**ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS**

**Cap QCO ROBSON OLIVEIRA DOS SANTOS**

# Características necessárias a um sistema assinador eletrônico para o Sistema de Fiscalização de Produtos Controlados

**Rio de Janeiro**
**2020**

ROBSON OLIVEIRA DOS SANTOS

# Características necessárias a um sistema assinador eletrônico para o Sistema de Fiscalização de Produtos Controlados

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau de Especialização em Ciências Militares.
Orientador: Maj Anderson Barros Torres

**Rio de Janeiro**
**2020**

ROBSON OLIVEIRA DOS SANTOS

**Características necessárias a um sistema assinador eletrônico para o Sistema de Fiscalização de Produtos Controlados**

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau de Especialização em Ciências Militares.
Orientador: Maj Anderson Barros Torres

Aprovado em: _____/_____/ 2020

COMISSÃO DE AVALIAÇÃO

_____

Presidente

_____

1º Membro

_____

2º Membro

# CARACTERÍSTICAS NECESSÁRIAS A UM ASSINADOR ELETRÔNICO PARA O SISTEMA DE FISCALIZAÇÃO DE PRODUTOS CONTROLADOS

Robson Oliveira dos Santos[1]

## RESUMO

A assinatura digital é uma forma de aumentar a eficiência na administração de uma forma geral, oferecendo um meio para a emissão de documentos eletrônicos com reconhecimento jurídico. A Administração Pública vem promovendo iniciativas para implementar a assinatura digital desde o início dos anos 2000, tendo se intensificado nos últimos anos com as estratégias de governo digital. Dentre as áreas de atuação do Exército Brasileiro, a Fiscalização de Produtos Controlados se apresenta com grande interação com a sociedade na emissão de documentos, tendo recebido orientações do Tribunal de Contas da União para implementar processos eletrônicos que dependem de um mecanismo para assinatura digital de documentos. Desse modo, o presente trabalho utilizou a ciência aplicada com método quantitativo em uma pesquisa exploratória para identificar os requisitos legais, técnicos e de negócio aplicáveis ao Sistema de Fiscalização de Produtos Controlados, paralelamente a partir de busca por ferramentas com potencial de atendimento selecionou-se os assinadores eletrônicos para avaliação do nível de aderência dessas ferramentas aos requisitos previamente relacionados. Com isso, chegou-se a um modelo para análise e ranqueamento que permitiu identificar de forma objetiva a opção que melhor atende ao Sistema, podendo ser usado como metodologia para avaliação de outras ferramentas para uso na Administração Pública Militar.

**Palavras chave:** assinatura digital, documento eletrônico, reconhecimento jurídico, Administração Pública, governo digital, assinador eletrônico, Exército Brasileiro, Fiscalização de Produtos Controlados

## ABSTRACT

The digital signature is a way to increase efficiency in administration in general, offering a means for the issuance of electronic documents with legal recognition. The Public Administration has been promoting initiatives to implement digital signature since the early 2000s, having intensified in recent years with digital government strategies. Among the areas of activity of the Brazilian Army, the Inspection of Controlled Products presents itself with great interaction with society in issuing documents, having received guidance from the Federal Court of Accounts to implement electronic processes that depend on a mechanism for digital signature of documents. Thus, the present work used applied science with a quantitative method in an exploratory research to identify the legal, technical and business requirements applicable to the Controlled Products Inspection System, at the same time, from the search for tools with potential for service, electronic signatures were selected to assess the level of adherence of these tools to previously listed requirements. With this, a model for analysis and ranking was reached that allowed to identify objectively the option that best suits the System, and can be used as a methodology for evaluating other tools for use in the Military Public Administration.

---

1 Capitão QCO Informática da turma de 2012. Tecnólogo em Análise e Desenvolvimento de Sistemas pelo IFRR em 2011. Especialista em Aplicações Complementares às Ciências Militares pela EsFCEx em 2012.

**Keywords:** digital signature, electronic document, legal recognition, Public administration, digital government, electronic signature, Brasilian Army, Inspection of Controlled Products

# SUMÁRIO

**1 INTRODUÇÃO..... 6**

**2 METODOLOGIA..... 9**

**3 REFERENCIAL TEÓRICO..... 10**

3.1 LEGISLAÇÃO PERTINENTE..... 10
3.2 INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL)..... 12
3.3 SEGURANÇA..... 14
3.4 CRIPTOGRAFIA..... 15
3.5 ASSINADOR ELETRÔNICO DE DOCUMENTOS..... 17
3.6 TECNOLOGIAS PARA INTEGRAÇÃO DE SISTEMAS..... 19

**4 RESULTADOS..... 22**

4.1 REQUISITOS NECESSÁRIOS AO SISTEMA ASSINADOR ELETRÔNICO DE DOCUMENTOS PARA ATENDER O SISGCORP..... 22
*4.1.1 Quanto ao formato da assinatura digital..... 22*
*4.1.2 Quanto à Política de assinatura digital..... 22*
*4.1.3 Quanto à geração da assinatura digital..... 23*
*4.1.4 Quanto aos algoritmos utilizados..... 23*
*4.1.5 Quanto à validação da assinatura digital..... 23*
*4.1.6 Quanto à interoperabilidade..... 24*
4.2 LEVANTAMENTO DOS SISTEMAS ASSINADORES ELETRÔNICOS DE DOCUMENTOS COM MECANISMOS DE VERIFICAÇÃO DE AUTENTICIDADE..... 26
*4.2.1 Assinador SERPRO..... 26*
*4.2.2 Assinador do Projeto SIGA-Doc..... 26*
*4.2.3 Assinador do SEI..... 26*
*4.2.4 Assinador Digital PDF..... 27*
4.3 LEVANTAMENTO DAS CARACTERÍSTICAS DOS SISTEMAS CATALOGADOS..... 27
4.4 ANÁLISE DO NÍVEL DE ADERÊNCIA DAS CARACTERÍSTICAS DOS MECANISMOS ASSINADORES COMPARADAS AOS REQUISITOS E RESTRIÇÕES DO SISGCORP..... 28

**5 DISCUSSÃO..... 29**

**6 CONCLUSÃO..... 30**

**REFERÊNCIAS..... 32**

# 1 INTRODUÇÃO

Uma das formas de validar um documento, seja público ou privado, se dá por meio da aposição de uma assinatura de autoridade competente que é a “pessoa legalmente investida de poder e a quem cabe e compete o dever ou o direito de executar determinada ação” (MICHAELIS, c2020), como nos casos da assinatura de contratos para aquisição de bens ou a emissão de certidões por órgãos públicos. Com a edição da Medida Provisória 2200 em 2001 estabeleceu-se os critérios para validade jurídica de documentos digitais, permitindo a emissão de documentos por meio eletrônico em substituição à tradicional impressão e assinatura, fazendo uma transformação na forma de emitir um documento.

A partir da MP 2200/2001 houve um aperfeiçoamento dos atos normativos que versaram sobre os variados temas direcionados à transformação digital da administração pública. A linha do tempo apresentada na figura 1 a seguir, demonstra o esforço dos diversos governantes em transformar os serviços públicos em serviços digitais.

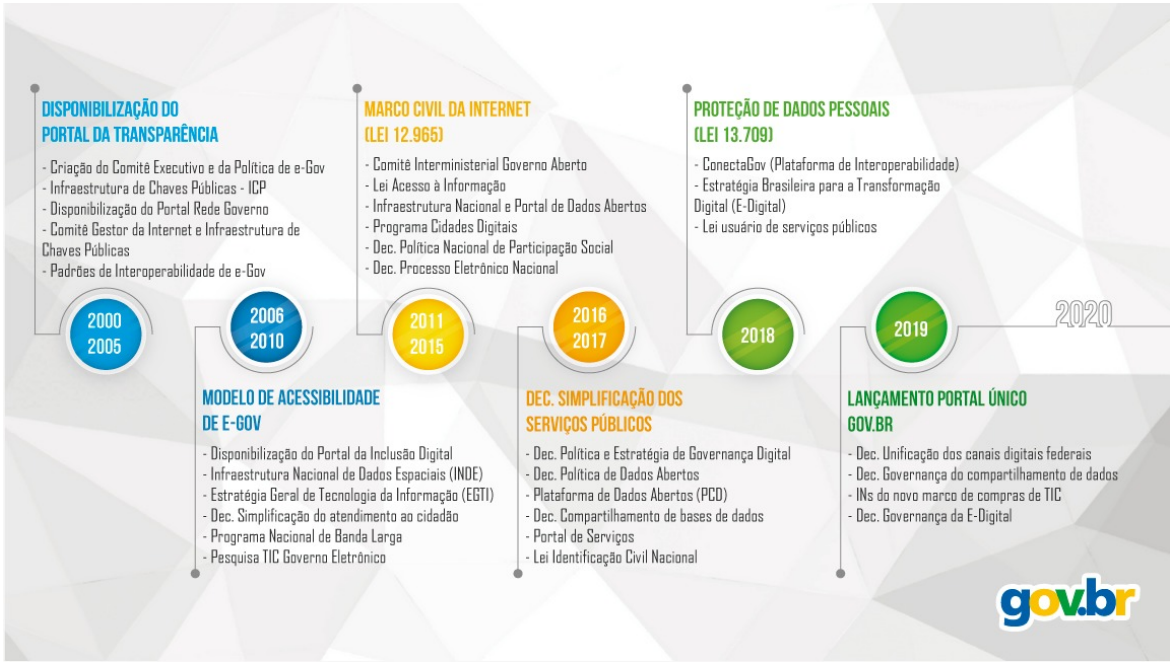


Figura 1 – Linha do Tempo Governo Eletrônico (BRASIL, 2019)

O que se pode observar é uma evolução dos temas afetos à tecnologia da informação nessa linha do tempo, de 2000 a 2005 tem-se a Criação da ICP-Brasil e o estabelecimento do padrão de interoperabilidade de e-Gov (Governo Eletrônico), de

2006 a 2010 a Estratégia Geral de Tecnologia da Informação e o Programa Nacional de Banda Larga, de 2011 a 2015 a Lei de Acesso a Informação e o estabelecimento do Processo Eletrônico Nacional e de 2016 a 2019 a Política e Estratégia de Governança Digital, o Lançamento do Portal de Serviços, a Criação da Plataforma de Interoperabilidade e o Lançamento do Portal Único Gov.br.

Conforme visto ainda na Figura 1, em 2015 o Governo Federal editou o Decreto 8539 para estabelecer o Processo Eletrônico Nacional (PEN). Esse decreto veio disciplinar o uso de sistemas para a gestão de processos por meio eletrônico, tendo como base a implantação do Sistema Eletrônico de Informações (SEI) pelo então Ministério do Planejamento, Desenvolvimento e Gestão (MPDG) a partir de 2013. Sistema este que permitiu a gestão eletrônica de documentos e processos ao MPDG e aos demais órgãos do governo que passaram a utilizá-lo, conforme estudo de caso apresentado por Saraiva (2018).

Paralelamente a esses acontecimentos, o Exército Brasileiro empreendeu diversas iniciativas para modernizar seus processos. Nesse sentido, foram implementados sistemas para automatizar o controle em substituição a burocracia tradicional baseada no papel, como o Sistema de Materiais do Exército (SIMATEX) / Sistema de Controle Físico (SISCOFIS) a partir do ano 2000, o Sistema de Boletim (SISBOL) a partir do ano 2004, o Sistema de Protocolo Eletrônico de Documentos (SPED) a partir do ano 2012 e o Sistema de Gestão Corporativo (SisGCorp) para atender o Sistema de Fiscalização de Produtos Controlados (SisFPC) a partir de 2019.

Em que pesem as ações do Exército Brasileiro no sentido de iniciar a automação de processos, em auditoria operacional do TCU sofrida pela Diretoria de Fiscalização de Produtos Controlados (DFPC) em 2016 foi emitido o acórdão 604/2017, recomendando a implantação de processos eletrônicos em benefício do SisFPC (Tribunal de Contas da União, 2017). Mais que isso, aquele Tribunal sugeriu a possibilidade de uso do SEI como ferramenta de automação dos processos. Após avaliação, o Exército Brasileiro entendeu não ser pertinente o uso do SEI no âmbito do SisFPC (Tribunal de Contas da União, 2018). Alternativamente, a DFPC iniciou, em dezembro de 2017, o desenvolvimento do SisGCorp para automação dos processos do SisFPC (Diretoria de Fiscalização de Produtos Controlados[1], 2020).

Apesar do desenvolvimento e do aprimoramento do SisFPC, a DFPC ainda

não possui, em seus sistemas, um mecanismo para verificação de validade e autenticidade de seus documentos emitidos. Desta forma, este trabalho identificou as características necessárias a um sistema assinador eletrônico de documentos, com mecanismo de verificação de validade e autenticidade de documentos, que fosse integrável ao SisGCorp, utilizado pelo SisFPC, considerando as limitações legais e restrições tecnológicas.

Para se chegar a tais características foi necessário inicialmente descrever as características de um sistema assinador eletrônico de documentos, em seguida apresentar as formas de funcionamento de mecanismos públicos de verificação de validade e autenticidade de documentos utilizados pela administração pública. Posteriormente, foram identificados os requisitos de um sistema assinador que atendesse funcionalmente as necessidades do SisGCorp, bem como sua integração, tendo sido em seguida analisado o nível de aderência das características dos mecanismos assinadores comparadas aos requisitos e restrições do SisGCorp, para ao fim, apresentar uma seleção ranqueada dos assinadores eletrônicos disponíveis a parir do nível de aderência às limitações regulamentares e restrições técnicas para integração ao SisGCorp.

O estudo de um assinador eletrônico que se integre ao SisGCorp beneficia diretamente a DFPC e por conseguinte o SisFPC, com uma proposta de solução para os mais de 450.000 documentos emitidos por ano, conforme apresentado por Diretoria de Fiscalização de Produtos Controlados (2020). Existe ainda a possibilidade de o estudo ser aproveitado para aperfeiçoamento de outros sistemas da DFPC e do Exército Brasileiro que eventualmente não possuam assinadores eletrônicos com as características que foram apresentadas por este estudo.

Espera-se que o conhecimento sobre o uso de assinadores eletrônicos e métodos de validação de documentos assinados eletronicamente trazidos no presente estudo contribua com um caminho inicial para iniciativas de implementação. Com os resultados da pesquisa, espera-se a possibilidade de avaliar a integração dessas ferramentas a sistemas existentes, bem como apresentar uma metodologia que possibilite identificar soluções que se integrem a outros sistemas, ressalvadas as limitações legais bem como as restrições tecnológicas impostas a cada um desses sistemas.

## 2 METODOLOGIA

Quanto à natureza foi pesquisa aplicada, pois, de acordo com Zanella (2009), a motivação é a solução de problema concreto, mas também, contribuindo com novos fatos para compreensão teórica.

Quanto ao método e à forma de abordar o problema, a pesquisa foi quantitativa, pois, como mostra Zanella (2009), é aquela que se caracteriza pelo emprego de instrumentos estatísticos, tanto na coleta como no tratamento dos dados, preocupando-se com representatividade numérica: com a medição objetiva e a quantificação dos resultados.

Quanto aos objetivos, foi pesquisa exploratória, pois tem, segundo Zanella (2009), a finalidade de ampliar o conhecimento a respeito de um determinado fenômeno. Esse tipo de pesquisa, aparentemente simples, explora a realidade buscando maior conhecimento, para depois planejar uma pesquisa descritiva. Segundo a mesma autora, a pesquisa exploratória é bastante flexível, já que o pesquisador não possui clareza do problema nem da hipótese a serem investigados.

Com a finalidade de alcançar o objetivo geral proposto, em um primeiro passo foram levantados os sistemas assinadores eletrônicos de documentos existentes nos órgãos públicos por meio de busca no Portal de Serviços do Governo Federal. Em seguida foram levantados os disponíveis no mercado, que atendam pessoas jurídicas de direito privado. Essa etapa foi necessária para que se conheçam as ferramentas existentes bem como seu funcionamento.

Após o levantamento inicial, esses sistemas foram catalogados e analisados com o intuito de relacionar suas características, possibilidades e limitações. Nessa etapa foram tabuladas as características de cada sistema, com a finalidade de formar o catálogo dos selecionados.

Por se tratar de um órgão da administração pública e de uma organização militar do Exército Brasileiro, nesta etapa foram investigadas as normas e legislações pertinentes ao tema. Inicialmente para o governo federal como um todo e em seguida restringindo para o Exército Brasileiro. Essa ação se deve à necessidade de adequação legal dos sistemas de informação utilizados pela administração pública, bem como ao Exército Brasileiro.

Na etapa seguinte foram investigados os requisitos necessários ao sistema

assinador eletrônico de documentos para atender o SisGCorp. Esses requisitos têm como balizamento as limitações legais e tecnológicas impostas pela administração pública federal ou pelo Exército Brasileiro. Essa etapa foi importante para se ter os parâmetros necessários ao atendimento do SisGCorp.

Nessa etapa foram avaliadas as limitações impostas pelas legislações vigentes aplicáveis ao Exército Brasileiro, bem como as restrições técnicas para uma eventual integração ao SisGCorp. De posse dos levantamentos das etapas anteriores, as informações foram pontuadas e comparadas com os requisitos do SisGCorp para que se verificasse o grau de aderência.

A partir dos dados da etapa anterior, foi possível ranquear as opções disponíveis a partir do nível de aderência às limitações regulamentares e restrições técnicas para integração ao SisgCorp.

# 3 REFERENCIAL TEÓRICO

A revisão de literatura a seguir foi elaborada para reunir e expor alguns conceitos que foram explorados no presente trabalho.

## 3.1 LEGISLAÇÃO PERTINENTE

A Constituição da República Federativa do Brasil de 1988 estabeleceu a responsabilidade da administração pública na gestão documental, explicitado no “Art. 216, § 2º: Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.”(BRASIL, 1988, Art .216). Nesse sentido, com o objetivo de disciplinar a gestão da documentação governamental, foi editada a Lei 8.159/91que traz em seu art. 26 a criação do Conselho Nacional de Arquivos - CONARQ e também a instituição do Sistema Nacional de Arquivos – SINAR, conforme Brasil (2020)

De acordo com esses dispositivos legais e conforme consta em Brasil (2020), o SINAR, cuja competência, organização e funcionamento estão regulamentados pelo Decreto nº 4.073, de 3 de janeiro de 2002, tem por finalidade implementar a política nacional de arquivos públicos e privados, visando à gestão, à preservação, e ao acesso aos documentos de arquivo. Nessa estrutura, o CONARQ é o órgão central, tendo por finalidade definir a política nacional de arquivos públicos e

privados, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo. (BRASIL, 2014)

A partir da edição da MP 2200/2001, o CONARQ passou a ser o responsável por definir também a política de documentos digitais. Essa MP é o marco legal que institui o reconhecimento jurídico de documentos digitais no Brasil, bem como a possibilidade de utilização de outros meios de comprovação de autoria e integridade de documentos em forma eletrônica, conforme contido em seu artigo 10 a seguir:

> Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.
>
> § 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.
>
> § 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. (BRASIL, 2001)

Para tanto, a MP 2200 instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), que tem por finalidade “(...) 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” (BRASIL, 2001, Art. 1º). A referida norma define também a estrutura, organização e funcionamento da ICP-Brasil, conforme será apresentado a seguir.

Quanto a interoperabilidade dos sistemas, conforme apresentado por ePING (2020), o Governo Federal elaborou a arquitetura ePING – Padrões de Interoperabilidade de Governo Eletrônico, que define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de governo eletrônico com os demais Poderes e esferas de governo e com a sociedade em geral. O Padrão e-PING estabelece que o uso de criptografia e certificação digital, para a proteção do tráfego, armazenamento de dados, controle de acesso, assinatura digital e assinatura de código deve estar em conformidade com as regras da ICP-Brasil.

No âmbito do Exército Brasileiro, as Instruções Gerais para a Correspondência do Exército (EB-IG-01.001), Portaria 769, de 7 de dezembro de

2011, delegaram ao Departamento de Ciência e Tecnologia (DCT) a realização de estudos para implantação da certificação digital no Exército Brasileiro.

## 3.2 INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL)

Com o objetivo de estabelecer a ICP-Brasil foi delegado ao Instituto Nacional de Tecnologia da Informação (ITI), que é uma autarquia federal vinculada a Casa Civil da Presidência da República, a missão de manter e executar as políticas da Infraestrutura da ICP-Brasil, como entidade superior. Ao ITI compete ainda ser responsável por assegurar a credibilidade das entidades encarregadas de realizar a gestão dos certificados digitais.

A ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão ITI (2017). A figura 3 apresenta a representação dessa hierarquia. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única.

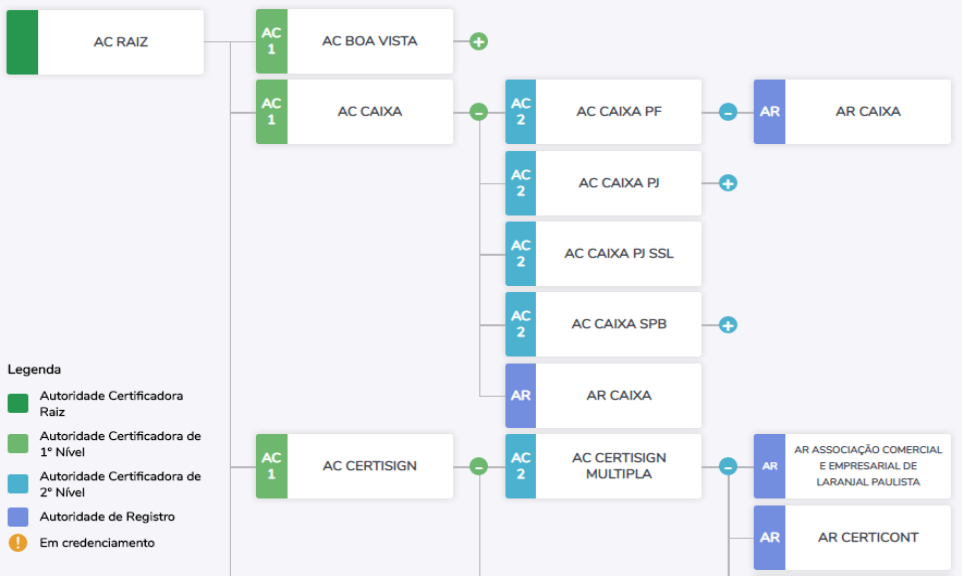


Figura 3 – Estrutura ICP-Brasil (ITI, 2020)

A Autoridade Raiz (AC Raiz) é a primeira autoridade da cadeia de certificação, ou seja, é a responsável por atestar a confiança dos demais integrantes da estrutura e emitir a lista de certificados revogados, sendo estabelecido o ITI como AC Raiz da ICP-Brasil. O ITI cumpre sua missão com base nas normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, conforme consta em Brasil (2001). O Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (CG ICP-Brasil) exerce a função de autoridade gestora de políticas de certificação digital (BRASIL, 2008).

De acordo com ITI (2017), as Autoridades Certificadoras (AC) são entidades públicas ou pessoas jurídicas de direito privado credenciadas à AC-Raiz e que emitem certificados digitais. Essa atribuição decorre da MP 2200-2/2001, que dispõe como competências da AC "emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações". (BRASIL, 2001)

O Exército Brasileiro está inserido no escopo da AC-DEFESA, conforme consta em AC Defesa (2020):

> A Autoridade Certificadora do Ministério da Defesa (AC Defesa) tem como missão emitir e fornecer certificados digitais para o Ministério da Defesa (MD), bem como para as três Forças: Marinha do Brasil (MB), Exército Brasileiro (EB) e Força Aérea Brasileira (FAB).
> A AC Defesa é composta de uma Autoridade Certificadora Principal em Brasília, uma Autoridade Certificadora Reserva no Rio de Janeiro, uma Autoridade de Registro (AR) em Brasília e diversos postos de validação distribuídos em guarnições militares em todo o território nacional. (AC DEFESA, 2020)

As Autoridades de Registros (AR), conforme ITI (2017) também podem ser entidades públicas ou pessoas jurídicas de direito privado credenciadas pela AC-Raiz, sendo sempre vinculadas operacionalmente a alguma AC. De acordo com Brasil (2001), compete à AR "identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações", ou seja, registrar as pessoas para emissão dos certificados digitais.

Conforme consta em ITI (2017), o Comitê Gestor da ICP-Brasil, que possui a função de coordenar a implantação e o funcionamento da infraestrutura (art. 4º, inc. I, da M.P. 2.200-2/01), em reunião realizada no dia 10 de fevereiro de 2009, definiu que o certificado digital é tratado como um produto, e não serviço. Explica ainda que esse produto deve ser compreendido como um *software* personalíssimo por não se tratar de um produto igual para todos os adquirentes. No procedimento de sua emissão são verificadas as características pessoais de cada adquirente, configurando na prática uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos.

Esse certificado digital é gerado e assinado por uma terceira parte confiável, a Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de

chaves criptográficas, sendo a segurança da informação condição indispensável a esse certificado digital.

Para geração de assinatura digital utilizando um certificado digital ICP-Brasil, o ITI (2020), elaborou um conjunto de normativos para regulamentar a geração e verificação de assinaturas digitais no âmbito da ICP-Brasil. Esses documentos estão organizados e nomeados como DOC-ICP, estando no DOC-ICP-15 os principais conceitos e a lista dos demais documentos que compõem as normas da ICPBrasil sobre a assinatura digital. No DOC-ICP-15.01 constam os requisitos obrigatórios a serem observados na criação e verificação de assinaturas digitais na ICP-Brasil e no DOC-ICP-15.03 constam os requisitos das políticas de assinatura digital na ICP-BRASIL.

## 3.3 SEGURANÇA

Alguns princípios relacionados à segurança da informação acompanham os diversos meios por onde tramitam. Seja *hardware* ou *software* há de se atentar às variáveis que podem influenciar na segurança. Conforme MIT (2020), “Muitas consultorias e fabricantes da área de segurança concordam com o modelo de segurança padrão conhecido como CIA, ou *Confidentiality, Integrity, and Availability* (Confidencialidade, Integridade e Disponibilidade)”. Esse modelo de três pilares estabelece as características esperadas para se obter efetivamente uma segurança da informação.

> - Confidencialidade — Informações delicadas devem estar disponíveis apenas para um conjunto pré-definido de indivíduos. A transmissão ou o uso não autorizado de informações devem ser restritos.
> - Integridade — As informações não devem ser alteradas de modo a torná-las incompletas ou incorretas.
> - Disponibilidade — As informações devem estar acessíveis a usuários autorizados sempre que precisarem. A disponibilidade é a garantia de que aquela informação pode ser obtida com uma frequência e periodicidade pré-definidas. Isto é frequentemente medido em termos de porcentagens e definido formalmente nos Acordos de Nível de Serviço (Service Level Agreements - SLAs) usados por provedores de serviços de rede e seus clientes corporativos. (MIT, 2020)

No escopo deste trabalho serão consideradas além das características do modelo padrão CIA, características necessárias à segurança em sistemas de informação. Nesse sentido, ressaltam-se a legalidade e autenticidade, conforme descreve Sêmola (2003):

> - legalidade - garantia de que a informação foi produzida em conformidade com a lei;
> - autenticidade - garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.
> (SÊMOLA, 2003)

Por fim, considerar-se-á a característica de não repúdio. Conforme define Côrte (2014) não repúdio é a propriedade que garante a impossibilidade de negar a autoria em relação a uma transação feita anteriormente. Essa característica somada às apresentadas acima, trazem a segurança para as transações.

Para se obter essas características de segurança, utiliza-se métodos para proteger, ocultar ou simplesmente marcar a informação, de forma a ter confiança no conteúdo da mensagem. Quando se busca a segurança da informação necessariamente usam-se métodos de criptografia.

## 3.4 CRIPTOGRAFIA

De acordo com Weber (1995), criptografia caracteriza-se como a ciência (ou arte) de escrever em códigos ou em cifras, tornando incompreensível uma informação, de forma a permitir que apenas as pessoas autorizadas consigam decifrá-la e compreendê-la. O processo de codificar mensagens vem sofrendo evoluções há milênios, sendo os métodos modernos aqueles que utilizam chaves que decifram a mensagem original (SINGH, 2013).

Marcacini (2010) sustenta que existem dois métodos de criptografia: criptografia simétrica e assimétrica. Criptografia simétrica, também conhecida como criptografia de chave secreta, diz respeito ao remetente e o destinatário, sendo que a mesma chave é usada para criptografar e decodificar uma mensagem. A criptografia assimétrica, ou criptografia de chave pública usa o que é chamado de um ‘par de chaves’ – uma chave pública para criptografar a mensagem e uma chave privada para decodificá-la.

A criptografia simétrica compara-se a chave como um segredo conhecido pelas partes que farão uso do sistema de codificação e decodificação. Ao codificar a mensagem usando um método de criptografia simétrica, o segredo que o emissor usar para codificar será o mesmo que o receptor usará para decodificar, ou seja, ambos têm que conhecer o segredo para decifrar ou ter certeza do conteúdo.

Na criptografia assimétrica tem-se duas chaves para se obter a codificação e decodificação. Nesse método estabelece-se uma chave pública, de conhecimento comum, e uma privada, reservada ao emissor. Dependendo da necessidade do emissor ele pode obter confidencialidade ou autenticidade. Na descrição dada por Marcacini (2010) tem-se a confidencialidade, pois uma vez codificada com a chave pública somente a chave privada pode decodificar, sendo de conhecimento reservado ao emissor. Se ocorre o contrário, codificação com a chave privada, tem-se a autenticidade, pois com o uso da chave pública será possível decodificar confirmando assim a autenticidade.

Os métodos de criptografia são implementados por algoritmos, o mais antigo que se tem notícia é o algoritmo de César, que consistia em substituir cada letra da mensagem pela 3ª na sequência do alfabeto. Desde então os algoritmos vêm sendo aperfeiçoados, conforme apresenta Kryptosgraphein (2020), os principais algoritmos que usam chave simétrica são: DES, Triple-DES, AES, RC2, RC4, IDEA e Skipjack. Por sua vez, os algoritmos Diffie-Hellman, RSA, Merkle-Hellman e SSL utilizam chaves assimétricas.

A técnica de *hash* não utiliza uma chave, como nas anteriores, mas um valor matemático de tamanho fixo calculado sobre o texto plano, conforme apresentado por Stallings (2015). Esse *hash* é utilizado para verificar a integridade dos dados, sendo utilizadas ambas as técnicas nos Certificados Digitais da ICP-Brasil.

Oliveira (2012) apresenta que o algoritmo Secure Hash Algorithm (SHA-1), é uma função de espalhamento unidirecional desenvolvida pela National Security Agency (NSA), Agência de Segurança Nacional dos Estados Unidos responsável, entre outras atribuições, pela segurança da informação. O SHA-1 gera um valor *hash* de 160 bits, a partir de um tamanho qualquer de mensagem.

Júnior e Fernandes (2018) apresentam que o SHA-256 é um algoritmo de *hash* pertencente à família SHA-2, a qual compreende mais três algoritmos, o SHA-224, o SHA-384 e o SHA-512, que tem como principal diferença entre eles a quantidade de iterações dentro do *loop* principal e o comprimento em bits do código *hash*, sendo a parte decimal do nome referente a esse quantitativo.

> O algoritmo RSA foi desenvolvido no Massachussets Institute of Technology (MIT) em 1978 por Rom Rivest, Adi Shamir e Leonard Adleman, e batizado com as niciais de seus nomes. Esse algoritmo é matematicamente baseado

> na Teoria dos Números, principalmente nas áreas de Aritmética Modular e Primalidade. (ANDRADE E SILVA, 2012)

De acordo com Moreira (2006), o algoritmo ECDSA - Elliptic Curve Digital Signature Algorithm, assinatura digital com curvas elípticas equivale ao DSA –Digital Signature Algorithm, algoritmo de assinaturas digitais, porém utilizando Criptografla de Curvas Elípticas (ECC-Elliptic-curve cryptography). O ECDSA foi proposto inicialmente por Scott Vanstone em 1992 para o NIST (National Institute of Standard and Technology), tendo sido aceito em 1998 pelo ISO (International Standards Organization) [ISO 14888-3], em 1999 pela ANSI (American National Standards Institute) [ANSI X69.2] e em 2000 pelo IEEE (Institue of Eletrical and Eletronic Engineers) [IEEE P1363].

Conforme apresentado pelo ITI (2020), o DOC-ICP-01.01 traz os padrões e algoritmos criptográficos da ICP-Brasil, estabelecendo para as assinaturas digitais os algoritmos SHA – 1, SHA – 256 e SHA – 512 nas funções resumo e o conjunto de algoritmos sha1WithRSAEncryption, sha256WithRSAEncryption, sha256WithECDSAEncryption, sha512WithRSAEncryption, sha512WithECDSAEncryption para as assinaturas propriamente ditas.

## 3.5 ASSINADOR ELETRÔNICO DE DOCUMENTOS

Conforme apresentado em Kryptosgraphein (2020), existem situações em que a criptografia é desnecessária, bastando apenas provar quem os escreveu e garantir a autenticidade do documento. Nessa situação, o que se requer são serviços de autenticação e integridade de dados, podendo ser realizados por dois mecanismos: Código de Autenticação de Mensagem (*Message Authentication Code* - MAC) e Assinaturas Digitais.

Os Códigos de Autenticação de Mensagem são mecanismos usados com sistemas de criptografia simétrica, conforme nos apresentam Trinta e Macêdo (1998). Quando esses códigos são executados em parte da informação, este modo de criptografia da informação gera um valor (pequeno pedaço de dados) que serve como código para o documento.

Se dois entes utilizam a chave simétrica compartilhada, é possível que um deles execute um sistema de criptografia com a chave simétrica em comum sobre os dados e obtenha o MAC da mensagem. Ao enviá-lo junto com a mensagem o

segundo ente, utilizando-se do mesmo sistema de criptografia com a chave simétrica em comum obterá um MAC para a mensagem recebida. Se a cifragem obtida sobre os dados recebidos for igual ao MAC enviado, significa que a mensagem está íntegra, ou seja, não sofreu adulteração.

Uma assinatura digital é um tipo específico de MAC que resulta de sistemas de criptografia assimétrica, onde existe uma chave privada de conhecimento apenas do emissor e uma chave pública que permite validar as ações da chave privada, conforme apresenta Trinta e Macêdo (1998), sendo usado também para proteger a informação. Para assinar uma mensagem, uma função *Message Digest* (MD) é usada para processar o documento, produzindo um *hash*. Uma MD é uma função matemática que refina toda a informação de um arquivo em um único pedaço de dados de tamanho fixo, conforme definem Trinta e Macêdo (1998).

De acordo com Kryptosgraphein (2020), o motivo para se usar funções MD está diretamente ligado ao tamanho do bloco de dados a ser criptografado para se obter a assinatura. O autor explica que o processo de criptografia de mensagens longas pode durar muito tempo, enquanto criptografar *hashs*, blocos de dados pequenos e de tamanho fixo, torna o processamento mais rápido.

Uma vez computada uma MD, criptografa-se o *hash* gerado com uma chave privada. O resultado de todo este procedimento é chamado de assinatura digital da informação. A assinatura digital é uma garantia que o documento é uma cópia verdadeira e correta do original. Uma vez gerada a assinatura digital de um documento, pode-se verificar sua integridade e autenticidade executando-se a mesma função MD sobre o documento recebido, obtendo-se um *hash* para aquele documento, e posteriormente, decifra-se a assinatura digital com a chave pública do remetente. O resultado deve ser o mesmo *hash* gerado pela função MD, caso contrário o documento não é confiável, conforme descreve Trinta e Macêdo (1998).

Essa técnica de uso de resumo de mensagens para gerar assinaturas eletrônicas é a utilizada pelos assinadores eletrônico de documentos. Vale ressaltar que o uso das melhores técnicas não é suficiente para assegurar o reconhecimento jurídico ou mesmo a confiança, uma vez que para que uma assinatura digital seja reconhecida juridicamente ela precisa ser gerada utilizando a cadeia de certificação

ICP-Brasil, ou seja, utilizando um Certificado Digital emitido por uma AC integrante da ICP-Brasil, conforme estabelecido na MP 2200/2001 em Brasil (2001).

Independente do algoritmo utilizado e como a assinatura digital usa o método de criptografia assimétrica, a validação se dá em três etapas, a figura 4 a seguir ilustra essas etapas. Sendo a primeira a execução da função MD, usando o mesmo algoritmo MD que foi aplicado ao documento na origem, obtendo assim um *hash* para aquele documento. Na segunda etapa, decifra-se a assinatura digital com a chave pública do remetente. A terceira consiste em comparar os resultados, assinatura digital decifrada deve produzir o mesmo *hash* gerado pela função MD executada anteriormente.

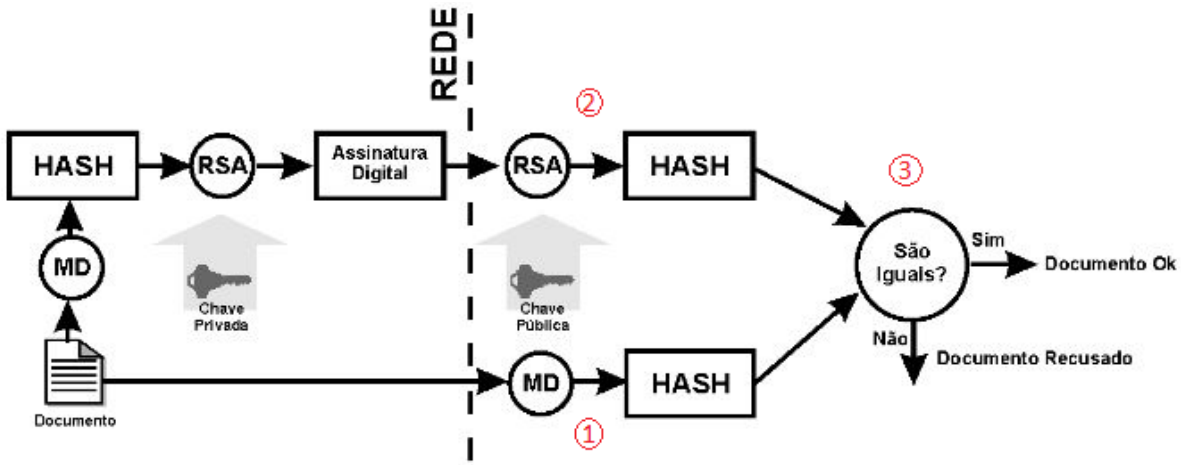


Figura 4 – Geração e verificação de assinatura digital, adaptado de Trinta e Macêdo (1998)

O modelo apresentado na figura 4 pode ser aplicado a qualquer sistema que necessite de assinatura digital. A partir disso pode-se obter um sistema responsável por implementar a assinatura digital e permitir sua integração com outros sistemas que necessitem dessa funcionalidade.

## 3.6 TECNOLOGIAS PARA INTEGRAÇÃO DE SISTEMAS

Integração de Sistemas é a capacidade de integrar sistemas de informação com fim de compartilhar recursos, sejam eles dados ou funcionalidades, contemplando a interoperabilidade independente da tecnologia de suporte, conforme define Martins (2005). Uma integração de sistemas em uma organização pode ocorrer considerando diferentes focos, sendo um deles quanto ao nível de implementação, que se refere a forma como será realizada, pode-se citar por

exemplo, se é uma integração a nível de aplicação ou de banco de dados. Quanto ao nível de implementação, de acordo com Martins (2005), a integração de sistemas pode ser classificada como:

•Aplicações Compostas: nessa classificação as aplicações são integradas por meio de uma camada de *software* que as conectam. Essa camada é a *API* (*Application Programming Interface*, ou Interface de Programação de Aplicação);

•Informação Centralizada: quando os sistemas têm acesso à mesma base de dados, inclusive os metadados; e

•Sistemas Integrados de Gestão: sistemas fechados e compostos por módulos internos independentes. Esta integração é realizada, comumente, em nível de código-fonte.

As classificações acima podem ser observadas nas organizações que se utilizam de mais de uma forma de implementação de integração. Um exemplo de aplicações integradas com o uso de API são as validações de dados pessoais vinculados ao Cadastro de Pessoa Física (CPF) na base de dados da Receita Federal ou o serviço de Código de Endereço Postal (CEP) disponibilizado pelos correios, onde as aplicações se valem dessas informações para alimentarem seus sistemas. Na informação centralizada tem-se a integração por meio da base de dados comum aos sistemas, como nos sistemas de vendas que utilizam as informações de funcionários para vincular às vendas ou o de controle de estoque. Nas soluções dos Sistemas Integrados de Gestão a integração está no nível do processo de negócio, mas pode ser implementado parcialmente, de acordo com os módulos utilizados pela organização.

Na integração com Aplicações Compostas, a arquitetura de um *software* representa a estrutura que abrange os componentes desse *software*, suas propriedades externamente visíveis e as relações entre ambos, como define Pressman (2001). A Arquitetura Orientada a Serviço (Service-Oriented Architecture (SOA)) vem sendo utilizada na integração de sistemas disponibilizados como serviços.

A SOA é um paradigma que visa a organização e utilização de recursos que podem estar sob controle de diferentes proprietários, pela disponibilização de um meio uniforme de oferta, descoberta, interação e uso de funcionalidades para produção de efeitos desejados (OASIS, 2008). A característica determinante é a

oferta das funcionalidades em forma de serviços, que dispõem de um meio comum para comunicação.

A Utilização de SOA com o propósito de integração é chamada de Service-Oriented Integration (SOI), conforme define Hensle et al (2010), cujo objetivo é criar uma integração entre múltiplos sistemas, modificando pouco ou nada suas implementações. Essa técnica expõe dados, funcionalidades e processos para serem consumidos pelos sistemas participantes da integração.

Uma das formas de se implementar a SOI é por meio de *Web Services*, fornecendo uma interface de serviço que permite que consumidores interajam com provedores de serviço (COULOURIS et al, 2013), como no exemplo do serviço de fornecimento de CEP disponibilizado pelos correios. As formas de implementação de Web Services mais comumente encontradas são Simple Object Access Protocol (SOAP) e Representional State Transfer (REST).

SOAP é um protocolo que utiliza a linguagem Web Services Description Language (WSDL), baseada em XML[2], para descrever funcionalidades oferecidas por um Web Service (ZUR et al, 2005). O SOAP provê um padrão básico de comunicação, no qual cada operação é representada por seu terminal, descrito no documento XML enviado na requisição, ao invés de um método HyperText Transfer Protocol (HTTP), como utilizado no REST (ZUR et al, 2005).

REST é uma abstração dos princípios que fazem a World Wide Web (WWW) escalável (ZUR et al, 2005). Permite fornecer serviços identificados por um *Uniform Resource Identifier*[3] (URI), com a utilização de métodos HTTP 1.0: GET, POST, DELETE e PUT. O uso destes métodos define a operação a ser feita: GET lista registros, POST insere novo registro, DELETE remove um registro, e PUT atualiza um registro (FIELDING, 2000).

Como REST não se trata de um protocolo, como o SOAP, mas, sim, de uma arquitetura (FIELDING, 2000), o retorno das chamadas pode ser formatado conforme os requisitos da aplicação, por exemplo, utilizando Javascript Object Notation (JSON) em vez de XML.

---

2 XML - eXtensible Markup Language é um formato de texto simples e flexível, originalmente projetado para atender aos desafios da publicação eletrônica em larga escala, o XML também está sendo utilizado na troca de grande variedade de dados na Web. (W3C 2020)

3 URI é uma forma uniforme de identificação de recursos em rede. O tipo mais conhecido de URI é o *Uniform Resource Location* (URL) (ZUR et al, 2005).

# 4 RESULTADOS

## 4.1 REQUISITOS NECESSÁRIOS AO SISTEMA ASSINADOR ELETRÔNICO DE DOCUMENTOS PARA ATENDER O SISGCORP

Os requisitos levantados e tratados a seguir foram identificados de acordo com critérios técnicos normativos, legais ou de negócio. Sua avaliação levou em consideração os normativos da ICP-Brasil e o padrão e-PING para interoperabilidade. O amparo legal foi baseado na MP-2200/2001 e os de negócio foram baseados nas informações disponíveis no site da DFPC.

### 4.1.1 Quanto ao formato da assinatura digital

O assinador eletrônico de documentos deve ser capaz de implementar a assinatura digital ICP-Brasil no formato Assinatura Digital com Referencias para Arquivamento (AD-RA). Conforme descrito no DOC-ICP-15.01, uma assinatura digital ICP-Brasil com Referencias para Arquivamento é formada por uma assinatura digital ICP-Brasil com Referência de Tempo (AD-RT) a qual foram acrescentadas referências de validação e todos os dados necessários para validação da assinatura. Um carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil e criado sobre todo esse conjunto de dados, ficando anexado ou logicamente conectado ao conjunto.

Este é um requisito legal, técnico normativo e de negócio. É requisito legal para atender o reconhecimento jurídico, é técnico normativo para atender à ICP-Brasil e é de negócio pela necessidade de manutenção dos arquivos dos processos do SisFPC no tempo. Torna-se um requisito obrigatório por ser indispensável atender aos três critérios.

### 4.1.2 Quanto à Política de assinatura digital

O assinador eletrônico de documentos deve utilizar a política ICP-Brasil para assinatura digital com referências para arquivamento com base nos padrões PDF/PADES, pois o PDF é o padrão utilizado pela administração militar para emissão de documentos, bem como este tipo de assinatura é adequado para aplicações que necessitam realizar o arquivamento do conteúdo digital assinado por longos períodos, oferece ainda segurança quanto à irretratabilidade, e permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da

chave privada da AC que emitiu o certificado do signatário, conforme descrito no DOC-ICP-15.03. Este documento descreve ainda os padrões CMS Advanced Electronic Signatures (CadES) e XML Advanced Electronic Signatures (XadES), que por não atenderem às necessidades de negócio atuais, não são obrigatórios, mas desejáveis para possibilidades de uso futuro.

O padrão PDF/PADES é um requisito técnico normativo e de negócio. É requisito técnico normativo para atender à ICP-Brasil e é de negócio pela necessidade de manutenção dos arquivos dos processos do SisFPC no tempo. Torna-se um requisito obrigatório por ser indispensável atender ao critério técnico.

### 4.1.3 Quanto à geração da assinatura digital

Para a geração da assinatura digital o assinador eletrônico deverá atender aos requisitos técnicos definidos para a geração de assinaturas digitais da ICP-Brasil, que estão disponíveis no DOC-ICP-15.01, exigindo-se ainda que o certificado digital seja validado no momento da assinatura. Este é um requisito técnico normativo para atender à ICP-Brasil. Torna-se um requisito obrigatório por ser indispensável atender ao critério técnico.

### 4.1.4 Quanto aos algoritmos utilizados

Os algoritmos utilizados devem estar entre os definidos no DOC-ICP-01.01, sendo no caso de assinaturas digitais ICP-Brasil SHA-1, SHA-256 e SHA-512 para a função resumo e sha1WithRSAEncryption, sha256WithRSAEncryption, sha256WithECDSAEncryption, sha512WithRSAEncryption e sha512WithECDSAEncryption para a suíte de assinaturas. Este é um requisito técnico normativo para atender à ICP-Brasil. Torna-se um requisito obrigatório por ser indispensável atender ao critério técnico.

### 4.1.5 Quanto à validação da assinatura digital

O assinador deverá verificar a conformidade da assinatura digital com os padrões ICP-Brasil, ou seja, verificar o atendimento dos requisitos necessários à geração da assinatura, para tanto o validador da assinatura digital deve utilizar o documento eletrônico para o qual a assinatura digital foi criada, a assinatura digital do documento eletrônico, o certificado digital do signatário, os status de revogação dos caminhos de certificação, do usuário e da ACT, a política de assinatura e o algoritmo definido. O objetivo é assegurar que a criptografia da assinatura digital é

válida, o caminho de certificação do signatário é válido no período de tempo referenciado, bem como se o carimbo de tempo é válido.

Este é um requisito de negócio pela necessidade de validação dos documentos assinados utilizando os padrões estabelecidos de assinatura. Porém, para atender a esse requisito de negócio é obrigatório que atenda aos critérios técnicos normativos.

### 4.1.6 Quanto à interoperabilidade

Deve possibilitar a geração de assinatura e validação das mesmas por meio de Web Service, que deve estar de acordo com os padrões definidos na arquitetura ePING – Padrões de Interoperabilidade de Governo Eletrônico, podendo usar XML (eXTENSIBLE Markup Language) ou JSON (Javascript Object Notation) como linguagens para intercâmbio de dados e os protocolos SOAP e HTTP/1.1 para acesso a Web Service.

Este é um requisito de negócio pela necessidade de integração do assinador ao sistema objeto da pesquisa, SisGCorp. É obrigatório para atender tal necessidade. Para atender a esse requisito de negócio é desejável que atenda aos critérios técnicos normativos definidos na arquitetura ePING.

No Quadro 1 a seguir, estão consolidados os requisitos necessários ao sistema assinador eletrônico de documentos para atender o SisGCorp, conforme foram apresentados nos itens anteriores. Este formulário compreende a síntese dos requisitos que servirão para a verificação da adequação dos assinadores eletrônicos de documentos a serem avaliados.

Na coluna referente à classificação estão estabelecidos os identificadores para os requisitos conforme sejam obrigatório, desejável, técnico normativo, legal ou de negócio. Na coluna referente ao peso, foram atribuídos valores para cada classificação, conforme o grau de importância. O peso de cada atributo foi calculado pela soma dos pesos da classificação de cada atributo.

**Quadro 1 – Requisitos necessários ao assinador eletrônico de documentos**

| **Formulário de requisitos necessários ao sistema assinador eletrônico de documentos para atender o SisGCorp** | | |
|---|---|---|
| **Requisito** | **Classificação**<br>**O – Obrigatório**<br>**D – Desejável**<br>**T – Técnico Normativo**<br>**L – Legal**<br>**N – de Negócio** | Peso<br>**2**<br>**1**<br>**1**<br>**3**<br>**2** |
| Quanto ao Formato da Assinatura Digital | | |
| Implementa assinatura digital com referência para arquivamento (AD-RA) | O – T – L – N | 8 |
| Quanto à Política de Assinatura Digital | | |
| Implementa a política AD-RA nos padrões PDF/PadES | O – T – N | 5 |
| Implementa a política AD-RA nos padrões CMS/CadES | D– T – N | 4 |
| Implementa a política AD-RA nos padrões CMS/XadES | D– T – N | 4 |
| Quanto à Geração da Assinatura Digital | | |
| Atende requisitos ICP-15-01 | O – T | 3 |
| Valida Certificado no Momento da Assinatura | O – T | 3 |
| Quanto ao Algoritmo Utilizado | | |
| Utiliza o algoritmo SHA256 ou SHA512 | O – T | 3 |
| Quanto a Validação da Assinatura | | |
| Para validação utiliza o (a): | | |
| - documento eletrônico para o qual a assinatura foi gerada | O – T – N | 5 |
| - assinatura digital do documento eletrônico | O – T – N | 5 |
| - certificado digital do signatário | O – T – N | 5 |
| - status de revogação dos caminhos de certificação do usuário | O – T – N | 5 |
| - status de revogação dos caminhos de certificação da ACT | O – T – N | 5 |
| - política de assinatura e o algoritmo definido | O – T – N | 5 |
| - política de assinatura | O – T – N | 5 |
| - algoritmo definido | O – T – N | 5 |
| Verifica validade da criptografia da assinatura digital | O – T – N | 5 |
| Verifica validade do carimbo de tempo | O – T – N | 5 |
| Verifica se o caminho de certificação do signatário é válido no período de tempo referenciado | O – T – N | 5 |
| Quanto a Interoperabilidade | | |
| Possibilita geração de assinatura por *WebService* de acordo com o padrão ePING | O – T – N | 5 |
| Possibilita validação de assinatura por *WebService* de acordo com o padrão ePING | O – T – N | 5 |
| Total dos pesos | | 95 |

Fonte: O autor (2020)

Para o cálculo do nível de aderência do software avaliado aos requisitos necessários ao sistema assinador eletrônico de documentos para atender o SisGCorp, deve-se utilizar a seguinte fórmula:

$$\% \text{ do Nível de aderência} = \frac{\text{Somatório dos Pesos de cada requisito presente}}{95} \times 100$$

## 4.2 LEVANTAMENTO DOS SISTEMAS ASSINADORES ELETRÔNICOS DE DOCUMENTOS COM MECANISMOS DE VERIFICAÇÃO DE AUTENTICIDADE

### 4.2.1 Assinador SERPRO

Ferramenta desenvolvida pelo Serviço Federal de Processamento de Dados (SERPRO) para assinar documentos com certificado digital ou validar documentos já assinados, conforme apresentado por SERPRO (2020). O referido assinador trata-se de um *software* disponível para instalação pelo usuário que utiliza recursos on-line para validação de listas de certificados revogados, sendo ainda necessário, para a função de assinatura, que o usuário possua um certificado digital emitido por autoridade certificadora credenciada junto à ICP-Brasil. Na validação de uma assinatura não é preciso ter um certificado digital, bastando seguir as instruções de validações de assinatura do software.

### 4.2.2 Assinador do Projeto SIGA-Doc

O Sistema de Gestão Administrativa (SIGA) é composto de diversos módulos dentre os quais está o SIGA-Doc, Sistema de Gestão de Documentos em meio físico ou digital, conforme apresentado por TRF2 (2020), o SIGA-Doc é uma aplicação web implementada em Java e utiliza componentes padrões de mercado, sendo ainda um software livre que pode ser utilizado por qualquer órgão interessado.

### 4.2.3 Assinador do SEI

O Sistema Eletrônico de Informações (SEI) é um sistema de produção e gestão de documentos e processos eletrônicos desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF4) e cedido à administração pública, conforme apresentado por GOV.BR (2020). O SEI ainda foi selecionado para a solução de processo eletrônico no âmbito do projeto Processo Eletrônico Nacional (PEN), que foi uma iniciativa conjunta de órgãos e entidades de diversas esferas da

administração pública para desenvolver uma infraestrutura pública de processos e documentos administrativos eletrônicos.

### 4.2.4 Assinador Digital PDF

A Secretaria da Fazenda do Estado do Mato Grosso do Sul desenvolveu o Assinador Digital PDF, que é um aplicativo que assina digitalmente documentos PDF. Trata-se de uma aplicação com parte instalada na máquina do usuário e parte com funcionamento web, conforme apresentado por SEFAZ-MS (2020).

## 4.3 LEVANTAMENTO DAS CARACTERÍSTICAS DOS SISTEMAS CATALOGADOS

O Quadro 2 a seguir, apresenta a aplicação da metodologia desenvolvida para avaliar a aderência dos assinadores eletrônicos de documentos levantados nos itens anteriores aos requisitos necessários para atender o SisGCorp. Ao Formulário do Quadro 1 foram acrescidas as colunas correspondentes aos assinadores eletrônicos avaliados, sendo incluído o valor do peso quando da existência da característica naquele software.

**Quadro 2 – Aplicação da metodologia para avaliar os assinadores**

| **Formulário de requisitos necessários ao sistema assinador eletrônico de documentos para atender o SisGCorp** | | | | | | |
|---|---|---|---|---|---|---|
| **Requisito** | | **Classificação**<br>O – Obrigatório<br>D – Desejável<br>T – Técnico Normativo<br>L – Legal<br>N – de Negócio | **Sistema/Peso** | | | |
| | | | **4.3.1** | **4.3.2** | **4.3.3** | **4.3.4** |
| Quanto ao Formato da Assinatura Digital | | | | | | |
| 1 | Implementa assinatura digital com referência para arquivamento (AD-RA) | O – T – L – N | 8 | 8 | 8 | 8 |
| Quanto à Política de Assinatura Digital | | | | | | |
| 2 | Implementa a política AD-RA nos padrões PDF/PadES | O – T – N | 5 | 5 | 5 | 5 |
| 3 | Implementa a política AD-RA nos padrões CMS/CadES | D– T – N | 4 | 4 | 4 | - |
| 4 | Implementa a política AD-RA nos padrões CMS/XadES | D– T – N | 4 | 4 | 4 | - |
| Quanto à Geração da Assinatura Digital | | | | | | |
| 5 | Atende requisitos ICP-15-01 | O – T | 3 | 3 | 3 | 3 |
| 6 | Valida Certificado no Momento da Assinatura | O – T | 3 | 3 | 3 | 3 |
| Quanto ao Algoritmo Utilizado | | | | | | |
| 7 | Utiliza o algoritmo SHA256 ou SHA512 | O – T | 3 | 3 | 3 | 3 |
| Quanto a Validação da Assinatura | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Para validação utiliza o (a): | | | | | |
| 8 | - documento eletrônico para o qual a assinatura foi gerada | O – T – N | 5 | 5 | - | - |
| 9 | - assinatura digital do documento eletrônico | O – T – N | 5 | 5 | - | - |
| 10 | - certificado digital do signatário | O – T – N | 5 | 5 | - | - |
| 11 | - status de revogação dos caminhos de certificação do usuário | O – T – N | 5 | 5 | - | - |
| 12 | - status de revogação dos caminhos de certificação da ACT | O – T – N | 5 | 5 | - | - |
| 13 | - política de assinatura e o algoritmo definido | O – T – N | 5 | 5 | - | - |
| 14 | - política de assinatura | O – T – N | 5 | 5 | - | - |
| 15 | - algoritmo definido | O – T – N | 5 | 5 | - | - |
| 16 | Verifica validade da criptografia da assinatura digital | O – T – N | 5 | 5 | - | - |
| 17 | Verifica validade do carimbo de tempo | O – T – N | 5 | 5 | - | - |
| 18 | Verifica se o caminho de certificação do signatário é válido no período de tempo referenciado | O – T – N | 5 | 5 | - | - |
| Quanto a Interoperabilidade | | | | | | |
| 19 | Possibilita geração de assinatura por *WebService* de acordo com o padrão ePING | O – T – N | - | 5 | - | 5 |
| 20 | Possibilita validação de assinatura por *WebService* de acordo com o padrão ePING | O – T – N | - | 5 | - | - |
| Total dos Pesos | | | 85 | 95 | 30 | 27 |

Fonte: O autor (2020)

## 4.4 ANÁLISE DO NÍVEL DE ADERÊNCIA DAS CARACTERÍSTICAS DOS MECANISMOS ASSINADORES COMPARADAS AOS REQUISITOS E RESTRIÇÕES DO SISGCORP

Aplicando a fórmula para o cálculo do nível de aderência do assinador SERPRO, tem-se que o percentual foi de 89,47%, tendo deixado de atender ao requisito de interoperabilidade, pois não possibilita a integração por meio de *WebService*. O assinador do SIGA-Doc atende 100% dos requisitos. O assinador do SEI atende 31,27% dos requisitos, não atendendo aos referentes a validação de assinatura, por não possuir esta funcionalidade, bem como a possibilidade de integração por *WebService*. O assinador digital PDF da SEFAZ-MS atende 28,42% dos requisitos, satisfazendo apenas ao padrão PDF quanto à política e como não possui validador, não atende aos requisitos de validação.

Conforme avaliação realizada, segue na Tabela 1 a lista dos assinadores eletrônicos avaliados com seu respectivo grau de aderência. A lista está organizada do mais aderente ao menos aderente.

**Tabela1 – Seleção ranqueada dos assinadores eletrônicos avaliados**

| Assinadores eletrônicos avaliados | % de Aderência |
|---|---|
| 1 – Assinador do Projeto SIGA-Doc | 100% |
| 2 – Assinador SERPRO | 90% |
| 3 – Assinador do SEI | 35% |
| 4 – Assinador Digital PDF | 30% |

Fonte: O autor (2020)

## 5 DISCUSSÃO

A elaboração do Formulário de requisitos necessários ao sistema assinador eletrônico de documentos para atender o SisGCorp apresenta a possibilidade de avaliar quaisquer soluções de *software* disponíveis para atender esse tipo de necessidade. O levantamento desses requisitos envolveu a busca pelo conhecimento dos normativos que tratam da assinatura digital, bem como pelo conhecimento das técnicas empregadas.

Pôde-se observar que a normatização existente para assinatura digital é ampla e abrangente, possuindo requisitos técnicos e normativos claros que possibilitaram o desenvolvimento desta pesquisa. Nessa busca, observou-se ainda que a certificação digital, estabelecida pela ICP-Brasil, trouxe o conhecimento sobre os padrões existentes que foram empregados na solução do problema.

A pesquisa apresentou como resultado os requisitos necessários ao sistema assinador de documentos que possa ser integrado ao SisGCorp, conforme proposto no objetivo. Analisou ainda as opções de *software* disponíveis, apresentando-as ranqueadas conforme o grau de aderência aos requisitos, atingindo assim os objetivos a que se propôs.

Os resultados alcançados não se restringem a atender ao problema específico do SisFPC, pois podem ser utilizado por toda instituição pública que ainda não tenha implementado a assinatura digital em seus sistemas, podendo ainda ser utilizado como requisito para desenvolvimento de *software*, possibilitando uma integração efetiva aos sistemas existentes da instituição.

# 6 CONCLUSÃO

O uso de documentos digitais após o marco regulatório instituído pela MP 2200/2001 ganhou força pela possibilidade do reconhecimento jurídico. Sua implantação ocorre com a criação da ICP-Brasil pelo ITI que materializa o uso de documentos digitais com reconhecimento jurídico.

No Exército Brasileiro o esforço iniciado nos anos 2000 para automação está em andamento e é percebido na iniciativa do desenvolvimento do SisGCorp, bem como com sua participação na AC Defesa e na determinação para realização de estudos para uso da certificação digital no âmbito do Exército contida na Portaria 769 de 2011.

A pesquisa apresentou o conhecimento dos normativos e especificações técnicas das áreas de certificação digital, interoperabilidade e documentos. Estes foram os elementos da pesquisa que estabeleceram os critérios para se obter um assinador eletrônico com as características necessárias ao atendimento do objetivo.

Acredita-se que a pesquisa tenha cumprido seus objetivos, de forma que apresentou as características necessárias a um sistema assinador eletrônico de documentos, com mecanismo de verificação de validade e autenticidade de documentos, que fosse integrável ao SisGCorp, utilizado pelo SisFPC, bem como apresentou ainda um Formulário capaz de orientar a seleção de aplicações disponíveis e fornecer os requisitos iniciais para o desenvolvimento de uma aplicação.

A pesquisa limitou-se aos requisitos necessários ao atendimento do SisGCorp e por este motivo pode ser necessária alguma adaptação para aplicação do Formulário desenvolvido para atender outros *softwares* da administração pública que necessitem dessa funcionalidade, cabendo uma avaliação do interessado.

O presente estudo contribui com um caminho inicial para iniciativas de implementação de assinadores digitais com métodos de validação de das assinaturas em quaisquer órgãos públicos. Possibilita ainda avaliar a integração das ferramentas avaliadas a sistemas existentes, bem como apresenta uma metodologia que possibilita identificar outras soluções que atendam às necessidades do órgão.

Como proposta de trabalhos futuros pode-se utilizar os requisitos pesquisados para a pesquisa e desenvolvimento de uma solução que atenda a administração pública, de forma a permitir a aplicação da interoperabilidade desejada aos softwares governamentais.

## REFERÊNCIAS


AC DEFESA, 2020. Disponível em:<https://www.acdefesa.mil.br/ >. Acesso em: 16 Jul 2020.

ACÓRDÃO 604/2017 PLENÁRIO. **Tribunal de Contas da União**, 2017. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/resultado/acordao-completo/604%252F2017/%2520/%2520?ts=1594585574438&pb=acordao-completo >. Acesso em: 12 Jul 2020.

ACÓRDÃO 733/2018 PLENÁRIO. **Tribunal de Contas da União**, 2018. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/resultado/acordao-completo/733%252F2018/%2520/%2520?ts=1594585601230&pb=acordao-completo >. Acesso em: 12 Jul 2020.

ANDRADE, Rafael Santos; SILVA, Fernando dos Santos. **ALGORITMO DE CRIPTOGRAFIA RSA:análise entre a segurança e velocidade.** Revista Eventos Pedagógicosv.3, n.3, p. 438-457, Ago – Dez 2012. Disponível em: <https://www.academia.edu/download/31637339/967-2954-1-PB.pdf>. Acesso em: 19 Set 2020.

Assinador digital PDF. **SEFAZ-MS**, 2020. Disponível em: <http://www.dfe.ms.gov.br/assinadordigitalpdf/#/home>. Acesso em: 7 Set 2020.

ASSINADOR SERPRO. **SERPRO**, 2020. Disponível em: <https://serpro.gov.br/links-fixos-superiores/assinador-digital/assinador-serpro>. Acesso em: 5 Set 2020.

ASSINATURA DIGITAL. **Kryptosgraphein**, 2020. <https://sites.google.com/site/kryptosgraphein/algoritmossimetricos>. Acesso em: 16 Jul 2020.

BRASIL[1]. **Medida Provisória 2200**, de 28 Jun 2001. Disponível em:< http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200.htm>. Acesso em: 6 Jul 2020.

BRASIL[2]. **Medida Provisória 2200-2**, de 24 Ago 2001. Disponível em:< http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm>. Acesso em: 6 Jul 2020.

BRASIL, **Decreto 6.605**, de 14 de outubro de 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6605.htm >. Acesso em 23 Jul 2020.

BRASIL. **O SINAR**, [s.d.]. Disponível em:<http://conarq.gov.br/o-sinar.html>. Acesso em: 7 Jul 2020.

BRASIL. **O CONARQ**, 2014. Disponível em: <http://conarq.gov.br/o-conselho.html>. Acesso em: 7 Jul 2020.

BRASIL. Do Eletrônico ao Digital. **Governo Digital**, 2019. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletro-

nico-ao-digital> Acesso em 06 Jul 2020.

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

BREVE HISTÓRICO. **Diretoria de Fiscalização de Produtos Controlados**[1], 2020. Disponível em: <http://www.dfpc.eb.mil.br/index.php/noticias-menu/561-breve-historico>. Acesso em: 12 Jul 2020.

CÔRTE, K. **Segurança da Informação Baseada no Valor da Informação e nos Pilares Tecnologia, Pessoas e Processos.** 2014, 212p. Tese (Doutorado em Ciencia da Informação) –Universidade de Brasília –Faculdade de Ciência da Informação, Brasília.

COULOURIS, G., Dollimore, J., Kindberg, T. & Blair, G. **Sistemas Distribuidos-: Conceitos e Projeto**. Bookman Editora. 2013.

Documentos Principais. **ITI**, 2020. Disponível em: <https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais>. Acesso em: 13 Set 2020.

ESTRUTURA ICP-BRASIL. **ITI**, 2020. Disponível em: <https://estrutura.iti.gov.br/ >. Acesso em 21 Jul 2020.

EXTENSIBLE MARKUP LANGUAGE (XML). **W3C**, 2020. Disponível em: <http://www.w3c.org/XML/>. Acesso em: 21 Jul 2020.

FIELDING, R. T. **Architectural styles and the design of network-based software architectures**. University of California, Irvine, 2000.

HENSLE, B.; Booth, C.; Chappelle, D.; McDaniels, J.; Wilkins, M. & Bennett, S. Oracle **Reference Architecture - Service-Oriented Integration**, Release 3.0.Oracle, 2010.

ICP-BRASIL. **ITI**, 2017. Disponível em:<https://www.iti.gov.br/perguntas-frequentes/41-perguntas-frequentes/130-sobre-a-icp-brasil>. Acesso em: 16 Jul 2020.

JÚNIOR, Carlos E. B. Santos; FERNANDES, Marcelo A. C.. **Proposta de implementação do algoritmo SHA-256 em Hardware.** In: ANAIS PRINCIPAIS DO SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 18. , 2018, Natal. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018 . p. 17 – 24. Disponível em: <https://sol.sbc.org.br/index.php/sbseg/article/view/4265>. Acesso em: 19 Set 2020.

MARCACINI, Augusto Tavares Rosa. **Direito e Informática: uma abordagem jurídica sobre a Criptografia**. São Paulo, 2010.

MARTINS, V. M. M. **Integração de Sistemas de Informação: Perspectivas, normas e abordagens**. Universidade do Minho - Guimarães - Portugal, 2005.

MICHAELIS, c2020. Disponível em: <http://michaelis.uol.com.br/busca?id=1OQQ>. Acesso em: 15 Jul 2020.

MOREIRA, Márcio Aurélio Ribeiro. **ECDSA (Elliptic Curve Digital Signature Algorithm)**, 2006. Disponível em: <http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5630/material-cripto-seg/crpt_trabalho_ecdsa.pdf >. Acesso em: 19 Set 2020.

O que é o SIGA-Doc?. **TRF2**, 2020. Disponível em: <https://www10.trf2.jus.br/ti/produtos-open-source/o-que-e-o-siga-doc/>. Acesso em: 7 Set 2020.

OLIVEIRA, Ronielton Rezende. **Criptografia simétrica e assimétrica: os principais algoritmosde cifragem**, 2012. Disponível em: <http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf>. Acesso em: 19 Set 2020.

OASIS, Organization for the advancement of structured information standards. **Service-Oriented Architecture**. Disponível em: <http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-pr-01.pdf>. Acessado em 16/07/2020. 2008.

Padrões de Interoperabilidade de Governo Eletrônico – ePING. **ePING**, 2020. Disponível em: <http://eping.governoeletronico.gov.br/>. Acesso em 13 Set 2020.

PRESSMAN, R. S. **Software engineering: a practitioner's approach**. McGraw-Hill, McGraw-Hill, 2001.

RED HAT ENTERPRISE LINUX 4: GUIA DE SEGURANÇA. **MIT**, 2020. Disponível em: <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/ch-sgs-ov.html#:~:text=Muitas%20consultorias%20e%20fabricantes%20da,Confidencialidade%2C%20Intergridade%20e%20Disponibilidade).&text=Disponibilidade%20%E2%80%94%20As%20informa%C3%A7%C3%B5es%20devem%20estar,usu%C3%A1rios%20autorizados%20sempre%20que%20precisarem>. Acesso em: 16 Jul 2020.

SARAIVA, André. A Implementação do SEI**. Biblioteca Digital da Administrçaão Pública,** 2018. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/3455/4/SEGES%20%20Enap.%20SARAIVA%20Andr%C3%A9.%20SEI.%20estudo%20de%20caso.%202018.%20portug%C3%Aas.pdf >. Acesso em 06 Jul 2020.

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

SINGH, G. **A study of encryption algorithms (rsa, des, 3des and aes) for information security.International Journal of Computer Applications.** Foundation of Computer Science, v. 67,n. 19, 2013.

Sistema Eletrônico de Informações. **GOV.BR**, 2020. Disponível em: <https://www.gov.br/fazenda/pt-br/assuntos/sei>. Acesso em: 7 Set 2020.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas.** 6ª edição, Person Education do Brasil, São Paulo, SP, BRA, 2015.

TRINTA, Fernando A.M.; MACÊDO, Rodrigo C. **Um Estudo sobre Criptografia e Assinatura Digital**, 1998. Disponível em: <https://www.cin.ufpe.br/~flash/ais98/cripto/criptografia.htm >. Acesso em 21 Jul 2020.

WEBER, Raul Fernando. Criptografia contemporânea. In: **VI Simpósio de Computadores Tolerantes a Falhas**. 1995. p. 7-32.

ZANELLA, Liane Carly Hermes. **Metodologia de Estudo e Pesquisa em Administração**. Florianópolis: UFSC, 2009.

ZUR, M. M.; NICKERSON, J. V.; SWENSON, K. D. **Developing web services choreography standards — the case of REST vs. SOAP**. Decision Support Systems, Elsevier, 40, 9-29, 2005.