FACULDADE DE TECNOLOGIA ALCIDES MAYA - AMTEC

CURSO TÉCNICO EM INFORMÁTICA

LEONARDO ROSSATO JUDES
MARLON EDUARDO NUNES DE OLIVEIRA

AMPLIAÇÃO DA SEGURANÇA DOS CERTIFICADOS E ASSINATURAS DIGITAIS

Porto Alegre

2019

LEONARDO ROSSATO
MARLON EDUARDO NUNES DE OLIVEIRA

AMPLIAÇÃO DA SEGURANÇA DOS CERTIFICADOS E ASSINATURAS DIGITAIS

Projeto de Pesquisa apresentado como requisito parcial para obtenção do título de Técnico em informática, Faculdade de Tecnologia Alcides Maya - AMTEC

Orientador: Prof. Vinicius Avila Rossamai

Porto Alegre

2019

LISTA DE SIGLAS

ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
CNPJ	Cadastro Nacional da Pessoa Jurídica
CPF	Cadastro de Pessoa Física
CA	Autoridade de Certificação
AC	Autoridade de Certificação
RA	Autoridade de Registro
ACT	Autoridades de Carimbo do Tempo
PSS	Prestadores de Serviço de Suporte
DPC	Declaração de Práticas de Certificação
PCN	Plano de Continuidade de Negócio
CG	Comitê Gestor
PC	Políticas de Certificado

SUMÁRIO

1 INTRODUÇÃO

Com o passar dos tempos o mundo foi-se adaptando com o avanço em muitos aspectos, na qual o ser humano hoje em dia não saberia viver sem, e uma delas se não a mais importante, é o avanço tecnológico, ressaltando que tudo em que tocamos, mexemos e vivenciamos hoje em dia gira em torno da tecnologia, seja ela pequena ou grande. Isto não seria possível se com o passar dos tempos, as pessoas não quisessem descobrir o que elas não sabem, e foi assim que muitas formas que antes só se podia existir fisicamente, foram melhoradas e adaptadas para a tecnologia virtual, sem a necessidade de sair do seu próprio local em que se encontra, seja para entregar documento, assinar e enviar.

O documento digital e a assinatura digital, é nada mais do que um meio em que foi encontrado para agilizar e poupar tempo na hora de receber ou assinar documentos pelo próprio dispositivo eletrônico, assim melhorando a forma em que empresas conseguem fazer a sua comunicação de forma mais rápida e confiável de empresa/cliente. Ainda sim é muito duvidoso entre pessoas essa “nova” forma de fazer tudo isso apenas digitalmente, já que nossa assinatura e documento, muitas vezes precisam ser um tanto quanto sigiloso. Sendo assim Bill Gates afirma de forma explicativa como funciona a assinatura nesse mundo tecnológico:

> Quando você mandar uma mensagem pela estrada da informação, ela será “assinada” pelo seu computador, ou outro dispositivo de informação, com uma assinatura digital que só você será capaz de aplicar, e será codificada de forma que só seu destinatário real será capaz de decifrá-la. Você enviará uma mensagem, que pode ser informação de qualquer tipo, inclusive voz, vídeo ou dinheiro digital. O destinatário poderá ter certeza quase absoluta de que a mensagem é mesmo sua, que foi enviada exatamente na hora indicada, que não foi nem minimamente alterada e que outros não podem decifrá-la.Bill Gates(1995, apud, AGNALDO, PAOLA, JACOB, p.11).

1.1 Definição do Tema ou Problema

Certificados e assinaturas digitais e a sua veracidade em um ambiente de trabalho.

1.2 Delimitações do Trabalho

Certificado e assinaturas digitais em microempresas: o empreendedor pode transferir seu Token pessoal para uso em documentos a seus colaboradores?

1.3 Objetivos

Os objetivos dividem-se em: geral e específicos.

1.3.1 Objetivo Geral

Analisar a viabilidade do uso de assinaturas digitais na segurança dos documentos de uma empresa.

1.3.2 Objetivos Específicos

a) Compreender os perigos envolvidos em transferir senha pessoal para colegas;
b) Analisar os comportamentos dos usuários diante da segurança do Token;
c) Investigar formas para a ampliação da segurança dos documentos digitais.

1.4 Justificativa

O uso de tecnologia dentro de microempresas está se tornando cada vez mais natural, duas dessas tecnologias são os certificados e assinaturas digitais.

A segurança deste serviço de maneira externa é algo de total confiança, mas se analisarmos ele de maneira interna dentro de uma empresa pode trazer falhas, como compartilhamentos ou extravio da senha. Este ponto de vulnerabilidade desse serviço é um ponto útil para ser abordado.

2 REVISÃO BIBLIOGRÁFICA

2.1 Documentos

2.1.1 O que é um documento?

Um tanto quanto simples que essa pergunta possa parecer, muitas pessoas não sabem a definição de um documento.

Segundo nosso dicionário Aurélio, documento é: “Título ou diploma que serve de prova: documento histórico; qualquer objeto ou fato que serve de prova, confirmação ou testemunho: documentos fotográficos. ”

Já de acordo com Janice (p. 16):

> No senso comum, o documento costuma ser entendido como tudo aquilo que possa registrar (e atestar) o cumprimento de deveres do indivíduo, enquanto cidadão, ou mesmo servir como garantia de direitos; e, em geral, ‘documento’ também costuma estar identificado a ‘documento escrito’.

Por mais que as palavras possam parecer distintas para alguns, a definição é a mesma, documento é um registro de informações que servem para provas, lembranças ou confirmação de algo.

2.1.2 Gestão de documentos no meio institucional

Meios para a organização de documentos surgiu nos Estados Unidos, principalmente com a crise econômica de 1930 e logo em seguida com a Segunda Guerra Mundial. Com esses dois acontecimentos históricos em um curto prazo de tempo, o número de documentos cresceu exponencialmente, graças às pesquisas na época.

A gestão de documentos apareceu para obter uma melhor administração nas organizações públicas dos E.U.A. Planejava-se um meio para melhor eficiência dos procedimentos, assim, reduzindo os custos e gerando menos arquivos desnecessários (ALVES, 2014).

Os objetivos da gestão de documentos, segundo Caldeira (2008, p.22) são:

- Assegurar o pleno exercício da cidadania;

- Agilizar o acesso aos arquivos e às informações;
- Promover transparência das ações administrativas;
- Garantir economia, eficiência e eficácia na administração pública ou privada
- Controlar o fluxo de documentos e a organização dos arquivos
- Racionalizar a produção de documentos

A busca da preservação de documentos sempre foi um problema recorrente entre as instituições. Afinal, o que importava mesmo era a sua informação, não o documento em si. A preservação destes documentos são obrigatoriedade para quando preciso, ter acesso à informação contida nele (INNARELLI, 2018).

2.1.3 Documentos digitais

Com o surgimento da internet e o uso corporativo de computadores em empresas, os documentos padrões de papéis passaram a ser substituídos pelo documento digital, até pela sua forma mais fácil de arquivamento e acesso, como confiram Marcondes e Sayão(p. 43) “O surgimento da Internet a partir dos anos 90 vem mudando de maneira radical o papel das bibliotecas no ciclo intermediação e acesso ao documento.”

Ainda com a tecnologia em nosso dia a dia, empresas ainda são forçadas a guardar o documento físico para alguns casos jurídicos, pois não são todos os tipos de documentos que são aceitos com efeito legais. Atualmente somente documentos com certificados digitais são aceitos, documentos digitalizados são apenas para consulta e/ou preservação do documento original, sem outros fins (SCHÄFER; FLORES, 2013).

2.2 Segurança do documento digital

O documento digital tem como validade, a mesma integridade jurídica de um documento tradicional (papel impresso). No Brasil foi criada a ICP- Brasil (Infraestrutura de chaves Públicas Brasileiras) que possibilita a confiança para emissão de certificados digitais conseguindo assim a identificação de pessoas públicas ou jurídicas. Junto a este documento digital vem a Autoridade certificadora que é mais um meio de autenticação do documento, é ela que fica responsável por distribuir as chaves para assinatura digital ou criptografia, é ela também que disponibiliza os certificados digitais, que podem ser definidos em pessoas públicas

ou jurídicas, fazendo a identificação de quem você é para terceiros que estão a utilizar o documento.

“As técnicas de assinatura feitas por meio da Criptografia consistem numa mistura de dados ininteligíveis onde é necessário o uso de duas chaves, a pública e a privada, para que ele possa se tornar legível. É como se fosse um cofre forte que somente para quem tem o seu segredo é acessível” (BITTENCOURT, Angela Brasil).

O certificado digital é um documento eletrônico que é capaz de identificar o seu portador para assinaturas digitais do mesmo. De forma geral ele é como uma identificação digital fazendo com que cada um tenha a sua chave.

Já o certificado digital para pessoas jurídicas (e-CNPJ ou e-PJ) é um documento digital capaz de “representar” a empresa para qualquer tipo de utilização em documentos digitais, sendo emitido por uma autoridade certificadora do tipo A1 que fica armazenada em seu próprio computador ou do tipo A3 representado por mídia física, como token ou smart card.

2.2.1 Criptografia

Criptografia é a ciência que disfarça o significado de uma mensagem e usa a matemática para cifrar e decifrar tais mensagens. (FRANÇA, 2005).

Pelo o que indica na história, a criptografia começou a ser praticada cerca de 1.900 a.C. por um arquiteto chamado Khnumhotep II. Em alguns documentos escritos por ele para encontrar tesouros, ele trocava palavras por símbolos estranhos para atrapalhar ladrões que tentassem roubar.

Séculos após começaram outros métodos para criptografar mensagens. Esses métodos foram muito usados para guerras e fins de espionagem (ALMEIDA, 2012).

2.2.1.1 Criptografia moderna

Hoje a criptografia é usada comumente entre pessoas, empresas e governo. O uso dela é para a segurança de documentos com informações pessoais, bancários ou até mesmo jurídicos.

Os princípios básicos da criptografia atual são:

Integridade: Garante que a pessoa que recebeu a mensagem, a recebeu de forma correta sem nenhuma alteração.

Confidencialidade: O mantimento do sigilo da mensagem, que somente pessoas com a chave possam ter acesso a ela.

Autenticação: É a prova de quem enviou e recebeu a mensagem.

Não repúdio: Tanto a pessoa que enviou quanto a que recebeu não podem negar tal ato. (FIARRESGA, 2010).

2.2.1.2 Criptografia simétrica

Conhecida também como chave privada, criptografia simétrica é o modelo mais antigo da criptografia. Normalmente ela é usada para acessar algo ou para troca de mensagens entre duas pessoas (OLIVEIRA, 2007).

Essa chave deve ser reconhecida pelo remetente e destinatário da mensagem. Por esse fato ocorre o maior problema desse modelo: distribuições seguras das chaves. Ainda existe outro problema, a distribuição das chaves para muitas pessoas (AMARO, 2006).

> As principais vantagens da criptografia simétrica:
> - Velocidade, pois os algoritmos são muito rápidos, permitindo cifrar uma quantidade de dados em pouco tempo.
> - As chaves são relativamente pequenas e simples, permitindo gerar cifradores extremamente robustos.
> - Atinge aos objetivos de confidencialidade e de privacidade, mantendo os dados seguros.
>
> As principais desvantagens:
> - A chave pode ser compartilhada, o que pode complicar a gerência das chaves
> - Não permite autenticação do remetente.
> - Não permite o não-repúdio do remetente.
>
> (AMARO, 2006)

2.2.1.3 Criptografia assimétrica

O conceito de chave assimétrica ou também chave pública, foi primeiramente citado por Whitfield Diffie e Martin Hellman.

Diferentemente da criptografia simétrica, a assimétrica utiliza uma chave pública para codificar e uma chave privada para decodificar. A chave privada fica em posse do proprietário e não pode ser explícita a ninguém além dele, já a chave pública, como o próprio nome diz, serve para ser compartilhada (PEREIRA, 2003).

A criptografia assimétrica funciona a partir da dificuldade em calcular a operação inversa em determinadas operações problemáticas. Atualmente, existem três categorias de problemas matemáticos dos quais é construído o algoritmo de chaves públicas: fatoração inteira (IFP), logaritmo discreto (DLP) e o logaritmo discreto sobre curvas elípticas (ECDLP) (AMARO, 2006).

2.2.2 Certificado Digital

Segundo Dilma Resende (2009, p.4): “O certificado digital é um documento eletrônico que contém um nome e um número público exclusivo, chamado de chave pública. ”

Ele é um meio seguro de identificar o trânsito de uma mensagem ou negócio eletrônico, ainda possibilita a assinatura digital, com isso todos os arquivos trocados tem integridade, validade jurídica e confidencialidade (RESENDE, 2009). Ele pode ser emitido por pessoas físicas e jurídicas, equipamentos e aplicações. Isso é feito via Autoridade Certificadora, é a responsável por vincular o usuário ao um par de chaves criptográficas (pública e privada). Para o funcionamento do certificado digital é necessário a chave pública do destinatário e programas que associem (RIBEIRO, 2015).

2.2.2.1 Certificado digital na prática

ALFA precisa mandar um documento para BRAVO. Para que esse documento não sofra alterações até chegar no BRAVO, ALFA utiliza a chave pública

do BRAVO para criptografar este documento. Assim, somente BRAVO com a sua chave privada poderá decifrar essa mensagem.

Quando é um documento que não precisa sigilo, e sim somente manter sua integridade. ALFA usa sua chave privada para criptografar o documento, mantendo gerando uma criptografia referente aos bits contidos naquele documento (VERONESE, 2007).

2.2.2.2 O impacto nas empresas

Essa tecnologia causou inúmeros impactos no dia a dia das empresas. Redução de custos, menos burocracia, otimização do tempo e também maior segurança, já que o documento só pode ser modificado com autorização do titular (CAVALCANTI, 2012).

Os benefícios que o certificado digital tem alcançado são altos, A certificação digital à internet tornou-se outro meio de comunicação para diversos tipos de operações, com maior agilidade, facilidade de acesso (VIEIRA, 2016).

2.2.2.3 Tipos de certificados

São encontrados 8 tipos de certificados na ICP-Brasil. Duas séries conhecidas como A e S, e cada uma possui quatro tipos (1,2,3,4). (Ribeiro, 2015).

Certificado tipo A: é o mais utilizado, ele serve para realizar assinaturas digitais em todos os tipos de documentos. Ele identifica quem assina, atesta a autenticidade e confirma a integridade do documento (PEREIRA, 2018).

Certificado tipo S: ele serve para manter o sigilo de uma transição. Com ele somente um certificado digital autorizado é capaz de decifrar a criptografia imposta em um documento. Tornando o arquivo inacessível a pessoas não autorizadas (PEREIRA, 2018).

2.2.2.4 Tipos de certificados por segurança

Certificado tipo A1/S1: é armazenado no computador do usuário. É protegido por uma senha de acesso e somente com ela é possível acessar, mover, e copiar a chave privada associada a ele (RIBEIRO, 2015).

Certificado tipo A3/S3: esse é considerado o mais seguro que o modelo A1. É armazenado em um hardware criptográfico, normalmente um cartão inteligente ou token. Apenas quem tem a senha de acesso pode utilizar a chave privada (RIBEIRO, 2015).

2.2.2.5 Certificados da receita federal

O e-CPF e o e-CNPJ são certificações digitais que pessoas físicas e jurídicas podem usar no Brasil para acessar serviços online que necessitam sigilo. Foi criado em 2002 pela Secretaria da Receita Federal (RIBEIRO, 2015).

e-CNPJ: Ele é obtido online. Utilizado para emitir notas fiscais e outros comprovantes administrativos (MARQUEZ, 2018).

e-CPF: Ele é obtido através de software. Serve para fazer todas as tramitações pertinentes ao documento tradicional, como declarar imposto de renda (MARQUEZ, 2018).

2.2.3 Assinatura Digital

Um documento criado digitalmente não pode ser assinado de forma manuscrita, com isso surge a assinatura digital.

Os documentos digitais são fáceis de ser manipulados e alterados, mas a partir da assinatura digital este documento fica único e íntegro, sem ser possível alteração. Caso haja alguma mudança, é possível ser constatado (GANDINI; SALOMÃO; JACOB, 2001).

Quando se assina digitalmente, cria-se um resumo da mensagem chamado de “função hash”. É uma operação matemática única que permite checar se houve alguma alteração. Ela é enviada junto com o certificado digital, quando o destinatário recebe essa mensagem, ele verifica a mensagem com o valor dessa

operação criada no resumo. O destinatário também pode checar a assinatura com a chave pública do remetente. Pode-se cifrar o resumo, no lugar da mensagem. Isso acontece graças ao problema de decifrar mensagens muito longas (FREITAS; VERONESE, 2007).

Apesar da similaridade, a assinatura digital não se confunde com a criptografia assimétrica, suas finalidades são diferentes. Assinatura digital é para manter a integridade da mensagem ou documento e pela autenticidade de quem assinou e enviou (BEHRENS, 2005).

2.2.4 Biometria Digital

Biometria digital, especificamente é uma tecnologia de alta performance para reconhecer seu proprietário através de sua impressão digital em seu objeto ou eletrônico. Ela vem sendo bastante utilizada para cadastramento de documentos, identificações criminais e acesso a dispositivos móveis. Estima-se que daqui alguns anos tudo que o ser humano venha a utilizar, precisa-se ser posto primeiro sua biometria digital, como: casas, veículos, documentos entre outros. Esta tecnologia já está sendo utilizada desta forma, porém ainda não em um número exponencialmente (SILVEIRA, 2016).

2.2.4.1 Segurança na biometria digital

O principal ponto para terem criado esta tecnologia foi para uma maior segurança em qualquer ato que o proprietário venha a fazer ou desbloquear, já que para isso só depende de sua própria impressão digital que é única de pessoa para pessoa.

> Os dispositivos biométricos comerciais, na sua maioria, operam no modo verificação ou autenticação. Isto significa que o indivíduo apresenta sua impressão digital que será comparada com um template armazenado no banco de dados Jain et al(1997, apud COSTA, 2001, p.30).

Após a comparação ser feita o cidadão será aceito pelo sistema que denominam um-para-um que basicamente compara imagem com impressão digital para ter a total certeza de que é a mesma pessoa utilizando a impressão digital, mas

para isto acontecer o mesmo precisa estar cadastrado em um banco de dados, assim como em outros sistemas biométricos.

2.2.4.2 Falhas na biometria digital

Biometria digital comparada com outras tecnologias de reconhecimento é a mais aceita para ser utilizada, atrás dela fica a tecnologia por reconhecimento da íris do olho e reconhecimento da mão.

Porém nem tudo é perfeitamente seguro, a biometria vem sendo bastante “julgada” por ter alguns problemas, que em alguns casos são pequenos, mas que na maioria das vezes se torna uma dor de cabeça para quem a utiliza.

O principal problema é a falha da biometria quando uma respectiva pessoa utiliza a mesma, dando o erro de não reconhecer a pessoa por diversas tentativas, dando-lhe uma dor de cabeça por não acessar o que precisa rapidamente, além de ficar fazendo o mesmo ato por várias tentativas.

Outro erro, que na verdade pode ser dito como crime, é que na biometria outras pessoas podem “clonar” a impressão de terceiros. Isto acontece, pois, nossas impressões ficam em qualquer lugar em que tocamos, embora seja algo que acontece muito em filme, não se pode deixar passar pois utilizando os materiais certos isto pode ocorrer facilmente com quem deseja “roubar” a impressão de outra pessoa e utilizá-la para acessar seus pertences (SINFIC, 2005).

2.2.5 Infraestrutura de Chaves Públicas

A infraestrutura de chaves públicas, é uma lei criada para poder emitir os certificados digitais para identificação virtual de cada usuário em que irá usá-lo, no Brasil foi criada a ICP- Brasil (Infraestrutura de chaves Públicas Brasileiras) que possibilita a confiança para emissão de certificados digitais conseguindo assim a identificação de pessoas públicas ou jurídicas

Leva-se em conta que o Brasil usou o método de certificação com raiz única, em que o ITI (Instituto nacional de tecnologia da informação) tem o objetivo de ser a Autoridade certificadora raiz - AC Raiz, e que também pode credenciar e

descredenciar os demais participantes, supervisionar e fazer auditoria de processos (ICP-BRASIL; 2017).

Não existe também um único meio para identificação e autenticação das chaves públicas, existem dois métodos que geralmente inclui Autoridade de certificação (CAs) e Autoridade de registro (RAs). O CAs fornece os demais serviços, tais como:

-- Emissão de certificados digitais

-- Validação de certificados digitais

-- Revogação de certificados digitais

-- Distribuição de teclas públicas

É também um tanto quanto curioso quanto a segurança dessas chaves, já que há o compartilhamento delas entre 2 ou mais pessoas. É sempre indicado que não faça entre mais usuários, mas ainda sim as pessoas compartilham ou algo semelhante, isso existe em muitos meios virtuais, essa chave é basicamente uma senha que deveria ser guardada apenas com seu respectivo dono. Existe também bastante pessoas com uma má intenção a fim de burlar o sistema usando essa “distração” dos usuários na hora em que compartilham suas chaves (IBM, 2018).

2.2.5.1 Obrigações da AC Raiz

É também de suma importância saber as obrigações de cada parte na hora de obter suas chaves e certificado para que não haja transtorno caso venha a acontecer algum problema entre ambos.

Ao que se refere às obrigações por parte da empresa, segundo a Declaração das Práticas de Certificação da Autoridade Certificadora raiz da ICP-Brasil; versão 4.5.

> A. A geração e o gerenciamento do seu par de chaves criptográficas;
> B. A emissão e distribuição do seu certificado digital;
> C. A emissão, a expedição e a distribuição de certificados de AC de nível imediatamente subsequente ao seu;
> D. A publicação de certificados por ela emitidos;
> E. A revogação de certificados por ela emitidos;
> F. A emissão, o gerenciamento e a publicação de sua Lista de Certificados Revogados – LCR;
> G. A fiscalização e a auditoria das ACs, das Autoridades de Carimbo do Tempo (ACTs), das ARs e dos Prestadores de Serviço de Suporte (PSS)

> habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor da ICP-Brasil (CG da ICP-Brasil);
> H. A implementação de acordos de certificação cruzada, conforme as diretrizes estabelecidas pelo CG da ICP-Brasil;
> I. Adotar medidas de segurança e controle, previstas nesta DPC e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [1], envolvendo seus processos, procedimentos e atividades;
> J. Manter os processos, procedimentos e atividades em conformidade com a legislação vigente e com as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
> K. Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
> L. Manter e testar regularmente seu Plano de Continuidade de Negócio (PCN).

Ao que se refere às obrigações por parte dos usuários, segundo a Declaração das Práticas de Certificação da Autoridade Certificadora raiz da ICP-Brasil; versão 4.5.

> A. Toda informação necessária para a identificação da AC titular de certificado deve ser fornecida de forma completa e precisa, ao aceitar o certificado emitido pela AC Raiz. A AC titular é responsável por todas as informações por ela fornecidas, contidas neste certificado.
> B. A AC titular de certificado emitido pela AC Raiz deve operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que será implementada em conformidade com os documentos

2.3 Comportamento humano com senhas digitais

Atualmente, empresas têm investido muito em segurança da informação. Desde a parte na infraestrutura, quanto na parte de softwares, mas todo esse investimento será inútil se o colaborador não for conscientizado e capacitado sobre a importância na proteção dos dados (FONSECA, 2009).

Um dos grandes problemas é a limitação da memória humana. Quanto mais complexa a senha, maior será a dificuldade para um hacker decifrar ela com algum malware, mas também é mais difícil para um humano memorizar ela, então normalmente isso é anotado em algum lugar específico para a pessoa recordar, e se avaliarmos, isso traz outro risco de alguém achar essa anotação com a senha (SILVA; STEIN, 2007).

Isso ocorre em muitas empresas com o seu token do certificado digital, em muitas vezes deixando a senha padrão visível na sua mesa, disponível para a visualização de qualquer colaborador, mesmo que na sua função hierárquica ele não poderia ter tal acesso.

2.3.1 Engenharia Social

Engenharia social, mais conhecida também como Segurança da informação, é um ato na qual um usuário com más intenções vem a fazer contra uma empresa ou pessoa. Isto não tem relação com roubar ou praticar crimes fisicamente, mas sim em roubar informações sigilosas que muitas vezes não é levada em tamanha consideração quanto a segurança pela empresa ou pessoa que está disponibilizando o tal documento ou produto. Muitas pessoas ainda acham que se trata de um “roubo” com tamanho esforço e uso de alta tecnologia, mas na verdade o que realmente faz com que isso aconteça é a falta de segurança que a empresa deposita neste produto. Isto faz com que tudo seja mais facilmente acessível e assim roubado ou divulgado na internet, tais como propagandas de produtos, documentos, plantas, estratégias.

Autoconfiança, facilidade de comunicação, aptidão profissional e grande capacidade de persuasão são características de um engenheiro social, sendo assim algumas pessoas já deram inúmeras declarações na qual nem sabiam que tinham passado informações que não deviam, e com isso teve o que mantinha em sigilo, vazado (CIPOLI, 2012).

A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia Kevin Mitnick (2003, apud, COSTA, 2010, p.4).

Nos certificados digitais, é um tanto quanto seguro saber se o uso está sendo de total segurança ou não, já que a autoridade certificadora fica responsável por emitir os certificados digitais que identificam sites na internet e seus proprietários (donos). Quando assinado, a autoridade certificadora relaciona a identidade do portador do certificado. Os navegadores seguros validam “dizendo” se a página visitada tem um certificado válido, caso não tenha o site é falso (COSTA, 2010, p.7).

2.3.2 Métodos que as empresas devem adotar

A empresa deve deixar claro aos seus colaboradores a importância na confidência das informações. Deve-se anotar políticas de segurança da informação, traçar os cargos hierárquicos de cada um dentro da empresa, para somente pessoas autorizadas consiga acesso a dados mais privilegiados, criar uma conscientização aos colaboradores como palestras, estudos e reuniões sobre o risco em transferir sua senha pessoal para alguém de um cargo não equivalente ao seu, pois como disse Fonseca (2009, p. 15) “Para evitar que esse tipo de situação ocorra é necessário criar políticas de segurança e disseminá-las para que seus colaboradores possam ter uma referência sobre o que é segurança da informação”.

3 METODOLOGIA

Pesquisa do tipo exploratória com abordagem qualitativa baseada no método de análise de documentos.

Através da análise de periódicos acadêmicos, jornais, livros e revistas em busca da compreensão dos certificados e assinaturas digitais e a sua veracidade em um ambiente de trabalho nas microempresas aplica-se a interpretação de forma comparativa e associativa das informações a fim de elaborar conclusões, limitando ao material pesquisado sem a oportunidade de experimento de campo.

4 CONCLUSÃO

Por mais que a criptografia tenha inovado com o tempo, nós humanos evoluímos muito pouco comparado aos avanços tecnológicos, por isso, muitos citam que as pessoas são o elo mais fraco da segurança. Abordamos os riscos que envolvem o engenheiro social no meio da segurança da informação. Microempresas apesar de sofrerem com a instabilidade financeira, devem investir na capacitação de seus colaboradores, já que bem treinados saberão lidar com futuras ameaças.

Consumamos que a biometria digital é uma tecnologia que complementará à segurança dos certificados e assinaturas digitais. Como cada humano tem sua própria biometria, aumentará a legitimidade e integridade do documento assinado digitalmente.

5 CRONOGRAMA

Atividades	Projeto Final							
	Projeto 1				Projeto 2			
	1ª sem	2ª sem	3ª sem	4ª sem	1ª sem	2ª sem	3ª sem	4ª sem
Definição das duplas Orientação e definição do tema Entrega: Tema, Delimitação	X							
Objetivos, referências e justificativa		X						
Fundamentação teórica			X					
Fundamentação teórica e Descrição da solução				X				
Metodologia, Validação (quando houver), Conclusão e Cronograma					X			
Conclusão, Cronograma e Introdução						X		
Anexos e entrega preliminar (últimos ajustes)							X	
Entrega do projeto finalizado								X

6 REFERÊNCIAS BIBLIOGRÁFICA

ALMEIDA, Paulo. **Criptografia e Segurança**. 2012. Departamento de matemática da Universidade de Aveiro.

ALVES, Geisiane da Silva. **GESTÃO DE DOCUMENTOS: UMA ANÁLISE DOS ASPECTOS DE RELEV NCIA DE UM SISTEMA DE GESTÃO DE DOCUMENTOS DIGITAIS NAS ORGANIZAÇÕES**. 2014. Universidade Federal Fluminense.

AMARO, George. **CRIPTOGRAFIA SIMÉTRICA E CRIPTOGRAFIA DE CHAVES PÚBLICAS: VANTAGENS E DESVANTAGENS**. 2006.

BEHRENS, Fabiele. **A Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira**. 2005. PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ.

CALDEIRA, Michel. **GESTÃO DOCUMENTAL: Programa de Demandas Customizadas**. 2018. Escola de Serviço Público do Espírito Santo.

CAVALCANTI, Vitor. **Entenda o impacto da certificação digital nas empresas**. 2012. Disponível em: <https://itforum365.com.br/entenda-o-impacto-da-certificacao-digital-nas-empresas/>. Acesso em: 19/04/2019.

CIPOLI, Pedro. **Engenharia social: Como funciona**. 2012 Disponivel em: <https://canaltech.com.br/seguranca/O-que-e-Engenharia-Social/>. Acesso em: 27/04/2019.

COSTA, Pedro Henrique Braga. **Técnicas de Engenharia Social**. 2010. Universidade Federal do Rio de Janeiro.

COSTA, Silva Maria Farini. **CLASSIFICAÇÃO E VERIFICAÇÃO DE IMPRESSÕES DIGITAIS**. 2001. USP.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática.** 2010. Universidade de Lisboa Faculdade de Ciências.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação: O Fator Humano**. 2009. Pontifícia Universidade Católica do Paraná.

FREITAS, Christiana Soares; VERONESE, Alexandre. **Segredo e Democracia: certificação digital e software livre**. 2007. Informática Pública vol. 8.

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. **A SEGURANÇA DOS DOCUMENTOS DIGITAIS**. 2001.

GONÇALVES, Janice. **COMO CLASSIFICAR E ORDENAR DOCUMENTOS DE ARQUIVO**. 1998. São Paulo.

IBM. **Métodos para gerenciamento de chaves públicas**. 2018. Disponivel em: <https://www.ibm.com/support/knowledgecenter/pt-br/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q009900_.htm >. Acesso em: 21/04/2019.

ICP-Brasil. **DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL**. 2015.

INNARELLI, Humberto Celeste. **PRESERVAÇÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: INTRODUÇÃO À GESTÃO DA PRESERVAÇÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS**. 2018.

ITI. **ICP-Brasil - Infraestrutura das chaves públicas**. 2017. Disponível em: <https://www.iti.gov.br/icp-brasil>. Acesso em: 21/04/2019.

MARCONDES, Carlos Henrique; SAYÃO, Luis Fernando. **Documentos digitais e novas formas de cooperação entre sistemas de informação em C&T**. 2002.

MARQUEZ, Gabriel. **Tipos de certificados digitais: como solicitar, atualizar e usar em seu negócio**. 2018. Disponível em: <https://nfe.io/blog/assinatura/tipos-certificados-digitais/>. Acesso em: 21/04/2019.

OLIVEIRA, Ronielton Rezende. **Criptografia simétrica e assimétrica: os principais algoritmos de cifragem**. 2007.

PEREIRA, Alex Sandro da Silva. **Tipos de certificados digitais**. 2018. Disponível em: <https://www.bry.com.br/blog/tipos-de-certificados-digitais/>. Acesso em: 20/04/2019.

PEREIRA, Fernando Carlos. **Criptografia Temporal: Aplicação Prática em Processos de Compra**. 2003. UFSC: PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO.

RESENDE, Dilma. **CERTIFICAÇÃO DIGITAL**. 2009. Revista UNIGRAN.

RIBEIRO, Gisele. **Certificado Digital.** 2015. Contabil Estoril.

SCHÄFER, Murilo Billig; FLORES, Daniel. **A DIGITALIZAÇÃO DE DOCUMENTOS ARQUIVÍSTICOS NO CONTEXTO BRASILEIRO**. 2013

SILVA, Denise Rangheti Pilar; STEIN, Lilian Milnitsky. **Segurança da informação: uma reflexão sobre o componente humano**. 2007. Pontifícia Universidade Católica do Rio Grande do Sul.

SILVEIRA, Debora Pricila. **Biometria Digital: COMO FUNCIONA**. 2016, disponível em: <https://www.oficinadanet.com.br/post/17100-o-que-e-e-como-funciona-a-biometria>Acesso em 13/04/2019.

SINFIC. **Vantagens e Problemas da biometria digital**. 2005. Disponível em: <http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=24095> Acesso em: 13/04/2019.

VERONESE, Alexandre. **A política de certificação digital: processos eletrônicos e a informatização judiciária**. 2007.

VIEIRA, Kássia Raquel de Lima. **O IMPACTO DO CERTIFICADO DIGITAL NAS EMPRESAS: UM ESTUDO DE CASO NA EMPRESA FLUXO NA CIDADE DE SANTA LUZIA-PB**. 2016. UEPB.