba está no caminho certo ao adotar a Internet como ferramenta de relacionamento com seus contribuintes e demais interessados envolvidos nesta relação (contadores, estabelecimentos gráficos, etc.).

Destacamos, porém, dois aspectos críticos nessa relação: a) a exclusividade de alguns serviços, que só podem ser utilizados pela Internet; b) não há certificação digital dos

contribuintes e demais envolvidos, quando estes acessam os serviços restritos ou quando enviam arquivos de dados.

6.3.1. Acesso exclusivo de serviços via Internet

É inegável que quase a totalidade dos contribuintes tem aderido ao relacionamento via Internet, ao invés de deslocar-se às repartições fiscais, o que possibilita a celeridade processual.

Porém, o que nos chama a atenção é o fato de que, se o Regulamento do ICMS da Bahia estabelece que alguns desses relacionamentos só são possíveis pela Internet, retirando dos contribuintes e demais interessados a possibilidade de obter esses serviços e prestar informações diretamente na repartição fiscal.

Convém lembrar que nem todos os contribuintes possuem acesso à Internet, geralmente aqueles de baixa capacidade econômica. Tal exclusividade só se justificaria se todos possuíssem microcomputadores. Essa falta de opção pelo atendimento pessoal faz com que o contribuinte fique refém de alguns privilegiados, que cobram pelos serviços prestados e assumem o papel de agentes intermediadores em situações em que a presença na repartição fiscal os tornaria dispensáveis.

6.3.2. Certificação Digital de contribuintes

Os contribuintes, ao utilizarem os serviços da SEFAZ-Ba na Internet, têm a segurança de que estão se relacionando com um site que realmente pertence à Administração Tributária Baiana, e que os softwares copiados no referido site foram por ela desenvolvidos e que as informações enviadas pela Internet estão devidamente protegidas, íntegras e seguras. Porém, em relação ao contribuinte, o não uso de Certificação Digital implica em:

> **Risco de repúdio** – Se os contribuintes só pudessem enviar informações ou documentos assinados digitalmente, através da utilização de Certificação Digital, a SEFAZ-Ba não correria o risco de que, no futuro os remetentes desses documentos eletrônicos venham a repudiar a informação enviada, negando a sua autoria.
>
> **Risco de Autenticidade** – O uso de Certificação Digital também garantiria para a SEFAZ-Ba de que o documento que está sendo enviado realmente provém do contribuinte ou interessado que se identificou digitalmente.

O Estado do Ceará já está utilizando um serviço de certificação de chave pública, apesar de ser um esquema de proprietário, desenvolvido internamente (FERREIRA, 2001: p. 6 e 7). O

serviço é denominado *SefazNet*, que é o sistema que cria a "Assinatura Eletrônica". O usuário obtém um sistema no site da Secretaria, e após instalá-lo em seu computador, criará uma fórmula pessoal (chave-privada) que codificará (criptografará) todos os arquivos que serão transmitidos pelos usuários. No momento em que o usuário se cadastrar na Sefaz entregará a fórmula que decodificará os seus arquivos (chave pública), a qual é gerada no momento da instalação do *SefazNet*, e gravada em disquete. Assim, todos os arquivos transmitidos pelo usuário serão codificados com a sua chave privada, como se fosse sua assinatura, e somente serão decodificados com a chave pública entregue no cadastramento[20].

Essa talvez não seja a solução menos onerosa, mais certamente a mais segura, quando comparado ao simples uso de senhas.

Cremos que o sistema ideal seria aquele em que todos os contribuintes possuíssem seu próprio Certificado Digital, fornecido gratuitamente pela própria SEFAZ-Ba, a exemplo do Banco do Brasil, conforme já abordado no tópico 3.3, ou criação de seu próprio PKI a exemplo da Secretaria da Fazenda do Ceará.

[20] SefazNET – Informações Gerais – In: Secretaria da Fazenda do Estado do Ceará. [Internet] http://www.sefaz.ce.gov.br/produtos&servicos/sefaznet/snet1.htm [Capturado em 30.Nov.2001]

VII - CONSIDERAÇÕES FINAIS

Com base nos estudos efetuados podemos afirmar que a Internet é a melhor tecnologia atualmente disponível para melhorar o processo de gestão tributária, oferecendo as melhores condições para aperfeiçoar a relação fisco-contribuinte, permitindo que a Administração Tributária obtenha informações de maneira confiável, e de forma rápida, imprimindo alta qualidade na prestação de serviços aos usuários, otimizando, inclusive, o sistema de arrecadação e o cumprimento das obrigações acessórias.

Alguns problemas de ordem jurídica estão envolvidos nesta relação digital, entre fisco-contribuinte, e se referem principalmente aos aspectos de segurança e validade jurídica dos documentos eletrônicos que são produzidos. Mas estes já estão sendo resolvidos, à medida que começa a ser estabelecido no país, um sistema que dará segurança jurídica às operações realizadas através da Internet, bem como validar esses documentos e respectivas assinaturas digitais.

Percebemos ainda que vários atos administrativos estão legitimando a prática do uso da Internet, substituindo gradualmente os documentos em papel, pelos equivalentes, em meio magnético, antecipando-se à pacificação do reconhecimento jurídico de sua eficácia.

As normas tributárias baianas já deveriam estar convalidando de forma explícita os documentos eletrônicos produzidos nesta relação digital, pois até então, tanto o Regulamento do ICMS quanto as Portarias editadas, limitam-se a esclarecer os mecanismos de utilização dos respectivos serviços, sem explicitar claramente que tais documentos têm a mesma validade dos produzidos em papel. Essa lacuna já está inserida não só no texto da Medida Provisória nº 2.200/01, como também nos Projetos de Lei em tramitação no Congresso Nacional.

Cremos que a Secretaria da Fazenda do Estado da Bahia está trilhando de forma bastante acertada na política de utilização da Internet para imprimir qualidade no atendimento ao usuário, quer seja ele contribuinte, contador ou demais interessados em interagir com a Secretaria da Fazenda.

ANEXOS

ANEXO 1

GLOSSÁRIO

BBS Bulletin Board System – Uma base de dados que pode ser acessada via linha telefônica, onde normalmente são disponibilizados arquivos de todos os tipos, softwares de domínio público e conversas on-line. Perdeu bastantes usuários com a expansão da Internet, que oferece uma interface mais amigável, o que não é realidade em uma BBS.

Backbones O termo backbone refere-se aos principais caminhos de informação de uma rede de computadores. O backbone da Internet representa sua estrutura central, transmitindo dados de modo semelhante à forma como a medula espinhal transfere informações entre o cérebro e o corpo.

Quase sempre, não importa sua origem, uma informação viajará pelo backbone para chegar até seu comutador de destino. Os dados nem sempre percorrem a mesma rota entre computadores, seu curso é determinado pela disponibilidade de rede. O backbone, composto por computadores poderosos e conexões rápidas inclui redes de propriedade comercial e redes dedicadas à pesquisa e educação.

Para possibilitar, a capilarização da Internet no Brasil foram interligadas às espinhas dorsais de âmbito nacional, espinhas dorsais de abrangência regional, estadual ou metropolitana.

Espinhas Dorsais Nacional

Embratel
Rede Nacional de Pesquisa
Unisys
Global-One
IBM

Espinhas Dorsais de Âmbito Estadual

ANSP (SP)
Rede Bahia (BA)
Rede Catarinense (SC)
Rede Internet Minas (MG)
Rede Norte-riograndense de Informática (RN)
Rede Pernambuco de Informática (PE)
Rede Rio (RJ)
Rede Tchê (RS)

Benchmark Termo que indica os "melhores resultados" dentre as organizações concorrentes, em determinados itens de controle. Observa-se atualmente a tendência de ultrapassar a análise dos concorrentes e procurar apresentar um desempenho ainda melhor como referencial. Assim, empresas têm se utilizado dessa metodologia para fazer comparação sistemática de seus produtos e serviços com

	os oferecidos pela concorrência ou por empresas considerados excelentes em algo determinado. O objetivo do "benchmarking" é o de conhecer e, se possível, de incorporar o que os outros estão fazendo de melhor.
Chave Privada	Chave matemática (mantida em segredo pelo usuário) usada para criar assinaturas digitais e, dependendo do algoritmo, para decriptografar mensagens ou arquivos criptografados com a chave pública correspondente.
Chave Pública	Chave matemática que pode ser compartilhada com segurança, de modo que outros possam lhe enviar informações criptografadas, e que somente sua chave privativa possam decodificar. A chave pública pode também confirmar a veracidade de assinaturas criadas com sua correspondente chave privativa. Dependendo do algorítmo, as chaves públicas também podem ser utilizadas para criptografar arquivos ou mensagens que são decriptografados com as chaves privativas correspondentes.
Ciberterrorismo	Ação terrorista que se utiliza os recursos disponíveis na Internet para planejar e executar suas ações criminosas.
Correio Eletrônico	Correspondência que se pode enviar e receber diretamente pelo computador através da Internet. Nesta correspondência, além de textos, imagens e sons, os usuários podem anexar arquivos diversos (do inglês = e-mail). Para que se possa desfrutar dos serviços de correio eletrônico é necessário ter um endereço eletrônico do tipo alexandre@sefaz.ba.gov.br , por exemplo. Cabe lembrar que um endereço eletrônico é único, ou seja, não pode haver na Internet outro endereço exatamente igual. Isso garante que a mensagem chegará ao destinatário correto.
Criptografia	Ciência matemática usada para garantir a confidencialidade e veracidade de informações, codificando-as, de modo a ocultar seu conteúdo, impedir alterações indevidas e/ou uso não autorizado. Deste modo, apenas o destinatário pretendido pode entendê-las (kriptós = escondido, oculto; grápho = grafia).
Criptografia Assimétrica	Vide Criptografia de Chave Pública
Criptografia de Chave Pública	Tipo de criptografia que utiliza um par de chaves criptográficas, matematicamente relacionadas. A chave pública pode estar disponível para qualquer um que desejar utlilizá-la e pode criptografar informações e confirmar a veracidade de assinaturas digitais; a chave privativa é mantida em segredo por seu portador e pode descriptografar informações ou criar uma assinatura digital.
Domínio, Nome de	Vide Endereço IP
Endereço IP	O endereço IP (Internet protocol) é uma seqüência numérica que identifica máquinas (ou domínios) dentro da rede mundial de computadores. O endereço eletrônico é uma representação em forma de texto de sites dentro de domínios, utilizado para fazer

	referência a páginas de conteúdo HTML, diretórios de FTP ou qualquer outro serviço disponível na Internet. O endereço de correio eletrônico (e-mail) é uma seqüência de caracteres contendo o nome de login no sistema de correio eletrônico seguido por uma arroba (@) e pelo endereço do servidor de correio eletrônico do usuário; funciona como seu endereço postal para receber mensagens pessoais. É uma identificação, unívoca de um computador ligado á Internet mundial, e é equivalente ao número de telefone composto por <*Código de País/Código de Área/Número do Assinante*> no mundo das redes. È através da identificação de um número IP de um destinatário que a comunicação a partir de um ponto de origem é viabilizada, de computador a computador. Exemplos : Endereços e-mail – alexandre@sefaz.ba.gov.br, onde "alexandre", que está (@) em uma entidade denominada "sefaz.ba", que é um estabelecimento governamental (gov), registrada na estrutura Internet do Brasil (br). Endereços de domínio - http://www.sefaz.ba.gov.br
FTP	File Transfer Protocol – É o protocolo usado na Internet para transferência de arquivos entre computadores. O objetivo do FTP é promover transferência de arquivos de modo rápido e eficiente.
Hardware	Componentes físicos de um computador. Ex: teclado e monitor.
Home-banking	É o tipo de serviço oferecido pelas instituições bancárias, que possibilita o acesso do correntista a vários serviços bancários através do uso da Internet. Exemplo: solicitação e talões de cheques, extratos, transferências de numerários, pagamentos de duplicatas, etc.
Host	Em uma rede qualquer, é o nome dado ao principal computador, que comanda e controla as ações de outros. Na Internet, um host é um computador que abriga sites ou diretórios de arquivos para download.
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira – É um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública. Instituído através da MP nº2.200/01.
IP, Protocolo	IP – Internet Protocol – Vide Protocolo
Modem	O modem é uma ponte entre os sinais analógicos e digitais. Ele converte os dados digitais ligado e desligado (1 e 0) em um sinal analógico variando, ou modulando a freqüência de uma onda eletrônica, um processo similar ao utilizado pelas estações de FM. Como ponta de recepção de uma conexão eletrônica , o Modem faz exatamente o oposto: demodula os sinais analógicos em códigos digitais. Os dois termos, MOdular e DEModular, deram ao modem seu nome.

Protocolo Conjunto de normas que regulam a comunicação entre dispositivos. Para que as comunicações tenham sucesso, todos os dispositivos envolvidos devem respeitar as mesmas normas, ou seja, devem utilizar o mesmo protocolo.

Na Internet, o principal protocolo utilizado é o TCP/IP, o qual é um conjunto de protocolos de comunicação criados pelo Departamento de Defesa dos Estados Unidos e que acabaram se afirmando como forma de conectar, em redes, equipamentos não compatíveis entre si.

Provedores Empresa comercial que mantém computadores conectados de forma permanente à Internet. Esses computadores são conhecidos como hosts, ou anfitriões. O provedor faz um investimento em linhas telefônicas, computadores, software e na própria conexão permanente com a Internet, aumentando sua largura de banda e, conseqüentemente, sua capacidade de conectar mais clientes ao mesmo tempo à grande rede.

Roteador Roteamento é a procura de um determinado equipamento na Internet com a função de envio de dados ao mesmo. O roteamento na Internet é feito através do protocolo IP responsável pela entrega de informações geradas pelas aplicações aos seus destinos de forma correta e eficiente. A execução desta tarefa é feita através de tabelas de roteamento existentes em todos equipamentos conectados à Internet, onde constam as rotas a serem seguidas pelas informações em função de seu destino

Scanner (ótico) Equipamento com dispositivo de entrada para computador que utiliza um raio luminoso para detectar os focos de luz e obscuridade (ou as cores) da superfície do papel, e que converte a imagem em sinais digitais manipuláveis com um *software* de tratamento de imagens ou com reconhecimento ótico de caracteres, formando formando imagens dos documentos processados.

Sites Conjunto de documentos escritos em linguagem HTML, pertencentes a um mesmo endereço (URL), disponível na Internet.

Softwares Conjunto de instruções, programas e dados a eles associados, empregados durante a utilização do computador. O mesmo que programa ou aplicativo. É um termo abrangente, que se utiliza em contraste com hardware, para referenciar todos os programas de um sistema de computador.

TCP, Protocolo TCP – Transmission Control Protocol – Vide Protocolos

Telnet Protocolo de Terminal Virtual – É o protocolo Internet que torna possível a conexão com computadores de qualquer parte do mundo, e a través dele é possível usar um computador que está longe, como se fosse o seu próprio microcomputador. É o que se convencionou chamar de conexão remota, a qual permite a execução de programas e comando em outra máquina, como se um teclado de um computador estivesse ligado diretamente em outro computador. – Vide Protocolos

Vírus	Programa ou pedaço de código executável, geralmente maléfico, que invade sistemas e interfere no funcionamento normal de um computador. Seu nome advém dos vírus biológicos, pois também invadem hospedeiros e causam disfunções. O vírus da informática tem o poder de se introduzir em um computador, em seu sistema operacional ou demais softwares, sem o conhecimento ou a permissão do usuário, causando um comportamento indesejado no hardware ou nos softwares presentes. Uma de suas principais características é a habilidade de se reproduzir, aumentando assim a infecção e se propagando para outras máquinas, o que o torna perigoso e de difícil controle.
WWW	World Wide Web (ou W3) - Biblioteca de recursos disponíveis para usuários de computadores através da Internet. Permite aos usuários visualizar uma grande variedade de informações, incluindo arquivos de revistas, bibliotecas públicas e universitárias, atualidades e notícias de negócios. Os recursos da World Wide Web (WWW) são organizados de modo que os usuários possam se mover facilmente de um recurso para outro. As conexões para computadores de fontes diferentes, ou servidores, na rede é feita automaticamente sem ser vista pelo usuário. Essas conexões são feitas com o uso de hipertexto e hipermídia. Geralmente, os usuários navegam através da informação na WWW com a ajuda do programa conhecido como WWW browser ou cliente. O browser apresenta texto, imagem, som ou outros objetos de informação na tela do computador do usuário na forma de uma página, que é obtida a partir do servidor WWW. Ele é a responsável pela massificação da Internet.

Nota sobre o glossário

Este glossário foi construído a partir das referências bibliográficas citadas ao final do estudo. Alguns verbetes foram transportados, de forma fiel, ao constante nas obras ou sites visitados, e outros a partir do nosso entendimento e estudo das fontes de consulta.

ANEXO 2

DEMONSTRATIVO DOS SERVIÇOS OFERECIDOS NO SITE DA SEFAZ-Ba

Tabela 5 – Lista dos Serviços Oferecidos no Site da SEFAZ-Ba.

Serviço	Restrição de Acesso
Aplicação: Legislação	
Consultas a Legislação Vigente (atual)	Público
Consultas ao histórico das alterações da Legislação	Público
Índice Remissivo dos textos de legislação	Público
Download de textos da Legislação	Público
Perguntas e respostas mais freqüentes de legislação	Público
Plantão Fiscal on-line para dúvidas	Público
Novidades Tributárias (boletim eletrônico por e-mail)	Público
Aplicação: Pareceres Tributários (CPT)	
Consulta Formal	Senha
Solicitação de Regime Especial	Senha
Reconhecimento de Diferimento	Senha
Parecer de uma consulta formal	Senha
Base de Pareceres de Consulta Formal e Regimes Especiais	Público
Aplicação: Cadastro de Contribuintes (CAD)	
Consulta básica ao cadastro SINTEGRA	Restrito (por CNPJ, CPF ou IE)
Consulta básica ao cadastro BA	Restrito (por CNPJ, CPF ou IE)
Consulta ampliada ao cadastro	Senha
Consulta a estabelecimentos de uma empresa	Público
Consulta para o contador (cadastro e empresas vinculadas)	Senha
Consulta de sócios e responsáveis	Restrito (informando CNPJ ou CPF)
Alteração no cadastro de contadores	Senha
Solicitação de Inscrição Estadual	Restrito
Alteração no cadastro de contribuintes	Senha
Certidão de baixa	Restrito (informando IE)
Download de Inscrições Ativas	Público
Solicitação de baixa de contribuinte	Senha
Habilitação para diferimento	Senha
Aplicação: Informações Econômico Fiscais (IEF)	
Entrega de Declarações (DMA, DME, DMD)	Senha
Entrega de Declarações GIA_ST	Senha
Informações de EPP	Público
Orientações sobre entrega dos arquivos do Convênio 57	Público
Consulta a entrega das declarações	Senha
Download dos dados entregues na declaração (DMA, DMD, DME)	Senha
Segunda via do recibo de entrega de DMA/DMD/DME	Senha

Serviço	Restrição de Acesso
Aplicação: Impressão de Documentos Fiscais (AIDF)	
Autorização para emissão de AIDF	Senha
Consulta a AIDF (pelo seu número)	Público
Ficha histórica de AIDFs concedidas a uma empresa	Senha
AIDF autorizadas para gráficas	Senha
Consulta de validade de nota fiscal (autorização de emissão)	Público
Aplicação: Uso de Processamento de Dados (SEPD)	
Comunicação de uso de Processamento de Dados	Senha
Inclusão de novo documento na Comunicação de uso PD	Senha
Consulta de comunicação de uso e documentos de PD	Senha
Aplicação: Equipamentos Emissores de Cupom Fiscal (ECF)	
Consulta ECF para contribuinte	Senha
Informação de uso de ECF (pelo contribuinte)	Senha
Solicitação de manutenção de uso ECF (pelo contribuinte)	Senha
Solicitação de Cessação de ECF (pelo contribuinte)	Senha
Renovação de informação de uso de ECF (pelo contribuinte)	Senha
Consulta ECF para credenciada	Senha
Intervenção de informação de uso ECF	Senha
Intervenção de manutenção ECF	Senha
Intervenção de cessação de ECF	Senha
Impressão de Atestados de Intervenção	Senha
Segunda via do atestado de intervenção	Senha
Aplicação: Crédito Tributário	
Extrato de Parcelas	Senha
Aplicação: Certidões de Crédito	
Emissão de Certidão Negativa	Restrito (informando IE ou, CPF)
Consulta a Certidões Emitidas (por número da certidão)	Restrito
Aplicação: Arrecadação	
Emissão de DAEs com código de barras	Público
Consulta a pagamentos realizados (histórico)	Senha
DAE com data de pagamento futuro	Público
Aplicação: IPVA	
Tabela de pagamento de IPVA	Público
Consulta ao IPVA pelo número do Renavam	Restrito (informando Renavam)
Emissão de DAE avulso de IPVA	Restrito (informando Renavam)
Histórico dos pagamentos do IPVA	Restrito (informando Renavam)
Pagamento de IPVA para veículos novos	Público
Certidão negativa de IPVA	Restrito (informando Renavam)
Consulta a certidões de IPVA emitidas	Público
Parcelamento de IPVA	Público

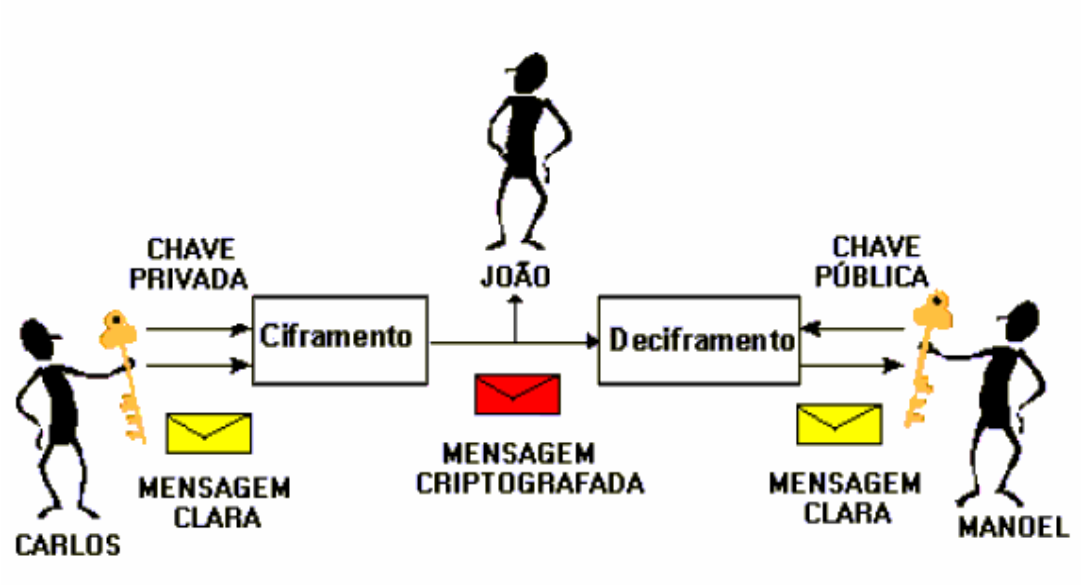
Serviço	Restrição de Acesso
Aplicação: Protocolo	
Consultas a Tramitação de Processos	Restrito (informando no. Protoc.)
Consulta a processos de um interessado	Senha
Aplicação: Senhas	
Solicitação de senha	Público
Troca de senha	Senha
Autenticação	-
Cancelamento de senha	Senha
Aplicação: Denúncia Fiscal	
Denúncia Fiscal	Público

Fonte: SGF/DTI/GEDES – Gerência de Desenvolvimento de Sistemas e Administração de Dados (Coordenação GEDES - Web) – SEFAZ-Ba

APÊNDICE

FUNCIONAMENTO DO SISTEMA DE ASSINATURA DIGITAL BASEADO EM CRIPTOGRAFIA ASSIMÉTRICA

Figura 2 – Diagrama do Funcionamento do Sistema PKI



O diagrama acima demonstra o funcionamento da certificação digital baseado em criptografia assimétrica. Assinar digitalmente uma mensagem possibilita que o destinatário (**MANOEL**) possa verificar se a mesma partiu de determinada pessoa (**CARLOS**), e não de alguém que tente passar por ela (**JOÃO**), garantindo ainda a sua mensagem enviada encontra-se íntegra, sem nenhuma espécie de adulteração, trazendo a certeza de que ninguém modificou-la enquanto ela percorreu o seu trajeto. Portanto, a assinatura eletrônica não é uma mera subscrição, mas o modo de garantir que os documentos provem de seu autor e que seu conteúdo não foi adulterado. Esta assinatura pode ser utilizada em documentos eletrônicos, mensagens de correio eletrônico, autenticação para acesso a sistemas eletrônicos, bem como, utilizada na troca de chaves, para estabelecimento de sessão criptografada.

No caso de envio de uma mensagem por Correio Eletrônico (e-mail), o processo de Certificação Digital funciona da seguinte maneira[21]:

[21] **Certificação Digital: Como Funciona**. In: Boletim eletrônico PC World de 07/11/2001. [Internet] http://pcworld.terra.com.br/pcw/testes/internet/0075.html [Capturado em 16.Nov.2001]

1. O programa de Correio Eletrônico, instalado no computador do emissor da mensagem, gera uma versão reduzida da mesma, a qual é em seguida criptografada com base na sua Chave Privada, servindo de assinatura digital.

2. Esta mensagem e sua respectiva versão original são enviadas ao destinatário.

3. O programa de Correio Eletrônico do destinatário, com base na Chave Pública do emissor, descriptografa a versão reduzida e a compara com a original. Não havendo nenhuma divergência, o destinatário é informado de que a mensagem foi enviada pelo emissor e que está íntegra.

Podemos resumir as funções das Chaves Públicas e Privadas da seguinte maneira:

Tabela 6 – Quadro resumo das funções das Chaves Públicas e Privadas

Tipo da Chave	Quem Utiliza a Chave	Objetivo
Pública do destinatário	Emissor	Enviar uma mensagem criptografada
Privado do emissor	Emissor	Enviar uma mensagem assinada
Privada do destinatário	Destinatário	Decodificar uma mensagem
Pública do emissor	Destinatário	Decodificar uma mensagem autenticada

Fonte: Boletim Eletrônico PCWORLD (adaptado)

No processo de emissão de um certificado, a Autoridade Certificadora (AC) envia, para o solicitante do Certificado, um programa que irá efetuar um cálculo em seu computador particular, gerando a Chave Privada (que será gravada em seu computador) e uma Chave Pública, que além de ser gravada, é enviada automaticamente para a AC, ficando guardada para efeito de conferência por todos quantos quiserem saber detalhes sobre os mesmos como, por exemplo, a data de emissão e expiração da mesma.

REFERÊNCIAS BIBLIOGRÁFICAS

Livros, Jornais e Revistas

AVOLIO, Luiz Francisco Torquato. **As Provas Ilícitas no Processo Civil**. São Paulo: Revista Panorama da Justiça, Ano IV, nº 26, p. 18-20.

BARBAGALO, Erica Brandini. **Contratos Eletrônicos**. São Paulo : Saraiva , 2001.

BONILHA, Paulo Celso Bergstrom. **Da Prova no Processo Administrativo Tributário**. São Paulo: LTR Editora, 1992.

BRAGA, Rosana. **Terminais eletrônicos lê impressão digital**. São Paulo: Gazeta Mercantil, Caderno Tecnologia da Informação. 18 jul. 2001. p. 3

BRASIL, Angela Bittencourt. **Assinatura Digital não é Assinatura Formal**. São Paulo: Revista Panorama da Justiça, Ano V, nº 27, p. 18-20.

BRENER, Eliana de Moraes. **Elaboração de Trabalhos Acadêmicos – Projeto de Pesquisa, monografia e artigo**. Salvador: UNIFACS - Universidade Salvador, Coordenação de Pesquisa, 2000.

BRUNO, Marcos Gomes da Silva. **Aspectos Jurídicos dos Contratos Eletrônicos**. São Paulo: Revista Panorama da Justiça, Ano V, nº 30, p. 26-29.

CARVALHO, Paulo de Barros. **A Prova no Procedimento Administrativo Tributário.** Revista Dialética de Direito Tributário, nº 34. São Paulo: Dialética, Jun.1998.

CASTELLS, Manuel. **A Sociedade em Rede, Volume 1.** São Paulo: Paz e Terra, 1999

COMER, Douglas E. Interligação em Redes TCP/IP – Volume 1 – Princípios, protocolos e arquitetura. Rio de Janeiro: Editora Campus, 1998.

CONCERINO, Arthur José. **Internet e Segurança são Compatíveis?** In: LUCCA, Newton de; FILHO, Adalberto Simão (org.). Direito & Internet – Aspectos Jurídicos Relevantes. São Paulo: Edição conjunta - EDIPRO e Instituto Brasileiro de Proteção e Defesa dos Consumidores de Internet, 2000.

FERNANDES, Andréa Gomes; AFONSO, José Roberto Rodrigues. **e-Governo no Brasil: Experiências e Perspectivas.** Rio de Janeiro: Revista do BNDES V. 8 - nº 15, Jun 2001.

GOMES, Olavo José Anchieschi. **Segurança total – Protegendo-se contra os Hackers**. São Paulo: Makron Books, 2000.

GRECO. Marco Aurélio. **Direito e Internet**. São Paulo: Dialética, 2ª Edição, 2000.

HOFFMANN, Susy Gomes. **Teoria da Prova no Direito Tributário**. Campinas: Copola Editora, 1999.

JUNQUEIRA, Miriam. **Contratos Eletrônicos**. Rio de Janeiro: MAUAD Consultoria e Planejamento Editorial, 1997.

LUCCA, Newton de. **Títulos e Contratos Eletrônicos – O Advento da Informática e seu Impacto no Mundo Jurídico**. In: LUCCA, Newton de; FILHO, Adalberto Simão (org.). Direito & Internet – Aspectos Jurídicos Relevantes. São Paulo: Edição conjunta - EDIPRO e Instituto Brasileiro de Proteção e Defesa dos Consumidores de Internet, 2000.

MELO, José Eduardo Soares de Melo. **Imposto sobre Serviço de Comunicação**. São Paulo: Malheiros Editores, 2000.

NUNES, Luiz Antonio Rizzato. **Manual da Monografia Jurídica.** São Paulo: Saraiva, 1999.

PAESANI, Liliana Minardi. **Direito e Internet**. São Paulo: Atlas, 2000.

PAULON, Rosana Marques. **O Documento Eletrônico no Processo Administrativo Fiscal**. Revista Dialética de Direito Tributário, nº 60. São Paulo: Dialética, Set.998.

QUEIRÓZ, Regis Magalhães Soares de. **Assinatura Digital e o Tabelião Virtual.** In: LUCCA, Newton de; FILHO Adalberto Simão (org.). Direito & Internet – Aspectos Jurídicos Relevantes. São Paulo: Edição conjunta - EDIPRO e Instituto Brasileiro de Proteção e Defesa dos Consumidores de Internet, 2000.

SANTOS, Moacyr Amaral dos. Primeiras Linhas de Direito Processual Civil - 2º Volume. São Paulo: Saraiva, 1977.

SILVA, De Plácido e. **Vocabulário Jurídico - 15ª edição**. São Paulo: Forense, 1999.

TUCCI, José Rogério Cruz e. **Eficácia Probatória dos Contratos Celebrados pela Internet**. In: LUCCA, Newton de; FILHO, Adalberto Simão (org.). Direito & Internet – Aspectos Jurídicos Relevantes. São Paulo: Edição conjunta - EDIPRO e Instituto Brasileiro de Proteção e Defesa dos Consumidores de Internet, 2000.

VOLPI, Marlon Marcelo. **Assinatura Digital - Aspectos Técnicos, Práticos e Legais**. Rio de Janeiro: Axcel Books, 2001.

Internet – Artigos e Documentos

BAIÃO, José; FERREIRA, Antonio Sergio Seco. **Gestión de los Recursos de Tecnología de la Información en el Contexto de la Modernización Gubernamental.** In: BID – Banco Interamericano de Desarrollo. Mayo 2000. [Internet] http://www.iadb.org/int/fiscal/documents/Gestion_TI_gob_esp.htm [Capturado em 20.Nov.2001]

BLUM, Renato M. S. Opice. **A Internet e os tribunais**. [Internet] http://www.apriori.com.br/artigos/internet_e_tribunais.htm [Capturado em 10.Jan.2001]

BRASIL, Angela Bittencourt. **Contratos Virtuais**. In: Jurinforma - Jurisprudências on line, [Internet] http://jurinforma.com.br/notas/0155.html [Capturado 01.Ago.2001]

_____. **O documento físico e o documento eletrônico**. In: Jus Navigandi, n. 42. [Internet] http://www1.jus.com.br/doutrina/texto.asp?id=1781 [Capturado 29.Nov.2001]

BRASIL. Ministério da Ciência e Tecnologia. **Sociedade da Informação no Brasil – Livro Verde**. Brasília: Setembro 2000 [Internet] http://www.socinfo.org.br/livro_verde [Capturado em 26.Abr.2001]

BRASIL. Ministério da Ciência e Tecnologia. Secretaria de Política de Informática. **Internet Comercial – Conceitos, Estatísticas e Aspectos Legais**. Brasília: Abr.2001 [Internet] ftp://ftp.mct.gov.br/Unidades/SEPIN/Palestras/E_commerce.pdf [Capturado em 12.Nov.2001]

BRASIL. Ministério das Relações Exteriores, Departamento de Cooperação Científica, Técnica e Tecnológica. **Lei Modelo da UNCITRAL sobre Comércio Eletrônico (1996)**

com Guia para sua Incorporação ao Direito Interno. obtido na web em 15/10/2001 http://www.dct.mre.gov.br/e-commerce/seminario_e-commerce_lei.htm

BRUNO, Gilberto Marques. **Algumas considerações sobre a questão da validade, eficácia e valor probatório dos documentos eletrônicos.** In: Jus Navigandi, n. 51. [Internet] http://www1.jus.com.br/doutrina/texto.asp?id=2174 [Capturado em 29.Nov.2001]

CASTELLS, Manuel. **La nueva Sociedad.** Entrevista concedida a Jordi Goula. In: Chile Hoy [Internet] http://chule-hoy.de/sociedad/130300_entrevista_a_castells.htm [Capturado em 21.Nov.2001]

DAOUN, Alexandre Jean. **Os novos crimes de informática**. [Internet] http://www.apriori.com.br/artigos/novos_crimes_de_informatica.htm [Capturado em 15.Nov.2001]

FERREIRA, Antonio Sergio Seco. **Tecnología de la Información Aplicada a la Administración Tributaria. Best Practice Paper, 2ª Edición.** In: BID – Banco Interamericano de Desarrollo. Brasília, 2000. [Internet] http://www.iadb.org/int/fiscal/documents/pdf/bpp_tiat2_esp.pdf [Capturado em 06.Nov.2001]

_____. **Governo Eletrônico e as Administrações Tributárias Estaduais Brasileiras: Segundo Benchmark** In: UCP/PNAFE. Brasília: Set/2001 [Internet] http://www.esaf.fazenda.gov.br/cst/arquivos/e-fisco&Benchmark-2.pdf [Capturado em 16.Nov.2001]

FILHO, Demócrito Reinaldo. **A questão da validade jurídica dos atos negociais por meios eletrônicos**. [Internet] http://www.infojus.com.br/area1/democritofilho13.htm [Capturado em 08.Nov.2000]

LIMA JR., Carlos Daniel Vaz de. **O sigilo do cadastro de clientes dos provedores de acesso à Internet**. [Internet] http://orbita.starmedia.com/~carlosdaniel.net/direito/sigilo.htm [Capturado em 28.Nov.2001]

MARCACINI, Augusto Tavares Rosa. **O documento eletrônico como meio de prova**. (Monografia. 1998) [Internet] http://www.marcacini.cjb.net/textos/docelet2.html [Capturado em 28.Nov.2001]

MOURA, Gevilacio Aguiar Coelho de. **Citações e Referências a Documentos Eletrônicos - Glossário** [Internet] http://www.quatrocantos.com/tec_web/refere/10gloss.htm [Capturado em 15.Nov.2001]

QUEIROZ, Luiz. **E-Gov economizou R$ 500 milhões em um ano** [Internet] http://www.computerworld.com.br/templ_textos/noticias.asp?id=15762 [Capturado em 30.Nov.2001]

SILVA, Alexandre Alcantara da. **A internet, o Documento Eletrônico e a Assinatura Digital** [Internet] http://sites.uol.com.br/alexalcantara/artigos/Alexandre_Documentoeletronico.rtf [Capturado em 15.Set.2001]

SILVA, Mauro. MELLO, Eduardo Piza G. de. **Cartórios virtuais – Receita atropela a Constituição**. [Internet] http://www.irib.org.br/birib/birib275_5.htm [Capturado em 29.Nov.2001]

SILVA, Rosana Ribeiro da. **Contratos Eletrônicos**. [Internet] http://www.apriori.com.br/artigos/contratos_eletronicos.htm [Capturado em 10/01/2001]

Internet – Outros sites consultados

BID - Banco Interamericano de Desenvolvimento – Divisão Fiscal. http://www.iadb.org/int/fiscal/portuguese

Coletânea de Legislação sobre Informática e Automação (BRASIL – Ministério da Ciência e Tecnologia) - http://www.mct.gov.br/legis/info.htm

Comitê Executivo do Comércio Eletrônico (BRASIL - Ministério do Desenvolvimento, Indústria e Comércio Exterior) – http://ce.mdic.gov.br

Comitê Gestor INTERNET do Brasil (BRASIL - Ministério das Comunicações) – http://www.cg.org.br

FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo - http://www.fapesp.br/

ICP – Infra-Estrutura e Chaves Públicas do Brasil (BRASIL - Presidência da República). http://www.icpbrasil.gov.br

PNAFE - Programa Nacional de Apoio à Administração Fiscal para os Estados Brasileiros (BRASIL - Ministério da Fazenda) - http://www.fazenda.gov.br/ucp/pnafe

RNP – Rede Nacional de Pesquisas - http://www.rnp.br/

Secretaria Fazenda do Estado da Bahia – http://www.sefaz.ba.gov.br

Secretaria Fazenda do Estado do Ceará – http://www.sefaz.ce.gov.br

Legislação

BAHIA – Decreto nº 6.284, de 14 de março de 1997 – Aprova o Regulamento do ICMS do Estado da Bahia.

BAHIA - Portaria nº 582 de 29/12/2000 – Dispõe sobre o fornecimento de senhas para utilização dos serviços oferecidos pela Sefaz através da Internet.

BRASIL – Constituição Federal de 05/10/1988

BRASIL – Medida Provisória nº 2.200-2 de 24/08/2001 – Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de tecnologia da Informação em autarquia e dá outras providências

BRASIL – Código Civil Brasileiro – Lei n º 3.071 de 01/01/1916

BRASIL – Código de Processo Civil - Lei nº 5.869 de 11/01/1973

BRASIL – Lei nº 8.935 de 18/11/1994 – Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais de registro.

BRASIL – Decreto nº 3.505 de 13/06/2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

BRASIL – Decreto nº 3.587 de 05/09/2000 – Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov, e dá outras providências.

BRASIL – Decreto nº 3.872 de 18/07/2001 – Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, sua Secretaria Executiva, sua Comissão Técnica Executiva e dá outras providências.

BRASIL – Decreto nº 3.996 de 31/10/2001 – Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

BRASIL – Portaria Interministerial MCT/MC n° 147 de 31/05/1995 – Cria o Comitê Gestor INTERNET Brasil

BRASIL – Portaria Interministerial MCT n° 148 de 31/05/1995 – Aprova a Norma 4/95 - Dispõe sobre o Uso de Meios da Rede Pública de Telecomunicações para acesso à Internet.

Multimeios

MICROSOFT. [CD-ROM] **Enciclopédia Encarta 2001**. Equipamento Mínimo: PC 133 Mhz; Sistema Windows 95; 24 MB RAM; Monitor Super VGA, 256 cores; Unidade de CD-ROM com velocidade quádrupla ou superior; Placa de som de 16 bits com alto-falantes ou fones de ouvido; Monitor Super VGA de 256 cores e resolução de 640 X 480 ou superior; Microsoft Mouse; Vídeo de barramento local com memória de vídeo de 1 MB ou superior.

Alexandre Alcantara da Silva

Graduado em Ciências Contábeis pela Fundação Visconde de Cairú – Salvador – BAHIA;

Concluinte do Curso de Pós-Graduação em Direito Tributário, pela Fundação Faculdade de Direito da UFBA;

Aluno do Curso de Pós-Graduação em Gestão Tributária – Universidade Salvador – UNIFACS;

Auditor Fiscal da Secretaria da Fazenda do Estado da Bahia, onde exerce a função de Coordenador de Fiscalização de Empresas de Grande Porte da Diretoria de Administração Tributária Sul.