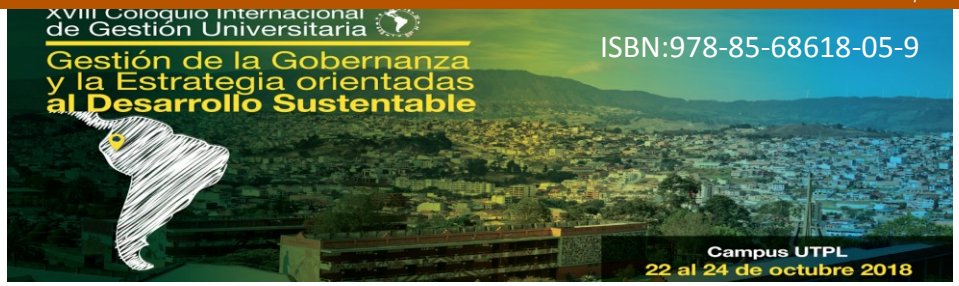

A GESTÃO UNIVERSITÁRIA EM UMA PERSPECTIVA SÓCIO-TÉCNICA SOBRE O USO DA CERTIFICAÇÃO DIGITAL EM NUVEM NA UNIVERSIDADE FEDERAL DE SANTA CATARINA, SEGUNDO AS NORMATIVAS 06 E 10 DE 2017 DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

ANDRE PAVANATI
Universidade Federal de Santa Catarina
andre.p@ufsc.br

FERNANDO LAURO PEREIRA
Universidade Federal de Santa Catarina
fernando.pereira@ufsc.br

ALESSANDRA DE LINHARES JACOBSEN
Universidade Federal de Santa Catarina
alessandra.jacobsen@ufsc.br

JEAN EVERSON MARTINA
Universidade Federal de Santa Catarina
jean.martina@ufsc.br

RESUMO

O desenvolvimento de tecnologias na área da segurança da informação trouxe grandes avanços no tocante à produção documental. A transformação substancial dos processos elaborados na gestão das universidades começou com a criação de documentos digitais e, posteriormente, com a utilização do certificado digital conferindo maior segurança, agilidade e integridade, contribuindo para a sustentabilidade ambiental. Vantagens e cuidados são necessários no uso desta ferramenta, pois é através dela que se identifica de forma inequívoca o titular em ambiente virtual que não poderá repudiar essa identificação ou a assinatura em documentos digitais. O custo dessa ferramenta ainda é elevado para o poder público. Este trabalho trata-se de uma pesquisa qualitativa, descritiva, aplicada e bibliográfica que tem como objetivo mostrar como as Instruções Normativas nº 06 e nº 10 de 2017 do ITI podem dar apoio aos gestores públicos no sentido de facilitar o acesso ao certificado digital através da validação pelo SIGEPE e a mobilidade do titular do certificado digital armazenado na nuvem, assim como garantir a integridade, originalidade e autenticidade dos documentos assinados e aos acessos por ele realizados.

Palavras Chave: gestão universitária, certificação digital na nuvem, validação SIGEPE.

1. INTRODUÇÃO

A constante evolução tecnológica nas áreas da administração e segurança da informação, impactam diretamente nas atividades cotidianas da gestão universitária, tanto nas realizadas com grande eficiência quanto as realizadas de forma burocrática e ineficaz, e seguem sofrendo constantes modificações evolutivas com o passar do tempo devido a interferência de novas ferramentas tecnológicas e necessidades em desempenho e segurança no serviço público.

Na administração universitária o tratamento da informação e os trâmites processuais de documentos físicos e digitais, relativos à gestão acadêmica e administrativa, são intensos e geram grandes volumes de trabalho, criando um cenário suscetível a falhas e fraudes. Percebe-se a falta de entendimento por parte dos gestores sobre o entendimento quanto às diferenças entre documento digital e documento digitalizado, bem como quanto ao uso da certificação digital na administração universitária e o que se entende por assinatura digital e por assinatura digitalizada. Especialmente no que tange a necessidade de se imprimir um documento criado em um processador de texto utilizando um computador, para assiná-lo e posteriormente digitalizá-lo. Não se age com ciência técnica nem com conhecimento da legislação nestes casos. O mesmo ocorre no que diz respeito ao uso do Certificado Digital no trato das tarefas administrativas, não se sabe como utilizar na maioria das vezes, tampouco se conhece seus benefícios.

Como servidores públicos federais da ativa, atuando na Universidade Federal de Santa Catarina - UFSC, os pesquisadores observam a existência das práticas suso mencionadas, que geram retrabalho, perda de tempo e desperdício de insumos. Se conduz à ideia de que se repense as ferramentas disponíveis e como se poderia utilizá-las no aprimoramento da gestão universitária, pela tramitação de documentos e processos com eficiência. Bem como garantir agilidade e economicidade aos processos, qualidade no ambiente de trabalho, usabilidade nas atividades, bem como garantir a integridade, autenticidade, confidencialidade, confiabilidade e segurança das informações.

Assim como no tratamento de documentos físicos, impressos e assinados, existe a necessidade da chancela de um tabelionato, para conferir autenticidade e segurança às informações, por meio do trabalho de um agente, portador de fé pública, que confirma a autenticidade da assinatura do autor. De modo equivalente, no tratamento de documentos natos digitais (que nunca foram impressos), a certificação digital garante a autenticidade do autor, a integridade do documento, garantindo que este não foi alterado após ter sido assinado digitalmente, agregando confiabilidade, confidencialidade e segurança neste tipo de tratamento da informação. A diferença é que o agente que confere fé pública neste caso, não precisa confirmar a autenticidade do autor a cada assinatura, basta fazê-la no ato da emissão do certificado digital do autor. A partir daí, o uso do certificado digital pelo mesmo garante por si só sua autenticidade, desde que este certificado digital tenha sido emitido por um Agente de Registro, devidamente credenciado em uma Autoridade de Registro, confiada por uma Autoridade Certificadora, autorizada pela Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, criada pela Medida Provisória 2.200 de junho de 2001. A cadeia de confiança em questão, é a responsável pela garantia dos direitos concomitantes ao uso do Certificado Digital ICP-Brasil.

Na UFSC, a Coordenadoria de Certificação Digital da Sala Cofre CCD-UFSC, vinculada a Secretaria de Planejamento e Orçamento da Universidade, é responsável por todas as demandas que envolvem certificação digital nos Campi. Desde a emissão de certificados digitais do tipo SSL para serviços online (sites e sistemas) até o atendimento às necessidades de certificados digitais para pessoas, bem como na capacitação, suporte e assistência aos servidores em seus centros, departamentos, pró-reitorias e à administração universitária. Atuam tanto na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, quanto na Infraestrutura de Chaves Públicas de Ensino e Pesquisa - ICP-Edu. Estas infraestruturas possuem equivalência técnica, porém somente a ICP-Brasil é coberta pela Medida Provisória 2.200/2001. A segunda atende demandas específicas às IFEs em suas pesquisas e extensões de forma gratuita à comunidade universitária. Ambas são utilizadas na UFSC em sinergia com projetos e operações, conforme a aplicabilidade demandada. A CCD, por manter uma equipe técnica especializada e ser responsável pela manutenção de um ambiente seguro de alta disponibilidade na UFSC, chamada Sala Cofre, com 5 níveis de segurança, rígido controle de acesso, Acordo de Nível de Serviço de 99,9%, certificada pela ABNT NBR 15247 e Procedimento Específico PE 047-7, mantém um termo de cooperação com o ITI, ligado à Casa Civil da Presidência da República como Prestador de Serviço de Suporte na ICP-Brasil e projetos com a Rede Nacional de Ensino e Pesquisa - RNP, mantenedora da ICP-Edu. No que tange às pesquisas e extensões acadêmicas na área de criptografia, certificação digital e segurança computacional, a UFSC possui um dos laboratórios mais renomados do Brasil, com referências em trabalhos e projetos internacionais, vinculado ao Centro Tecnológico, o Laboratório de Segurança Computational - LabSEC. Este também mantém Termos de Cooperação bem como Projetos de Pesquisa e Extensão com a ICP-Brasil e a ICP-Edu, no desenvolvimento de soluções em criptografia, segurança e certificação digital.

O ITI utiliza uma série de documentações que correspondem a versões das resoluções da ICP-Brasil em vigor, organizadas de forma a facilitar a leitura e compreensão daquele que as estuda. São manuais, notas técnicas, portarias, decretos, resoluções e instruções normativas. Em agosto de 2017, uma Instrução Normativa em particular causou certa agitação no serviço público federal, a IN nº 06 que dispôs da validação de solicitação de certificados digitais para servidores públicos da ativa e militares da união. Esta normativa abre novas possibilidades no processo de emissão de certificados digitais ICP-Brasil no serviço público federal. Em dezembro do mesmo ano, foi publicada a IN nº 10 que criou o DOC-ICP-17.01 para tratar dos procedimentos operacionais mínimos para os Prestadores de Serviço de Confiança - PSC - da ICP-Brasil. Visto que o PSC terá a tarefa primária de armazenar os certificados digitais dos usuários finais na ICP-Brasil, mantendo o controle, uso e conhecimento exclusivo por parte do seu titular, dentro de dispositivos criptográficos (HSM) que poderão estar em uma solução de nuvem, com alta capacidade de performance e segurança. Segundo o ITI, o Projeto de Certificação Digital em Nuvem (HSM/PSC da ICP-Brasil) visa, assim como feito no padrão europeu, entregar à sociedade brasileira uma nova forma para armazenar os certificados digitais dos usuários finais e regulamentar os portais de assinaturas digitais para dados, documentos e transações eletrônicas.

A pesquisa tem como objetivo demonstrar como as IN nº 06 e nº 10 do ITI podem impactar na Gestão Universitária, sob a luz de uma perspectiva sócio-técnica direcionada ao uso do Certificado Digital em Nuvem na UFSC. Para isso, caracterizou-se esta como uma pesquisa qualitativa. Quanto aos meios é uma pesquisa bibliográfica e documental. No que diz respeito aos fins, caracteriza-se como uma pesquisa descritiva.

2. FUNDAMENTAÇÃO TEÓRICA

Nesta seção serão abordados os tópicos necessários para que subsidiem o leitor acerca da gestão universitária, segurança da informação e a tecnologia da certificação digital, no sentido de sua estrutura. Na sequência, será explanado o que dispõem as instruções normativas nº 06 e nº 10 de 2017 do ITI.

2.1. GESTÃO UNIVERSITÁRIA

O compromisso de diferentes segmentos acadêmicos em sinergia com a gestão universitária, se vinculam à formulação de um modo de produzir que seja mais eficiente socialmente, sem que se exima os responsáveis pelo poder decisório de uma reorganização interna, o trabalho acadêmico (Catani, 2001). O mesmo autor trata também a organização e a gestão universitária quanto a necessidade de modernização-modelação institucional requerida pelos gestores, no sentido da formulação de sistemas de informação supracitadas, associados a políticas que tornem mais ágeis e eficientes o trabalho nos trâmites universitários.

A gestão de uma Universidade Federal obedece leis federais e diretrizes do Ministério da Educação. No entanto, a autonomia que lhe foi concedida pelo artigo 207 da Constituição Federal Brasileira de 1988 – CF/88 (BRASIL, 1988), oferece liberdade à maneira como pode ser administrada. Assim, a autonomia universitária trata da autonomia didático-científica, administrativa e de gestão financeira e patrimonial (BRASIL, 1988). No âmbito das Universidades, inclui-se ainda os respectivos estatutos e regimentos próprios, à partir destes os administradores gestam e cumprem a burocracia presente em sua cultura organizacional, processos, pessoas e tecnologias na busca pela eficiência operacional, das quais os princípios da administração pública preconizam.

2.1.1. Processos

Processo é a forma pela qual um conjunto de atividades cria, trabalha ou transforma insumos (entradas), agregando-lhes valor, com a finalidade de produzir bens ou serviços, com qualidade, para serem entregues a clientes (saídas), sejam eles internos ou externos, afirma Cruz (2010). Biazzi (2007, p.28) menciona que, ao se adotar "uma visão por processo, tem-se um enfoque do trabalho como um todo, e não apenas das partes que ocorrem em cada departamento, visão esta que se insere na perspectiva da teoria dos sistemas".

Nas atividades administrativas das Instituições Federais de Ensino Superior - IFES, encontram-se os processos burocráticos, necessários para que seja efetivada a sua gestão. Dentre esses processos existem os que, por exemplo, são relativos às compras, a abertura de pregão, inexigibilidade de licitação, dispensa de licitação ou processos relativos a pagamento de fornecedores. Outros exemplos são os da área de gestão de pessoas como os processos para acompanhamento de estágio probatório de iniciativa da administração, conforme estabelece o Art. 41 da Constituição Federal da República Federativa do Brasil de 1988 (BRASIL, 1988), ou solicitado pelo servidor como nos casos de progressão por capacitação profissional ou incentivo à qualificação. O conselho universitário na UFSC também realiza a apreciação de processos que foram abertos e incluídos na pauta de reuniões ordinárias e extraordinárias. Percebe-se que diversas são as áreas dentro da universidade que necessitam a abertura de processos. Cada instituição realiza a montagem dos processos, atendendo o que exige a legislação.

Di Pietro (2009) lembra que o princípio da legalidade remete à ideia de que a vontade da Administração Pública é aquela decorrente da lei.

Para Weber (1982, p. 229), "a burocracia moderna funciona sob formas específicas e está sob a regência de áreas de jurisdição fixas e oficiais, ordenadas por leis e normas administrativas". Reforçando os pensamentos de Max Weber, Chiavenato (1987) afirma que a burocracia se caracteriza pelo conjunto de cargos, delimitados por normas, na qual cada indivíduo ocupa um cargo bem definido, cada um com nome específico e regido por normas escritas que estabelecem direitos e deveres para os ocupantes dos cargos. O autor ratifica que na burocracia prevalece o que está escrito sobre a expressão verbal, de modo que sempre que possível, estando as ações provadas e embasadas em documentos.

No contexto da gestão universitária, o poder do funcionário especializado é valorizado e a qualificação, como forma de especialização crescente, resulta em benefício na qualidade do serviço prestado. Este preconiza pontos positivos descritos por Weber (1982, p. 269) que afirma: - "em relação à burocracia são que ela potencializa o conhecimento e as intenções". No contexto universitário, resgata-se Meyer Jr. (2007) quando se afirma que a instituição de ensino superior é um ambiente complexo, onde se pode ter o melhor das duas realidades, o padrão e o controle beneficiados pela burocracia descrita por Weber (1982).

Na UFSC um processo é autuado no Sistema de Processos Administrativos - SPA. Dentro do SPA existem duas opções para o cadastro de processos, sendo eles o cadastro de processo físico e o cadastro de processo digital. O fluxo de cadastro de processo físico consiste em três etapas: a primeira em juntar fisicamente as peças do processo, ordená-las em uma pasta e, em cada folha, carimbar, numerar e rubricar cada página. A segunda etapa consiste em entrar no módulo "cadastro de processo físico" no SPA, informar os dados básicos do setor de abertura e do interessado pelo processo, além de uma descrição sobre o assunto. Na terceira etapa é impressa a etiqueta, colada na pasta física e realizada a tramitação na aba "tramitação" do processo no SPA para o volume ser despachado fisicamente ao destino via malote.

No processo digital o trabalho consiste em juntar todas as peças do processo em forma digital, ou seja, peças que nasceram originalmente digitais ou peças físicas que foram digitalizadas e estão prontas para serem inseridas aos autos. Na UFSC, essa modalidade de fluxo de cadastro também segue três etapas sendo: a primeira consiste em acessar o módulo "cadastro de processo digital", preencher os dados básicos do setor de abertura e do interessado pelo processo, além de uma breve descrição sobre o assunto. Na segunda etapa é feita a juntada das peças do processo de forma digital, incluindo esses arquivos na aba "peças", nomeando cada arquivo para facilitar a consulta; a numeração de páginas é feita automaticamente. É possível assinar cada peça com certificado digital. Na terceira etapa o solicitante do processo acessa a aba "tramitação", informa o motivo da movimentação processual e o seu destino, finalizando o cadastro do volume que estará digitalmente disponível ao destinatário no momento em que a tramitação for concluída pelo sistema.

Para Cruz (2010) o objetivo da análise de processos é a criação, implantação e melhoria do processo que vai suportar o negócio. Afirma ainda que a análise da cadeia de valores, com vistas a determinar a real necessidade de cada etapa do processo, é também uma importante função na análise de processos. Este tipo de análise permite que o administrador tenha uma visão ampliada dos problemas e oportunidades.

2.1.2. Pessoas

Na instituição, as pessoas são organizadas em grupos de trabalho, que por sua vez operam imersos em uma cultura organizacional, esta se refere aos elementos do referido grupo, que são mais estáveis e menos maleáveis, sendo que uma vez desenvolvida, cobre todo o funcionamento de um grupo, afirma Schein (2009). De outro modo, Morgan (1996, p.115-116) diz que cultura "refere-se tipicamente ao padrão de desenvolvimento refletido nos sistemas sociais de conhecimento, ideologia, valores, leis e rituais cotidianos. A palavra é também habitualmente usada para fazer referência ao grau de refinamento evidente em tais sistemas de crenças e práticas". A cultura é o meio de comunicação do homem (Hall, 1984). O autor afirma que a cultura possui três características: ela não é inata, e sim aprendida; suas distintas facetas estão inter-relacionadas; ela é compartilhada e de fato determina os limites dos distintos grupos. No tocante, Morgam (1996, p.116) ratifica que "diferentes grupos de pessoas têm diferentes estilos de vida". O autor comenta que, "ao se falar sobre cultura, na verdade, está sendo feita uma referência ao processo de construção da realidade que permite às pessoas ver e compreender eventos, ações, objetos, expressões e situações particulares de maneiras distintas".

No âmbito universitário há uma cultura influenciada por regras institucionais, leis, tecnologias disponíveis e métodos de trabalho definidos implicitamente pelos próprios grupos. Neste contexto é fundamental identificar a realidade social desta cultura aceita pelo grupo, verificar a compatibilidade desta com a implantação de inovações, a exemplo da certificação digital no processo de gestão. Na cultura organizacional, a resistência à mudança pode impedir a inovação na gestão se esta exigir o aprendizado de uma nova tecnologia.

2.1.3. Tecnologia

O desenvolvimento da tecnologia tem proporcionado muitos ganhos para as organizações, instituições públicas, universidades e para a sociedade como um todo. Os processos burocráticos foram se modificando com o desenvolvimento de novas aplicações para rotinas de trabalho que, anteriormente, eram feitas à mão, ou seja, toda a cadeia produtiva era feita pelo homem. Atividades contábeis, de engenharia, arquitetura e administrativas ganharam programas para solucionarem problemas e ganhar tempo. O tempo que um contador levaria para elaborar e calcular um balancete ou um arquiteto para elaborar um projeto foi reduzido. Com isso novos aprendizados e novas formas de trabalho surgiram, assim como muitas dúvidas. A necessidade em resolver essa lacuna que se forma em relação ao novo faz com que o ser humano se desenvolva e transforme as atividades rotineiras em outras mais eficientes.

Na administração, muitos documentos são elaborados através de editores de texto e trafegam pela internet. Outras vezes esses documentos são impressos e assinados fisicamente. Em alguns momentos podem ter uma imagem de assinatura física escaneada ou podem ser assinados digitalmente. Muitas dúvidas ainda existem em relação à assinatura digital e a assinatura digitalizada. A assinatura digitalizada pode ser obtida através de uma assinatura feita de próprio punho, onde a imagem da assinatura foi capturada por um scanner ou máquina fotográfica digital e inserindo essa imagem a um documento que está sendo elaborado de forma digital (VALID, 2016). Esse tipo de documento não tem validade pois não garante a autoria e a integridade do documento digital. Já a assinatura digital é uma forma de garantir, através de um certificado digital,

que o documento assinado tenha integridade e seja considerado original, podendo garantir que a pessoa que o assinou no mundo virtual é realmente ela no mundo físico.

2.2. SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA

A transformação das comunicações, telecomunicações e desenvolvimento da computação fez com que a forma como os documentos, registros e processos fossem se modificando em um curto espaço de tempo. O apelo pela redução do consumo de papéis fez com que novas tecnologias fossem empregadas nesse sentido. Com isso, a formalização se fez necessária com o objetivo de garantir que documentos que transitam no ambiente virtual através do comércio eletrônico e serviços do governo para o cidadão tivessem reconhecimento e fé pública, imprimindo autenticidade às informações. Nesse contexto surgiu, por meio do Decreto nº 2.200 de 28 de junho de 2001 a ICP-Brasil, buscando garantir a integridade, autenticidade e validade jurídica de documentos em forma eletrônica, realização de transações eletrônicas de forma segura, aplicações de suporte a aplicações que utilizem certificação digital (BRASIL, 2001).

2.2.1. Infraestrutura de chaves públicas brasileira

A infraestrutura de chaves públicas brasileira é uma cadeia hierárquica de confiança que tem como incumbência a emissão de certificados digitais com a finalidade de identificar pessoa física, jurídica ou servidores no ambiente virtual. Tendo característica de raiz única, sendo o ITI a AC-Raiz, tem também a função de credenciar ou descredenciar os agentes que compõem a cadeia, assim como fiscalizá-los e auditar os seus processos. A estrutura da ICP-Brasil está disposta conforme o esquema:

Figura 1: Hierarquia da ICP-Brasil - **Fonte:** Victorino e Fortunato (2012)

2.2.1.1. Autoridade certificadora - AC

As Autoridades Certificadoras são as responsáveis pela emissão dos certificados digitais. Vinculado à Casa Civil da Presidência da República, o Instituto Nacional de Tecnologia da Informação (ITI) fiscaliza as Autoridades Certificadoras. É considerada autoridade máxima brasileira no que se refere à certificação digital e é a Autoridade Certificadora Raiz (AC-Raiz). Dentro da cadeia de certificação o ITI é a primeira autoridade de certificação na análise do certificado digital emitido. Sobre as cadeias de certificação digital observa-se que

> A autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovados pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu. (ITI, 2017).

Através dessa informação verifica-se que a AC-Raiz é quem tem a responsabilidade de gerenciar as outras AC's no Brasil, que encontram-se inferiores hierarquicamente, na cadeia de certificação. É a responsável por emitir a Lista de Certificados Revogados - LCR e de fiscalizar e auditar as demais AC's, AR's e prestadores de serviço habilitados na ICP-Brasil. Tem como tarefa verificar se as AC's estão atuando de acordo com as diretrizes e normas técnicas conforme estabelece o Comitê Gestor da ICP-Brasil (ITI, 2018).

Podendo ser de direito público ou privado, as autoridades de nível inferior ao da AC-Raiz são responsáveis por "emitir, distribuir, renovar, revogar e gerenciar os certificados digitais" (ITI, 2018). É sob a responsabilidade das AC's que é feita a verificação se os titulares dos certificados digitais possuem as chaves privadas correspondentes às chaves públicas. Compete às Autoridades Certificadoras, também, criar e assinar digitalmente o certificado do assinante, sendo que o certificado por aquela AC emitido representará a identidade do titular, que possui um par único de chaves (pública e privada).

Como todo certificado digital tem prazo de validade, após expirado é de responsabilidade da AC incluí-lo em uma Lista de Certificados Revogados, além de manter os registros de suas operações, obedecendo às diretrizes da Declaração de Práticas de Certificação - DPC. Compete, também, às AC's estabelecer e fazer cumprir as políticas de segurança das Autoridades de Registro - AR à elas vinculadas, a fim de garantir a autenticidade da identificação efetuada pelos seus agentes (ITI, 2018).

2.2.1.2. Autoridade de registro - AR

Responsável por fazer a interface entre usuário e a AC, a Autoridade de Registro recebe o usuário, faz a identificação presencial e documental, além de validar os documentos exigidos para a emissão do certificado, o encaminhamento de solicitações de emissão de novos certificados e, também, de revogação dos certificados que tiveram sua segurança colocada em risco. Precisa manter os registros de todas as suas operações. A AR pode estar localizada dentro de uma AC ou também pode estar localizada em outro espaço físico onde, neste caso, será considerada uma AR remota (ITI, 2018).

2.2.1.3. Agente de registro

É a pessoa física credenciada por uma AC para atuar dentro de uma AR, com a tarefa de fazer a identificação presencial e documental do solicitante, além da coleta das características biométricas (foto e digitais) da pessoa que está requisitando o certificado. É atribuído a um segundo Agente de Registro que faça a conferência de toda a documentação e informações identificadas pelo primeiro agente, com o objetivo de validar as informações registradas pelo primeiro para, se estiver tudo correto, fazer a emissão do certificado ao solicitante. Cabe ao Agente de Registro, quando solicitado pelo titular, fazer a revogação do certificado digital (CERTISIGN, 2018).

2.2.1.4. Prestador de serviço de suporte - PSS

Tem como atribuição desempenhar as atividades descritas nas Políticas de Certificado - PC e na DPC da AC a qual possuir vínculo, classificando-se em três categorias conforme o tipo de atividade prestada, podendo disponibilizar: infraestrutura física e lógica; recursos humanos especializados; ou irá disponibilizar infraestrutura física, lógica e recursos humanos especializados (ITI, 2018).

2.2.1.5. Prestador de serviço de confiança - PSC

Segundo o DOC-ICP-17 do ITI, o

> PSC da ICP-Brasil é uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de armazenamento de chaves privadas para usuários finais, nos termos do DOC-ICP-04 [11], ou serviços de assinaturas e verificações de assinaturas digitais padrão ICP-Brasil nos documentos e transações eletrônicas ou ambos (ITI, 2017, p.7).

É no PSC que ficam localizados os HSM, responsáveis por guardar as chaves privadas dos usuários que possuem certificados digitais em nuvem.

2.2.2. Certificado digital

O certificado digital é uma credencial eletrônica, garantida por meio de um processo que envolve uma hierarquia de confiança e segredos compartilhados, que dependendo do tipo, podem ser armazenados em um dispositivo criptográfico (token, smartcard ou HSM), ou seja, em equipamentos que garantam a "escrita secreta por meio de abreviaturas ou de sinais convencionados de modo a preservar a confidencialidade da informação" (SILVA et al, 2008, p.13), composto por um par de chaves que obedecem a uma função algorítmica que tem como finalidade aplicar e conferir originalidade e integridade aos documentos digitais. O documento só passa a ser assinado digitalmente quando combinadas as chaves criptográficas. Essas chaves são denominadas de chave pública e chave privada. A primeira refere-se à chave que é de domínio público, assinado pela Autoridade Certificadora Raiz - AC-Raiz. A segunda chave é de domínio privado que fica armazenada em um dispositivo criptográfico e só é liberada para a combinação e assinatura do documento mediante senha pessoal. No documento assinado digitalmente são incorporados dados que permitem consultar a sua originalidade e integridade

A tecnologia de criptografia envolvida na certificação digital foi desenvolvida com o intuito de garantir a segurança da informação entre origem e destino, sendo que tem como objetivo proteger as informações das organizações de ataques e ameaças, garantindo a continuidade das atividades, mantendo as oportunidades de negócios e o retorno dos seus investimentos (SILVA et al, 2008). Essa segurança tem como base algoritmos criptográficos, garantindo que as informações criadas em um documento digital possam trafegar entre origem e destino sem que tenham seu conteúdo alterado, ou seja, com a certeza de que a conferência da originalidade e integridade do documento sejam confirmadas pelo destinatário através da assinatura digital. A criptografia assimétrica utilizada na tecnologia da assinatura digital traz a autenticidade de que, ao receber o documento e conferir a assinatura digital, não haja dúvidas sobre o seu autor. Sobre a criptografia assimétrica trata-se de algoritmos de criptografia que utilizam um

par de chaves sendo uma privada que fica guardada, em segredo, com o portador do certificado e a outra chave de domínio público que é distribuído abertamente. Esse algoritmo possibilita, além de recursos diversos, operações como a assinatura digital e a criptografia (FERREIRA, 2008). Os certificados digitais são validados e emitidos através de apresentação pessoal e documental do interessado (pessoa física ou do representante legal de pessoa jurídica), e emitidos por uma Autoridade Certificadora - AC. No momento da assinatura, o sistema que possui o dispositivo assinador identifica o certificado digital da parte interessada e solicitará ao indivíduo que insira a sua chave privada mediante a sua senha pessoal. Uma vez inserida a senha o documento é assinado digitalmente, com a garantia de autenticidade das cadeias hierárquicas que compõem o certificado digital.

A identidade no ambiente virtual é conferida através do certificado digital. Conforme visto anteriormente, essa identidade passa por um processo de reconhecimento físico nas AC's mediante a apresentação de documentos que comprovem que aquela pessoa é quem diz ser. Nesse sentido, todo documento digital assinado digitalmente não pode ser negado no sentido de sua autenticidade ou repudiado pela parte autora. Sobre o certificado digital e sua garantia de identidade o ITI (2017) esclarece que o certificado digital ICP-Brasil, no ambiente virtual, é equivalente a um documento físico de identidade, garantindo de forma segura e inequívoca a pessoa certificada no ambiente virtual em transações digitais como na web, sendo que esse documento digital é gerado e assinado por uma terceira parte confiável que é uma Autoridade Certificadora, seguindo as regras que foram estabelecidas pelo Comitê Gestor da ICP-Brasil.

2.3 - A VALIDAÇÃO DE SOLICITAÇÃO DE CERTIFICADOS PARA SERVIDORES PÚBLICOS DA ATIVA E MILITARES DA UNIÃO - IN 06/2017/ITI

Com a crescente prática da criação de documentos digitais e com a necessidade de promover a sustentabilidade ambiental, assim como a eficiência dos gastos públicos, foi editada pelo ITI no dia 11 de agosto de 2017 a portaria nº 06, com o objetivo de facilitar a emissão de certificados digitais para os servidores públicos da ativa e aos militares da União.

Atualmente, o processo de validação de um certificado digital é composto pelas etapas de solicitação do certificado e validação com agente de registro, através de uma AC. Além das conferências realizadas pelo agente de registro, é efetuado também o cadastramento biométrico do solicitante, com a coleta de fotografia e das digitais, sendo que após esses registros e verificações o certificado já estará pronto para a emissão (ITI, 2017).

Com a portaria nº 06 do ITI, os servidores públicos passaram a ter a facilidade de validar os seus documentos através do SIGEPE, no caso dos agentes vinculados à esfera federal. O banco de dados do Sistema de Gestão de Pessoas é alimentado por um servidor público que já fez a identificação e a verificação de toda documentação do agente no momento da sua posse ao cargo admitido, sendo que essas informações registradas no banco de dados carregam a presunção de legitimidade e veracidade. Lembrando o que diz Maria Sylvia Zanella di Pietro (2009, p.197-198)

> **presunção de legitimidade** diz respeito à conformidade do ato com a lei; em decorrência desse atributo, presumem-se, até prova em contrário, que os atos administrativos foram emitidos com observância da lei. A **presunção de veracidade** diz respeito aos **fatos**; em decorrência desse atributo, presumem-

> se verdadeiros os fatos alegados pela Administração. Assim ocorre com relação às certidões, atestados, declarações, informações por ela fornecidos, todos dotados de fé pública.

Partindo do princípio que esse sistema é alimentado por um servidor público e que de acordo com o direito administrativo tem a presunção de veracidade na inserção das informações, consideram-se verdadeiros os registros depositados no banco de dados do SIGEPE, para fins de validação do certificado digital. Nesse sentido, conforme a portaria nº 06 (ITI,2017), o agente público não precisa mais se dirigir até uma agência de registro, no entanto precisará se apresentar fisicamente ao servidor público com poderes para autorizar a emissão do certificado. Esse servidor será formalmente cadastrado na AC autorizada e ficará responsável pela emissão dos certificados na instituição.

Os órgãos públicos precisarão obedecer outras características no momento da validação. Essas características são a consulta de registros biométricos através das bases de dados do Tribunal Superior Eleitoral - TSE ou dos Prestadores de Serviços Biométricos - PSBios, que são entidades que possuem capacidade técnica para fazer a identificação biométrica, de forma confiável e que sejam credenciados pela ICP-Brasil. A base de dados onde estão contidos os dados dos servidores serão indicadas pelo Ministério do Planejamento, Desenvolvimento e Gestão - MP e, no caso dos militares, pelos comandos militares, de forma que esses registros não sofram alterações pois serão emitidos à AC para que seja efetuada a emissão dos certificados (ITI, 2017).

Para estabelecer a comunicação entre o serviço público e o órgão certificador, a portaria nº 06 do ITI (2017, p.2) dispõe que seja utilizado um "Módulo Eletrônico da AR do Ministério do Planejamento, Desenvolvimento e Gestão e dos Comandos Militares", sendo que esse módulo deverá ser um sistema que seja vinculado a uma AC credenciada à ICP-Brasil e que possua trilhas de auditoria, conforme DOC-ICP-05 do ITI. Precisará também ter comunicação direta e utilizar protocolos para que se conecte de forma segura com os sistemas que foram determinados formalmente com o MP, Comandos Militares, TSE e PSBios.

Primeiramente para poder operar, o módulo da AR do MP precisa-se passar por auditoria pré-operacional, além de possuir listas atualizadas com os nomes e CPF ou outra forma que possa indexar os servidores públicos federais ou os militares autorizadores, com a comprovação auditável da resposta dos sistemas Biométricos do TSE ou dos PSBios da ICP-Brasil. Os servidores autorizadores serão formalmente designados por meio dos órgãos competentes, por instrumento normativo do MP ou dos Comandos Militares (ITI, 2017).

2.4 - CERTIFICADO DIGITAL EM NUVEM - IN 10/2017/ITI

A Comissão Técnica Executiva - COTEC e o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira CG ICP-Brasil finalizou no mês de outubro de 2017 pesquisas para que se viabilizassem, de forma segura, uma solução para a utilização do certificado digital ICP-Brasil que fiquem armazenados em nuvem, sendo esse um ambiente onde é possível acessar arquivos, aplicativos, serviços e informações sob demanda, onde basta apenas ter um dispositivo conectado à essa plataforma (PEDROSA; NOGUEIRA, 2011), e não mais em dispositivos criptográficos de forma física sob a guarda dos usuários. Esse projeto teve por finalidade disponibilizar aos titulares dos certificados digitais uma nova modalidade de utilização, promovendo

formas de regulamentar as transações eletrônicas, documentos e portais de assinaturas digitais para dados (ITI, 2017).

Em 15 de dezembro de 2017 o ITI editou a IN nº 10, onde suplementa procedimentos operacionais aos Prestadores de Serviços de Confiança no âmbito da ICP-Brasil. O PSC é a parte integrante da ICP-Brasil que tem a responsabilidade de armazenar as chaves privadas dos usuários dos certificados digitais que ficam na nuvem. A IN nº 10 apresenta as obrigações, limitações e formas de operação por parte dos PSC's. Salienta também que os PSC's deverão apresentar, ao solicitarem credenciamento à ICP-Brasil, as Políticas de Segurança da Informação e suas diretrizes, normas e procedimentos, descrevendo os procedimentos que devem ser seguidos dentro das suas dependências e atividades.

Dentre os níveis de segurança às quais os PSC's precisam seguir para a operacionalização estão:

a) Segurança pessoal: estabelece a forma de admissão, demissão, critérios para garantir juridicamente o sigilo das informações, além de identificar a capacidade técnica dos colaboradores;
b) Segurança física: estabelece a forma e os níveis de acesso dos colaboradores, prestadores de serviço de manutenção, e equipamentos externos que necessitem dar entrada no ambiente, além da estrutura necessária que garanta a segurança de todo o sistema;
c) Segurança lógica: formas de acesso aos usuários autorizados, com trocas periódicas de senhas, o acesso aos usuários nos sistemas e a vedação a acessos remotos;
d) Segurança de rede: proteção contra danos ou perdas, exposição indevida e acessos externos. Deverão ser feitos testes mensais com com aplicativos especializados. Deverão ser documentados e ter as suas vulnerabilidades corrigidas.

As exigências de segurança garantem que os certificados digitais na nuvem possam conceder originalidade, autenticidade e segurança aos documentos produzidos e transmitidos em ambiente virtual, dando mais agilidade e promovendo mobilidade aos usuários, sendo de grande importância para a presente pesquisa.

3. METODOLOGIA

Os fundamentos metodológicos utilizados na pesquisa passaram por meio de uma revisão da literatura referente ao tema. Este estudo enquadra-se, segundo sua finalidade como pesquisa aplicada. Gil (2008) afirma que a pesquisa aplicada é voltada à aquisição de conhecimentos com o objetivo de aplicá-las numa situação específica, neste caso a utilização do certificado digital em nuvem como nova ferramenta para a gestão universitária. Segundo Ganga (2012), este tipo de pesquisa busca criar conhecimentos para a aplicação prática voltados à solução de problemas específicos.

Por se tratar de uma pesquisa descritiva que tem como finalidade conhecer e interpretar a realidade, Gil (2008) explica que para o pesquisador nesse tipo de estudo o interesse é em descobrir e observar os fenômenos, procurando descrever, classificar e interpretar.

Após a classificação do estudo, pode-se dizer que a proposta de desenvolvimento da pesquisa foi centrada de início com a pesquisa bibliográfica, tendo

como abordagem a Gestão Universitária, o certificado digital e a estrutura da ICP-Brasil e as IN nº 06 e nº10 de 2017 do Instituto Nacional de Tecnologia da Informação, discutindo sobre a importância da validação via SIGEPE e a emissão de certificados digitais na nuvem como estratégia para dar apoio aos gestores na administração universitária, apontando suas características, vantagens e cuidados.

Este levantamento bibliográfico permitiu que fosse realizada uma análise qualitativa buscando maior entendimento sobre certificado digital na nuvem e as vantagens que essa ferramenta pode promover como apoio à Gestão Universitária.

4. RESULTADOS E DISCUSSÕES

Observa-se que se tem buscado utilizar novas ferramentas na gestão universitária, com o objetivo de aplicá-las para aprimorar cada vez mais os resultados esperados pela comunidade universitária, composta por docentes, discentes, técnicos administrativos em educação e a sociedade onde está inserida. Dentre as ferramentas em questão, encontra-se a certificação digital.

O certificado digital, além de assinar documentos, dá acesso aos ambientes que precisem comprovar que a pessoa que virtualmente está acessando determinada aplicação é realmente quem diz ser. Além de acesso à ambientes também pode ser feita a assinatura de documentos. Documentos que nasceram digitalmente não precisam ser materializados para a coleta física de assinatura. Como verificado, a criptografia assimétrica garante a segurança ao certificado digital que é utilizado para assinar o documento digital. No entanto os certificados digitais ainda tem um custo elevado. Com a IN nº 06 de 2017 do ITI, a etapa de validação em uma AR comercial não se faz mais necessária, pois cria-se uma AR na instituição pública, podendo um servidor público credenciado, de uso das informações contidas no SIGEPE, emitir o certificado digital para o corpo funcional da instituição, diminuindo o valor final do certificado e aproximando o acesso ao serviço para os interessados na instituição.

Com a IN nº 10 de 2017 do ITI, elimina-se o dispositivo criptográfico que fica em posse dos titulares dos certificados digitais pois a chave privada fica armazenada com os PSC's na nuvem. Dessa forma o valor poderá cair ainda mais, podendo popularizar a utilização do certificado digital nas universidades. Dessa forma a utilização do certificado digital poderá se difundir e o seu uso, vantagens e cuidados ficarão mais evidentes.

Com o certificado digital ICP-Brasil armazenado dentro do hardware criptográfico (token), estando este em posse do seu proprietário e não sendo permitido sua utilização por outras pessoas, visto que o Certificado Digital ICP-Brasil garante o não repúdio, o token ganha um papel fundamental e de alta relevância para acesso a sites de serviço do governo, assinaturas digitais, entre outras funcionalidades. A facilidade que o gestor tem em poder assinar um documento ou movimentar um processo mesmo estando em viagem, proporciona maior agilidade e eficiência ao utilizar seu certificado digital em token para se identificar de forma digital nestes. No entanto, se algo acontecer com este token, como um defeito, perda ou inutilização, além de se identificar um prejuízo à Universidade, poderá comprometer sua utilização pelo gestor em assunto de alta relevância. Essa prática pode colocar em risco a utilização do certificado digital do titular pois, segundo o ITI, o certificado digital atesta a identidade digital de um indivíduo ou empresa, garantindo a integridade, autoria e o não repúdio de documentos e transações eletrônicas (ITI, 2018), ou seja, o mal uso por parte de

terceiros é de inteira responsabilidade do titular e este não pode dizer que não foi ele quem assinou o documento, acarretando em consequências para ele e para a instituição.

Com a ferramenta do certificado digital na nuvem, conforme estabelece a IN nº 10 de 2017 do ITI, o gestor espera que dificuldades em assinar um documento por não estar em posse do seu token sejam dizimadas. Pois com o certificado em nuvem o titular precisa apenas ter acesso ao seu aparelho celular, desde que este seja compatível com o aplicativo que gerencia os dispositivos autorizados, os certificados digitais e a interface com a camada de serviço, que funciona em níveis de segurança superior ao do hardware criptográfico em nuvem no Prestador de Serviço de Confiança. Observa-se que quando solicitado, um aplicativo previamente instalado no seu dispositivo móvel irá avisar que uma assinatura está sendo solicitada. O certificado digital na nuvem auxilia o gestor das universidades a manter a integridade, autenticidade e originalidade dos documentos por ele assinados, conferindo maior agilidade nos processos que têm prazos curtos para atendimento. É uma ferramenta sofisticada, com amparo legal e dispositivos de segurança bem estabelecidos pelo Instituto Nacional de Tecnologia da Informação, que garantem a sua confiabilidade pelos PSC. A emissão de certificados digitais em nuvem gera agilidade, flexibilidade, mobilidade e economicidade ao serviço público nas universidades, visto que seu custo é inferior ao seu equivalente em token ou cartão.

5. CONSIDERAÇÕES FINAIS

As vantagens e facilidades do certificado digital em nuvem, assim como a validação dos certificado digitais pelo SIGEPE e sua posterior emissão, além da gestão universitária a qual trata este artigo, também podem ser aplicados nos entes da administração pública direta, indireta, autárquica e fundacional. A difusão dessa ferramenta assim como o amplo conhecimento pelos servidores públicos trará grandes benefícios para a sociedade como um todo, pois garantirá a integridade, originalidade e segurança das informações, assim como os benefícios para a sustentabilidade pois contribuirá significativamente com a redução do uso de papéis.

REFERÊNCIAS

BIAZZI, Mônica R. de. **Instituições públicas de ensino superior:** estudos de casos de aperfeiçoamento de processos administrativos. p117. Dissertação (mestrado em engenharia) - Faculdade Poli'tecnica, Universidade de São Paulo, São Paulo, 2007.

BRASIL**. Constituição** (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. 292 p.

_____. Medida provisória n.° 2.200-2, de 24 de agosto de 2001. **Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICPBrasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.** Diário Oficial da União, Brasília, DF, 28 agosto. 2001.

CATANI, Afrânio Mendes; DOURADO, Luiz F.; OLIVEIRA, João F. Natureza jurídica, organização acadêmica e gestão universitária. In: SGUISSARDI, Valdemar; SILVA JR., João dos Reis (Orgs.). **Educação superior: análise e perspectivas de pesquisa.** São Paulo: Xamã, 2001.

CERTISIGN. Certisign Explica. **Conheça o agente de registro.** Disponível em: <http://www.certisignexplica.com.br/conheca-o-agente-de-registro/>. Acesso em: 17 julho 2018.

CHIAVENATO, Idalberto. **Teoria geral da administração:** abordagens prescritivas e normativas. 3. ed. São Paulo: Makron Books, 1987. São Paulo.

CRUZ, T. **Sistemas, Organizações & Métodos:** Estudo Integrado das novas tecnologias da informação e introdução à gerência do Conteúdo e do Conhecimento. Editora Ated. 2010.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo.** 22ª ed. 2ª reimp. São Paulo: Atlas, 2009.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação:** guia prático para elaboração e implementação. 2. ed. rev. e ampl. Rio de Janeiro: Ciência Moderna, 2008.

GANGA, Gilberto Miller Devós. **Trabalho de Conclusão de Curso (TCC) na engenharia de produção: um guia prático de conteúdo e forma.** São Paulo, Atlas, 2012.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2008.

HALL, R. H. **Organizações: estruturas e processos.** Rio de Janeiro: PrenticeHall do Brasil, 1984.

ITI – Instituto Nacional de Tecnologia da Informação. **Como obter.** Casa Civil da Presidência da República. Disponível em: <http://www.iti.gov.br/certificado-digital/como-obter>. Acesso em: 17 julho 2018.

___ – Instituto Nacional de Tecnologia da Informação. **Entes da ICP-Brasil.** Casa Civil da Presidência da República. 2017. Disponível em: <http://www.iti.gov.br/icp-brasil/entes-da-icp-brasil>. Acesso em: 17 julho 2018.

___ – Instituto Nacional de Tecnologia da Informação. **Requisitos mínimos para as declarações de práticas dos prestadores de serviço de confiança da ICP-Brasil.** Casa Civil da Presidência da República. Disponível em: <http://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/DOC_ICP_17_-_verso_1.0_REQUISITOS_MINIMOS_PARA_AS_DECLARACOES_DE_PRATICAS_DOS_PRESTADORES_DE_SERVICO_DE_CONFIANCA_DA_ICP-BRASIL.pdf>. Acesso em 17 julho 2018.

MEYER JR, V. A escola como organização complexa. In: EYING, A; GHISI, M.L. **Políticas e Gestão da Educação Superior.** Curitiba: Champagnat, 2007.

MORGAN, G. **Imagens da organização.** São Paulo: Atlas. 1996.

PEDROSA, Paulo H. C.; NOGUEIRA, Tiago. **Computação em nuvem.** Disponível em: <http://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf>. Acesso em 19 jul. 2018.

SCHEIN, E. H. **Cultura Organizacional e Lideranca.** Editora At ed. São Paulo, 2009.

SILVA, L. G. C. da *et al*. **Certificação digital:** conceitos e aplicações. Rio de Janeiro: Ciência Moderna, 2008.

VALID, Certificadora Digital. **Assinatura digital e assinatura digitalizada são a mesma coisa?** Disponível em: <http://blog.validcertificadora.com.br/?p=7995>. Acesso em: 19 julho 2018.

VICTORINO, C. R.; FORTUNATO, C. **Benefícios e Aplicações da Certificação Digital ICP Brasil.** Estúdio Grafen, Brasília, 2012.

WEBER, M. **Ensaios de sociologia.** 5. ed. Rio de Janeiro: LTC Editora, 1982.