

CENTRO UNIVERSITÁRIO ATENAS

VAGNER CLAUDINO DE MELO

**ASSINATURA DE DOCUMENTOS POR MEIO DA
AUTENTICAÇÃO DIGITAL**

Paracatu

2019

VAGNER CLAUDINO DE MELO

ASSINATURA DE DOCUMENTOS POR MEIO DA AUTENTICAÇÃO DIGITAL

Monografia apresentada ao curso de Sistemas de Informação do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Área de Concentração: Autenticação digital de documentos.

Orientador: Prof. Msc. Felipe Neto Vasconcelos

2019

VAGNER CLAUDINO DE MELO

ASSINATURA DE DOCUMENTOS POR MEIO DA AUTENTICAÇÃO DIGITAL

Monografia apresentada ao curso de Sistemas de Informação do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Área de Concentração: Saúde da Mulher

Orientador: Prof. Msc. Felipe Neto Vasconcelos

Banca Examinadora:

Paracatu – MG, __ de _____ de 2019.

Prof. Msc. Felipe Neto Vasconcelos
Centro Universitário Atenas

Prof.: Msc. Raranna Alves da Costa
Centro Universitário Atenas

Prof.: Msc. Fatima das Neves Martins Santos
Centro Universitário Atenas

AGRADECIMENTOS

Agradeço primeiramente a Deus, que sem ele não seria possível chegar até aqui, é nele que busco força para encarar todos os obstáculos da vida, obrigado por não me deixar desistir dos meus sonhos. Obrigado por me abençoar para conseguir chegar ao final desta jornada acadêmica.

Aos meus pais, pelo amor, incentivo e apoio incondicional nas horas difíceis, de desânimo e cansaço.

A minha esposa Mariele Dantas Melo que apesar de todas as dificuldades me fortaleceu sempre me motivando a não desistir, o que para mim foi muito importante.

As minhas irmãs Natane Aparecida Claudino de Melo e Daniela Pereira da Silva que são muito importante na minha vida.

Agradeço a todos os professores por me proporcionar o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação no processo de formação profissional, por tanto que se dedicaram a mim, não somente por terem me ensinado, mas por terem me feito aprender. A palavra mestre, fará justiça aos professores dedicados aos quais sem nomear terão os meus eternos agradecimentos.

Agradeço aos meus orientadores Jefferson Tavares de Pádua e Prof.Msc. Felipe Neto Vasconcelos por me auxiliar na elaboração do meu trabalho de conclusão de curso, com orientações claras e objetivas e ter paciência.

E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado. Que Deus os abençoe.

RESUMO

Na busca pela otimização de processos empresariais é necessário o uso de soluções tecnológicas que otimizem as tarefas e possibilitem um ganho de tempo em processos. Nesse sentido, o presente trabalho foi elaborado visando auxiliar o processo de autenticação de documentos por meio digital. Este processo tem intuito de organizar, agilizar, disponibilizar e armazenar informações em tempo hábil, por meio de uma interface onde o usuário possa visualizar, adicionar informações que poderão ser salvas em um banco de dados podendo ser visualizadas a qualquer momento.

Palavras chave: Autenticação. Software. Documentos. Segurança. Informações.

ABSTRACT

In the pursuit of business process optimization, it is necessary to use technological solutions that optimize the tasks and enable a time saving in processes. In this sense, the present work was elaborated aiming to assist the document authentication process by digital means. This process aims to organize, streamline, make available and store information in a timely manner, through an interface where the user can view, add information that can be saved in a database and can be viewed at any time.

Keywords: *Authentication. Software Documents Safety. Information*

LISTA DE ABREVIATURAS E SIGLAS

ISO - é uma entidade de padronização e normatização

UML - é um acrônimo para a expressão Unified Modeling Language

SGBD - Sistemas de Gestão de Base de Dados

PHP – Hypertext Preprocessor

CSS - Folhas de estilo em cascata

LISTA DE FIGURAS

Figura 1 - Tela de autenticação	35
Figura 2 - Tela de dashboard	35
Figura 3 - Tela de Dashboard	36
Figura 4 - Tela de upload	36
Figura 5 - Tela de cadastro de cliente	37
Figura 6 - Modelo conceitual	38
Figura 7 - Modelo Logico	38

SUMÁRIO

1 INTRODUÇÃO	9
1.1 PROBLEMA	9
1.2 HIPÓTESE	10
1.3 OBJETIVOS	10
1.3.1 OBJETIVOS GERAIS	10
1.3.2 OBJETIVOS ESPECÍFICOS	10
1.4 JUSTIFICATIVA DO ESTUDO	10
1.5 METODOLOGIA DO ESTUDO	11
2 AUTENTICAÇÃO DIGITAL	13
2.1 ASPECTOS DA SEGURANÇA DAS INFORMAÇÕES	14
2.2 PROBLEMAS RELACIONADOS À SEGURANÇA	14
2.3 PRESERVAÇÃO DE DOCUMENTOS DIGITAIS	15
3 VANTAGENS E DESVANTAGENS DA UTILIZAÇÃO DA AUTENTICAÇÃO DIGITAL NA PRESTAÇÃO DE SERVIÇOS	18
4 DESENVOLVIMENTO DO SISTEMA DE AUTENTICAÇÃO DIGITAIS.	22
4.1 LINGUAGEM DE PROGRAMAÇÃO	22
4.2 PHP	22
4.3 BOOTSTRAP FRAMEWORK	23
4.4 MYSQL	24
4.5 BANCO DE DADOS	24
4.6 LINGUAGEM DE MODELAGEM UNIFICADA (UML)	25
5 CONSIDERAÇÕES FINAIS	28
REFERÊNCIAS	29
APÊNDICE A – TELAS DO SISTEMAS	35

1 INTRODUÇÃO

Com o avanço acelerado da tecnologia, o número de informações que trafegam pelos meios eletrônicos é cada dia mais crescente e é fundamental garantir a segurança dessas informações, sejam elas pessoais ou profissionais. Existem diversos recursos que possibilitam o envio e recebimento de documentos/informações de maneira segura, dentre eles o processo de autenticação digital. (Dilma A. Resende, 2009)

A autenticação digital pode ser definida como sendo uma ferramenta ou mecanismo para confirmação ou certificação da identidade de um indivíduo no ambiente digital, capaz de substituir com segurança documentos em papel assinados de maneira física. (Dilma A. Resende, 2009)

A autenticação digital foi criada com o propósito de contribuir na integridade e veracidade dos documentos digitais podendo auxiliar fortemente nos processos de uma empresa. Várias organizações já aderiram ao uso da autenticação digital para documentos, dispensando o uso de documentos físicos o que proporciona vários benefícios, como o acesso ágil às informações desejadas, redução de custo com materiais de escritório, papéis e locais físicos para armazenamento de documentos e a redução de prejuízo com a perda de documentos importantes.

O processo de migração da documentação em papel para a digital está acontecendo aceleradamente, de modo que contratos, os textos artísticos, os pareceres, os trabalhos em geral, são produzidos, enviados, discutidos e acertados eletronicamente (Lopes, 2008).

Diante deste cenário, percebemos que a cada dia os processos feitos de maneira física vem sendo descontinuados e assim surge a necessidade de segurança das informações que trafegam no meio digital.

1.1 PROBLEMA

De que maneira a autenticação digital pode contribuir na documentação e controle da prestação de serviços em uma empresa?

1.2 HIPÓTESE

A) Com o uso da Autenticação Digital em documentos dentro de uma organização pode-se elevar os níveis de segurança e confiabilidade das informações, além de possibilitar a praticidade e eficiência na gestão de documentos.

B) Com a utilização de um processo de autenticação digital, obtém-se a confirmação de atendimentos prestados de maneira mais segura e conseqüentemente reduz o uso de papéis e locais para seu armazenamento.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Encontrar diretrizes que auxiliem na autenticação digital de documentos na área de prestação de serviços.

1.3.2 OBJETIVOS ESPECÍFICOS

- a) Definir os conceitos de Autenticação digital.
- b) Apresentar as vantagens e desvantagens da utilização da certificação digital na prestação de serviços.
- c) Apresentar um software que realize a autenticação digital de documentos.

1.4 JUSTIFICATIVA DO ESTUDO

A utilização da autenticação digital nas empresas proporciona vários benefícios para a área de prestação de serviços, dentre os quais é possível citar a segurança, agilidade e praticidade no processo de documentação dos atendimentos prestados.

Na maioria das empresas, em um processo simples, quando alguém solicita um atendimento é necessário que o técnico tenha em mãos uma ficha de observação impressa para que ao final seja documentado, de forma manual, todo o

procedimento realizado para solução da situação, e em seguida, quem solicitou o atendimento assine aprovando/confirmando (Vieira, 2016).

Levando em conta a mesma situação acima e considerando que neste cenário exista o processo de autenticação digital implantado nos processos da empresa, a documentação do atendimento seria realizada de forma digital e no momento da assinatura do solicitante, seria considerado sua chave digital para assinatura da ficha de atendimento.

Apesar dos benefícios da autenticação digital aparentar atender a todas as necessidades dentro de uma organização em termos de controle de documentação, deve-se levar em consideração que existem entraves no processo, pois para que a autenticação digital esteja em atividade depende-se de fatores externos, como por exemplo acesso à rede, equipamentos eletrônicos (computador, smartphone.) Dentre outros. Outro ponto que devesse considerar é que caso seja disponibilizado uma senha de autenticação para uma determinada pessoa e outra pessoa tenha conhecimento desta ela pode realizar a assinatura de um documento sem que a primeira pessoa tenha conhecimento ou consentimento (Ottoni, 2005)

1.5 METODOLOGIA DO ESTUDO

O método é a ordem que deve ser aplicada a diferentes processos necessários para atingir um resultado desejado. Nas ciências, compreende-se como método o conjunto de processos que o indivíduo deve empregar na investigação e demonstração da verdade (Cervo e Bervian, 1983).

De acordo com Marconi e Lakatos (2003)

“A Metodologia Científica, mais do que uma disciplina, significa introduzir o discente no mundo dos procedimentos sistemáticos e racionais, base da formação tanto do estudioso quanto do profissional, pois ambos atuam, além da prática, no mundo das ideias.”

Ainda de acordo com Cervo e Bevia (1983) “o método científico quer descobrir a realidade dos fatos, e estes, ao serem descobertos, devem, por sua vez, guiar o uso do método”. O método atua diretamente no processo de pesquisa para conduzi-la a fim de alcançar resultados de determinadas situações.

Nas palavras de Gil (2010) uma pesquisa é um procedimento racional que tem por objetivo desenvolver respostas a problemas propostos, e a pesquisa é usada quando se tem um déficit de informação para expor respostas ao problema, e também

quando as informações estão em estado de desordem, impossibilitando sua resolução. A pesquisa é desenvolvida com conhecimentos disponíveis e a utilização de técnicas e métodos de investigação, que podem ser descritas como fases desde a adequação do problema até a apresentação de resultados favoráveis à sua resolução.

Gil (2010) destaca que um projeto de pesquisa é um conjunto de metas definidas com o propósito de estabelecer aspectos como, por exemplo, o tempo em cada ação, recursos humanos, materiais e financeiros para possibilitar maior satisfação na execução do projeto.

As pesquisas necessitam ser classificadas, sendo assim Gil (2010) descreve que a tendência de classificação é uma característica humana, que possibilita a melhor organização dos fatos e conseqüentemente o seu entendimento, como cada pesquisa é diferente da outra, surge a necessidade de previsão e provisão de recursos em relação a qual classificação a pesquisa se encaixa, fazendo com que o pesquisador utilize melhor os recursos dispostos de modo a maximizar o tempo final da pesquisa.

Este projeto em questão se enquadra em uma pesquisa exploratória que, de acordo com as palavras de Gil (2010) têm em vista se aproximar do problema, construindo hipóteses, em seu planejamento e considera-se variáveis e fenômenos que têm participação na pesquisa. A coleta de dados é feita a partir de pessoas que tiveram experiências práticas com o assunto, por meio de embasamento bibliográfico. Ainda de acordo com Gil (1999) “a pesquisa exploratória é desenvolvida no sentido de proporcionar uma visão geral acerca de determinado fato” e, portanto, foi feito com base em diversos materiais bibliográficos, incluindo livros, artigos e outros periódicos, procurando compreender as influências da ciência e da tecnologia.

Este projeto também possui requisitos de uma pesquisa descritiva que, segundo Antônio Carlos Gil (2010) tem por objetivo a descrição das características de determinada população, podendo também identificar possíveis relações entre as variáveis. As pesquisas descritivas, na maioria das vezes, são realizadas para objetivos profissionais.

O projeto tem natureza aplicada com propósito imediato de gerar produtos e/ou processos. Seu objetivo é exploratório com enfoque em conteúdos bibliográficos com a finalidade de obter informações que concernem a autenticação digital.

2 AUTENTICAÇÃO DIGITAL

Atualmente grande parte dos processos de uma empresa giram em torno de dispositivos eletrônicos. Pode-se dizer que, hoje a maioria das grandes empresas não sobrevivem sem os recursos digitais. Pode-se observar também que o número de documentos eletrônicos que trafegam pelos meios digitais aumenta significativamente a cada dia, enquanto que o documento de papel vem perdendo o valor por não oferecer o dinamismo que as empresas necessitam.

Com esta revolução, a grande preocupação das pessoas é em como comprovar que os documentos eletrônicos são verdadeiros. Para isso necessita-se de recursos que comprovem sua veracidade, como por exemplo, a autenticação digital.

De acordo com Aurélio Buarque de Holanda Ferreira, a palavra autenticação é o ato que consiste no reconhecimento de um documento como sendo autêntico ou verdadeiro (BIDERMAN, 2000). Já a palavra digital refere-se aos sistemas, dispositivos ou processos que empregam tal modo de representação discreta, por oposição à analógico (BIDERMAN, 2000).

Unindo os dois termos descritos acima, temos a autenticação digital, ou seja, o ato de reconhecer um documento por meio de um dispositivo eletrônico.

A autenticação digital é uma tecnologia que garante a identidade certa da origem de um documento eletrônico. Autenticação digital é utilizada como meio de citar o procedimento de autenticação digital que aprova ou assegura a identificação da pessoa que preparou o documento.

Esse processo, além da aprovação de que o documento foi elaborado por algum indivíduo com permissão, igualmente aprova a procedência e a integridade de determinado documento.

Existem múltiplos artifícios da autenticação eletrônica que podem ser utilizadas para certificar a identidade do usuário, desde uma senha até níveis mais elevados de segurança que empregam a autenticação multifatorial (Processo de confirmação da identidade reivindicar de um utilizador do sistema), para isso são considerados vários aspectos da segurança da informação.

2.1 ASPECTOS DA SEGURANÇA DAS INFORMAÇÕES

Nota-se que, as tecnologias geraram uma infinidade de informações das mais diversas formas e dos mais diversos tipos. Por essa razão, conforme mostra Brito (2018) as informações geradas por meio de computadores passaram a necessitar de proteção contra eventuais problemas, pois muitos processos em papel, foram transformados em documentos digitais.

Segundo Sêmola (2014), a segurança da informação não é uma ciência exata. Se fôssemos classificá-la, ela estaria relacionada a gestão de riscos. E na gestão de riscos são considerados vários processos como, conhecer, planejar, agir, auditar, educar, monitorar, aprender, gerenciar, dentre outros.

Para a segurança da informação, deve-se investir na aplicação de regras, regulamentos, políticas, normas e programas de proteção a informação. Estas são ações consideradas importantes em uma organização, porém para aumento da sua eficiência é indispensável que os membros da organização, independentemente do seu nível hierárquico, se tornem conscientes desse assunto e se sintam responsáveis e comprometidos em cumprir processo no dia-a-dia que asseguram a integridade das informações (FONTES, 2006).

Nesse sentido, os integrantes de uma organização devem ter ciência de que proteger uma informação significa garantir sua disponibilidade, integridade e confidencialidade, e que todos devem trabalhar em prol a segurança da informação para que assim sejam mitigados e eliminados problemas relacionados à segurança.

2.2 PROBLEMAS RELACIONADOS À SEGURANÇA

Diante de uma realidade mais dinâmica e digital, há uma grande tendência para aumento de transações de documentos nos meios tecnológicos. Com isso é crescente o número de ataques que possam alterar o conteúdo dos documentos, comprometendo a sua integridade e para isso existem recursos que contribuem para que uma informação permaneça íntegra, dentre eles, o Não Repúdio.

De acordo com Ress (2011) "não Repúdio é a capacidade de garantir que um usuário ou sistema realmente realizou uma operação em um sistema de informação, não permitindo a existência de dúvidas ou questionamentos sobre a sua realização."

Para se estabelecer uma associação entre um indivíduo e uma identidade deve ser realizada uma análise em duas categorias: autenticação e identificação. Autenticação refere-se ao processo de confirmar ou negar uma referida identidade do indivíduo, enquanto identificação, refere-se ao processo de estabelecer a identidade, desconhecida a partir de um indivíduo (THIAN, 2001).

Mesmo com os vários recursos existentes, não é possível garantir a um indivíduo a total segurança e confiabilidade dos documentos, pois esta questão não está exclusivamente relacionada a tecnologia, depende-se de outros fatores, como por exemplo a confiança das partes envolvidas.

De acordo com o Conarq (2011):

“A confiabilidade está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza e ter seus procedimentos de produção bem controlados. Dificilmente pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável” (CONARQ, 2011, p. 21).

Considerando a frase “uma corrente é tão resistente quanto seu elo mais fraco”, e aplicando a segurança da informação podemos definir o usuário como o elo mais fraco da corrente uma vez que recursos computacionais já estariam protegidos por processos tecnológicos. Acre (2003) cita que os equipamentos e recursos das estações de trabalho e seus usuários seriam os mais vulneráveis a ataques internos e externos. Com isso faz-se necessário refletir sobre a preservação segura de documentos digitais.

2.3 PRESERVAÇÃO DE DOCUMENTOS DIGITAIS

O assunto segurança da informação vem se tornado mais conhecido na medida em que:

- a) As empresas têm suas informações processadas e guardadas em ambiente computacional;
- b) As empresas são dependentes do ambiente computacional para realizarem seus negócios;
- c) As informações computacionais estejam disponíveis a todos os contribuintes da empresa.

Segundo Beal (2005) segurança da informação é definida como sendo um processo de proteção da informação das ameaças a fim de mantê-la íntegra, disponível e confidencial.

Sêmola (2003) assevera que a segurança da informação é “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.”. Diante disso pode-se definir que a segurança da informação é uma área que luta para manter protegida uma informação.

Segundo a ISO/IEC 17799:2005, para a segurança da informação as propriedades abaixo devem estar envolvidas para garantia de uma informação segura:

- a) Integridade: tem como objetivo garantir que a informação seja exata.
- b) Disponibilidade: é a garantia de que a informação estará disponível para que pessoas autorizadas consigam acessá-las sempre que necessário.
- c) Confidencialidade: garante que somente pessoas autorizadas tenham acesso à informação.

Sêmola (2003) adiciona ainda estes dois objetivos:

- a) Legalidade: segurança de que a informação foi criada em concordância com a lei;
- b) Autenticidade: certeza de que em um procedimento de comunicação, os remetentes sejam realmente quem dizem ser e que a mensagem ou informação não foi corrompida após a emissão ou validação.

A segurança da informação é um conjunto de orientações, normas, procedimentos, políticos de demais atuações que tem como objetivo resguardar o recurso de informação, permitindo que o negócio de empresa seja concretizado e a sua missão seja atingida. (Gonçalves, 2017).

Ainda segundo Gonçalves (2017) “a segurança da informação existe para amenizar os riscos do negócio em relação a dependência do uso dos recursos de informação para o funcionamento da organização. ”

De acordo com Ferreira (2003, p. 2)

“A informação agrega valor quando permite à empresa perceber oportunidades e ameaças à sua operação, detectando tendências ou problemas. E ainda, talvez na sua função mais nobre, a informação agrega valor ao negócio quando da sua análise chega-se a novas maneiras de fazer negócio, a novos serviços e novos produtos. ”

Ferreira (2003, p. 2) complementa que “[...] as informações usadas no processo de tomada de decisão, o talento dos colaboradores, a rede de contatos,

enfim toda uma nova categoria de “ativos” passa a ser mais importante na avaliação de uma empresa”. Neste sentido, classifica-se a informação como um dos principais e mais importantes ativos de uma organização.

O nome “Ativo” pode não ser muito conhecido para algumas pessoas, mais é bastante utilizada na ISO 27001 por abranger quaisquer elementos (seja humano, tecnológico, software, ou etc.) que suportam um ou mais procedimentos de negócios de uma unidade ou campo de negócios. Pode-se classificar ativo a qualquer recurso que tenha valor para uma organização.

Quando se fala em segurança da informação por “inventário de ativos” necessitamos compreender um conjunto mais amplo de ativos, que contemplam sistemas, pessoas, ambientes físicos, dentre outros.

A regra ISO 27001 não especifica claramente como os ativos tem que ser identificados. Sabe-se por conhecimento que os ativos parecidos podem ser agrupados e cadastrados com um único nome. Um exemplo seria, uma empresa com 50 computadores no setor de tecnologia e ao invés de cadastrar individualmente todas as unidades, cada qual com uma descrição distinta, pode-se inventariar somente um destes, usando o nome “Estações de Trabalho Tecnologia”

Existem alguns ativos que podem ser utilizados em mais de um processo de negócios nas empresas. Um bom exemplo seria o serviço de e-mail, que na maioria das corporações este ativo suporta praticamente todos os procedimentos de negócios. Tendo em vista o valor de um ativo/informação em uma organização, torna-se importante sua preservação e armazenamento autênticos.

A preservação digital teve início entre o século XX e XXI e surgiu da necessidade de resguardar documentos físicos que rapidamente sofrem desgastes com o passar do tempo.

A preservação de documentos digitais é a parte mais demorada e complexa, pois é necessário manter os documentos seguros e acessíveis a qualquer momento e em qualquer lugar.

Segundo Hedstrom (1996), a preservação digital é um processo distribuído que envolve o “planejamento, alocação de recursos e aplicação de métodos e tecnologias para assegurar que a informação digital de valor contínuo permaneça acessível e utilizável”.

3 VANTAGENS E DESVANTAGENS DA UTILIZAÇÃO DA AUTENTICAÇÃO DIGITAL NA PRESTAÇÃO DE SERVIÇOS

A internet é considerada como um meio de comunicação que permite que numerosas pessoas se comuniquem simultaneamente, num momento escolhido, em escala global.

De acordo com Castells (2003) "se a tecnologia da informação é hoje o que a eletricidade foi na Era Industrial, em nossa época a Internet poderia ser equiparada tanto a uma rede elétrica quanto ao motor elétrico, em razão de sua capacidade de distribuir a força da informação por todo o domínio da atividade humana."

A internet que pode proporcionar uma comodidade, agilidade e eficiência nos processos do dia-a-dia, no manuseio e transferência de dados. A internet é um marco para a economia e para os negócios, e permite que milhares de pessoas se reúnam em torno de ideais em locais virtuais, criando um meio de interação entre as pessoas, por meios físicos e jurídicos.

Dessa forma criam-se várias oportunidades de negócios em uma rede, gerando revoluções no meio econômico, no mercado de trabalho, na relação dos consumidores e na sociedade em geral.

Um dos grandes responsáveis da revolução tecnológica no mundo, Bill Gates, afirma que as empresas que alcançarão o sucesso na atualidade serão aquelas que optarem pela implantação de recursos e ferramentas digitais afim de inovar seu modelo de trabalho.

Bill Gates (1995) assevera ainda que:

“O papel estará conosco infinitamente, mas sua importância como meio de encontrar, preservar e distribuir informação já está diminuindo. (...) À medida que os documentos ficarem mais flexíveis, mais ricos de conteúdo de multimídia e menos presos ao papel, as formas de colaboração e comunicação entre as pessoas se tornarão mais ricas e menos amarradas ao local onde estão instaladas”.

Segundo GANDINI, SALOMÃO e JACOB (2002) é possível perceber que existe um grande crescimento da utilização de documentos eletrônicos no dia-a-dia das pessoas, que estão presentes desde atividades corriqueiras, como o envio e recebimento de arquivos de textos que trafegam pelas redes sociais, quanto documentos com maior grau de importância que são utilizados nas grandes organizações para processos distintos.

Dentro dessa realidade pode-se dizer que as organizações estão optando pelo armazenamento eletrônico de documentos e arquivos, uma vez que propicia facilidade no armazenamento e identificação do documento. Além disso pode-se dizer que temos um ganho em relação a durabilidade do documento. (GANDINI; SALOMÃO; JACOB, 2002)

Os tradicionais documentos de papel vêm perdendo força no mercado e cada dia sendo menos utilizados devido às suas limitações no quesito transferência e segurança. Além disso sabemos que o papel está sujeito a muitos danos, podendo comprometer a durabilidade e autenticidade do documento.

Para ter acesso a esses documentos, os usuários precisam realizar um procedimento de autenticação criterioso. A informação utilizada no processo, por sua vez, precisa ser protegida de maneira que não corram o risco de ser descoberto pelos navegantes inconstitucional. Já os criadores dessa classe de aplicação mantêm-se gradativamente alarmado com a segurança dos sistemas e realizando teste e melhoria constantes para reforça-la. (GANDINI; SALOMÃO; JACOB, 2002)

Todo o desenvolvimento da autenticação digital pode ser considerado uma confiança, quer dizer, que uma vez que é feita a autenticação, o desfrutador e conceituado autêntico para a aplicabilidade.

Segundo Rainer e Cegielski (2011) o sistema de informação permite que seja realizado diversas tarefas como, reduzir custos das transações rotineiras comerciais, melhorar qualidade do fluxo de informações eliminando ou reduzindo erros, eliminar processos em papel e suas ineficiências e custos relacionados e facilitar a transações de informações entre usuários.

A certificação digital, atualmente, pode ser ponderada como um dos modos mais garantidos de se comprovar que algo disponível em ambiente digital seja realmente de quem a reivindica ou venha reivindicar, pois o certificado proporciona a garantia que o conteúdo de mensagens ou escrita, do seu autor e data seja confirmado por meios de procedimentos e métodos que podem proporcionar segurança a comunicação e transações eletrônicas (CASAGRANDE, 2011).

Com o nascimento da internet e o aumento de dados sendo gerados e transmitidos na rede, teve a necessidade da criação de uma tecnologia para certificá-los e garantir a uma pessoa e/ou instituição que suas informações são legítimas e seguras.

Dessa maneira, em 2001 criou-se a ICP-Brasil uma autarquia federal ligada à Casa Civil da Presidência da República, responsável por conservar a base de Chaves Públicas Brasileiras- ICP-Brasil constituindo a primeira autoridade de cadeia de certificação – AC Raiz (SILVA JÚNIOR, 2016).

“Art. 1º Fica instituída a Infraestrutura de Chaves Públicas Brasileira - ICPBrasil, 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.” (BRASIL, 2001).

A ICP-Brasil é uma infraestrutura combinada por hardware, software, pessoas, políticas e processos para fazer a criação, gerenciamento, distribuição, usar, armazenamento e revogar certificados digitais. Os primeiros certificados foram criados assim como permissões para novas Autoridades Certificadoras –AC (SILVA JÚNIOR, 2016).

Conforme dicionário Aurélio, criptografia é uma palavra de origem grega, e seu significado é escrita escondida, ou seja, escrita sigilosa (BIDERMAN, 2000).

“Dentre as diversas tentativas de definir criptografia de maneira precisa, pode-se dizer de um modo simples, que criptografia é a ciência de fazer com que o custo de adquirir uma informação de maneira imprópria, seja maior que o custo obtido com a informação”. (SILVA apud CASAGRANDE, 2011).

Apesar disso, esse preço pode diminuir se a pessoa que tem interesse em conseguir as informações obter um grande conhecimento na área da tecnologia. Para impedir que tal pessoa use o seu conhecimento para obter as informações, precisará aumentar o tamanho da chave utilizada para fazer a criptografia e descriptografar.

“Chave é um valor numérico para cifrar e decifrar um texto. A segurança de um criptossistema pode então ser mensurado baseado no tamanho do espaço de chaves e no poder computacional atualmente disponível. ” (SILVA apud CASAGRANDE, 2011).

Atualmente, existem dois tipos de tecnologias para criação das chaves: chave simétricas e assimétricas. A chave simétrica tem apenas uma chave que faz os dois tratamentos, de cifrar e decifrar, a parte de decifrar deve estar somente em posse de uma da parte que irão fazer a troca de informações. A chave assimétrica, popularmente conhecida como chave pública, possui a chave pública, responsável por cifrar as informações e para descriptação da informação, existe apenas uma outra chave privada, que está de posse de quem está autorizado a ler as informações. (SILVA apud CASAGRANDE, 2011).

Sabendo da chave pública não se consegue chegar à chave privada correspondente, porém se relacionam por meio de algum dos algoritmos existentes. Atualmente, há algoritmos que são considerados os mais seguros e práticos para se trabalhar, segundo o Professor Rezende do Departamento de Ciência da Computação - CIC da UNB, 2012

A tecnologia de Hash, onde informado o valor da entrada e fácil computar o valor da saída, mais se o valor da saída for informado é difícil computar e chegar até o valor da entrada.

O professor Barros do curso de Pós-Graduação, Redes de Computadores, do UNICEUB menciona “a quebra de um prato é um bom exemplo de função unidirecional. É fácil quebrar um prato em um milhão de pedaços, entretanto não é fácil juntar todos os pequenos pedaços de forma a formar novamente o prato original” (BARROS, 2012, p.12)

A função hash é um procedimento matemático que quando receber um valor (EX: 38 bytes) na entrada vai transformá-lo em um novo valor geralmente menor na saída (EX: 18), esse novo valor é chamado de hash. Na resolução número 63 de 2009 o CG da ICP-Brasil comunica determinadas significações para que seja melhor compreendido o documento, em meio a elas está a seguinte definição.

“Função hash - uma transformação matemática que faz o mapeamento de uma sequência de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor conhecido como resultado hash ou resumo criptográfico de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado hash, não é possível recuperar a mensagem que o gerou)” (ITI, 2009)

4 DESENVOLVIMENTO DO SISTEMA DE AUTENTICAÇÃO DIGITAIS.

4.1 LINGUAGEM DE PROGRAMAÇÃO

Nota-se que, para a criação de um sistema computacional se faz necessário o uso de algumas tecnologias computacionais, dentre elas, uma linguagem de programação, que se refere a uma técnica que desenvolvedores usam para expressar as instruções de um programa para um computador. Ela segue um conjunto de regras sintáticas e semânticas para definir uma sequência de instruções lógicas que serão codificadas em um software de computador, e assim cabe apresentar que as regras sintáticas dizem respeito a forma de escrita e regras semânticas ao conteúdo. (GOTARDO 2015).

Uma linguagem de programação é um método que segue um padrão para expressar as instruções de um programa a um computador programável. Seguindo um conjunto de regras sintáticas e semânticas para definir um programa de computador. Regras sintáticas dizem respeito a forma de escrita e regras semânticas ao conteúdo. Através da especificação de uma linguagem de programação pode-se definir quais dados o computador irá usar, como eles serão tratados, armazenados, transmitidos e quais ações deverão ser tomadas em determinadas circunstâncias (Gotardo, 2015).

Quando se trata de linguagem para web e impossível não citar o HTML, pois a mesma é a base para qualquer página existente na web, sendo criada para facilitar o entendimento dos seres humanos e máquinas, porém devemos considerar que na criação de sites mais completos e dinâmicos é necessário utilizar mais recursos e estes estão disponíveis em linguagens web, como a linguagem PHP. Esta linguagem ganhou seu espaço pela sua simplicidade de utilização e pela variedade de recursos que possui.

4.2 PHP

A linguagem de programação PHP (Hypertext Preprocessor) é muito utilizada para o desenvolvimento de páginas WEB, e foi criada por Rasmus Lerdorf em 1995, inicialmente era um pacote CGI para substituição dos Scripts Perl e permitia que os programadores criem aplicativos simples para a web, com o intuito de melhoria

do código, seu desenvolvedor disponibilizou o código fonte do php para que seus usuários pudessem aperfeiçoá-lo, adicionar novas funções e corrigir eventuais problemas.

O PHP é uma linguagem open source, isso significa que seu código está disponível para qualquer pessoa sem custos. Esse tipo de sistema aberto para uso não traz lucros aos desenvolvedores pois disponibilizam tudo para seu público, que por sua vez reporta erros e ajudam com as modificações de código fonte.

Segundo Niederauer (2011), o PHP é uma das linguagens de programação voltada totalmente para o desenvolvimento web, permitindo que os sites sejam completamente dinâmicos usando todas as técnicas que o mesmo oferece.

Pensando em sites dinâmicos e seguindo os critérios de qualidade de software citados anteriormente, é necessário que estes sites tenham um layout apresentável e que permita a fácil utilização, para isso podemos utilizar o CSS, que é uma linguagem de folha de estilos, tendo o papel de tornar uma página apresentável na web, relacionada diretamente com o design e aparência.

Ainda sobre aparência dos sites e seu dinamismo, existem os frameworks que irá permitir a utilização de funcionalidades específicas, previamente configuradas, que irá possibilitar a reutilização de códigos.

No dizer de Oglio(2007), o PHP sendo uma ferramenta de fácil utilização abre um leque de possibilidade por sua acessibilidade a vários bancos de dados, e por se orientado a objeto, possibilita a criação desde portais simples até algo mais complexos como por exemplo, aplicações de negócio

4.3 BOOTSTRAP FRAMEWORK

O Bootstrap framework é um conjunto de padrões, que nos oferece uma gama de estabilizações para nosso sistema web ou site, nos traz formas, botões, tabelas, opções de menus e layouts responsivos, entre várias outras formas.

Segundo Tormazini e Lopes (2015) é um conjunto de vários elementos e funções que nos permitem estabilizar e personalizar na construção de páginas web e projetos de códigos abertos, integrados previamente em uma única ferramenta. Em uma explicação mais simples, é um conjunto de ferramentas para facilitar o desenvolvimento (front-end.) de sites e sistemas web. Ao se desenvolver um site ou sistema web com o Bootstrap, os programadores e desenvolvedores podem escolher

e usar com bastante facilidade todos os seus recursos e elementos disponíveis para a sua respectiva estilização.

4.4 MYSQL

O Mysql é uma ferramenta de gestão de banco de dados, e através dela onde faremos a comunicação de um sistema de informação com um banco de dados de uma organização ou empresa, para se ter a disponibilidade e a manipulação dessas informações.

Segundo Ferreira e Junior (2016) o Mysql surgiu a partir das necessidades e dos processos baseados na equipe que criou o SGBD (Sistema de Gerenciamento de Banco de Dados), necessidades essas que são de se utilizar algum mecanismo que permitisse a conexão ou o relacionamento das tabelas criadas na linguagem mãe SQL para um determinado fim de uso dos dados e informações. No início, o grupo iria utilizar o SQL que também é um SGBD, mas logo perceberam que esta ferramenta não era tão rápida e eficiente o suficiente para atender as necessidades do projeto e seus determinados processos. O jeito foi criar uma solução própria, um SGBD próprio. Nasceu então o MySQL.

Segundo Silva (2016) o MySQL é um banco de dados relacional gratuito, eficiente e otimizados para aplicação Web e também desktops, e desenvolvido e mantido pela empresa MySQL AB, que também oferece uma licença (paga) para empresas. Esse SGBD também é multi-plataforma, sendo compatível com o Windows, Linux, MacOS, entre vários outros sistemas operacionais. As tabelas criadas podem ter tamanhos de até 4 GB de dados e informações. Fora isso o MySQL é compatível com várias linguagens de programação como PHP, C, JAVA, PYTHON, JAVASCRIPT entre outros.

4.5 BANCO DE DADOS

Banco de dados e sistemas gerencial de banco de dados atualmente se tornaram componentes de grande importância na sociedade atual. No decorrer do nosso dia a dia a maioria de nós está em alguma atividade que envolvem algum tipo de interação com o banco de dados, nos últimos anos os grandes crescimentos na tecnologia geraram recursos inovadores e interessantes para os sistemas de banco

de dados como banco de dados multimídias e banco de dados em tempo real. Cada uma com sua usabilidade específica para cada função (ELMASRI 2005).

Silberschatz, Korth e Sudarshan (2008) diz que sistemas de banco de dados são projetados para gerenciar informações em grande volume. Onde o gerenciamento das informações requer definições das estruturas de armazenamento e mecanismos para manuseio dessas informações. Devendo garantir a segurança das informações armazenadas contra possíveis problemas do sistema, além de impedir acesso não autorizado. Quando os dados são compartilhados entre vários usuários, deve evitar a ocorrência de resultados divergente, evitando assim, redundância, a incoerência de dados e isolamento são minimizados e os dados podem ser compartilhado entre usuários diversos, assim aumentando a integridade e segurança dos dados.

O sistema de gerenciamento de banco de dados é composto por uma série de dados inter-relacionados de uma coleção de programas para acessar esses dados. SGBD sistemas de gerenciamento do banco de dados, tem como objetivo proporcionar um ambiente que seja eficiente e conveniente para que as pessoas possam ter recursos como armazenar, recuperar informações. Os SGBD são geralmente projetados para armazenar e processar grandes quantidades de informações além disso oferece segurança para os dados armazenados.

A engenharia de software e uma metodologia de desenvolvimento e manutenção de sistemas e que através de processos dinâmicos integrados e interligados procura solucionar problemas de acordo com os requisitos. A engenharia de software e um estudo que se baseia na aplicação, desenvolvimento e na manutenção de sistema computacionais. A engenharia visa melhorar a produção, manutenção, e possíveis recuperações visando cumprir o prazo e custo estimados com o processo controlado e utilizando métodos e princípios de aprimoramento, produto vindos desse tipo de desenvolvimento asseguram um software de qualidade auxiliando os seus usuários na realização de suas tarefas de forma satisfatória.

4.6 LINGUAGEM DE MODELAGEM UNIFICADA (UML)

A UML é uma maneira simples e flexível modelagem de software, através da utilização de diagramas que auxiliam no processo de idealização e documentação. A UML conta com uma série de diagramas, cada um com o objetivo de ilustrar uma

etapa diferente do processo de desenvolvimento, como por exemplo, o diagrama de caso de uso e o diagrama de classes.

O diagrama de caso de uso é criado no início do projeto, e busca descrever o comportamento do sistema do ponto de vista do usuário. Esse diagrama serve de referência para estruturação do sistema e pode ser alterado várias vezes no decorrer do processo de desenvolvimento. A ideia é que todo sistema tenha pelo menos um diagrama de caso de uso com seus respectivos comportamentos, chamado de diagrama de caso de uso geral; em casos em que a criação do diagrama de caso de uso geral não seja suficiente, no entanto, podem ser criados diagramas secundários como forma de esclarecer melhor as interações do usuário com o sistema, o diagrama de caso de uso específico. (STADZISZ, 2002)

Na estrutura do diagrama de caso de uso, é possível identificar 3 componentes básicos, são eles: atores, casos de uso e associações. O ator é representado por um boneco, e deve possuir um nome. Na maioria das vezes o ator é definido como usuário, mas pode ser qualquer agente externo, como por exemplo, uma impressora. O caso de uso é ilustrado por uma bolha e se refere a alguma funcionalidade ou processo com o qual o ator interage. As associações ligam o caso de uso ao ator, ou a outros casos de uso, e indicam que existe interação entre as partes interligadas (GUEDES, 2011). Um exemplo de diagrama de caso de uso geral e específico pode ser visto nos apêndices C e D respectivamente.

Já o diagrama de classes representa a estrutura interna do sistema, através da definição de classes - principal primitiva das linguagens orientadas a objeto - e é o mais utilizado de todos os diagramas da UML (MILES; HAMILTON, 2006). Para Guedes (2011 p. 101), "Seu principal enfoque está em permitir a visualização das classes que compõem o sistema com seus respectivos atributos e métodos, bem como em demonstrar como as classes do diagrama se relacionam[...]".

O diagrama de classes é composto por classes (com seus atributos e métodos) e as associações que existem entre elas. A classe deve possuir um nome e opcionalmente, um ou mais atributos com seus respectivos tipos de dados, e ainda um ou mais métodos. A classe é representada por um retângulo, com duas ou três divisões - dependendo da existência de atributos e métodos. Para criar diferentes níveis de acesso, atributos e métodos podem ser precedidos dos símbolos +, -, # ou ~ que representam visibilidade: pública (pode ser utilizada por qualquer objeto), privada (o acesso só pode ser feito dentro da própria classe), protegida (o acesso

pode ser feito por classes ou subclasses), pacote (todas as classes no mesmo pacote podem ter acesso) respectivamente (MEDEIROS, 2004).

Outro item importante dos diagramas de classes são as associações. Associações são utilizadas para estabelecer relacionamento (ou permitir a comunicação) entre as classes envolvidas. A comunicação pode ser feita de forma unidirecional (apenas a classe A solicita serviços da classe B) ou bidirecional (ambas as classes solicitam serviços uma da outra) e não existe uma quantidade mínima ou máxima de associações que uma mesma classe pode receber (STADZISZ, 2002). Para entender melhor como esse diagrama funciona, consta no apêndice E o diagrama de classes que será utilizado no desenvolvimento do aplicativo.

5 CONSIDERAÇÕES FINAIS

A transição de documentos digitais é notoriamente de suma importância na vida de qualquer pessoa, seja no ramo profissional quanto pessoal, onde quer que ela esteja. Porém é notável que o entendimento das pessoas acerca do tema é limitado, sendo muitas vezes subestimado e ignorado o seu grau de importância.

A partir das pesquisas bibliográficas realizadas para o presente trabalho nota-se, que o objetivo geral desse trabalho foi alcançado por disponibilizar um software de autenticação digital para contribuir com os processos de confirmação de recebimento/envio de documentos de maneira a garantir a confiabilidade das informações e conseqüentemente reduzir o uso de papel, bem como impressoras e locais físicos para seu armazenamento, podendo assim contribuir de forma positiva com a preservação do meio ambiente.

Nesse mesmo sentido a hipótese a, que fala do uso da Autenticação digital em documentos dentro de uma organização não foi validada porquê o software não foi implantado e testado em uma organização.

De outro lado a hipótese b, que mostra que com a utilização de um processo de autenticação digital, obtém-se a confirmação de atendimentos prestados de maneira mais segura e conseqüentemente reduz o uso de papéis e locais para seu armazenamento, a mesma foi confirmada por que o software foi desenvolvido e testado em ambiente próprio, e comprovado a preservação dos documentos e a redução do uso de papel.

Neste trabalho foi possível também comprovar que a autenticação digital contribuir positivamente com os processos internos das organizações, uma vez que facilita a transição de documentos de forma mais segura e ágil.

REFERÊNCIAS

<[Http://msdn.microsoft.com/pt-br/library/ff716605.aspx](http://msdn.microsoft.com/pt-br/library/ff716605.aspx)>. Acesso em: 27 out. 2019.

BATISTA, Gabriella Pallos et al. **Escrituração Contábil Digital nas Empresas Tributadas pelo Lucro Real**. Revista Eletrônica do Departamento de Ciências Contábeis & Departamento de Atuária e Métodos Quantitativos (REDECA), v. 4, n. 2, p. 97-112, 2017.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** – São Paulo: Atlas, 2005.
BIDERMAN, Maria Tereza Camargo. Aurélio: sinônimo de dicionário? Alfa: Revista de linguística, v. 44, 2000.

BRITO, Samuel Henrique Bucke. **IPv6-O novo protocolo da Internet**. Novatec Editora, 2018.

CASTELLS, Manuel. **A Galáxia da Internet: Reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Jorge Zahar Editor, 2003.

Cervo, Amado Luiz; Bervian, Pedro Alcino. **Metodologia Científica**. 3 Edição. Editora McGraw-Hill do Brasil. São Paulo, 1983.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Câmara Técnica de documentos eletrônicos. e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos**. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: Acesso em: 15 mai. 2019.

CORRÊA, Amarílis Montagnolli Gomes. **Preservação digital: autenticidade e integridade de documentos em bibliotecas digitais de teses e dissertações**. 2014. Tese de Doutorado. Universidade de São Paulo.

ELMASRI, Ramez et al. **Sistemas de banco de dados**. 2005.

FERREIRA, Aurélio B. de Holanda. **Novo dicionário da língua portuguesa**. Rio de Janeiro: Nova Fronteira, 1996.

FERREIRA, Danielle Thiago. **Profissional da informação: perfil de habilidades demandadas pelo mercado de trabalho**. Disponível em: <http://revista.ibict.br/ciinf/article/view/1018/1073>. Acesso em: 30 out. 2019.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Editora Saraiva, 2017.

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

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. **A segurança dos documentos digitais**. Disponível em < <http://www.jus.com.br> >. Acesso em: Maio 2019.

GATES, Bill. **A estrada do futuro**. São Paulo: Companhia das Letras, 1995.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 5 ed. São Paulo: Atlas, 2010.

GOTARDO, REGINALDO APARECIDO. **Linguagem de Programação**. Rio de Janeiro: SESES, 2015.

GUEDES, Gilleanes T. A. **UML 2: uma abordagem prática**. 2. ed. São Paulo: Novatec Editora, 2011.

HEDSTRÖM, Peter; SWEDBERG, Richard. **Social mechanisms**. *Acta sociologica*, v. 39, n. 3, p. 281-308, 1996.

ISO 17799. ABNT NBR ISO/IEC 17799:2005 – **Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2005.

LOPES, Vítor. **Preservação digital**. Portugal: **Universidade do Minho, Guimarães, 2008**.

MAGALHÃES, Paulo Sérgio Tenreiro; **SANTOS, Henrique Dinis dos**. **Biometria e autenticação**. 2003.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamento de metodologia científica**. 5. ed. Atlas. São Paulo, 2003.

MEDEIROS, Ernani Sales de. **Desenvolvendo software com UML 2.0**. Sao Paulo: **Pearson Makron Books, 2004**.

MILES, Russ; HAMILTON, Kim. **Learning UML 2.0**. California: **O’Reilly, 2006**.

NIEDERAUER, Juliano. **Desenvolvendo Websites com PHP-2ª Edição: Aprenda a criar Websites dinâmicos e interativos com PHP e bancos de dados**. Novatec Editora, 2011.

OTTONI, Marcia Benedicto. **Certificação digital e segurança**. São Paulo: **Certisign, 2005**.

PEREIRA, Adriana Soares et al. **Metodologia da pesquisa científica**. Brasil, 2018.
PINTO, Maria Manuela. **Gestão de Documentos e meio digital: um posicionamento urgente e estratégico**. **Gestão do conhecimento, da informação e de documentos em contextos informacionais, 2013**.

R. RAINER, Kelly; CEGIELSKY, Casey G. **Introdução a Sistemas de Informação**. 3. ed. Rio de Janeiro: **Elsevier, 2011**.

RESENDE, Dilma A. **Certificação Digital**. Revista Jurídica UNIGRAN, v. 11, n. 22, p. 111, 2009.

RESS, Weber. **Começando em segurança**. MSDN. Set. 2011. Disponível em:
SÊMOLA, Marcos. **Gestão da Segurança da Informação**. Elsevier Editora Ltda, 2014.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva – Rio de Janeiro: Campus, 2003.

SILBERSCHARTZ,A; FORTH,H.F; SUDARSHAN,S. **Sistema de Banco de Dados**. 3. ed. 2008.

SILVA JÚNIOR, Sérgio Mota da. Certificação digital a importância para órgão público. 2016.

SILVA, Patrick Pedreira et al. **Integração das tecnologias VRML, PHP e MySQL para a construção de uma biblioteca virtual**. Revista Internacional del Libro, Digitalización y Bibliotecas, v. 2, n. 1, 2016.

STAZISZ, Paulo César. Projeto de software usando a UML. Disponível em:
<<http://www.etelg.com.br/paginaete/downloads/informatica/apostila2uml.pdf>>. Acesso em: 06 set. 2016.

TOMAZINI, Marcos; LOPES, Luiz Fernando Braga. **Web design responsivo– Bootstrap**. 2015.

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.

APÊNDICE A – Termo de Abertura de Projeto

Termo de Abertura de Projeto

NOME DO PROJETO: ASSINATURA DE DOCUMENTOS POR MEIO DA
AUTENTICAÇÃO DIGITAL

DATA DE ELABORAÇÃO: 12/08/2019

1 ESCOPO PRELIMINAR DO PROJETO

1.1 ESCOPO PRODUTO

O sistema irá fornecer uma ferramenta web, de assinatura digital de documentos, que irá facilitar o trabalho do dia-a-dia com agilidade, confiabilidade e segurança nos trâmites de documentos.

1.2 OBJETIVOS DO PROJETO

- a) Definir os conceitos de Autenticação digital.
- b) apresentar as vantagens e desvantagens da utilização da certificação digital na prestação de serviços.
- c) apresentar um software que realize a autenticação digital de documentos.

1.3 PREMISSAS DO PROJETO

- a) Falta de tempo para desenvolvimento.

1.4 RESTRIÇÕES DO PROJETO

- a) O Projeto deverá estar em conformidade com os parâmetros instituídos pelo Centro Universitário Atenas.
- b) Todas as ferramentas utilizadas deverão constar na parte escrita do projeto.

c) O usuário receberá uma senha mestra para seu uso.

d) O sistema será desenvolvido somente em versão web.

2 EQUIPE PRELIMINAR

Este projeto está sendo elaborado por Vagner Claudino de Melo

3 RISCOS PRELIMINARES

TABELA 1: RISCOS PLELIMINARES

TABELA 1: RISCOS PLELIMINARES

Identificação	Riscos
RP 01	Projeto não ser aceito
RP 02	Projeto não ser entregue em tempo
RP 03	Indisponibilidade de integrantes na participação do projeto
RP 04	Mudanças no cronograma do projeto
RP 05	Mudanças no escopo do projeto

Fonte: Elaborado pelo autor.

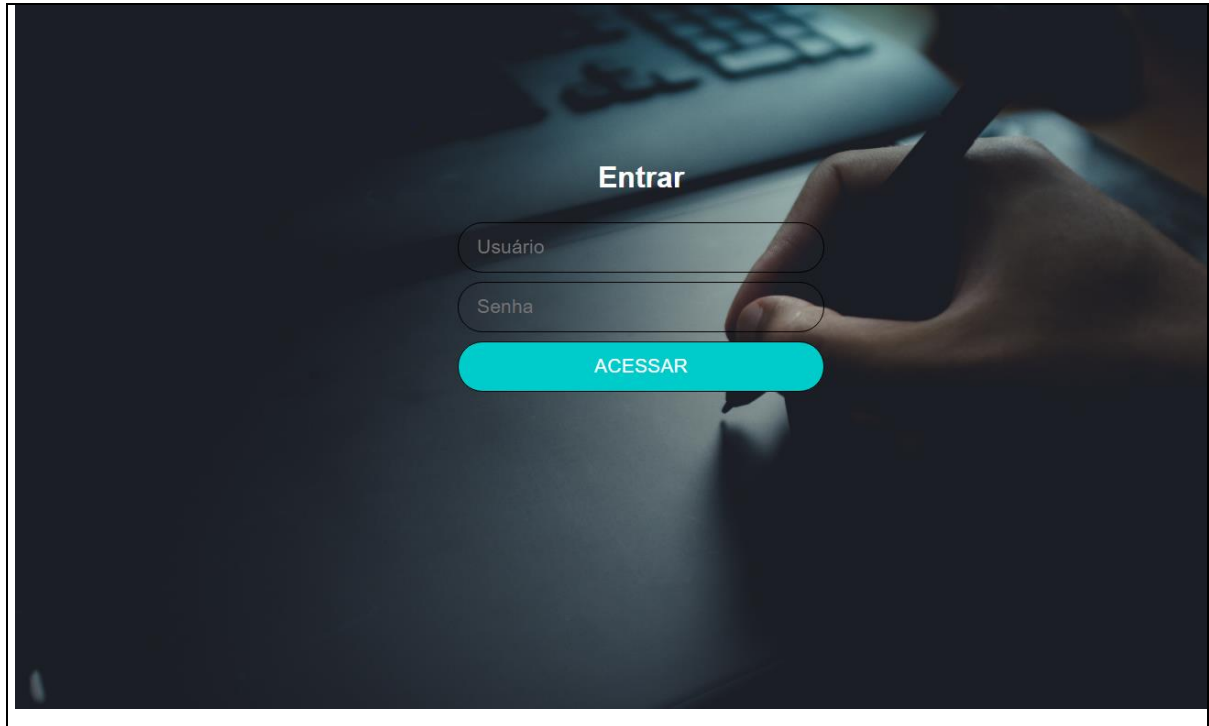
1 APROVAÇÃO

Data de Aprovação: 31 de Outubro de 2019.

Felipe Neto Vasconcelos

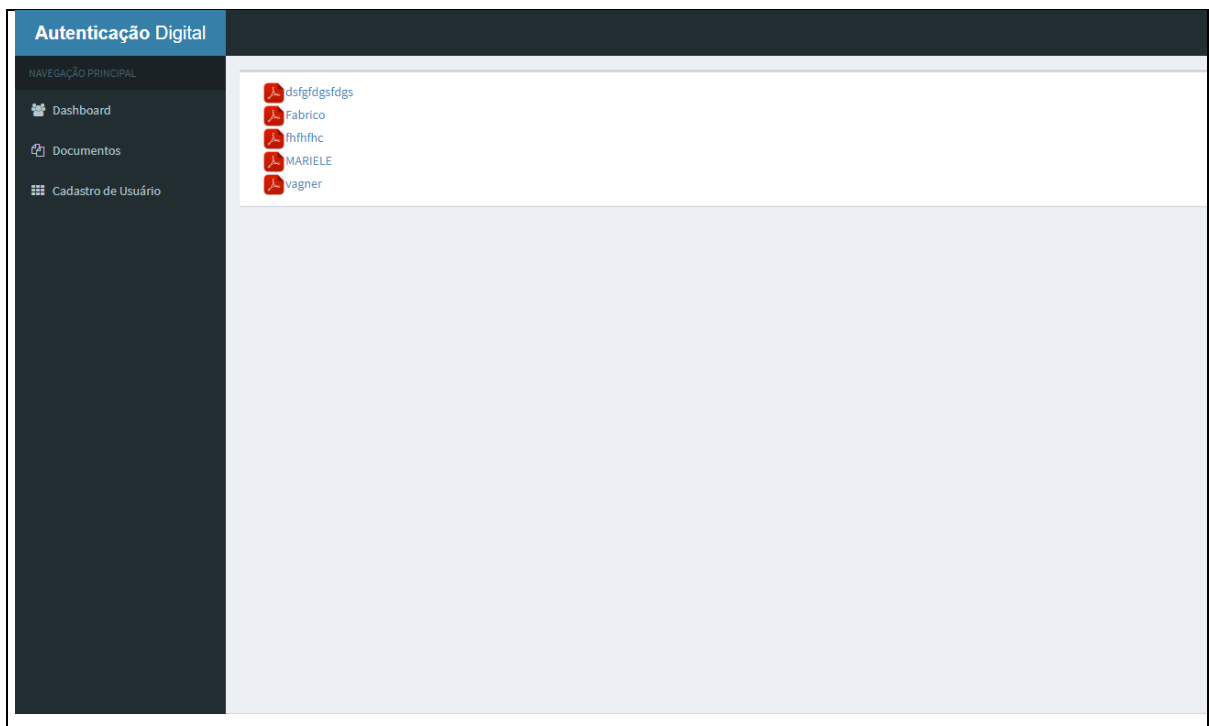
APÊNDICE A- TELAS DO SISTEMAS

Figura 1 - Tela de autenticação



Fonte: Elaborado Pelo Autor

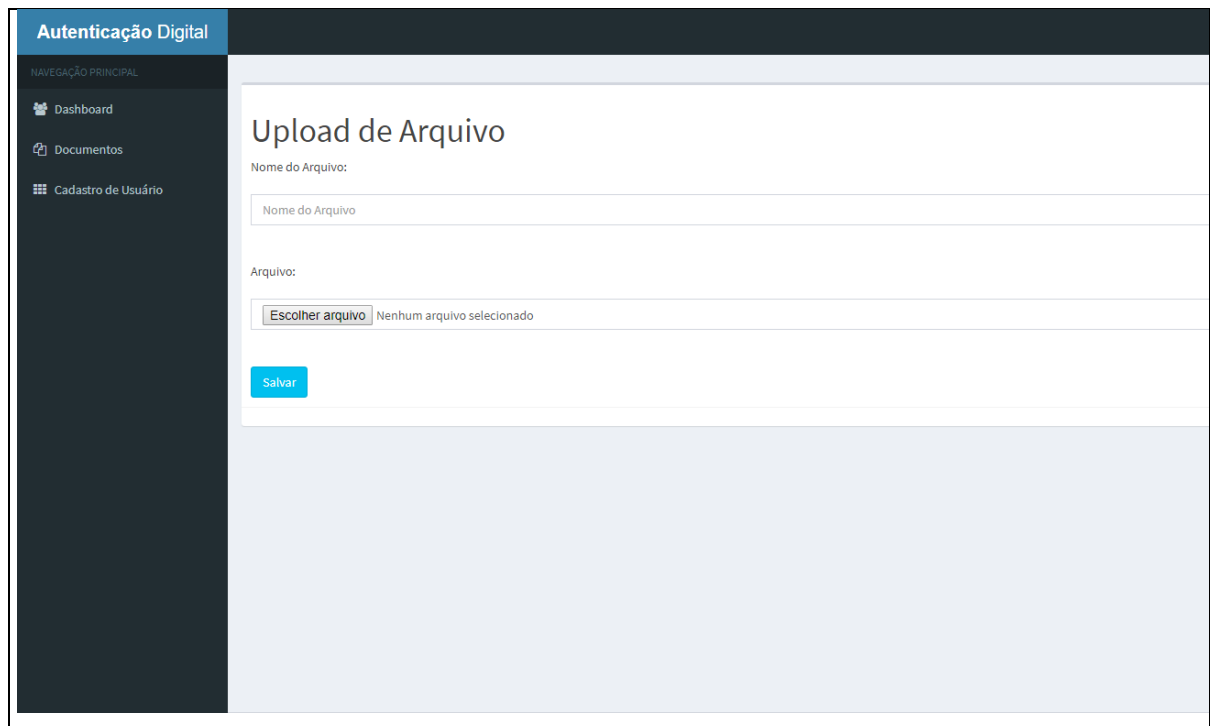
Figura 2 - Tela de dashboard



Fonte: Elaborado Pelo Auto

Figura 3 - Tela de Dashboard

Fonte: Elaborado Pelo Autor

Figura 4 - Tela de upload

Fonte: Elaborado Pelo Autor

Figura 5 - Tela de cadastro de cliente

The image shows a web application interface for digital authentication. On the left is a dark sidebar with the title 'Autenticação Digital' and a menu with options: 'Dashboard', 'Documentos', and 'Cadastro de Usuário'. The main content area is titled 'Cadastro de Usuários' and contains a registration form with the following fields: 'Nome Completo', 'Telefone', 'Email', 'Senha', and 'Confirmar Senha'. A blue 'CADASTRAR' button is located at the bottom of the form.

Autenticação Digital

NAVEGAÇÃO PRINCIPAL

- Dashboard
- Documentos
- Cadastro de Usuário

Cadastro de Usuários

Nome Completo

Nome Completo

Telefone

Telefone

Email

Email

Senha

Senha

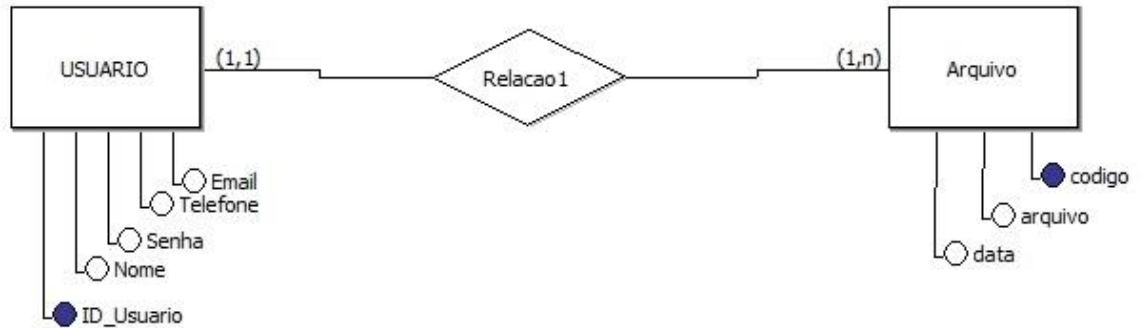
Confirmar Senha

Confirmar Senha

CADASTRAR

Fonte: Elaborado Pelo Autor

Figura 6 – Modelo conceitual



Fonte: Elaborado Pelo Autor

Figura 7 – Modelo Logico



Fonte: Elaborado Pelo Autor