UNIVERSIDADE FEDERAL DO PARANÁ

MARCIO PAPROSKI

SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA CERTIFICAÇÃO DIGITAL

CURITIBA
2008

MARCIO PAPROSKI

SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA CERTIFICAÇÃO DIGITAL

Monografia apresentada à disciplina Projeto de Pesquisa em Informação II do Curso de Gestão da Informação do Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná.

Orientador: Prof. Dr. Mauro José Belli

CURITIBA
2008

RESUMO

Apresenta a informação como recurso estratégico para as organizações. Relata sobre a segurança da informação e os principais conhecimentos que o gestor da informação precisa ter para atuar nesta área. Cita as principais normas e certificados sobre a segurança da informação. Apresenta a certificação digital como meio para garantir a privacidade, integridade e autenticidade das informações nas transações eletrônicas. Explica o processo de criptografia simétrica e assimétrica pela utilização de chaves públicas e privadas. Aborda os aspectos legais e tecnológicos referentes à certificação digital e os principais clientes do serviço que também atuam como autoridades certificadoras. Apresenta os resultados obtidos através de um questionário com um profissional da Receita Federal sobre a certificação digital para validação da pesquisa. Conclui que a certificação digital é um meio efetivo para garantir a segurança da informação nas transações eletrônicas e que o serviço de certificação digital deve ser ampliado e seu custo reduzido para que aumente o número de usuários.

Palavras-chave: Certificação digital. Informação. Segurança da informação.

ABSTRACT

It presents the information as a strategic resource for organizations. Reports on information security and the main knowledge that the manager of information need to act in this area. Cites the main standards and licenses on information security. It presents the digital certification as a means to ensure the privacy, integrity and authenticity of the information in electronic transactions. Explains the process of asymmetric and symmetric encryption through the use of public and private keys. It covers the legal aspects and technology relating to digital certification and the main customers of the service that also act as certification authorities. Presents the results from a questionnaire with a professional on the Federal Revenue digital certification for validation of the research. It concludes that the certification is an effective means to ensure information security in electronic transactions and that the digital certification service should be expanded and its low cost to increase the number of users.

Keywords: Digital certification, Information. Information security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABIN	-	Agência Brasileira de Inteligência
AC	-	Autoridade Certificadora
AC-JUS	-	Autoridade Certificadora da Justiça
AC PR	-	Autoridade Certificadora da Presidência da República
AC Raiz	-	Autoridade Certificadora Raiz
AR	-	Autoridade de Registro
CASNAV	-	Centro de Análises de Sistemas Navais
CCD	-	Centro de Certificação Digital
CDTC	-	Centro de Difusão de Tecnologia e Conhecimento
CEF	-	Caixa Econômica Federal
CEPESC	-	Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
CJF	-	Conselho da Justiça Federal
CNJ	-	Conselho Nacional de Justiça
COBIT	-	*Control objetives for information and related technology*
CSJT	-	Conselho Superior da Justiça de Trabalho
DOC	-	Documentos
e-Cac	-	Centro Virtual de Atendimento ao Contribuinte
e-CNPJ	-	Cadastro Nacional da Pessoa Jurídica eletrônico
e-Gov	-	Governo eletrônico
e-CPF	-	Cadastro de Pessoas Físicas eletrônico
FGTS	-	Fundo de Garantia do Tempo de Serviço
FINEP	-	Financiadora de Estudos e Projetos
GNU/GPL	-	GNU *General Public License*
ICP	-	Infra Estrutura de Chaves Públicas
ICP-Brasil	-	Infra Estrutura de Chaves Públicas Brasileira
IEC	-	*International Electrotechnical Commission*
ISO	-	*International Organization for Standardization*
ITA	-	Instituto Tecnológico da Aeronáutica
ITI	-	Instituto Nacional de Tecnologia da Informação
Módulo PAM	-	*Pluggable Authentication Modules*
MSC	-	Módulos de Segurança Criptográfica
RFB	-	Receita Federal do Brasil
RNP	-	Rede Nacional de Estudo e Pesquisa
SBP	-	Sistema de Pagamentos Brasileiro
SERASA	-	Centralização dos Serviços Bancários S/A
SERPRO	-	Serviço Federal de Processamento de Dados

SGC	-	*Server Gated Cryptography*
SPB	-	Sistema de Pagamentos Brasileiro
SRF	-	Secretaria da Receita Federal
SSL	-	*Secure Socket Layer*
STF	-	Supremo Tribunal Federal
STJ	-	Supremo Tribunal de Justiça
STM	-	Superior Tribunal Militar
TCP/IP	-	*Transmission Control Protocol/ Internet Protocol*
TSE	-	Tribunal Superior Eleitoral
TST	-	Tribunal Superior do Trabalho
UFSC	-	Universidade Federal de Santa Catarina
VTN	-	*VeriSign Trust Network*

SUMÁRIO

1 INTRODUÇÃO

O conhecimento tornou-se, hoje mais do que no passado, um dos principais fatores de superação de desigualdades, de agregação de valor, criação de emprego qualificado e de propagação do bem-estar. A nova situação tem reflexos no sistema econômico e político. A soberania e a autonomia dos países passam mundialmente por uma nova leitura e sua manutenção - que é essencial - depende nitidamente do conhecimento, da educação e do desenvolvimento científico e tecnológico.

Esta nova forma de organização e produção recebe o nome de Sociedade da Informação e o papel do gestor da informação é pensar e planejar estrategicamente, estruturar articulações políticas e analisar mercados e contextos. Para tal, exigem-lhe alto nível de mobilidade pessoal e profissional, para permiti-lo atuar não só como um empregado, mas como consultor e assessor, cuja competência estará igualmente sendo avaliada conforme seu grau de atualização, capacidade de empreendimento e criatividade.

Um dos grandes desafios estratégicos das organizações é proteger suas informações de toda e qualquer tipo de ameaça. A segurança da informação é uma área crescente que demanda novos profissionais para a proteção das informações de um modo geral.

A informação está presente em todos os setores das organizações e deve envolver todas as pessoas. Logo, a implantação de políticas de segurança da informação é extremamente necessária para uma boa gestão. Como forma de atender às necessidades referentes à segurança da informação e direcionar as grandes instituições foram criadas normas e certificados para o assunto.

As transações eletrônicas necessitam da adoção de mecanismos de segurança e a certificação digital é uma das tecnologias mais eficientes que provêem soluções confiáveis através da Internet, tornando-a um meio de comunicação alternativo e seguro para garantir uma maior agilidade, facilidade de acesso e substancial redução de custos.

Neste contexto a pesquisa demonstra o papel da certificação digital como recurso capaz de assegurar qualidade às informações, possibilitando utilizar a Internet como meio de comunicação alternativo e seguro para a disponibilização de diversos serviços.

1.1 PROBLEMA

É cada vez maior o número de invasões e acesso indevido de informações confidenciais no ambiente *Web*. A grande problemática está em como garantir a segurança da informação através da privacidade, integridade e autenticidade nas transações eletrônicas.

1.2 JUSTIFICATIVA

A segurança da informação é imprescindível para garantir o segredo do negócio das organizações e sua competitividade no mercado. Muitas organizações desconhecem os mecanismos de certificação digital e seus benefícios para garantir a qualidade das informações nas transações eletrônicas. Este trabalho visa, portanto, contribuir para a disseminação dos conhecimentos relativos à temática, de modo a subsidiar aqueles que necessitam agir em prol da segurança de suas informações.

1.3 OBJETIVOS

Este trabalho apresenta seus objetivos divididos em geral e específicos.

1.3.1 Objetivo Geral

O objetivo geral desta pesquisa é apresentar a certificação digital como um dos meios para garantir a segurança da informação nas organizações que se

utilizam da internet como meio para realizar transações envolvendo informações que necessitam garantia de qualidade nas dimensões de privacidade, integridade e autenticidade.

1.3.2 Objetivos Específicos

Para atingir o objetivo geral foram estabelecidos os seguintes objetivos específicos:

a) identificar e apresentar os principais conceitos envolvidos na temática segurança da informação;
b) analisar o papel do gestor da informação na temática;
c) apresentar as tecnologias disponíveis para a certificação digital;
d) realizar um estudo de caso na Receita Federal Brasileira envolvendo a certificação digital como meio para garantir a segurança da informação.

2 LITERATURA PERTINENTE

Na literatura pertinente serão apresentados os principais conceitos necessários para melhor compreensão da pesquisa. Este capítulo aborda aspectos relevantes sobre os temas de segurança da informação e certificação digital.

2.1 A INFORMAÇÃO

A informação tem um valor altamente significativo e pode representar grande poder para quem a possui, seja uma pessoa, ou uma instituição. Ela está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos financeiros, tecnologias etc. McGee e Prusak destacam que

> atualmente utilizar a informação como um recurso estratégico faz parte da gestão de negócios e é o diferencial no ambiente empresarial, tendo em vista que, a informação é um ativo presente em todos os departamentos e setores. Seja qual for o ramo de atividade e o interesse das organizações, estas tomam sua decisão baseando-se nas informações. No entanto, ao discutirmos o papel estratégico que a informação assume dentro de uma organização é preciso observar que a informação recebe ênfases diferentes de acordo com o ramo de atividade e o segmento econômico em que atuam, assumindo diferentes níveis de importância e valor entre as organizações (McGEE; PRUSAK; 1994, p. 26).

Sendo a informação um recurso estratégico, faz-se necessário compreender o ciclo de vida das informações dentro das organizações que, segundo Beal (2005, p. 5), envolve as seguintes etapas:

a) identificação das necessidades e dos requisitos - desenvolver serviços e produtos de informação para atender às necessidades interna e externa dos usuários, requer, fundamentalmente, identificar as necessidades de informação destes indivíduos;

b) obtenção - esta etapa compreende a obtenção de informações para suprir as necessidades identificadas na etapa anterior, levando-se em

consideração a necessidade de integridade dos dados coletados, ou seja, a sua é autenticidade e a confiabilidade de sua fonte;

c) tratamento - esta etapa é o processo de organização, formatação, estruturação, análise, síntese, apresentação e reprodução da informação, com a finalidade de deixá-la mais acessível aos usuários;

d) distribuição - a distribuição da informação possibilita sua disseminação a quem dela precisa;

e) uso - esta é uma das etapas mais importantes, pois não é a existência da informação que garante melhor resultado, e sim o uso que dela é feito;

f) armazenamento - o armazenamento permite o uso e o reuso da informação, sendo necessário assegurar sua conservação, incluindo-se aqui também o cuidado com as mídias utilizadas;

g) descarte – obedecendo-se as normas de política de descarte da empresa, quando uma informação se torna obsoleta ou perde a sua utilidade deve ser descartada. A exclusão de informações inúteis proporciona economia no armazenamento o que aumenta a eficiência na localização de informações, no entanto, este processo precisa ser realizado dentro das condições de segurança.

Neste particular, o gestor da informação conhece de forma aprofundada este ciclo de vida e o valor da informação bem administrada para as organizações, pois o aprendizado pertinente faz parte da sua formação acadêmica.

2.2 A SEGURANÇA DA INFORMAÇÃO

Segundo Barros (2007), a necessidade de implementação de medidas de segurança da informação tende a crescer cada vez mais. O valor da informação é importante para as empresas, que muitas vezes tem seu negócio e seu diferencial competitivo baseado unicamente em informações.

Garantir a privacidade, integridade e autenticidade da informação consistem basicamente em estabelecer políticas e controles de segurança, tendo como objetivo

a proteção das informações, controlando o risco de revelação ou alteração por pessoas não autorizadas.

O profissional da informação deve ser uma pessoa voltada a pesquisar, conhecer e aplicar as teorias de segurança em atividades destinadas exclusivamente para proteger as informações da organização.

A área de segurança da informação exige do profissional competências individuais, específicas e organizacionais.

Para o gestor da informação iniciar sua atuação na área deve ter conhecimento em dez áreas que podem ser aprofundados de acordo com sua especialização. Estas especialidades podem ser, segundo Neves (2007, p. 5):

a) arquitetura segura - conhecimento dos conceitos, princípios, estruturas e padrões utilizados para desenhar, programar e gerenciar um sistema computacional de forma segura;

b) controle de acesso - conhecimento do conjunto de mecanismos destinados a gerenciar o modo como as pessoas podem acessar e utilizar informações;

c) criptografia - conhecimento dos princípios, meios e métodos utilizados para implementar modelos criptográficos como ferramenta de proteção para a segurança das informações;

d) gestão de riscos - conhecimento das metodologias para identificar os riscos à segurança da informação, o dimensionamento do risco relacionado e o desenvolvimento e a administração de medidas de redução de risco;

e) legislação e investigação – conhecimento teórico e aplicado das leis e normas que estão relacionadas à segurança da informação;

f) planejamento (para continuidade dos negócios e recuperação de desastres) - conhecimento das metodologias relacionadas ao desenvolvimento de processos que garantam a continuidade e recuperação dos negócios de uma organização quando de uma parada inesperada;

g) segurança em aplicações - conhecimento do que é necessário fazer para criar ou administrar uma aplicação corporativa, de modo a respeitar os conceitos de confidencialidade, integridade e disponibilidade exigidos pela organização;

h) segurança em processos operacionais - conhecimento dos procedimentos que devem ser utilizados para administrar os níveis de

segurança em processos operacionais que sejam utilizados no manuseio das informações;

i) segurança em telecomunicações e redes de dados - conhecimento dos modelos de segurança que devem ser aplicados a uma rede de dados para garantir a manutenção dos níveis de segurança esperados;

j) segurança física e ambiental - conhecimento dos conceitos de segurança física e ambiental que devem ser utilizados como camada de proteção às informações.

De acordo com Starec, Gomes e Bezerra destacam que

> o gestor deve atuar de forma comprometida com os resultados da empresa atingindo as metas de *performance* de processos; metas de retorno dos investimentos; metas de risco; metas de confiabilidade e continuidade dos negócios (STAREC; GOMES; BEZERRA; 2005. p. 285).

A segurança da informação deve permear o planejamento estratégico auxiliando na tomada de decisão e permitindo o alcance das metas da organização.

> Ao descrever o cenário atual para o gerenciamento da segurança da informação, muitas literaturas apontam a necessidade e a importância de se alcançar um 'Modelo de Governança da Segurança da Informação'. Esse modelo deverá ser utilizado pelas organizações para que a Segurança da Informação não seja tratada apenas no âmbito tecnológico, mas reconhecida como parte integrante do planejamento estratégico das organizações no processo de tomada de decisão (BERNARDES et al, 2007, p. 3).

Dentre vários conceitos, Fontes (2006, p. 38) define que o gestor da informação é a pessoa que tem autoridade para liberar (ou negar) o acesso de qualquer usuário a uma determinada informação. A informação pertence à organização, mas é o gestor que operacionaliza sua liberação. A formalização do pedido e da deliberação da informação deverá ficar registrada e ser evidência para que, em qualquer tempo, possa-se saber quem autorizou determinado usuário a ter acesso a uma determinada informação. Proteger a informação significa garantir disponibilidade, integridade, privacidade, legalidade, auditabilidade e não repúdio de autoria.

É comum relacionar segurança da informação com a tecnologia da informação, entretanto as organizações se esquecem que é preciso zelar também pelas informações que estão em suporte físico. As pessoas desempenham um papel

crucial para a segurança da informação, portanto, aspectos humanos não podem ser descartados. Desta forma, aspectos físicos, lógicos e humanos precisam constar nas políticas de informações.

Para ingressar na área de segurança é necessário tomar conhecimento das normas e certificações existentes. Beal (2005, p. 30-36) afirma que as normas mais conhecidas e utilizadas nas organizações são:

a) ITIL (*It infrastructure library*) - conjunto de documentos desenvolvido pelo governo do Reino Unido visando o registro das melhores práticas na área de gestão de serviços de TI;

b) COBIT (*Control objetives for information and related technology*) - conjunto de diretrizes para a gestão e auditoria de processos de controles de TI, desenvolvido pela *Information System Audit and Control Association* (ISAC) e pelo *IT Governance Institute*;

c) ISO Guide 73 (*Risk management – vocabulary – guidelines for use in standards*) vocabulário que define 29 termos da Gestão de Riscos;

d) ISO/ IEC 13335 (*Guidelines for the management of IT security*) conjunto de diretrizes de gestão de segurança voltadas especificamente para a tecnologia da informação.

Como o mercado atingiu um nível de automação, de compartilhamento e de dependência de informação foi elaborada uma norma específica para a área de segurança da informação denominada BS7799, a qual deu origem à norma ISO/IEC 17799, que por sua vez deu origem à versão brasileira NBR/ISO17799, tradução fiel da norma internacional ISO. Esta tem o objetivo de definir um código de prática para a gestão da segurança da informação, através de um amplo conjunto de controles, dentre os quais Starec (2005, p. 300) destaca:

a) política de segurança - orientações e apoio para a implementação e manutenção de uma política de segurança;

b) segurança organizacional - recomendações para prover o estabelecimento de uma infra-estrutura para planejar e controlar a segurança da informação na organização;

c) classificação e controle dos ativos de informação - orientações sobre a realização de inventários dos ativos informacionais e atribuição de responsabilidades para manter a proteção adequada;

d) segurança em pessoas - orientações para a redução de riscos de erro humano, roubo fraude e uso indevido de instalações;

e) segurança física e do ambiente - orientações para prevenir acesso não autorizado, dano ou interferência dos recursos e instalações de processamento de informações;

f) gestão das operações e comunicações - orientações com vistas a garantir a operação correta e segura dos recursos de processamento da informação;

g) controle de acesso - orientações para o monitoramento e o controle de acesso à informação;

h) manutenção e desenvolvimento de sistemas - orientações para o uso de controles de segurança em todas as etapas do processo;

i) gestão da continuidade do negócio - orientações para que a organização neutralize as interrupções as atividades do negócio e proteção dos processos críticos contra falhas ou desastres;

j) conformidade - orientações para assegurar a conformidade dos sistemas com leis, regulamentações, políticas e normas internas de segurança.

O gestor da informação deve estar atento e em constante atualização sobre estas normas para garantir seu diferencial, principalmente no atual mercado de trabalho onde deve competir com os profissionais da área de Tecnologia da Informação.

2.3 A CERTIFICAÇÃO DIGITAL

O Instituto Nacional de Tecnologia da Informação (ITI) é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), sendo a primeira autoridade da cadeia de certificação eleita como Autoridade Certificadora Raiz (AC Raiz).

Segundo o ITI (2008) os computadores e a Internet são largamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto, estas transações eletrônicas necessitam

da adoção de mecanismos de segurança capazes de garantir autenticidade, privacidade e integridade às informações eletrônicas. A certificação digital é a tecnologia que provê estes mecanismos.

No cerne da certificação digital está o certificado digital, um documento eletrônico que contém o nome, um número público exclusivo denominado chave pública e muitos outros dados que identificam as pessoas para as pessoas e para os sistemas de informação. A chave pública serve para validar uma assinatura realizada em documento eletrônico.

A certificação digital tem trazido inúmeros benefícios para os cidadãos e para as instituições que a adotam. Com a certificação digital é possível utilizar a Internet como meio de comunicação alternativo para a disponibilização de diversos serviços com uma maior agilidade, facilidade de acesso e redução de custos. A tecnologia da certificação digital foi desenvolvida graças aos avanços da criptografia nos últimos 30 anos.

Para entender o processo de certificação digital é necessário compreender também como funciona o processo de criptografia. A palavra criptografia tem origem grega e significa a arte de escrever em códigos, escondendo a informação na forma de um texto incompreensível. A informação codificada é chamada de texto cifrado. O processo de codificação ou ocultação é chamado de cifragem, e o processo inverso, ou seja, obter a informação original a partir do texto cifrado chama-se decifragem.

A cifragem e a decifragem são realizadas por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa deve se comportar.

Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta é impossível decifrar um dado texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave.

Segundo o ITI (2008), existem dois tipos de criptografia: a simétrica e a assimétrica, também conhecida como criptografia de chave pública. A criptografia simétrica realiza a cifragem e a decifragem de uma informação através de algoritmos que utilizam a mesma chave, garantindo sigilo na transmissão e armazenamento de dados (FIGURA 1).

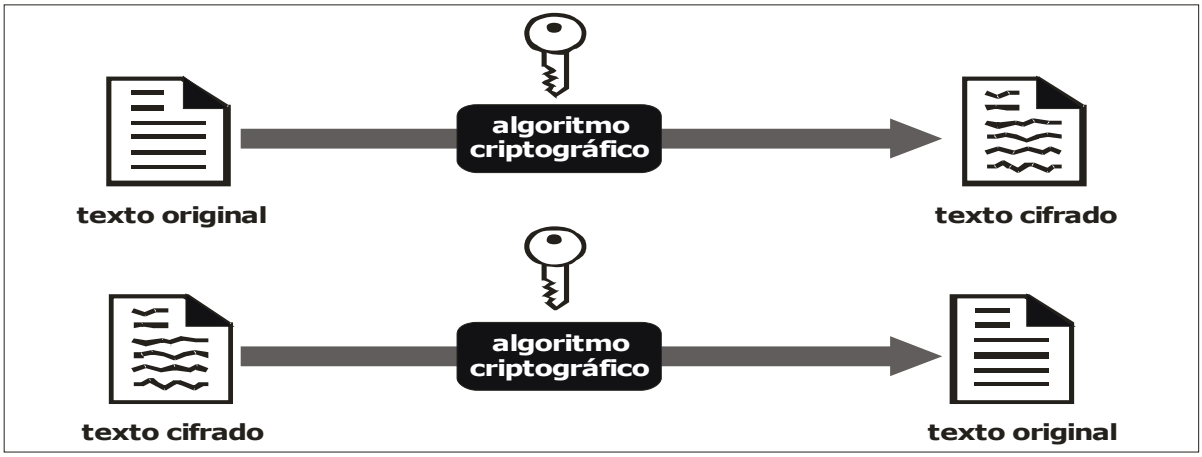

FIGURA 1 – PROCESSO DE CRIPTOGRAFIA SIMÉTRICA
FONTE : ADAPTADO DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (2008)

Como a mesma chave deve ser utilizada na cifragem e na decifragem, a chave deve ser compartilhada entre quem cifra e quem decifra os dados. O processo de compartilhar uma chave é conhecido como troca de chaves. A troca de chaves deve ser feita de forma segura, uma vez que todos que conhecem a chave podem decifrar a informação cifrada ou mesmo reproduzir uma informação cifrada.

A criptografia de chave pública, ou assimétrica, utiliza duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma seja revertida pela outra.

A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves. A chave pública é disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada correspondente. Os algoritmos criptográficos de chave pública permitem garantir tanto a confidencialidade quanto a autenticidade das informações por eles protegidas. O emissor que deseja enviar uma informação sigilosa deve utilizar a chave pública do destinatário para cifrar a informação. Para isto é importante que o destinatário disponibilize sua chave pública, utilizando, por exemplo, diretórios públicos acessíveis pela Internet (FIGURA 2).

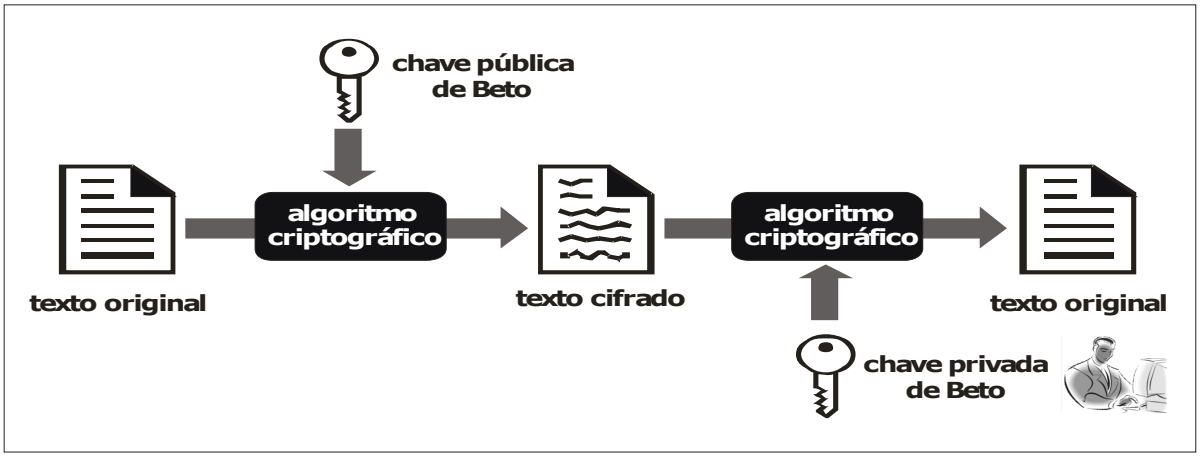

FIGURA 2 – PROCESSO DE CRIPTOGRAFIA ASSIMÉTRICA
FONTE : ADAPTADO DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (2008)

O sigilo ao acesso é garantido, já que somente o destinatário que possui a chave privada conseguirá desfazer a operação de cifragem, ou seja, decifrar e recuperar as informações originais. Como observamos para Alice compartilhar uma informação de forma secreta com Beto, ela deve cifrar a informação usando a chave pública de Beto. Somente Beto pode decifrar a informação pois somente Beto possui a chave privada correspondente.

No processo de autenticação, as chaves são aplicadas no sentido inverso ao da confidencialidade. O autor de um documento utiliza sua chave privada para cifrá-lo de modo a garantir a autoria em um documento ou a identificação em uma transação. Esse resultado só é obtido porque a chave privada é conhecida exclusivamente por seu proprietário, esse processo também é conhecido como assinatura digital (FIGURA 3).

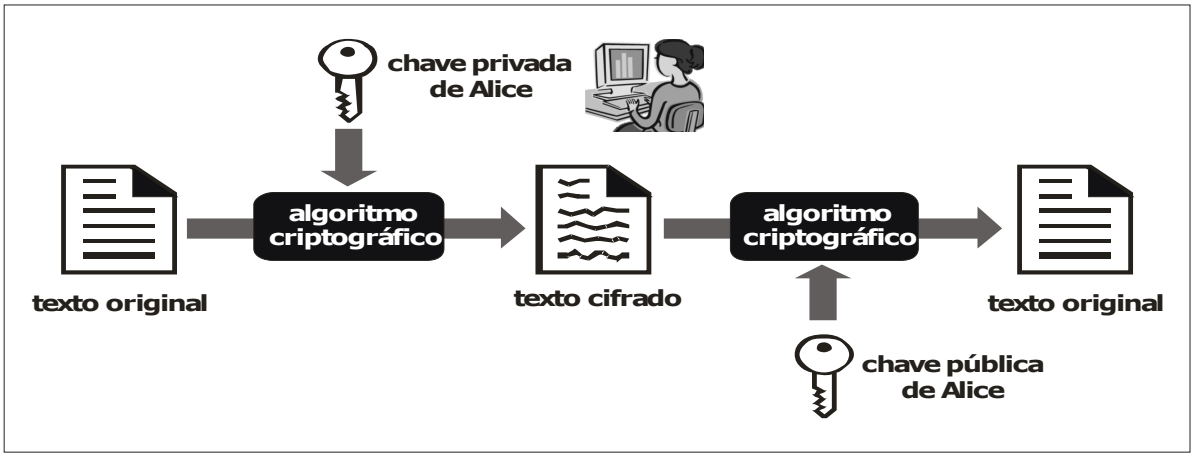

FIGURA 3 – PROCESSO DE ASSINATURA DIGITAL
FONTE : ADAPTADO DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (2008)

Assim, se Alice cifrar uma informação com sua chave privada e enviar para Beto, ele poderá decifrar esta informação, pois tem acesso à chave pública de Alice. Além disto, qualquer pessoa poderá decifrar a informação, uma vez que todos conhecem a chave pública de Alice. Por outro lado, o fato de ser necessário o uso da chave privada de Alice para produzir o texto cifrado caracteriza uma operação que somente Alice tem condições de realizar, garantindo-se que efetivamente a origem da informação é realmente quem diz ser, para o nosso exemplo, Alice.

2.3.1 Aspectos legais

Ao abordar aspectos legais no âmbito do Brasil, não se pode deixar de mencionar a Medida Provisória nº 2.200-2 (BRASIL, 2001), disponível no Anexo A, que institui a ICP-Brasil, transforma o ITI em autarquia, e dá outras providências.

Segundo a ICP-Brasil (2008), a instituição foi criada a partir da percepção do Governo Federal da importância de se regulamentar as atividades de certificação digital no país, denotando maior segurança nas transações eletrônicas e incentivando a utilização da Internet como meio para a realização de negócios.

A ICP-Brasil é composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras, composta pela Autoridade Certificadora Raiz (AC Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de Registro (AR).

A função de autoridade gestora de políticas é exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

Obter uma assinatura digital não é algo tão simples. Primeiro é necessário procurar uma entidade que faça esse serviço, isto é, deve-se procurar uma AC que tem a função de verificar a identidade de um usuário e associar a ele uma chave. Essas informações são, então, inseridas em um documento conhecido como certificado digital.

Um certificado digital contém a chave pública do usuário e os dados necessários para informar sua identidade. Esse certificado pode ser distribuído na Internet. Com isso, uma pessoa ou instituição que queira comprovar a assinatura digital de um documento pode obter o certificado digital correspondente. É válido saber que certificados digitais não são usados apenas em conjuntos com assinaturas digitais.

É importante frisar que a transmissão de certificados digitais deve ser feita através de uma conexão segura, como as que usam o protocolo *Secure Socket Layer* (SSL), que é próprio para o envio de informações criptografadas.

Como dito anteriormente, um certificado digital é um documento eletrônico que contém as informações da identificação de uma pessoa ou de uma instituição. Esse documento deve ser solicitado a uma AC ou ainda a uma AR que tem a função de solicitar certificados a uma AC.

Para que um certificado seja válido, é necessário que o interessado tenha a chave pública da AC para comprovar que aquele certificado foi, de fato, emitido por ela. A questão é que existem inúmeras ACs espalhadas pelo mundo e fica, portanto, inviável ter a chave pública de cada uma.

A solução encontrada para esse problema foi a criação de "ACs supremas" (ou "ACs-Raiz"), ou seja, instituições que autorizam as operações das ACs que emitem certificados a pessoas e empresas. Esse esquema é conhecido como Infra-estrutura de Chaves Públicas (ICP) ou, em inglês, *Public Key Infrastructure* (PKI).

No Brasil, a ICP-Brasil controla seis ACs: a Presidência da República, a Receita Federal do Brasil (RFB), o Serviço Federal de Processamento de Dados (SERPRO), a Caixa Econômica Federal (CEF), a Centralização dos Serviços Bancários S/A (SERASA) e a CertiSign. Isso significa que, para que tenha valor legal diante do governo brasileiro, uma dessas instituições deve prover o certificado.

Porém, para que isso seja feito, cada instituição pode ter requisitos e custos diferentes para a emissão, uma vez que cada entidade pode emitir certificados para finalidades distintas. E isso se aplica a qualquer AC no mundo.

Qualquer instituição pode criar uma ICP, independente de seu porte. Por exemplo, se uma empresa criou uma política de uso de certificados digitais para a troca de informações entre a matriz e suas filiais, não vai ser necessário pedir tais certificados a uma AC controlada pela ICP-Brasil. A própria empresa pode criar sua ICP e fazer com que um departamento das filiais atue como AC ou AR, solicitando ou emitindo certificados para seus funcionários.

Em relação aos custos para emitir um certificado digital, eles variam de acordo com a empresa certificadora, com o nível de segurança oferecido e com o tipo de portabilidade. Deve-se consultar os sítios de cada AC para obter os preços.

Segundo o ITI (2008) a Estrutura Normativa da ICP-Brasil é um documento que visa oferecer uma explicação sobre como são organizados e criados os documentos legislativos da Infra-Estrutura de Chaves Públicas no Brasil. Por meio dela, é possível compreender a organização e a hierarquia da ICP-Brasil dentro do sistema normativo interno. A estrutura normativa ICP-Brasil compõe-se de:

a) Medida Provisória 2.200-2;
b) decretos;
c) resoluções do Comitê Gestor da ICP-Brasil;
d) instruções normativas da AC Raiz;
e) e documentos complementares.

A Medida Provisória nº 2.200-2 (BRASIL, 2001) aborda os seguintes itens:

a) atribuição de valor legal às assinaturas digitais geradas com chave privada associada ao certificado digital;
b) modelo com Autoridade Certificadora Raiz única;
c) exigência de identificação presencial do titular para obtenção do certificado;
d) vinculação da entidade executora diretamente à Casa Civil da Presidência da República, como forma de garantir apoio político e orçamentário a longo prazo.

O Comitê Gestor da ICP-Brasil estabelece diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e define níveis da cadeia de certificação. Também atualiza, ajusta e revisa os

procedimentos e as práticas estabelecidas para a ICP-Brasil, garante sua compatibilidade e promove a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Para emanar essas diretrizes e normas, a ICP-Brasil utiliza Decretos, Resoluções, Instruções Normativas e documentos (ANEXO B), que são analisados pelos membros da Comissão Técnica e do Comitê Gestor.

A Resolução n° 33, de 21 de outubro de 2004, concedeu à AC-Raiz da ICP-Brasil a competência de criar instruções normativas com o objetivo de suplementar as normas do Comitê Gestor. Essa medida visou assegurar maior rapidez e objetividade às decisões da AC-Raiz em relação à aplicação das normas do Comitê Gestor, situando-as na proximidade dos fatos, pessoas ou problemas a atender. As instruções normativas também são publicadas no Diário Oficial da União e possuem numeração seqüencial, reiniciando-se a cada ano.

Segundo o ITI (2008), até abril de 2006, as resoluções e instruções normativas traziam, em seu próprio corpo, o conteúdo técnico a que se referiam. Atualmente as resoluções são sucintas, limitando-se a aprovar documentos em anexo, esses sim contendo as diretrizes técnicas a serem observadas.

Tais documentos são conhecidos por DOCICPnn. Possuem controle de versão e qualquer alteração deve sempre ser aprovada pelo Comitê Gestor da ICP-Brasil, por resolução. Para cada alteração em DOCICPnn, deve ser adotado um novo número de versão. Uma nova versão consiste num documento completo, contendo todo o texto da versão anterior mais as modificações aprovadas.

Caso necessário, tais documentos podem ser suplementados por outros, aprovados pela AC-Raiz por meio de instruções normativas e que recebem a nomenclatura DOCICPnn.mm

Além disso, formulários, modelos e outros elementos que podem necessitar de alterações mais freqüentes, sem prejuízo ao conteúdo das normas, foram separados do corpo dos documentos, criando-se para eles a categoria de Adendos denominados ADEICP.

Existe uma categoria específica de documentos para o processo de homologação denominado de Manuais de Condutas Técnicas classificados pela sigla MCT.nn, que detalha os requisitos técnicos que os dispositivos devem atender para receber o selo de homologação da ICP-Brasil, os materiais a depositar para análise e o rol de testes que serão realizados no material.

Os processos de certificação digital da RFB encontram-se na Instrução Normativa SRF nº 580, de 12 de dezembro de 2005 (ANEXO C) no qual fica instituído, no âmbito da Secretaria da Receita Federal (SRF), o Centro Virtual de Atendimento ao Contribuinte (e-CAC), com o objetivo de propiciar o atendimento aos contribuintes de forma interativa, por intermédio da Internet, no endereço eletrônico <http://www.receita.fazenda.gov.br>.

O e-CAC utiliza tecnologia que certifica a autenticidade dos emissores e destinatários dos documentos eletrônicos, com segurança quanto a sua privacidade e inviolabilidade.

O acesso ao e-CAC é efetivado mediante a utilização de certificados digitais Cadastro de Pessoas Físicas eletrônico (e-CPF) ou Cadastro Nacional da Pessoa Jurídica eletrônico (e-CNPJ), observado o disposto no art. 1º do Decreto 4.414, de 7 de outubro de 2002.

2.3.2 Aspectos tecnológicos

A revolução digital tem um agente universal chamado de *software*, que define e dá sentido ao ciberespaço, gerando novas culturas e dependências. Todo esse poder traz riscos e responsabilidades. A economia de escala nos seus processos de arquitetura, produção e negócio favorecem os monopólios, podendo implicar a dependência de formatos e padrões proprietários. Assim, a escolha e a adoção coletiva de formatos e padrões digitais para controlar o alcance, a natureza e o poder desta intermediação são de grande responsabilidade.

Segundo o ITI (2008) o papel social do *software* tanto pode promover quanto pode reprimir representações das liberdades humanas, submissas às liberdades do mercado na nova economia. O *software* livre, com seu código aberto e propriedade coletivizada, explora peculiaridades do ciberespaço para nos oferecer alternativas socialmente equilibradas, globalmente eficientes e sadias aos desafios da arquitetura, produção e negócio do *software*. Ele é fruto da consciência cidadã, que atua na dimensão social desse poder intermediador da inteligência e vontade humanas.

Provas de seu sucesso estão no conjunto de protocolos abertos para intercomunicação entre redes - o alicerce *Transmission Control Protocol/ Internet Protocol* (TCP/IP) da Internet, no sistema operacional GNU/Linux e em outros. Na economia do ciberespaço, a cooperação pode ter custo/benefício superior ao da competição. Os ganhos são amplificados pela estabilidade, agilidade e confiabilidade do seu produto, num mercado livre de pressões monopolistas, vendas casadas, forçadas ou precipitadas.

Consciente da importância do papel do Estado, tanto na intermediação no mercado de *software* quanto na construção de uma sociedade mais justa e solidária, o ITI, através do Centro de Difusão de Tecnologia e Conhecimento (CDTC), propõe a união de esforços entre os setores público e privado e as universidades, com objetivo de ampliar o conhecimento da sociedade no uso do *software* livre.

Segundo o CDTC (2008) este projeto considera que os recursos disponibilizados serão de intenso impacto social e ampliam as liberdades individuais com o acesso da tecnologia pela sociedade. Considera também que esses recursos permitem que a economia dos gastos despendidos anualmente em licenças proprietárias de *softwares* garanta o aquecimento de um mercado emergente e facilite o acesso e a apropriação tecnológica pelo próprio mercado nacional.

Segundo o ITI (2008), o objetivo inicial do projeto foi desenvolver uma nova plataforma criptográfica para a AC-Raiz da ICP-Brasil denominado Programa João de Barro. Essa plataforma, também conhecida por módulo de segurança, é composta por *hardware* e *software* que foram desenvolvidos com tecnologia nacional e são responsáveis pelo processo de emissão e revogação do certificado da AC-Raiz, além de gerenciar os certificados das Autoridades Certificadoras de primeiro nível.

Com o desenvolvimento do projeto possibilitou que entre 2003 e 2004, fossem firmados convênios entre o ITI e as seguintes instituições: Centro de Análises de Sistemas Navais (CASNAV), Universidade Federal de Santa Catarina (UFSC), Instituto Tecnológico da Aeronáutica (ITA), Agência Brasileira de Inteligência (ABIN), Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC), além da Financiadora de Estudos e Projetos (FINEP).

Cada uma dessas entidades desempenhou um papel diferente para a consolidação do projeto. Ao longo de 2005, o CASNAV especificou os requisitos do Programa João de Barro os quais foram entregues às outras instituições para que

cada uma desenvolvesse os módulos de acordo com sua área de competência. Entre 2005 e agosto de 2006, o projeto do *software* foi projetado e consolidado pela UFSC. Em fevereiro de 2006, o ITA iniciou ao projeto do *hardware*. A FINEP, por sua fez, foi responsável pelo financiamento de 20% da iniciativa que, também, contou com aporte financeiro direto do ITI.

Segundo o ITI (2008), no final de 2007, dada a necessidade imediata de emissão do novo par de chaves da ICP-Brasil, foi firmado um acordo de cooperação com a Rede Nacional de Estudo e Pesquisa (RNP) para a utilização do *hardware* desenvolvido por essa instituição. Os projetos de *hardware* da RNP com o do ITA serão fundidos. Por último, coube a ABIN/CEPESC desenvolver o gerador aleatório que foi repassado ao ITA.

Até o início de 2008, o investimento total do projeto foi de, aproximadamente, R$ 5 milhões. Para completar o projeto, foram investidos mais R$ 5 milhões na instalação de um ambiente seguro com sala cofre destinado a ações como testes de integração dos produtos *Server Gated Cryptography* (SGC) e Módulos de Segurança Criptográfica (MSC) em desenvolvimento no escopo do Programa João de Barro, com vistas a assegurar a sua qualidade e confiabilidade para posterior entrada em operação.

A sala cofre é um ambiente físico dispondo de equipamentos para a proteção da Autoridade Certificadora e suas Chaves Criptográficas. Composto, basicamente, por infra-estrutura predial, grupo gerador para suprimento de energia elétrica, sistema de prevenção e proteção contra incêndio, sala para armazenamento seguro de documentos e dados e núcleo de sala cofre construído na forma de célula estanque, imune a infiltrações e inundações. Todo este ambiente segue rigorosamente as normas da ICP-Brasil e serve para a realização de testes, além de auxiliar na formação de profissionais para a área.

Em 28 de maio de 2008, o Comitê Gestor da ICP-Brasil autorizou o ITI a gerar o novo par de chaves da ICP-Brasil utilizando a plataforma João de Barro, e, assim, emitir o novo certificado da AC-Raiz. O Comitê aprovou, também, a versão atualizada da Declaração de Práticas de Certificação (DPC) que estabelece os procedimentos que a própria AC Raiz deve adotar.

Até 30 de novembro de 2008, toda a cadeia de certificação ICP-Brasil estará renovada, com a emissão dos certificados em uma plataforma desenvolvida com tecnologia totalmente nacional e plenamente auditável.

Por meio da Portaria nº 41, publicada no Diário Oficial da União dia 28/06/2005, o ITI coloca à disposição da sociedade, três *softwares* desenvolvidos com licença da GNU *General Public License* (GNU/GPL).

Pode-se observar na referida Portaria que o licenciamento de programas de computador em regime livre é uma forma de compartilhamento dos bens públicos. Além disso, o uso desse bem por um cidadão não exclui a utilização do mesmo recurso pelos demais, inserindo essa iniciativa no contexto da colaboração solidária e de participação no desenvolvimento da inteligência coletiva.

Os programas disponibilizados facilitam a utilização da certificação digital no mundo Linux. Assim, assinar contratos digitalmente, encriptar/desencriptar mensagens ou dados e se relacionar com o fisco pela internet, são algumas das iniciativas que ficaram mais fáceis com o desenvolvimento dos três *softwares*.

Esses programas de computador são *softwares* de livre distribuição, o que significa que poderão e deverão sofrer os ajustes e as melhorias que outros órgãos do governo, empresas e usuários entendam ser importantes. As funcionalidades e o projeto inicial foram desenvolvidos pelo ITI, os códigos foram feitos por três empresas contratadas por meio de licitação pública. A Certisign desenvolveu o Assinador Digital e coube a Módulo Security, uma das mais importantes empresas da área de segurança da informação no Brasil e uma das maiores da América Latina, a responsabilidade sobre o Módulo PAM (*Pluggable Authentication Modules* ou Módulos de Autenticação Plugáveis/Modulares) e o Chaveiro Digital.

Apesar da existência de *softwares* livres, a concorrência entre as empresas no mercado da certificação digital é grande e a oferta de *softwares* pagos para garantir a autenticidade, integridade, privacidade e não-repúdio vem crescendo dia-a-dia através do desenvolvimento de novas tecnologias e serviços.

2.3.3 Clientes

Entre os principais clientes da certificação digital podemos citar a Presidência da República, o SERPRO, a Caixa Econômica Federal, o SERASA, a Receita Federal do Brasil, Certsign, a Autoridade Certificadora da Justiça, a Imprensa Oficial, o Banco Itaú, o Bradesco, a Microsoft, o Bank of America, o Citibank, o Cisco

Systems, o Departamento de Defesa dos EUA, o Deutsche Bank, o Banco Ibi, a Samsung, a Texas Instruments, a Receita Federal Americana, a VIVO, a Telefônica, a BrasilTelecom e a Embratel. Segue abaixo a descrição das seis ACs clientes e usuárias da certificação digital:

a) SERPRO

Segundo o ITI (2008) o SERPRO foi a primeira autoridade certificadora credenciada pela ICP-Brasil. A empresa busca desde a criação de seu Centro de Certificação Digital (CCD), em 1999, divulgar o uso dessa tecnologia para os vários segmentos com que trabalha.

O SERPRO é uma empresa pública, vinculada ao Ministério da Fazenda. Foi criada no dia 1º de dezembro de 1964, pela Lei nº 4.516, com o objetivo de modernizar e dar agilidade a setores estratégicos da Administração Pública brasileira. A Empresa, cujo negócio é a prestação de serviços em Tecnologia da Informação e Comunicações para o setor público, é considerada uma das maiores Organizações do setor, na América Latina.

O SERPRO desenvolve programas e serviços que permitem maior controle e transparência sobre a receita e os gastos públicos, além de facilitar a relação dos cidadãos com o governo. Dentre as várias soluções desenvolvidas com essas características destacam-se a declaração do Imposto de Renda via Internet (ReceitaNet), a nova Carteira Nacional de Habilitação, o novo Passaporte Brasileiro e os sistemas que controlam e facilitam o comércio exterior brasileiro (Siscomex).

Segundo o SERPRO (2008) O mercado de atuação da Empresa é o de finanças públicas, composto pelo Ministério da Fazenda com suas secretarias e demais órgãos, correspondendo a 85,2% do volume de negócios da Empresa. Outro segmento igualmente importante são as ações estruturadoras e integradoras da Administração Pública Federal cuja gestão e articulação compete ao Ministério do Planejamento, Orçamento e Gestão.

Ao longo de seus 43 anos, o SERPRO consolidou-se como uma referência, aprimorando e desenvolvendo tecnologias utilizadas por órgãos do setor público brasileiro, as quais foram incorporadas à vida dos cidadãos.

A empresa investe no desenvolvimento de soluções tecnológicas em *Software Livre*, como uma política estratégica que permite otimizar os recursos públicos,

incentivar o compartilhamento de conhecimento e estimular a cooperação entre as esferas federal, estadual, municipal, iniciativas do segmento acadêmico e sociedade.

O SERPRO, também, desenvolve projetos e programas que contemplem as questões sociais de acessibilidade e inclusão digital, e apóia as políticas do governo federal.

b) CAIXA ECONÔMICA FEDERAL

Segundo o ITI (2008) a CEF atualmente única instituição financeira credenciada como Autoridade Certificadora ICP-Brasil - utiliza, desde 1999, a tecnologia de certificação digital para prover a comunicação segura na transferência de informações referentes ao Fundo de Garantia do Tempo de Serviço (FGTS) e à Previdência Social, dentro do projeto Conectividade Social.

Segundo a CEF (2008) ela optou pela adoção da certificação digital a fim de oferecer aos seus clientes uma tecnologia de autenticação para transações eletrônicas que garanta a identificação inequívoca das partes envolvidas. Além disso, a certificação permite que o cliente assine digitalmente sua transação ou contrato, não sendo mais necessários sua presença ou o reconhecimento legal do documento.

Isso significa que a CEF não está garantindo apenas a segurança das transações no seu ambiente, mas expandindo seu serviço de Certificação Digital para o mercado com a qualidade e competência de uma das maiores instituições financeiras do país.

Com a Identidade Digital CAIXA, as empresas que utilizam serviços como FGTS, por exemplo, podem receber a Certificação e realizar as operações com muito mais tranqüilidade e segurança, além de possibilitar a melhoria dos processos eletrônicos.

c) SERASA

Segundo o ITI (2008) para a SERASA, a tecnologia de certificação digital é o instrumento que viabiliza a inserção dos diversos agentes econômicos e cidadãos brasileiros em uma sociedade digital.

A SERASA fornece a segurança dos certificados digitais para quase todos os grupos financeiros participantes do Sistema de Pagamentos Brasileiro (SPB).

A SERASA, uma das maiores empresas do mundo em análises e informações para decisões de crédito e apoio a negócios, atua com completa cobertura nacional e internacional, por meio de acordos com as principais empresas de informações de todos os continentes.

Segundo a SERASA (2008) ela está presente em todas as capitais e principais cidades do País, totalizando 140 pontos estratégicos. A SERASA conta com um quadro de pessoal com aproximadamente 2.500 profissionais e a retaguarda de um amplo centro de telemática. Como maior banco de dados da América Latina sobre consumidores, empresas e grupos econômicos, a Serasa participa da maioria das decisões de crédito e de negócios tomadas no Brasil, respondendo on-line/real-time, a 4 milhões de consultas por dia, demandadas por 400 mil clientes diretos e indiretos.

d) RECEITA FEDERAL DO BRASIL

Segundo o ITI (2008) a RFB disponibiliza uma grande quantidade de serviços na web, com o objetivo de simplificar ao máximo a vida dos contribuintes e facilitar o cumprimento espontâneo das obrigações tributárias. Por meio do serviço Receita222, a RFB presta atendimento aos contribuintes de forma interativa, via Internet, com uso de certificados digitais, garantindo a identificação inequívoca dos usuários.

A RFB é um órgão específico, singular, subordinado ao Ministério da Fazenda, exercendo funções essenciais para que o Estado possa cumprir seus objetivos. É responsável pela administração dos tributos de competência da União, inclusive os previdenciários, e aqueles incidentes sobre o comércio exterior, abrangendo parte significativa das contribuições sociais do País. Auxilia, também, o Poder Executivo Federal na formulação da política tributária brasileira, além de trabalhar para prevenir e combater a sonegação fiscal, o contrabando, o descaminho, a pirataria, a fraude comercial, o tráfico de drogas e de animais em extinção e outros atos ilícitos relacionados ao comércio internacional.

e) CERTISIGN

Segundo o ITI (2008) com o apoio da Certisign, empresa fundada em 1996 com foco exclusivamente no desenvolvimento de soluções de certificação digital para o mercado brasileiro, importantes instituições vêm adotando a tecnologia nas mais diversas formas.

Segundo a Certisign (2008) ela proporciona a seus clientes um ambiente digital mais seguro, ajudando-os a proteger informações, reduzir a fraude digital e o roubo de identidade. Fundada em 1996, a Certisign é líder no mercado brasileiro de certificação digital e responsável por mais de 70% dos certificados emitidos no país. Entre seus usuários estão contribuintes da Receita Federal, profissionais liberais, cerca de 80% dos sites de comércio eletrônico, a quase totalidade do setor bancário, empresas de todos os portes e entidades governamentais. Uma das três primeiras Autoridades Certificadoras do mundo a emitir certificados digitais e única no mercado brasileiro credenciada para operar em múltiplas hierarquias, como ICP-Brasil, VeriSign Trust Network (VTN) e hierarquia privada. A Certisign é parceira da Intel e VeriSign e tem a maior rede de distribuição de certificados do Brasil.

f) AUTORIDADE CERTIFICADORA DA JUSTIÇA

Segundo o ITI (2008) a Autoridade Certificadora da Justiça (AC-JUS) é gerenciada por um Comitê Gestor que, a partir de outubro de 2005, é composto por representantes do Supremo Tribunal Federal (STF), Supremo Tribunal de Justiça (STJ), Tribunal Superior do Trabalho (TST), Tribunal Superior Eleitoral (TSE), Superior Tribunal Militar (STM), Conselho Nacional de Justiça (CNJ), Conselho da Justiça Federal (CJF) e o Conselho Superior da Justiça de Trabalho (CSJT). Trata-se da primeira autoridade certificadora do Poder Judiciário no mundo. Sua implementação possibilitou a definição de regras e perfis de certificados, específicos para aplicações do Judiciário e resulta da necessidade crescente de transpor a mesma credibilidade e segurança existentes hoje no "mundo do papel" para o "mundo digital".

Segundo a AC-JUS (2008) ela foi criada após a edição da Medida Provisória nº 2.200-2 (BRASIL, 2001), que dá validade legal aos documentos assinados com certificados digitais emitidos dentro da hierarquia da ICP-Brasil. O Conselho da

Justiça Federal decidiu pela criação de uma Autoridade Certificadora para possibilitar a definição de regras e perfis de certificados, específicos para aplicações do Judiciário.

A AC-JUS alavancou definitivamente a implantação da Certificação Digital no Judiciário, com o desenvolvimento de aplicações para comunicação e troca de documentos, agora com validade legal, viabilizando dessa forma o advento do Processo Judicial Eletrônico.

g) IMPRENSA OFICIAL

Segundo o ITI (2008) a Imprensa Oficial é a Autoridade Certificadora Oficial do Estado de São Paulo e está credenciada e preparada para oferecer produtos e serviços de certificação digital para os poderes executivo, legislativo e judiciário, incluindo todas as esferas da administração pública, direta e indireta, nos âmbitos federal, estadual e municipal.

O Decreto 48.599 de 12 de abril de 2004, instituiu a Imprensa Oficial do Estado como Autoridade Certificadora Oficial do Estado de São Paulo tendo como AR preferencial o Banco Nossa Caixa.

h) AUTORIDADE CERTIFICADORA DA PRESIDÊNCIA DA REPÚBLICA

Segundo o ITI (2008) a Autoridade Certificadora da Presidência da República (ACPR) foi criada em abril de 2002, por uma iniciativa da Casa Civil, no âmbito do governo eletrônico (e-Gov) e tem como objetivo emitir e gerir certificados digitais das autoridades da Presidência da República, ministros de estado, secretários-executivos e assessores juridicos que se relacionem com a Presidência da República.

3 METODOLOGIA

A pesquisa caracterizou-se primeiramente pela coleta de informações referentes à segurança da informação e certificação digital e apresentou através de um estudo de caso, um exemplo prático sobre certificação digital.

3.1 CARACTERIZAÇÃO DA PESQUISA

Esse trabalho adotou o planejamento operacional baseado em metodologia exploratória de caráter bibliográfico e documental. Conforme Gil (1991, p. 45-46), pesquisas exploratórias são aquelas que têm como objetivo proporcionar mais familiaridade ao problema objetivando aprimorar idéias e a descoberta de intuições. Foi realizado um estudo de caso, que, conforme Fachin (2002, p. 42-43), é estudo intensivo que leva em consideração, principalmente, a compreensão, como um todo, do assunto investigado, e que pode ser auxiliado pela aplicação de questionários, formulários ou entrevistas. Sua principal função é a explicação sistemática dos fatos que ocorrem no contexto social e que geralmente se relacionam com multiplicidade de variáveis.

3.2 PROCEDIMENTOS METODOLÓGICOS

A pesquisa procurou verificar a relevância da segurança da informação através da certificação digital, possibilitando determinar aspectos importantes para as empresas garantirem a segurança de suas informações, a competitividade e a credibilidade no mercado.

Para conhecer sobre a certificação digital foram realizadas leituras referentes ao tema e um estudo de caso na Receita Federal Brasileira para constatar sua relevância e importância na organização.

O instrumento para a coleta de dados foi o questionário aplicado com Reinaldo Cesar Moscatto, Superintendente Adjunto da 9ª Receita Federal, com questões abertas, no qual foram identificados aspectos relevantes sobre a certificação digital e a organização.

O resultado do questionário foi à comparação das informações obtidas com a literatura pertinente.

Como resultado foi elaborado o relatório final da pesquisa.

4 ESTUDO DE CASO

A organização escolhida para a realização da pesquisa foi a Superintendência Regional da Receita Federal da 9ª Região Fiscal situada na cidade de Curitiba, estado do Paraná.

4.1 AMBIENTE DE PESQUISA

A Secretaria da Receita Federal do Brasil é um órgão específico, singular, subordinado ao Ministério da Fazenda, exercendo funções essenciais para que o Estado possa cumprir seus objetivos. É responsável pela administração dos tributos de competência da União, inclusive os previdenciários, e aqueles incidentes sobre o comércio exterior, abrangendo parte significativa das contribuições sociais do País. Auxilia, também, o Poder Executivo Federal na formulação da política tributária brasileira, além de trabalhar para prevenir e combater a sonegação fiscal, o contrabando, o descaminho, a pirataria, a fraude comercial, o tráfico de drogas e de animais em extinção e outros atos ilícitos relacionados ao comércio internacional.

A Secretaria da Receita Federal do Brasil é composta por unidades centrais e unidades descentralizadas, distribuídas por todo o território nacional, abrangendo uma área de 8,5 milhões de quilômetros quadrados.

Sua missão resume-se em:

a) prover o Estado de recursos para garantir o bem-estar social;
b) prestar serviços de excelência à sociedade;
c) prover segurança, confiança e facilitação para o comércio internacional.

Como visão de futuro, a SRF quer ser uma organização modelo de excelência em gestão, referência nacional e internacional em administração tributária e aduaneira.

Seus valores são:

a) respeito ao cidadão;
b) integridade;
c) lealdade com a Instituição;

d) legalidade;
e) profissionalismo.

4.2 ANÁLISE DOS RESULTADOS

A análise dos resultados é produto do questionário (APÊNDICE A) realizado na Receita Federal Brasileira.

De acordo com o questionário aplicado a informação tem papel fundamental para a Receita Federal do Brasil, por tratar-se de um dos principais insumos com que trabalha a Instituição, tanto no relacionamento com os contribuintes (fornecimento/coleta de informações) quanto no tratamento de informações para realização das atividades de administração tributária sob sua responsabilidade. Isso confirma o que a literatura aponta quando diz que a informação é um diferencial e ativo presente em todas as organizações. Assim, a RFB dá atenção especial tanto à área de Tecnologia da Informação (TI) quanto à área de Segurança da Informação (SI) visando garantir o sigilo das informações com que trabalha.

O Superintendente Adjunto responde que dentro da RFB, para atuar no processo de certificação digital interna, o servidor público recebe treinamento especial e deve seguir rigidamente as normas emitidas pela Instituição, todas baixadas com estrita observância às normas do ITI que é a Ac Raiz da ICP-Brasil. Isso permite observar que além das competências profissionais, o profissional que pretende atuar na área de certificação digital deve estar em constante especialização e observar as principais normas e diretrizes da organização.

O questionário confirmou que o certificado digital funciona como uma carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação feita nos meios virtuais, como a rede mundial de computadores - Internet. Tecnicamente, o certificado é um documento eletrônico que por meio de procedimentos lógicos e matemáticos asseguraram a integridade das informações e a autoria das transações.

Conforme apontado na literatura o documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora que, seguindo regras emitidas pelo Comitê Gestor da ICP-Brasil e auditada pelo ITI,

associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.

Os certificados contêm os dados de seu titular, tais como nome, número do registro civil, assinatura da Autoridade Certificadora que o emitiu, entre outros, conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

O certificado digital, diferentemente dos documentos utilizados usualmente para a identificação pessoal como CPF e RG, possui um período de validade. Só é possível assinar um documento enquanto o certificado é válido. O usuário pode solicitar a renovação do certificado para a AC após a perda da validade deste.

Realmente o custo da certificação digital é determinado pelo mercado e qualquer interessado (Pessoa Física ou Jurídica) pode adquirir um certificado digital.

Para a obtenção de um certificado digital, o interessado deve recorrer a uma Autoridade de Registro de uma das Autoridades Certificadoras da ICP-Brasil, seguindo as regras explicitadas na Política de Certificado correspondente.

Da mesma forma que uma pessoa física pode solicitar sua identidade digital, as empresas interessadas com um CNPJ válido podem solicitar também. Sugere-se que para maiores informações sobre este procedimento podem ser encontradas no documento DOC-ICP-05, vinculado à resolução nº 42 da legislação da ICP-Brasil.

Levantou-se a informação que a RFB trata da certificação de seus servidores (certificação digital interna), mediante expedição de normas internas específicas seguindo as diretrizes do ITI.

As respostas obtidas a partir do questionário dão conta que ainda não há dados concretos para utilização do sistema por parte dos usuários. A RFB, porém, aposta nesta alternativa segura de atendimento à distância mediante a contínua ampliação dos serviços disponíveis para acesso com certificado digital.

As principais vantagens da certificação digital são a facilidade na obtenção de serviços e segurança nas transações. A RFB, especialmente por tratar de informações sigilosas, dá atenção especial à segurança da informação mediante adoção de rígida política e compete observar as normas legais e orientações/determinações emitidas pelo ITI. Isso demonstra a importância de observar os aspectos legais abordados nesta pesquisa.

O questionário revelou que a RFB não trabalha com *softwares* livres, pois está em jogo a questão do sigilo fiscal e da segurança das informações. Um assunto bem polêmico entre os profissionais da área.

Segundo Moscatto o principal objetivo da certificação para a RFB é a prestação de serviços, de forma segura, sem necessidade da presença do contribuinte nas suas unidades físicas. Cita que as principais vantagens da certificação digital são:

a) agilidade nos processos bucrocráticos;
b) redução de custos;
c) segurança nas transações pela Internet;
d) respaldo legal;
e) sigilo nas negociações.

Para que a certificação digital seja difundida no território nacional falta basicamente, ampliação dos serviços oferecidos para acesso com certificado digital e redução do custo para obtenção do certificado digital.

Os principais planos da RFB em relação à certificação digital é ampliação dos serviços disponíveis para acesso com certificado digital.

5 CONSIDERAÇÕES FINAIS

A informação representa um papel estratégico e fundamental para as organizações. Na Receita Federal Brasileira a informação é um dos principais insumos, tanto no relacionamento com os contribuintes (fornecimento/coleta de informações) quanto no tratamento de informações para realização das atividades de administração tributária sob sua responsabilidade.

O gestor deve estar atento às principais normas e aspectos relacionados à segurança da informação para atuar na área, se especializar constantemente e observar as principais normas emitidas pelo ITI.

Apesar das inúmeras vantagens que a certificação digital proporciona, para que ela seja difundida no território nacional, falta basicamente a ampliação dos serviços oferecidos para acesso com certificado digital, para as pessoas físicas e jurídicas e redução do custo para obtenção do certificado digital, sendo que este último é determinado pelo mercado e tem prazo de validade.

O governo tem investido e incentivado o uso de *softwares* livres, entretanto as organizações ainda preferem a utilização de *softwares* pagos alegando maior sigilo e segurança para a troca de informações.

Não existem dados concretos para utilização do sistema por parte dos usuários. A Receita Federal Brasileira, porém, aposta nesta alternativa segura de atendimento à distância mediante a contínua ampliação dos serviços disponíveis para acesso com certificado digital, sendo que alguns dos serviços de entregas de declarações pela Internet são facultativos e outros obrigatórios o uso de certificação digital.

Os certificados digitais, além da utilização pela RFB, tenderão a ser utilizados por um público muito maior em função da segurança que oferece às transações desenvolvidas através de redes públicas, como a internet e também pelo fato que propiciam maior agilidade nos processos burocráticos, redução de custos, respaldo legal e sigilo nas negociações.

Mas esse movimento ainda se encontra num estágio inicial, pois somente as grandes corporações, principalmente àquelas vinculadas aos sistemas financeiros como observamos no item clientes deste trabalho, se deram conta da importância de melhorar as condições de segurança dos meios de contato com seus clientes. Isso

é facilmente explicável, pois essas organizações são as mais visadas para práticas fraudulentas.

REFERÊNCIAS

BARROS, A. Q. P. de. **Tendências do mercado de serviços de segurança da informação**. Disponível em: <https://www.certisign.com.br/certinews/imagem/materia_15.pdf>. Acesso em: 14 out. 2007.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BERNARDES, M. C.; MOREIRA, E. S. dos. **Um modelo para inclusão da governança da segurança da informação no escopo da governança organizacional**. Disponível em: <http://www.linorg.cirp.usp.br/SSI/SSI2005/artigos/14275.pdf>. Acesso em: 14 out. 2007.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Disponível em: <http://www.iti.gov.br/twiki/bin/view/ITI/Apresentacao>. Acesso em: 15 maio 2008.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 ago. 2001. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/MedidaProvisoria/MEDIDA_PROVIS_RIA_2_200_2_D.PDF>. Acesso em: 15 maio 2008.

RECEITA FEDERAL DO BRASIL. Disponível em: <http://www.receita.fazenda.gov.br/>. Acesso: 13 out. 2008.

FACHIN, O. **Fundamentos de metodologia**. 3. ed. São Paulo: Saraiva, 2002.

FERREIRA, F. N. F. **Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2003, 162 p.

FONTES, E. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

GIL, A.C. **Como eleborar projetos de pesquisa**. 3. ed. São Paulo: Atlas, 1991.

ICP-BRASIL. **Estrutura normativa da ICP-Brasil**. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaNormativa/ESTRUTURA_NORMATIVA_DA_ICP-BRASIL_v_1.3.pdf>. Acesso em: 9 out. 2008.

MCGEE, J. V.; PRUSAK, L. **Gerenciamento estratégico da informação**: aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. 12. ed. Rio de Janeiro: Campus, 1994.

NEVES, E. V. C. de. **O perfil do profissional de segurança da informação**. Disponível em: <http://www.camargoneves.com/Artigos/perfprofinfosec.pdf>. Acesso em: 14 out. 2007.

PAPROSKI, Marcio. Certificação Digital. [mensagem pessoal]. Mensagem recebida por: <reinaldo.moscatto@receita.fazenda.gov.br> em: 11 nov. 2008.

SILVA, L. S. da. **Public Key Infrastructure – PKI**: conheça a infra-estrutura de chaves públicas e a certificação digital. São Paulo: Novatec, 2004.

SILVA, W. D. F. da. **Introdução à gestão da informação**. São Paulo: Editora Alínea, 2003.

STAREC, C.; GOMES, E.; BEZERRA, J. **Gestão estratégica da informação e inteligência competitiva**. São Paulo: Saraiva, 2005.

APÊNDICES

APÊNDICE A - Questionário

QUESTIONÁRIO SOBRE ASPECTOS REFERENTES À CERTIFICAÇÃO DIGITAL DENTRO DA RECEITA FEDERAL

Este questionário faz parte do trabalho de conclusão do curso de Gestão da Informação da Universidade Federal do Paraná, cujo objetivo é verificar aspectos importantes referentes a certificação digital. Sua participação contribuirá para analisar os resultados com os estudos teóricos da área.

1) Qual o papel que a informação representa dentro da Receita Federal?

R. A informação tem papel fundamental para a Secretaria da Receita Federal do Brasil - RFB, por tratar-se de um dos principais insumos com que trabalha a Instituição, tanto no relacionamento com os contribuintes (fornecimento/coleta de informações) quanto no tratamento de informações para realização das atividades de administração tributária sob sua responsabilidade. Assim, a RFB dá atenção especial tanto à Área de Tecnologia da Informação (TI) quanto à Área de Segurança da Informação (SI) visando garantir o sigilo das informações com que trabalha.

2) Quais os conhecimentos necessários para um profissional atuar na área de certificação digital dentro da Receita Federal?

R. Dentro da RFB, para atuar no processo de certificação digital interna, o servidor recebe treinamento especial e devem seguir rigidamente as normas emitidas pela Instituição, todas baixadas com estrita observância às normas do ITI.

3) Como funciona a certificação digital?

R. No Brasil, o ITI – Instituto Nacional de Tecnologia da Informação é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira. Informações sobre o funcionamento da certificação digital podem ser obtidas no site daquela Instituição (www.iti.gov.br).

4) A certificação garante de fato a segurança das informações nas transações eletrônicas?

R. (conforme *texto extraído do site www.iti.gov.br):*

Na prática, o certificado digital funciona como uma carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação feita nos meios virtuais, como a rede mundial de computadores - Internet. Tecnicamente, o certificado é um documento eletrônico que por meio de procedimentos lógicos e matemáticos asseguraram a integridade das informações e a autoria das transações.

Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora que, seguindo regras emitidas pelo Comitê Gestor da ICP-Brasil e auditada pelo ITI, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.

5) Qual o conteúdo de um certificado digital?

R. (conforme *texto extraído do site www.iti.gov.br):*

Os certificados contêm os dados de seu titular, tais como nome, número do registro civil, assinatura da Autoridade Certificadora que o emitiu, entre outros, conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

6) A certificação tem prazo de validade?

R. (conforme *texto foi extraído do site www.iti.gov.br):*

Sim. O certificado digital, diferentemente dos documentos utilizados usualmente para a identificação pessoal como CPF e RG, possui um período de validade. Só é possível assinar um documento enquanto o certificado é válido. O usuário pode solicitar a renovação do certificado para a AC após a perda da validade deste.

7) Qual o custo para adquirir uma certificação? Qualquer pessoa pode solicitar esse serviço?

R. O custo é determinado pelo mercado. Qualquer interessado (Pessoa Física ou Jurídica) pode adquirir um certificado digital.

8) Comente sobre o processo de criptografia. (Chaves públicas e privadas - Criptografia Simétrica e Assimétrica).

R. Ver site do ITI (www.iti.gov.br), podendo a pesquisa ser iniciada por “O que é criptografia” (Pergunta Frequente nº. 1.5).

9) Como a Receita Federal faz as certificações nas empresas? Qual o papel dela como Autoridade Certificadora?

R. (conforme *texto foi extraído do site www.iti.gov.br):*

Para a obtenção de um certificado digital, o interessado deve recorrer a uma Autoridade de Registro de uma das Autoridades Certificadoras da ICP-Brasil, seguindo as regras explicitadas na Politica de Certificado correspondente. No site - http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp - encontra-se a lista de Autoridades Certificadoras credenciadas pela ICP-Brasil.
Sobre este assunto, ver também site do ITI (Pergunta Frequente nº. 1.8).

Como é feitas a certificação nas empresas?

Da mesma forma que uma pessoa física pode solicitar sua identidade digital, as empresas interessadas com um CNPJ válido podem solicitar também. Maiores informações sobre este procedimento podem ser encontradas no documento DOC-ICP-05, vinculado à resolução nº 42 da legislação da ICP-Brasil.

Nota: A RFB trata da certificação de seus servidores (certificação digital interna), mediante expedição de normas internas específicas seguindo a diretrizes do ITI.

10) Qual a estimativa de utilização do sistema por parte dos usuários?

R. Ainda não há dados concretos. A RFB, porém, aposta nesta alternativa segura de atendimento à distância mediante a contínua ampliação dos serviços disponíveis para acesso com certificado digital.

11) Quais são as grandes corporações clientes do sistema?(cite algumas das principais).

R. No site da RFB constam os serviços que podem ser acessados mediante utilização de Certificado Digital.

No caso de entrega de declarações (ver www.receita.fazenda.gov.br --> Declarações --> Entrega de Declarações Via Internet --> Entrega de Declarações assinadas com Certificado Digital) estão listados os casos de entrega Facultativa e Obrigatória com Certiifcado Digital.

a) Entrega FACULTATIVA Com Certificação Digital

- Dirf 2008
- Simples 2005 a 2008
- IRPF 2005 a 2008
- DCTF Semestral
- DIPJ 2005 e 2006 a 2008 para as empresas tributadas com base no lucro presumido, imunes ou isentas.
- ITR 2005 a 2008
- CNPJ
- PERDCOMP
- Final de Espólio 2006 e 2007
- Saída Definitiva 2006 a 2008
- Dif Cigarros
- Dif Papel Imune
- DNF
- DACON Semestral
- Dimob
- DPSN - Declaração de Pendências do Simples Nacional
- DBF
- Derc
- DTTA

b) Entrega OBRIGATÓRIA Com Certificação Digital

- DCTF Mensal
- AUDIN
- DPREV
- DACON Mensal
- CPMF Trimestral
- CPMF Não Incidência
- CPMF Mensal Consolidada
- Derex

- Dirf 2008 - para a pessoa jurídica obrigada à apresentação mensal da Declaração de Débitos e Créditos Tributários Federais (DCTF), nos termos do art. 3º da Instrução Normativa RFB nº 786, de 19 de novembro de 2007;

- PERDCOMP - para a pessoa jurídica obrigada à apresentação mensal da Declaração de Débitos e Créditos Tributários Federais (DCTF), nos termos do art. 3º da Instrução Normativa RFB nº 786, de 19 de novembro de 2007;

- Dimob - para a pessoa jurídica obrigada à apresentação mensal da Declaração de Débitos e Créditos Tributários Federais (DCTF), nos termos do art. 3º da Instrução Normativa RFB nº 786, de 19 de novembro de 2007;

- DIPJ2007 e 2008 - para as pessoas jurídicas tributadas, em pelo menos um período de apuração durante o ano-calendário, com base no lucro real ou arbitrado e para a pessoa jurídica obrigada à apresentação mensal da Declaração de Débitos e Créditos Tributários Federais (DCTF), nos termos do art. 3º da Instrução Normativa RFB nº 786, de 19 de novembro de 2007;

- DBF - para a pessoa jurídica obrigada à apresentação mensal da Declaração de Débitos e Créditos Tributários Federais (DCTF), nos termos do art. 3º da Instrução Normativa RFB nº 786, de 19 de novembro de 2007;

- Derc - para a pessoa jurídica obrigada à apresentação mensal da Declaração de Débitos e Créditos Tributários Federais (DCTF), nos termos do art. 3º da Instrução Normativa RFB nº 786, de 19 de novembro de 2007;

- DTTA - para a pessoa jurídica obrigada à apresentação mensal da Declaração de Débitos e Créditos Tributários Federais (DCTF), nos termos do art. 3º da Instrução Normativa RFB nº 786, de 19 de novembro de 2007;

- Dimof

Para transmissão das declarações acima, no caso de declarante pessoa física, pode-se optar pela utilização de certificado digital de pessoa física do declarante ou

de procurador habilitado por ele no Cadastro de Procurações da RFB, disponibilizado na página da Receita Federal do Brasildo Brasil na Internet. No caso de declarante pessoa jurídica, as declarações poderão ser assinadas com o certificado digital de pessoa jurídica emitido em nome da empresa, ou de certificado de pessoa física, emitido em nome do responsável pela empresa, ou em nome de procurador habilitado pela empresa no Cadastro de Procurações da RFB. Serão aceitos os certificados digitais da RFB, e-CNPJ e e-CPF, e demais certificados de pessoa jurídica e física que atendam as condições para emissão e manutenção desses certificados, conforme disposto nas IN RFB nº 462/2004 e IN RFB nº 580/2005.

12) Proteger a informação significa garantir disponibilidade, integridade, privacidade, legalidade, auditabilidade e não repúdio de autoria. Como a Receita Federal aborda estes itens?

R. De acordo com as normas do ITI.

13) Quais são as outras vantagens que a certificação digital proporciona para as organizações?

R. Facilidade na obtenção de serviços e segurança nas transações.

14) Sendo as pessoas os maiores ativos no processo de segurança da informação, investir apenas em tecnologias não é suficiente. É importante estabelecer também uma boa política de segurança da informação. Como a Receita Federal aborda essa questão dentro da organização?

R. A RFB, especialmente por tratar de informações sigilosas, dá atenção especial à segurança da informação mediante adoção de rígida política.

15) Comente sobre os aspectos legais referentes à certificação digital.

R. À RFB compete observar as normas legais e orientações/determinações emitidas pelo ITI.

16) A Receita Federal é uma autoridade certificadora e usuária da certificação digital. Qual o principal objetivo da certificação para a organização?

R. Prestação de serviços, de forma segura, sem necessidade da presença do contribuinte nas suas Unidades Físicas.

17) Como funciona o vínculo entre a Receita Federal e a ICP-Brasil?

R. Conforme a normas vigentes (Ver site www.iti.gov.br).

18) Comente sobre outros pontos importantes que você achar pertinente em relação à certificação digital. (incluindo os aspectos negativos).

R. Principais vantagens da certificação digital:

1) Agilidade nos processos bucrocráticos;
2) Redução de custos.
3) Segurança nas transações pela Internet.
4) Respaldo legal.
5) Sigilo nas negociações.

19) O que falta para que a certificação digital seja difundida no território nacional aumentando o número de adeptos do sistema?

R. Basicamente, ampliação dos serviços oferecidos para acesso com certificado digital e redução do custo para obtenção do certificado digital.

20) Quais são os principais planos da Receita Federal em relação a certificação digital?

R. Ampliação dos serviços disponíveis para acesso com certificado digital.

ANEXOS

ANEXO A – Medida Provisória Nº 2.200-2, de 24 de agosto de 2001

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 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.

O **PRESIDENTE DA REPÚBLICA**, no uso da atribuição que lhe confere o art. 62º da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras

formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e
VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.
Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.
Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.
Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.
Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.
Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.
Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.
Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.
Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.
Art. 10º Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.
§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.
§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.
Art. 11º A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei no 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.
Art. 12º Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13º O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.
Art. 14º No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.
Art. 15º Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.
Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.
Art. 16º Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.
§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.
§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.
Art. 17º Fica o Poder Executivo autorizado a transferir para o ITI:
I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia; e
II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei no 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.
Art. 18º Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.
Art. 19º Ficam convalidados os atos praticados com base na Medida Provisória no 2.200-1, de 27 de julho de 2001.
Art. 20º Esta Medida Provisória entra em vigor na data de sua publicação.
Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.
FERNANDO HENRIQUE CARDOSO
José Gregori Martus Tavares
Ronaldo Mota Sardenberg Pedro Parente

ANEXO B – Decretos,Resoluções, Instruções Normativas e documentos

DECRETOS

a) Decreto nº 3.505, de 13 de Junho de 2000: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

b) Decreto nº 3.872, de 18 de Julho de 2001: Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CGICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.

c) Decreto nº 3.996, de 31 de Outubro de 2001: Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

d) Decreto nº 4.414, de 07 de Outubro de 2002: Altera o Decreto no 3.996, de 31 de Outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

e) Decreto nº 4.689, de 07 de Maio de 2003: Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências.

RESOLUÇÕES

a) Resolução n° 3 de 25 de Setembro de 2001: Designa Comissão para auditar a Autoridade Certificadora Raiz - AC Raiz e seus prestadores de serviços. Esse texto não substitui o publicado no D.O.U. de 26 de Setembro de 2001.

b) Resolução n° 5, de 22 de Novembro de 2001: Aprova o Relatório de auditoria da AC Raiz. Este texto não substitui o publicado no D.O.U. de 23 de Novembro de 2001.

c) Resolução n° 15, de 10 de Junho de 2002: Estabelece as diretrizes para sincronização de freqüência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.Este texto não substitui o publicado no D.O.U. de 11 de Junho de 2002.

d) Resolução n° 16, de 10 de Junho de 2002. Este texto não substitui o publicado no D.O.U. de 11 de Junho de 2002.

e) Resolução n° 20, de 08 de Maio de 2002: Determina o desenvolvimento de uma plataforma criptográfica aberta, voltada à operação da AC Raiz. Este texto não substitui o publicado no D.O.U. de 09 de Maio de 2002.

f) Retificação da Resolução n° 28, de 20 de Novembro de 2003: Este texto não substitui o publicado no D.O.U. de 24 de Novembro de 2003.

g) Resolução n° 29, de 29 de Janeiro de 2004: Este texto não substitui o publicado no D.O.U. de 30 de Janeiro de 2004.

h) Resolução n° 33, de 21 de Outubro de 2004: Delega a AC RAIZ da ICP-Brasil atribuição para suplementar as normas do Comitê Gestor e dá outras providências. Este texto não substitui o publicado no D.O.U. de 27 de Outubro de 2004.

i) Resolução n° 36, de 21 de Outubro de 2004: Aprova o Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no âmbito da ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 27 de Outubro de 2004.

j) Resolução n° 39, de 18 de Abril de 2006: Aprova a versão 2.0 da Política de Segurança da ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 24 de Abril de 2006.

k) Resolução n° 41, de 18 de Abril de 2006: Aprova a versão 2.0 dos Requisitos Mínimos para as POLÍTICAS DE CERTIFICADO na ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 24 de Abril de 2006.

l) Resolução n° 42, de 18 de Abril de 2006: Aprova a versão 2.0 dos Requisitos Mínimos para as DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO das Autoridades Certificadoras da ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 24 de Abril de 2006.

m)Resolução n° 43, de 18 de Abril de 2006: Aprova a versão 2.0 das Diretrizes da POLÍTICA TARIFÁRIA da Autoridade Certificadora Raiz da ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 24 de Abril de 2006.

n) Resolução n° 44, de 18 de Abril de 2006: Aprova a versão 2.0 dos Critérios e Procedimentos para Realização de AUDITORIAS NAS ENTIDADES nas Entidades da ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 24 de Abril de 2006.

o) Resolução n° 45, de 18 de Abril de 2006: Aprova a versão 2.0 dos Critérios e Procedimentos para FISCALIZAÇÃO das Entidades Integrantes da ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 24 de Abril de 2006.

p) Resolução n° 47, de 03 de Dezembro de 2007: Aprova a versão 3.0 dos Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 14 de Dezembro de 2007.

q) Resolução n° 48, de 03 de Dezembro de 2007. Altera os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICPBrasil. Este texto não substitui o publicado no D.O.U. de 14 de Dezembro de 2007.

r) Resolução n° 49, de 03 de Junho de 2008. Aprova a versão 3.0 da Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil. Este texto não substitui o publicado no D.O.U. de 28 de Maio de 2008.

INSTRUÇÕES NORMATIVAS

a) IN nº 01-2008 Aprovação da versão 1.0 do DOC-ICP-05.01

b) IN nº 01-2007 Aprovação da versão 2.1 do DOC-ICP-10.01

c) IN nº 02-2007 Aprovação da versão 2.0 do DOC-ICP-10.02

d) IN nº 03-2007 Aprovação da versão 3.0 do DOC-ICP-10.03

e) IN nº 04-2007 Aprovação da versão 2.0 do DOC-ICP-10.04

f) IN nº 05-2007 Aprovação da versão 1.0 do DOC-ICP-10.05

g) IN nº 06-2007 Aprovação da versão 1.0 do DOC-ICP-10.06

h) IN nº 04-2006 Aprovação da versão 1.0 do DOC-ICP-01.01

i) IN nº 05-2006 Aprovação da versão 1.0 do DOC-ICP-04.01

j) IN nº 06-2006 Aprovação dos Adendos de Documentos (ADE-ICP) da ICP-Brasil

k) IN nº 08-2006 Estabelecimento das regras de adaptação das entidades

l) da ICP-Brasil de acordo com as resoluções de 38 a 45

m)IN nº 10-2006 Aprovação da versão 1.1 do DOC-ICP-03.01

n) IN nº 01-2005 Implementação do Controle de Versões de PC, DPC e PS

DOCUMENTOS ICP-BRASIL

a) DOC-ICP-01 Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil - v.3.0

b) DOC-ICP-01.01 Padrões e Algoritmos Criptográficos da ICP-Brasil - v.1.0

c) DOC-ICP-02 Política de Segurança da ICP-Brasil - v.2.0

d) DOC-ICP-03 Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil - v.3.0

e) DOC-ICP-03.01 Características Mínimas de Segurança para as AR da ICP-Brasil - v.1.1

f) DOC-ICP-04 Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil - v.2.0

g) DOC-ICP-04.01 Atribuição de OID na ICP-Brasil - v.1.0

h) DOC-ICP-05 Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil - v.2.1

i) DOC-ICP-05.01 Procedimentos de Identificação de Servidores do Serviço Exterior Brasileiro em Missão Permanente no Exterior - v.1.0

j) DOC-ICP-06 Política Tarifária da Autoridade Certificadora Raiz da ICP-Brasil - v.2.0

k) DOC-ICP-07 Diretrizes Para Sincronização de Freqüência e de Tempo na Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil - v.1.0

l) DOC-ICP-08 Critérios e Procedimentos para Auditoria das Entidades Integrantes da ICP-Brasil - v.2.0

m)DOC-ICP-09 Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP-Brasil - v.2.0

n) DOC-ICP-10 Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP-Brasil - v.1.0

o) DOC-ICP-10.01 Procedimentos Administrativos a serem observados nos Processos de Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP-Brasil - v.2.1

p) DOC-ICP-10.02 Estrutura Normativa Técnica e Níveis de Segurança de Homologação a serem utilizados nos Processos de Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP-Brasil - v.2.0

q) DOC-ICP-10.03 Padrões e Procedimentos Técnicos a serem observados nos Processos de Homologação de Cartões Inteligentes, (Smart Cards), Leitoras de Cartões Inteligentes e Tokens Criptográficos no Âmbito da ICP-Brasil - v.3.0

r) DOC-ICP-10.04 Padrões e Procedimentos Técnicos a serem observados nos Processos de Homologação de Softwares de Assinatura Digital, Sigilo e Autenticação no Âmbito da ICP-Brasil - v.2.0

s) DOC-ICP-10.05 Padrões e Procedimentos Técnicos a serem observados nos processos de homologação de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil - v.1.0

t) DOC-ICP-10.06 Padrões e Procedimentos Técnicos a serem observados nos processos de homologação de Softwares de Bibliotecas Criptográficas e Softwares Provedores de Serviços Criptográficos no Âmbito da ICP-Brasil - v.1.0

ANEXO C - Processos de certificação digital da receita federal

DOU de 13.12.2005

Institui o Centro Virtual de Atendimento ao Contribuinte da Secretaria da Receita Federal (e-CAC).
Retificada no DOU de 03/02/2006, Seção 1, pág. 37.

O **SECRETÁRIO DA RECEITA FEDERAL**, no uso da atribuição que lhe confere o inciso III do art. 230 do Regimento Interno da Secretaria da Receita Federal, aprovado pela Portaria MF nº 30, de 25 de fevereiro de 2005, resolve:

Art. 1º Fica instituído, no âmbito da Secretaria da Receita Federal (SRF), o Centro Virtual de Atendimento ao Contribuinte (e-CAC), com o objetivo de propiciar o atendimento aos contribuintes de forma interativa, por intermédio da Internet, no endereço eletrônico <http://www.receita.fazenda.gov.br>.

§ 1º O e-CAC utilizará tecnologia que certifica a autenticidade dos emissores e destinatários dos documentos eletrônicos, com segurança quanto a sua privacidade e inviolabilidade.

§ 2º O acesso ao e-CAC será efetivado mediante a utilização de certificados digitais e-CPF ou e-CNPJ, observado o disposto no art. 1º do Decreto 4.414, de 7 de outubro de 2002.

Das Opções de Atendimento

Art. 2º O e-CAC possibilitará, entre outras, as seguintes opções de atendimento:

I - consulta e regularização das situações cadastral e fiscal dos contribuintes pessoas físicas e pessoas jurídicas;

II - entrega de declarações e demais documentos eletrônicos, com aposição de assinatura digital;

III - obtenção de cópias de declarações e de outros documentos e seus respectivos recibos de entrega;

IV - alteração e solicitação de cancelamento da inscrição no Cadastro de Pessoas Físicas (CPF), e inscrição, alteração e solicitação de baixa da inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

V - emissão de certidões;

VI - cadastramento eletrônico de procurações;

VII - acompanhamento da tramitação de processos fiscais;

VIII - parcelamento de débitos fiscais;

IX - compensação de créditos fiscais;

X - prática de atos relacionados com o funcionamento de sistemas de comércio exterior;

XI - leilão de mercadorias apreendidas;

XII - criação de endereço eletrônico para comunicação entre a administração tributária e o sujeito passivo.

Parágrafo único. A disponibilização de cada opção de atendimento será efetivada mediante ato conjunto da Coordenação-Geral de Tecnologia e Segurança da Informação (Cotec) e da Coordenação-Geral responsável pela área vinculada ao atendimento.

Das Definições

Art. 3º O processo de certificação digital a que se refere o § 1º do art. 1º fundamentar-se-á nos seguintes conceitos:

I - documento eletrônico: aquele cujas informações são armazenadas exclusivamente em meios eletrônicos;

II - certificados digitais e-CPF e e-CNPJ: documentos eletrônicos de identidade emitidos por Autoridade Certificadora credenciada pela Autoridade Certificadora Raiz da ICP-Brasil (AC Raiz) e habilitada pela Autoridade Certificadora da SRF (AC-SRF), que certificam a autenticidade dos emissores e destinatários dos documentos e dados que trafegam em uma rede de comunicação, bem assim assegura sua privacidade e inviolabilidade;

III - assinatura digital: processo eletrônico de assinatura, baseado em sistema criptográfico assimétrico, que permite ao usuário usar sua chave privada para declarar a autoria de documento eletrônico a ser entregue à SRF, garantindo a integridade de seu conteúdo;

IV - Autoridade Certificadora da Secretaria da Receita Federal (AC-SRF): entidade integrante da ICP-Brasil em nível imediatamente subseqüente à AC Raiz, responsável pela assinatura dos certificados das Autoridades Certificadoras Habilitadas;

V - Autoridade Certificadora Habilitada: entidade integrante da ICP-Brasil em nível imediatamente subseqüente ao da AC-SRF, habilitada pela Cotec, em nome da SRF, responsável pela emissão e administração dos certificados digitais e-CPF e e-CNPJ;

VI - Autoridade de Registro da Secretaria da Receita Federal (AR-SRF): entidade operacionalmente vinculada à AC-SRF, responsável pela confirmação da identidade dos solicitantes de credenciamento e habilitação como Autoridades Certificadoras integrantes da ICP-Brasil, em nível imediatamente subseqüente ao da AC-SRF;

VII - Autoridades de Registro: entidades operacionalmente vinculadas a uma Autoridade Certificadora Habilitada, responsável pela confirmação da identidade dos solicitantes dos certificados e-CPF e e-CNPJ;

VIII - usuário: pessoa física ou jurídica, titular de certificado digital e-CPF ou e-CNPJ, respectivamente, bem assim de qualquer outro certificado digital emitido por Autoridade Certificadora não habilitada pela SRF e credenciada pela ICP-Brasil.

Do Usuário

Art. 4º Os usuários obterão os certificados e-CPF e e-CNPJ junto a qualquer Autoridade Certificadora Habilitada, mediante solicitação realizada por intermédio da Internet.

§ 1º A lista de Autoridades Certificadoras Habilitadas e seus respectivos endereços na Internet estarão disponíveis no sítio da SRF.

§ 2º A identificação dos usuários é realizada mediante seu comparecimento a uma das Autoridades de Registro vinculadas à Autoridade Certificadora Habilitada escolhida para emissão do certificado.

§ 3º O custo do processo de emissão do certificado é de responsabilidade do usuário.

Art. 5º O titular do certificado e-CPF ou e-CNPJ é responsável por todos os atos praticados perante a SRF com a utilização do referido certificado e sua correspondente chave privada, devendo adotar as medidas necessárias para garantir a confidencialidade dessa chave e requerer, imediatamente, à Autoridade Certificadora a revogação de seu certificado, em caso de comprometimento de sua segurança.

Parágrafo único. É obrigatório o uso de senha para proteção da chave privativa do titular do certificado e-CPF ou e-CNPJ.

Art. 6º Não poderão ser emitidos certificados:

I - e-CPF, para as pessoas físicas cuja situação cadastral, perante o CPF, esteja enquadrada na condição de cancelada ou nula;

II - e-CNPJ, para as pessoas jurídicas cuja situação cadastral, perante o CNPJ, esteja enquadrada na condição de suspensa, inapta, baixada ou nula.

§ 1º Deverão ser revogados os certificados e-CPF das pessoas físicas cuja situação cadastral, perante o CPF, seja alterada para a condição de cancelada ou nula.

§ 2º Deverão ser revogados os certificados e-CNPJ das pessoas jurídicas cuja situação cadastral, perante o CNPJ, seja alterada para a condição de inapta, baixada ou nula.

§ 3º A Cotec celebrará, em nome da SRF, convênio com as autoridades certificadoras a serem habilitadas, mediante o qual será verificado o atendimento às condições para emissão de certificados e-CPF e e-CNPJ.

Art. 7º Os usuários titulares de certificados e-CPF ou e-CNPJ terão, observado perfil pré-estabelecido, livre acesso ao e-CAC.

§ 1º Os usuários titulares de outros certificados digitais, independentemente do seu reconhecimento, não poderão ter acesso ao e-CAC nas hipóteses previstas nos incisos I e II do art. 6º.

§ 2º Para fins do disposto no § 1º, a SRF procederá a prévia verificação da situação cadastral do usuário.

Das Autoridades Certificadoras Habilitadas

Art. 8º A SRF habilitará, por intermédio da AC-SRF, no âmbito da ICP-Brasil, as Autoridades Certificadoras que emitirão os certificados e-CPF e e-CNPJ.

Art. 9º Poderá ser autorizada a emitir os certificados digitais e-CPF e e-CNPJ, na condição de Autoridade Certificadora Habilitada pela AC-SRF, a pessoa jurídica que:

I - estiver inscrita no CNPJ na condição Ativa, nas hipóteses do inciso I do art. 31 e do art. 55, da Instrução Normativa RFB nº 568, de 8 de setembro de 2005;

II - atender a todos os requisitos estabelecidos para o credenciamento de Autoridades Certificadoras no âmbito da ICP-Brasil;

III - implementar os procedimentos de validação dos dados fornecidos pelo usuário junto ao CPF e CNPJ.

Parágrafo único. A documentação comprobatória do atendimento das condições para o credenciamento da Autoridade Certificadora junto à ICP-Brasil e habilitação junto à SRF deve ser protocolizada na Cotec.

Art. 10. São atribuições das Autoridades Certificadoras Habilitadas:

I - emitir e revogar certificados e-CPF e e-CNPJ;

II - notificar, com antecedência mínima de um mês, o vencimento dos certificados e-CPF e e-CNPJ;

III - adotar as medidas necessárias para garantir a confidencialidade de sua chave privativa, devendo solicitar imediatamente à AC-SRF a revogação do seu certificado, em caso de comprometimento de sua segurança;

IV - manter, na Internet, de forma permanente, lista para acesso público contendo informação dos certificados e-CPF e e-CNPJ revogados;

V - disponibilizar para a SRF, com atualização diária, lista contendo os certificados emitidos e sua respectiva situação;

VI - exigir dos usuários exclusivamente informações indispensáveis à efetivação do processo de certificação, vedada sua divulgação ou cessão, a qualquer título ou forma, a terceiros;

VII - disponibilizar, na Internet, sua Declaração de Práticas de Certificação (DPC) e a Política de Certificados (PC) e-CPF e e-CNPJ implementada, aprovadas pela Cotec, observada a legislação aplicável;

VIII - disponibilizar, na Internet, mecanismo que permita aos usuários verificar a correta instalação dos certificados em seus equipamentos;

IX - contratar auditoria independente com a finalidade de verificar, a cada doze meses, o correto exercício das atividades de Autoridade Certificadora Habilitada;

X - informar, imediatamente, à SRF todas as revogações de certificados efetuadas.

§ 1º O resultado da auditoria prevista no inciso IX deste artigo deverá ser encaminhado à Cotec.

§ 2º Caso as obrigações previstas neste artigo não sejam cumpridas, a habilitação da Autoridade Certificadora será cancelada pela Cotec.

Art. 11. A Autoridade Certificadora responderá por perdas e danos sofridos pelos usuários ou por terceiros, em conseqüência do não cumprimento de suas obrigações ou da divulgação ou cessão de informações, bem assim pelos prejuízos oriundos da emissão ou revogação indevidas, ou ainda da não revogação em prazo hábil, de certificados.

Art. 12. Quando do encerramento das atividades ou do cancelamento da habilitação da Autoridade Certificadora todos os certificados por ela emitidos perderão sua validade e não serão aceitos para acesso aos serviços disponibilizados pela SRF, devendo toda a documentação referente ao processo de emissão de e-CPF e e-CNPJ ser imediatamente entregue à SRF.

Parágrafo único. A SRF poderá autorizar nova emissão dos certificados referidos no caput por outra Autoridade Certificadora Habilitada, devendo, neste caso, ser

transferida para esta toda a documentação referente à administração dos certificados e-CPF e e-CNPJ.

Da Autoridade Certificadora da SRF

Art. 13. A SRF atuará como AC-SRF por intermédio da Cotec, a quem compete:

I - gerenciar o processo de emissão e uso dos certificados digitais da SRF;

II - analisar as solicitações de credenciamento e habilitação;

III - autorizar as Autoridades Certificadoras a assinar os certificados e-CPF e e-CNPJ por elas emitidos, no âmbito da ICPBrasil;

IV - emitir certificados para as Autoridades Certificadoras credenciadas pela ICP-Brasil e habilitadas pela SRF;

V - revogar os certificados das Autoridades Certificadoras credenciadas pela ICP-Brasil e habilitadas pela SRF que deixarem de cumprir os requisitos estabelecidos;

VI - manter, na Internet, de forma permanente, lista para acesso público, assinada e atualizada, contendo informação de certificados emitidos e revogados de Autoridades Certificadoras Habilitadas;

VII - elaborar toda a documentação técnica necessária à operação da AC-SRF;

VIII - auditar, periodicamente, as atividades das Autoridades Certificadoras Habilitadas;

IX - analisar os relatórios de auditorias executadas por empresas de auditoria independente nas Autoridades Certificadoras Habilitadas;

X - notificar o vencimento do certificado da Autoridade Certificadora credenciada pela ICP-Brasil e habilitadas pela Cotec, com uma antecedência mínima de 13 meses;

XI - identificar e registrar todas as ações executadas pela AC-SRF;

XII - publicar os certificados emitidos para as autoridades certificadoras habilitadas no Diário Oficial da União;

XIII - arquivar toda a documentação referente ao processo de credenciamento e habilitação de Autoridades Certificadoras, bem assim as solicitações de emissão e revogação de certificados.

Da Autoridade de Registro da SRF

Art. 14. A SRF atuará como AR-SRF por intermédio da Cotec, a quem compete:

I - receber, validar e encaminhar para AC-SRF as solicitações de emissão e revogação de certificados digitais para as Autoridades Certificadoras habilitadas;

II - confirmar a identidade dos solicitantes de emissão e revogação de certificados digitais para as Autoridades Certificadoras habilitadas pela AC-SRF e armazenar a documentação de identificação recebida;

III - informar aos solicitantes a emissão ou a revogação de seus certificados;

IV - disponibilizar os certificados emitidos pela AC-SRF aos respectivos solicitantes;

V - identificar e registrar todas as ações executadas pela ARS RF.

Das Disposições Finais

Art. 15. No exercício da competência fixada nesta Instrução Normativa, a Cotec poderá expedir normas complementares.

Art. 16. Na resolução de quaisquer questões judiciais entre as Autoridades Certificadoras Habilitadas pela SRF e os usuários dos certificados e-CPF e e-CNPJ, fica estabelecido como foro a cidade brasileira onde se localiza a Autoridade Certificadora.

Art. 17. A partir de 12 de dezembro de 2005, a SRF disponibilizará no e-CAC as opções de atendimento a que se referem os incisos I a VI e VIII, X e XII do art. 2º, dispensadas, neste caso, a edição dos atos de que trata o parágrafo único do mesmo artigo.

Art. 18. Fica formalmente revogada, sem interrupção de sua força normativa, a Instrução Normativa SRF nº 222, de 11 de outubro de 2002, e o art. 1º da Instrução Normativa SRF nº 462 de 19 de outubro de 2004.

Art. 19. Esta Instrução Normativa entra em vigor na data de sua publicação.

JORGE ANTONIO DEHER RACHID