FACULDADE DE SÃO MARCOS
CURSO DE CIÊNCIAS CONTÁBEIS
PROFESSOR: QUERLI POLO SUZIN
ALUNO (A): JÉSSICA AVER MELARA E SAIURI SCAIN PELLISSARI

CERTIFICADO DIGITAL E SEU DIFÍCIL ENTENDIMENTO

São Marcos
Junho/2017

SUMÁRIO

1 INTRODUÇÃO.....3

2 REFERENCIAL TEÓRICO.....4

2.1 Certificado digital.....4

2.1.1 Quem emite o certificado digital.....4

2.1.2 Como obter o certificado digital.....5

2.2 Chaves Simétrica e Assimétrica.....6

2.3 A segurança do certificado digital.....7

2.4 Requisitos necessários para compor um certificado digital.....7

2.5 A certificação digital no Brasil.....7

2.6 Os tipos de certificado digital.....8

3 METODOLOGIA.....11

3.1 Características da pesquisa.....11

4 ANÁSILE E DISCUSSÃO DE RESULTADOS.....12

5 CONSIDERAÇÕES FINAIS.....13

REFERÊNCIAS.....14

APÊNDICE.....15

1 INTRODUÇÃO

O presente trabalho tem por finalidade, o esclarecimento sobre o certificado digital que tem por objetivo especifico a assinatura com validade jurídica, 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, contém informações que identificam uma pessoa, uma máquina, ou uma instituição da internet.

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.

Assim, este trabalho teve como problema de pesquisa a intenção de entender em geral a utilização do certificado digital nas empresas e com pessoas físicas, e analisar o quanto a população conhece esta tecnologia e a utiliza, apresentando as vantagens que a mesma oferece.

2 REFERENCIAL TEÓRICO

2.1 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. 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;

2.1.1 Quem emite o certificado digital?

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).

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

Isto é, o elemento que da 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.

2.1.2 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.

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.

2.2 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:

> “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”

2.3 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.

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 sua responsabilidade proteger sua chave privativa. Qualquer pessoa que obtiver sua chave privativa poderá falsificar sua assinatura digital e tomar atitudes em seu nome.

2.4 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.

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.

2.5 A certificação digital no Brasil

A autoridade certificadora Raiz da ICP- Brasil é a primeira autoridade da cadeia de certificação. Executa as politicas 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. O certificado contém os dados de seu titular conforme detalhado na politica de segurança de cada autoridade certificadora.

2.6 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:

- **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);

- 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);

- 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.

- 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.

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 METODOLOGIA

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).

Para confirmar o uso do certificado digital nas empresas e com a população, utilizou- se com base um questionário com duas empresas no município de São Marcos de diferentes setores e dezoito pessoas, com o intuito de esclarecer se realmente a conhecimento de tal assunto.

> “Curiosidade, criatividade, disciplina e especialmente paixão são algumas exigências para o desenvolvimento de um trabalho criterioso, baseado no confronto permanente entre o desejo e realidade.”
>
> (GOLDENBERG, 2002)

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A partir da pesquisa realizada com as dezessete pessoas e três empresas, comprovou- se que, dos entrevistados (pessoa física), a maioria não sabe a função do mesmo ou nunca precisou do certificado digital nas suas atividades.

A maioria das empresas (pessoa jurídica) atualmente tem utilizado este recurso, dentre as características 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 ao tema sobre certificado digital e seu difícil entendimento, recorrendo a pessoas físicas e jurídicas, com o intuito de adquirir informações sobre essa segurança que é tão pouco conhecida e tão necessária.

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 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.

REFERÊNCIAS BIBLIOGRÁFICAS

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

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.

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.

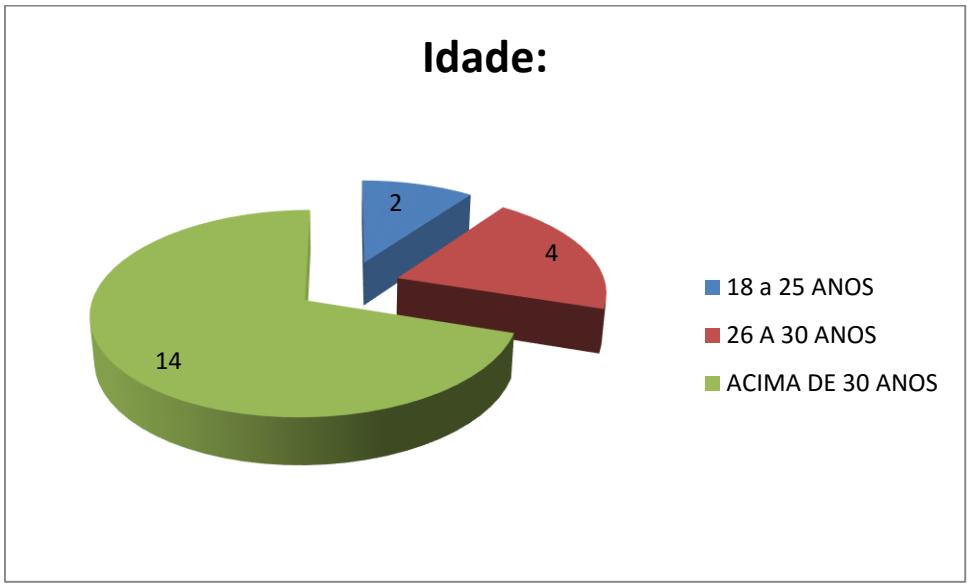
SERASA EXPERIAN. **Principais Usos do Certificado Digital.** Disponível em <https://serasa.certificadodigital.com.br/uso/> Acesso em 06 jun. de 2017.

APÊNDICES

GRÁFICOS:

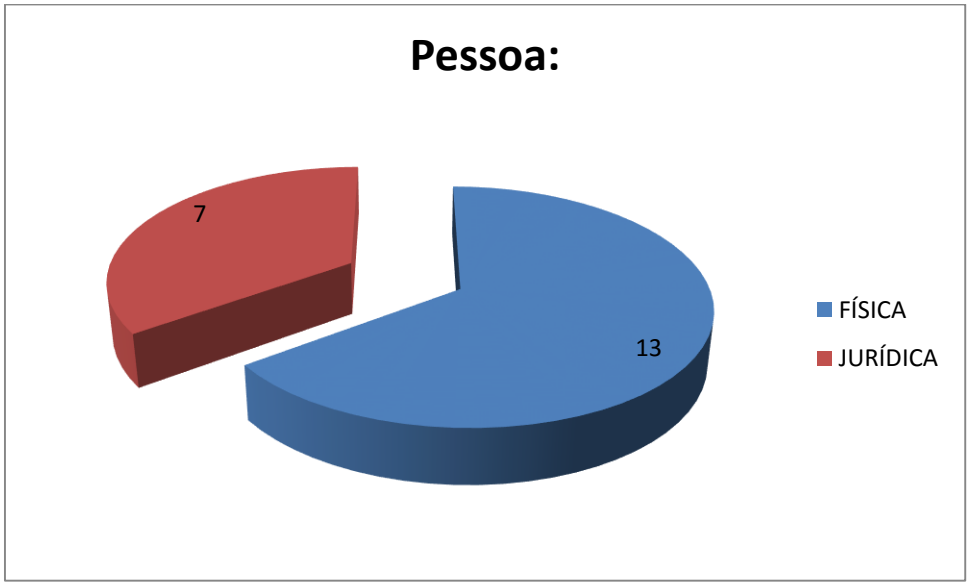
IDADE:

( ) 18 A 25 ANOS ( ) 26 A 30 ANOS ( ) ACIMA DE 30 ANOS



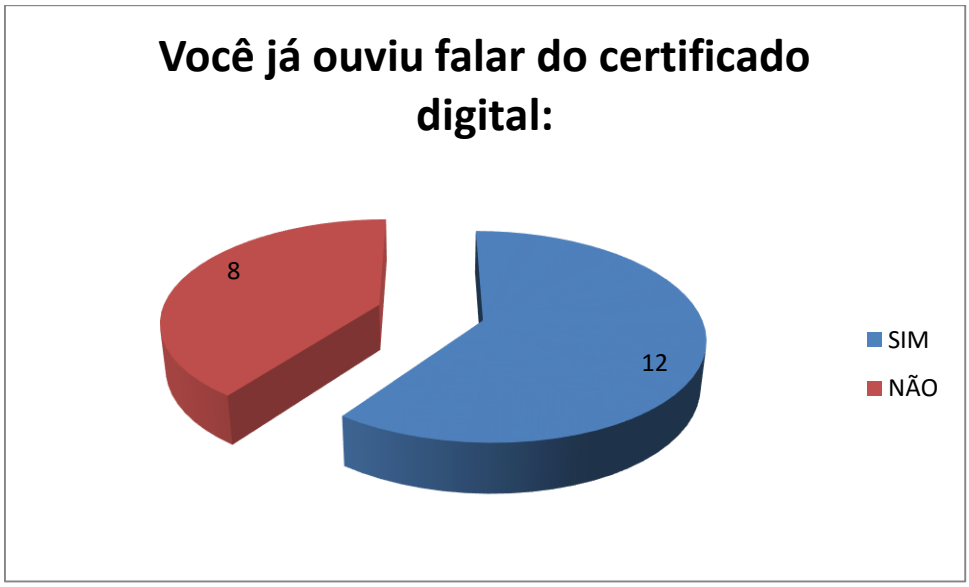
PESSOA:

( ) FÍSICA ( ) JURÍDICA



1-VOCÊ JÁ OUVIU FALAR DO CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

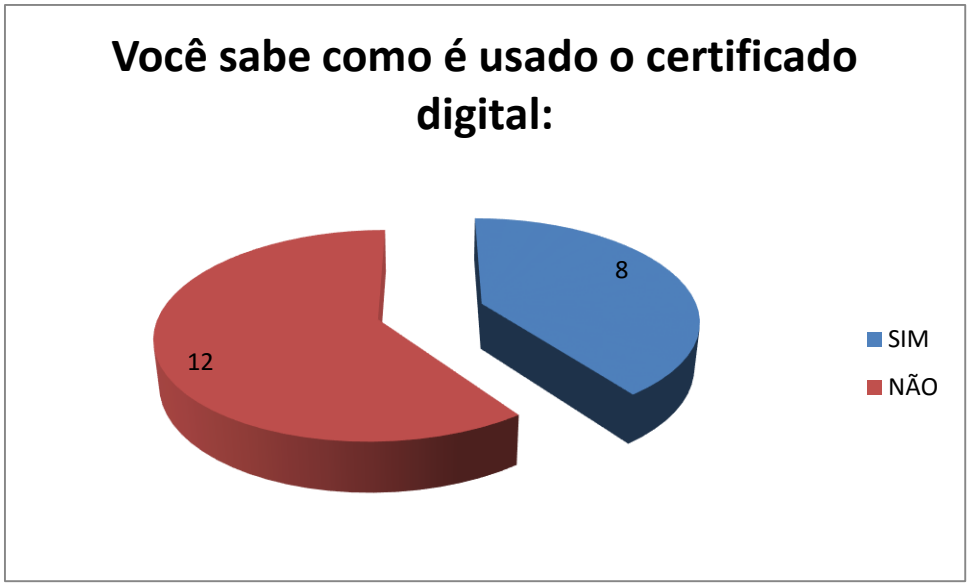


2 - VOCÊ SABE A IMPORTÂNCIA DO CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

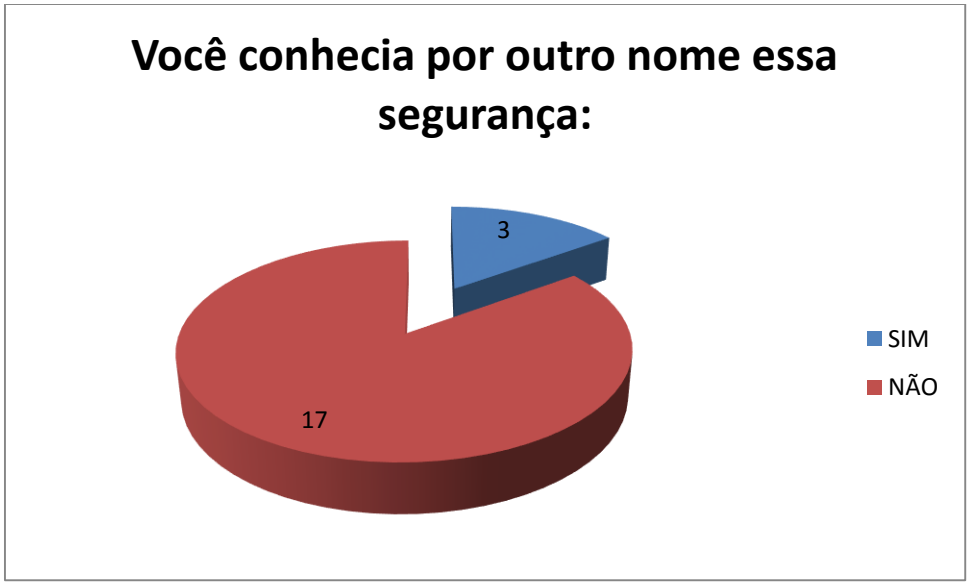
3-VOCÊ SABE COMO É USADO O CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO



4-VOCÊ CONHECIA POR OUTRO NOME ESSA SEGURANÇA?

( )SIM ( )NÃO



5- VOCÊ SABE PARA QUE SEJA USADO O CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

SE SIM, PARA QUE?

Na maioria dos entrevistados concordam que o certificado digital serve para segurança de arquivos e documentos para a empresa, e acesso a mensagens enviadas pela Receita Federal.

6 - VOCÊ SABE POR QUEM É USADO O CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

SE SIM, POR QUÊ?

Na maioria todos concordaram que e usado para acesso e internet banking, documentos fiscais e faturamento.

7- UTILIZA O CERTIFICADO DIGITAL EM SUAS ATIVIDADES?

12 pessoas sim

8 pessoas não

8- JÁ PRECISOU SE SOCORRER DE AJUDA DE OUTRO PROFISSIONAL PARA UTILIZAR O CERTIFICADO DIGITAL?

6 pessoas sim

14 pessoas não

QUESTIONÁRIO

IDADE:

( ) 18 A 25 ANOS ( ) 26 A 30 ANOS ( ) ACIMA DE 30 ANOS

PESSOA:

( ) FÍSICA ( ) JURÍDICA

1-VOCÊ JÁ OUVIU FALAR DO CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

2 - VOCÊ SABE A IMPORTÂNCIA DO CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

3-VOCÊ SABE COMO É USADO O CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

4-VOCÊ CONHECIA POR OUTRO NOME ESSA SEGURANÇA?

( )SIM ( )NÃO

5- VOCÊ SABE PARA QUE SEJA USADO O CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

SE SIM, PARA QUE?

_____
_____

6 - VOCÊ SABE POR QUEM É USADO O CERTIFICADO DIGITAL?

( ) SIM ( ) NÃO

SE SIM, POR QUÊ?

_____
_____

7- UTILIZA O CERTIFICADO DIGITAL EM SUAS ATIVIDADES?

_____
_____

8- JÁ PRECISOU SE SOCORRER DE AJUDA DE OUTRO PROFISSIONAL PARA UTILIZAR O CERTIFICADO DIGITAL?

_____
_____