Inclusão Digital: um Estudo a partir da Utilização do Certificado Digital na Atividade Profissional

Querli Polo Suzin, Jéssica Aver Melara, Saiuri Scain Pellissari

RESUMO

Os computadores e a internet são 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 de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas. O presente trabalho tem por objetivo demonstrar a dificuldade de alguns profissionais na utilização do certificado digital. A certificação digital é a tecnologia que provê estes mecanismos e 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 substancial redução de custos. O problema de pesquisa consiste em compreender quais dificuldades que a inclusão digital oferece, tendo por base a utilização do certificado digital por empresas e pessoas físicas? A metodologia utilizada foi a revisão bibliográfica e a entrevista a partir da adoção de um instrumento de coleta de dados.

Palavras-chave: Inclusão Digital. Tecnologia. Certificado Digital.

1 INTRODUÇÃO

O presente trabalho tem por finalidade o esclarecimento sobre a utilização do certificado digital, que tem por objetivo especifico a assinatura com validade jurídica e que garante proteção de documentos e serviços da web, permitindo que pessoas e empresas se identifiquem e assinem digitalmente de qualquer lugar do mundo com mais segurança e agilidade. Embora toda a segurança ofertada, alguns profissionais encontram grande dificuldade na utilização desta tecnologia.

As informações certificadas pelo certificado digital contêm dados que identificam uma pessoa, uma máquina, ou uma instituição da internet. Uma pessoa incluída digitalmente, tende a ganhar em qualidade de vida, na medida em que ganha tempo fazendo uso da tecnologia, pois pode realizar diversos serviços diretamente do seu computador, sem a necessidade de se dirigir a órgãos públicos e estabelecimentos privados para realizar atividades tais como: acesso à Receita Federal, processos em todas as Instâncias Judiciais as operações bancárias via Internet, as compras em lojas virtuais e supermercados que entregam em domicílio, cursos on-line, inclusive de educação à distância e serviços públicos variados.

Já existem serviços que exigem o uso ou garantem benefícios ao cidadão e empresa que emitir esses certificados. As vantagens geralmente resumem-se na eliminação de processos burocráticos ou na possibilidade de resolver tudo pela web, sem sair de casa e se dirigir a um cartório ou órgão público, por exemplo.

O referencial teórico está dividido nos conceitos de inclusão digital e do certificado digital e todas as suas espécies e normas de segurança.

O mercado que se utiliza do certificado digital está em plena expansão, sendo que não se trata mais de uma opção, ou de uma facilidade, mas de uma obrigatoriedade para acesso aos mais diversos serviços, o que implica em dificuldades para algumas pessoas que não fazem parte da inclusão digital, principalmente sendo uma barreira para o exercício profissional desses profissionais.

O problema de pesquisa consiste em compreender quais dificuldades que a falta de inclusão digital oferece, tendo por base a utilização do certificado digital por empresas e pessoas físicas?

2 REFERENCIAL TEÓRICO

2.1 INCLUSÃO DIGITAL

O termo inclusão digital tem sido frequentemente utilizado, em especial pelas organizações internacionais e pelo setor público, para compor um jargão apelativo nas abordagens políticas de caráter geral e populista. Uma espécie de nova e mirabolante solução para quase todos os entraves da sociedade contemporânea: pobreza, desigualdade social, carências educacionais, injustiça social, desemprego, violência, criminalidade, entre outros.

A definição de inclusão digital adotada pelo Programa Identidade Digital do Estado da Bahia, e mantida no atual Programa de Inclusão Sócio-Digital (2004), prevê as seguintes funcionalidades: a) possibilitar a apropriação da tecnologia e o desenvolvimento das pessoas nos mais diferentes aspectos; b) estimular a geração de emprego e renda; c) promover a melhoria da qualidade de vida das famílias; d) proporcionar maior liberdade social; e) incentivar a construção e manutenção de uma sociedade ativa, culta e empreendedora.

José de Souza Martins (2003) argumenta que denominamos exclusão o conjunto das dificuldades, dos problemas e dos modos precários e marginais de participação social que tem origem com as transformações econômicas. Para ele, esse é um processo de inclusão e não de exclusão, fazendo uma crítica ao discurso de exclusão:

> O discurso corrente sobre exclusão é basicamente produto de um equívoco, de uma fetichização, a fetichização conceitual da exclusão, a exclusão transformada numa palavra mágica que explicaria tudo. Rigorosamente falando, só os mortos são excluídos, e nas nossas sociedades a completa exclusão dos mortos não se dá nem mesmo com a morte física; ela só se completa depois de lenta e complicada morte simbólica. (MARTINS, 2003, p. 27)

Segundo Marlene Ribeiro (1999, p. 43), “a luta pela inclusão é também uma luta para manter a sociedade que produz a exclusão”, implica, a aceitação da ordem que “exclui”. Inserir supõe conceber os sujeitos passivos como peças de um jogo, designando a eles “um papel de meros objetos, seres amorfos que aceitam a inexorabilidade de sua exclusão” (1999, p. 42), como se as pessoas não pensassem, não optassem, não se movimentassem, não reivindicassem, não formassem opiniões e pudessem, assim, ser manobradas. Significa então que a dinâmica social não é considerada como resultante das nossas ações, interações e concepções, em relação e movimento.

As questões culturais e educacionais estão presentes quando se discute inclusão digital. No entanto, estas são questões também quase sempre abordadas de forma insuficiente.

Segundo Castells (2005), um excluído digital tem três grandes formas de ser excluído. Primeiro, não tem acesso à rede de computadores. Segundo, tem acesso ao sistema de comunicação, mas com uma capacidade técnica muito baixa. Terceiro, (para mim é a mais importante forma de ser excluído e da que menos se fala) é estar conectado à rede e não saber qual o acesso usar, qual a informação buscar, como combinar uma informação com outra e como a utilizar para a vida. Esta é a mais grave porque amplia, aprofunda a exclusão mais séria de toda a História; é a exclusão da educação e da cultura porque o mundo digital se incrementa extraordinariamente.

Portanto, a preocupação é com a cultura e com a educação. Embora ainda não estando presente em sua discussão a perspectiva da produção de conteúdos, de autoria e co-autoria dos

sujeitos no mundo digital, dimensão que efetivamente poderia ser significativa educacional e culturalmente para as comunidades, aponta para a necessidade de ir além da perspectiva técnica e do mero acesso.

2.2 CERTIFICADO DIGITAL

O Certificado Digital é uma assinatura com validade jurídica que garante proteção às transações eletrônicas e outros serviços via internet, permitindo que pessoas e empresas se identifiquem e assinem digitalmente de qualquer lugar do mundo com mais segurança e agilidade, contém informações que identificam uma pessoa, uma máquina, ou uma instituição da internet (SERASA, 2017). Para isso ele usa um software como intermediário - pode ser um navegador, o cliente de email ou de outro programa qualquer que reconheça essa informação. O certificado digital é emitido a pessoas físicas (cidadão comum), jurídicas (empresas ou municípios), equipamentos e aplicações. A possibilidade de envio de informações de forma segura, sem que haja, o risco de que outra pessoa, que não a destinatária, abra a mensagem contendo as informações enviadas, fez com que durante muitos anos, a criptografia fosse restrita às redes estatais. Essas redes utilizam tais recursos como forma de garantir a segurança e a inviolabilidade de informações secretas transmitidas e armazenadas, no interesse do estado.

Um Certificado Digital normalmente apresenta as seguintes informações:

- Nome da pessoa ou entidade a ser associada à chave pública;
- Chave pública;
- Período de validade do certificado;
- Nome e assinatura da entidade que assinou o certificado;
- Número de série.

2.2.1 Quem emite o certificado digital?

De acordo com a Certificadora Certisign (2017), a emissão é feita por uma entidade considerada confiável, chamada Autoridade Certificadora. É ela quem vai associar ao usuário um par de chaves criptográficas (pública e privada). São essas chaves, emitidas e geradas pelo próprio usuário no momento da aquisição do certificado, que transformam um documento eletrônico em códigos indecifráveis que trafegam de um ponto a outro sigilosamente. Enquanto a chave pública codifica o documento, a chave privada associada a ela decodifica. E vice-versa. Um certificado pode ser usado em conjunto com uma assinatura digital. Neste caso, a assinatura digital fica de tal modo vinculado ao documento eletrônico que qualquer alteração o torna inválido. Essa chave é compartilhada pelo remetente e pelo destinatário. A mensagem inicial, chamada de texto original, é transformada para o texto cifrado, o destinatário por sua vez, realiza a transformação reversa (do texto cifrado para o texto original).

Figura 1 – Operação de texto cifrado

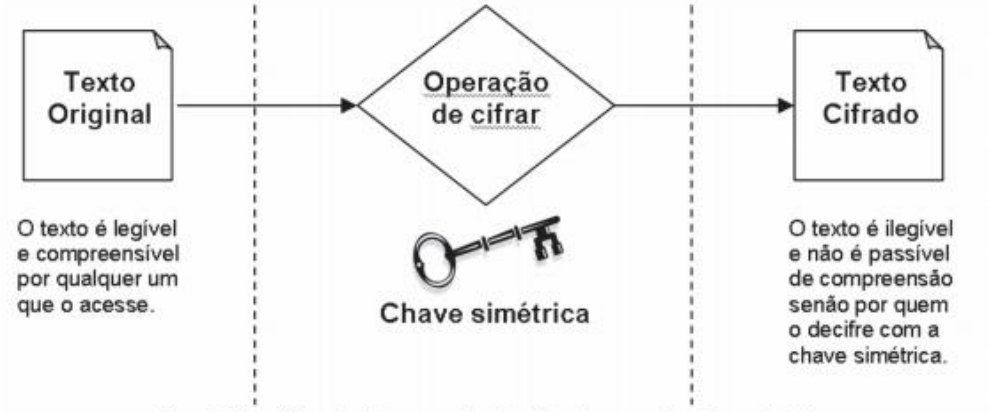

Fig. 1. Simplificação da operação de cifração por algoritmo simétrico
Fonte: Adaptado de [ABO02]

Fonte: ICP (2010)

Isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente esta chave é representada por uma senha, usada tanto para o remetente para codificar a mensagem em uma ponta como pelo destinatário para decodificá-la na outra.

2.2.2 Como obter o certificado digital

Já existem serviços que exigem o uso ou garantem benefícios ao cidadão e empresa que emitir um desses certificados. As vantagens geralmente resumem-se na eliminação de processos burocráticos ou na possibilidade de resolver tudo pela web, sem sair de casa e se dirigir a um cartório ou órgão público, por exemplo.

Para obter um certificado digital, o primeiro passo é escolher uma autoridade certificadora (AC), que funciona quase como um "cartório" digital. Há várias delas no mercado, todas subordinadas ao ICP-Brasil, serviço público criado em 2001, que monitora e regulamenta a emissão desses certificados no Brasil. O Instituto Nacional de Tecnologia da Informação (ITI), uma autarquia vinculada à Casa Civil da Presidência da República, credencia e audita as ACs brasileiras.

De acordo com o ICP-Brasil (2017), os certificados digitais mais populares são o e-CPF e o e-CNPJ que, como indicam em seus nomes, funciona tal qual uma versão eletrônica do seu CPF e CNPJ, estando inclusive vinculado a estes documentos e identificando você perante a Receita Federal. Com o e-CPF, você pode obter cópias de declarações do imposto de renda, simplificar o processo de recolhimento do FGTS ou realizar serviços cartoriais pela Internet. Já com o e-CNPJ, é possível assinar documentos digitais com validade jurídica, emitir notas fiscais eletrônicas ou realizar transações bancárias em meios eletrônicos.

2.3 CHAVES SIMÉTRICA E ASSIMÉTRICA

O modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Esta chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para decodificá-la na outra.

A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Se as chaves utilizadas forem complexas a elaboração

de um algoritmo de chave privada se torna bastante fácil, porém as possibilidades de interceptação são correlatas aos recursos empregados, entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação.

Cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. Neste caso, as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha). A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública.

A autenticidade pode ser garantida pela chave codificadora, como nos ensina Bill Gates (2002):

> A chave codificadora permite mais do que privacidade. Ela pode também garantir a autenticidade de um documento, porque a chave privada pode ser usada para codificar uma mensagem que só a chave pública pode decodificar. Funciona assim: se eu tenho uma informação que quero assinar antes de mandar de volta para você, meu computador usa minha chave privada para codificá-la. Só pode ser lida se minha chave pública que você e todo mundo conhece - for usada para decifrá-la. Essa mensagem é com certeza minha, pois ninguém mais tem a chave privada capaz de codifica-la dessa forma (Gates, 2002, on line).

2.4 A SEGURANÇA DO CERTIFICADO DIGITAL

Os Certificados Digitais são muito seguros. Para que se tenha o máximo de confiabilidade em suas transações, é necessário que você não compartilhe sua senha com ninguém. Se alguém conseguir roubar seu Certificado Digital, não poderá utilizá-lo, a menos que tenha a chave privativa correspondente e a senha para essa. Pense em sua senha como a chave de um cofre. Se você for à única pessoa a possuir a chave, o conteúdo do cofre estará seguro. Entretanto, se a chave for compartilhada com outras pessoas, você reduzirá a segurança do conteúdo do cofre.

De acordo com o ICP-Brasil (2017), a Chave Privativa é um arquivo gerado quando você se inscreve para obter o Certificado Digital, neste momento, seu navegador da web cria uma chave privativa que, em seguida, é armazenada no disco rígido do computador para que você possa controlar o acesso a ele. Ao gerar sua chave privativa, o software que você utiliza como seu navegador, provavelmente, lhe pedirá uma senha. Essa senha protege o acesso a sua chave privativa. Um terceiro pode acessar sua chave privativa, se tiver acesso ao arquivo em que sua chave está armazenada e conhecer a sua senha. Alguns softwares (programas) lhe permitem optar por não ter uma senha para proteger sua chave privativa, porém, se você usar esta opção, deve estar certo de que pessoas não autorizadas não tenham acesso ao seu computador. É responsabilidade do portador proteger sua chave privativa. Qualquer pessoa que obtiver sua chave privativa poderá falsificar sua assinatura digital e tomar atitudes em seu nome.

2.5 REQUISITOS NECESSÁRIOS PARA COMPOR UM CERTIFICADO DIGITAL

Para que o documento digital tenha validade jurídica é necessário que atenda alguns requisitos, que se referem tanto aos documentos tradicionais quanto aos documentos eletrônicos. Devem ser exigidas, para as duas modalidades de documento, a verificação da autenticidade, da integridade e da tempestividade.

De acordo com a regulamentadora ICP-Brasil (2017), a autenticidade de um documento

é relativa a possibilidade de verificação de sua procedência subjetiva; isso significa que poderemos assegurar a posse de determinado documento. Geralmente o que demonstra a autoria de um documento tradicional é a assinatura aposta no suporte material; em se tratando de documento eletrônico é a assinatura digital que tem função de autenticação. Já com relação aos documentos manuscritos não assinados, quanto à autenticidade, que estes podem ter sua autoria demonstrada por meio de análise grafológica, caso o suposto autor esteja negando a feitura dos escritos.

2.6 A CERTIFICAÇÃO DIGITAL NO BRASIL

A autoridade certificadora Raiz da ICP- Brasil é a primeira autoridade da cadeia de certificação. Executa as políticas de certificados e normas técnicas e operacionais aprovadas pelo comitê gestor da ICP- Brasil. Portanto compete a ela emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

Na prática, o certificado digital funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. “Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma autoridade certificadora que, seguindo regras estabelecidas pelo comitê gestor da ICP- Brasil associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas” (ICP-Brasil, 2017, on line). O certificado contém os dados de seu titular conforme detalhado na política de segurança de cada autoridade certificadora.

2.7 OS TIPOS DE CERTIFICADOS DIGITAIS

Em relação à forma de armazenamento e período de validade, o certificado digital pode ser do tipo:

- **A1**: O certificado digital é armazenado no seu computador e tem validade de um ano;
- **A3**: O certificado digital é armazenado em um dispositivo criptográfico (Token USB ou Smart Card) e tem validade de até três anos.

Referente à utilização e finalidade do certificado digital, ele pode ser do tipo:

2.7.1 e-CPF - Certificado digital para pessoas físicas, versão eletrônica do CPF

O e-CPF é um documento eletrônico de identidade em formato de certificado digital para pessoas físicas. Ele é utilizado por contribuintes, contadores, médicos, advogados, representantes legais de empresas e outros profissionais. Com ele, pode-se:

- Acessar os serviços e informações do site da Receita Federal;
- Entregar o Imposto de renda (DIPJ);
- Utilizar Escrituração Digital (SPED Contábil, somente e-CPF A3);
- Gerar procuração eletrônica para seu contador;
- Cumprir a IN 969, que determina que todas as empresas com impostos calculados pelo lucro real, presumido e arbitrário, utilizem Certificado Digital para enviar DIPJ;
- Assinar documentos eletrônicos com validade jurídica;
- Autenticar-se em sites e sistemas com segurança;
- Participar de Pregões Eletrônicos do Governo;
- Verificar a autenticidade das informações do Diário Oficial (versão on-line);

- Acessar outros serviços do Governo (Poder Judiciário, saúde, educação, etc);

2.7.2 e-CNPJ - Certificado digital para empresas, versão eletrônica do CNPJ

O e-CNPJ é um documento eletrônico em formato de certificado digital (versão digital do CNPJ). Ele garante a autenticidade e integridade das transações realizadas na internet por pessoas jurídicas. Com ele a sua empresa pode:

- Acessar os serviços e informações do site da Receita Federal;
- Entregar o Imposto de Renda (DIPJ);
- Utilizar Escrituração Digital (SPED Fiscal e Contábil, somente e-CNPJ A3);
- Gerar procuração eletrônica para seu contador;
- Acessar ao sistema de Conectividade Social ICP da CAIXA (FGTS);
- Cumprir a IN 969, que determina que todas as empresas com impostos calculados pelo lucro real, presumido e arbitrário, utilizem Certificado Digital para enviar DIPJ;
- Assinar documentos eletrônicos com validade jurídica;
- Autenticar-se em sites e sistemas com segurança;
- Participar de Pregões Eletrônicos do Governo;
- Verificar a autenticidade das informações do Diário Oficial (versão on-line);
- Acessar o SISCOMEX (Sistema Integrado de Comércio Exterior);
- Acessar outros serviços dos governos (Poder Judiciário, saúde, educação, etc);

2.7.3 NF-e - nota fiscal eletrônica

A Nota Fiscal Eletrônica ou NF-e, é um documento eletrônico fiscal e que tem por fim o registro de uma transferência de propriedade sobre um bem ou uma atividade comercial prestada por uma empresa e uma pessoa física ou outra empresa. A NF-e é a versão eletrônica do documento Nota Fiscal.

O governo programou um modelo nacional de documento fiscal eletrônico que venha substituir a sistemática atual de emissão do documento fiscal em papel, com validade jurídica, pela assinatura digital do remetente utilizando um certificado digital ICP-Brasil, simplificando as obrigações acessórias dos contribuintes e permitindo, ao mesmo tempo, o acompanhamento em tempo real das operações comerciais pelo Fisco.

A NF-e tem validade fiscal e jurídica garantida pela assinatura do emitente realizada com o uso de um certificado digital no padrão ICP-Brasil. É o certificado, portanto, que garante à Nota Fiscal Eletrônica a certeza de integridade e autoria.

2.7.4 NFC-e - nota Fiscal de Consumidor Eletrônica

A NFC-e ou Nota Fiscal de Consumidor Eletrônica é um documento de existência apenas digital, emitido e armazenado eletronicamente, com o intuito de documentar as operações comerciais de venda presencial ou venda para entrega em domicilio o consumidor final (pessoa física ou jurídica) em operação interna e sem geração de crédito de ICMS ao adquirente (SERASA, 2017).

A NFC-e substituirá o tradicional cupom fiscal emitido em lojas, supermercados, drogarias e comércio varejista em geral na maioria dos estados brasileiros.

A maior vantagem é que a impressão do cupom fiscal, que passará a ser chamado de DANFE NFC-e (Documento Auxiliar da Nota Fiscal de Consumidor Eletrônica) será opcional e tudo poderá ser controlado pela internet e por meio de tablets e smartphones.

3 PROCEDIMENTOS METODOLÓGICOS

A metodologia é compreendida como uma disciplina que consiste em estudar, compreender e avaliar os vários métodos disponíveis para a realização de uma pesquisa acadêmica. A metodologia, em um nível aplicado, examina, descreve, avalia métodos e técnicas de pesquisa que possibilitam a coleta e o processamento de informações, visando ao encaminhamento e à resolução de problemas e/ou questões de investigação. (Gil, 2008)

3.1 CARACTERÍSTICAS DE PESQUISA

A metodologia aplicada neste trabalho é a pesquisa descritiva que visa descrever as características e determinada população ou fenômeno ou estabelecimento de relações entre variáveis. Envolve o uso de técnicas padronizadas de coleta de dados: Questionário e observação sistemática. Assume, em geral, a forma de levantamento (pesquisa de campo).

De acordo com Goldenberg (2002) a curiosidade, a criatividade, a disciplina e especialmente, a paixão são algumas exigências para o desenvolvimento de um trabalho criterioso, baseado no confronto permanente entre o desejo e realidade (GOLDENBERG, 2002).

Para confirmar o uso do certificado digital, bem como as dificuldades apresentadas, utilizou-se a aplicação de um questionário em duas empresas do Município de São Marcos, sendo este respondido por dezoito entrevistados, todos colaboradores da área administrativa/financeira, com o intuito de esclarecer se realmente há conhecimento de tal assunto e as dificuldades apresentadas.

A pesquisa foi realizada entre os meses de maio de junho de 2017.

O questionário foi composto por sete perguntas direcionadas (questionário fechado) e uma pergunta aberta.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

A partir dos resultados obtidos com as entrevistas, comprovou-se que, dos entrevistados, a maioria não tem conhecimento de todas as funções do certificado digital ou nunca precisou do certificado digital nas suas atividades.

A maioria das empresas atualmente tem utilizado este recurso, dentre as funcionalidades principais, as mesmas utilizam para emissão de notas, parcelamentos na receita federal e internet banking, com este recurso as empresas alegam que ganham tempo em suas atividades e tem uma segurança maior e melhor não precisando recorrer a qualquer tipo de serviço pessoalmente.

Com base nas respostas obtidas, aplicou-se questões direcionadas e abertas ao tema sobre certificado digital e seu difícil entendimento, recorrendo a profissionais de áreas administrativa e financeira, e que portanto, deveriam fazer uso deste recurso, podendo, assim, fornecer informações sobre essa segurança que é tão pouco conhecida e tão necessária.

A primeira pergunta identificava a idade dos entrevistados, sendo que 02 entrevistados têm entre 18 a 25 anos, 2 entre 26 a 30 e 14 acima de 30 anos.

A segunda pergunta solicitava-se aos entrevistados se estes tinham conhecimento sobre o que era o certificado digital, sendo que 12 disseram que sim e 6 disseram que não.

A pergunta seguinte solicitava aos entrevistados se estes sabiam a importância do certificado digital, sendo que 10 responderam sim e 8 não.

Questionados sobre o conhecimento do uso do certificado digital, 12 responderam que sim e 6 e que não.

Dos entrevistados, 17 disseram que não conhecem esta segurança por outro nome.

Também foi perguntado aos entrevistados se estes tem conhecimento de outras utilizações, além das usuais, para o certificado digital, sendo que 50% dos entrevistados responderam que não.

Na maioria dos entrevistados (90%) referiu, no último questionamento, que o certificado digital serve para segurança de arquivos e documentos para a empresa, e acesso a mensagens enviadas pela Receita Federal, para acesso e internet banking, documentos fiscais e faturamento, desconhecendo as diversas outras utilidades para este recurso.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento dos estudos com base na criptografia simétrica e assimétrica possibilita o seu emprego nas assinaturas digitais, que constituem, em conjugação com os certificados digitais, meio seguro e eficaz de identificação em ambientes virtuais bem assim de atribuição de autoria de documentos eletrônicos.

As assinaturas e os certificados digitais servem para agregar os valores confiança e segurança às comunicações e negócios vinculados em ambiente virtual, especialmente na internet.

A inclusão digital serve para garantir que todas as pessoas, independente de classe social, etnia, religião ou poder econômico, tenham condições de usufruir as potencialidades das ferramentas tecnológicas de comunicação e informação.

A assinatura digital é viabilizada pelo emprego da criptografia simétrica/ assimétrica ou criptografia de chaves públicas.

Para agregar mais segurança às comunicações virtuais, é necessário outro elemento que dê certeza àquela pessoa que recebeu uma mensagem eletrônica assinada digitalmente de que a pessoa que a assinou é realmente quem diz ser. Aí que entram os certificados digitais. É preciso que um terceiro de confiança de ambas as partes ateste que a chave pública daquela pessoa que assinou digitalmente realmente lhe pertence. O certificado digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável que associa o nome e atributos de uma pessoa a uma chave pública. O fornecimento de um certificado digital é um serviço semelhante ao de identificação para a expedição de carteiras de identidade. O interessado é identificado mediante a sua presença física pelo terceiro de confiança, com a apresentação dos documentos necessários e este lhe emite o certificado digital.

A criptografia protege a informação que não pertence à esfera pública e que, portanto, deve permanecer sob o controle dos indivíduos. O sistema criptográfico surge como uma forma de salvar e guardar as informações individuais, evitando o risco de crimes e a invasão.

No entanto, de nada adianta tal tecnologia, e a obrigatoriedade de uso desta, se a população e profissionais que dela se utilizam não sabem operar ou não tem conhecimento de suas funcionalidades.

A partir do resultado obtido pela entrevista, observou-se que profissionais sequer sabem da existência dessa tecnologia, e aqueles que a conhecem, 50% destes não sabem da existência de outras funcionalidades.

Tal constatação fica evidente inclusive na dificuldade de se encontrar material para pesquisa, sendo que os poucos dados encontrados ficam restritos aqueles fornecidos pelas empresas certificadoras, sendo esta a grande dificuldade desta pesquisa, ou seja, encontrar material bibliográfico para consulta.

Portanto, considerando a larga escala em que se é utilizada, bem como a obrigatoriedade de utilização deste recurso por órgãos públicos, fica evidente a necessidade de inclusão digital de seus usuários a partir meios que facilitem a sua compreensão, como cursos gratuitos e unidades de apoio ao cidadão e profissionais.

REFERÊNCIAS

BANESTES. **Segurança do Certificado Digital.** Disponível em <http://www.banestes.com.br/seguranca/index_certificado.htm>. Acesso em 30 mai. 2017.

BONILLA, Maria Helena S.; PRETTO, Nelson L. **Inclusão Digital: Polêmica Contemporânea.** Salvador: EDFBA.2011.

CASTELLS, Manuel. **O caos e o progresso**. 2005. Entrevistadora: Keli lynn Boop. Portal do Projeto Software Livre do Brasil. Disponível em: http://www.softwarelivre.org.

GIL. A. C. **Métodos e técnicas de pesquisa social**. 6ª ed. São Paulo: Atlas. 2008.

INSTITUTO NACIONAL DE TECNOLOGIA E INFORMAÇÃO**. Comitê Gestor da ICP-Brasil Aprova todos os Itens da Pauta.** Disponível em < www.iti.gov.br> Acesso em 01 jun. 2017.

MARTINS, José de Souza. **Exclusão social e a nova desigualdade**. 2. ed. São Paulo: Paulus, 2003. (Coleção Temas de Atualidade).

NETO, Ângelo B. , NABASA, Gustavo. UFSC. **Certificado digital.** Disponível em <http://egov.ufsc.br>. Acesso em 20 mai. 2017.

RADIPSSL. **Certificados Digitais ICP Brasil**. Disponível em <ttp://www.rapidssl.com.br/certificado-digital>. Acesso em 02 jun. 2017.

RIBEIRO. Marlene. **Exclusão: problematização do conceito**. Educação e Pesquisa. São Paulo, v. 25, n. 1, p. 35-49 , jan./jun. 1999.

SERASA EXPERIAN. **Principais Usos do Certificado Digital.** Disponível em <https://serasa.certificadodigital.com.br/uso/> Acesso em 06 jun. de 2017.