



## INSTRUÇÃO OPERACIONAL

Nº	IO-001
ÓRGÃO	COSIG.F
REVISÃO	01
VIGÊNCIA	01/06/2020
PÁGINA	1 / 14

TÍTULO	UTILIZAÇÃO DA ASSINATURA DIGITAL NA INB
--------	---

### SUMÁRIO

1	FINALIDADE .....	2
2	APLICAÇÕES .....	2
3	DEFINIÇÕES.....	2
4	PROCEDIMENTOS.....	3
4.1	ENTENDENDO A ASSINATURA DIGITAL .....	3
4.2	INSTALAÇÃO DO DRIVER E DOS ASSINADORES .....	4
4.3	ASSINATURA DIGITAL EM DOCUMENTOS DA INB .....	5
4.3.1	<i>Documentos de Suprimentos.....</i>	5
4.3.2	<i>Documentos Técnicos e Administrativos .....</i>	6
4.4	ASSINANDO DOCUMENTOS .....	6
4.5	VALIDANDO ASSINATURAS.....	10
4.5.1	<i>Validando pelo Site do ITI.....</i>	10
5	DOCUMENTOS DE REFERÊNCIA.....	11
6	ANEXOS.....	12
6.1	ANEXO 1 - TERMO DE REFERÊNCIA ASSINADO DE EXEMPLO. ....	12
6.2	ANEXO 2 – JUSTIFICATIVA TÉCNICA ASSINADA DE EXEMPLO. ....	13

## 1 FINALIDADE

A finalidade desse documento é estabelecer os procedimentos para que os empregados que possuírem o certificado digital e-CPF, padrão ICP-Brasil, possam assinar digitalmente os documentos em que forem necessários esse tipo de assinatura.

## 2 APLICAÇÕES

Todos os documentos emitidos pelas áreas, que necessitem de assinatura dos gestores ou de técnicos designados, ou por força de lei ou por força normativa, deixarão de ser assinados fisicamente em documentos impressos e passarão a ser assinados digitalmente, em seu formato eletrônico, utilizando o PBAD. A assinatura de documentos eletrônicos, em especial documentos no formato PDF, será realizada com certificado digital e-CPF, padrão ICP-Brasil, e o Assinador da INB, desenvolvido internamente.

## 3 DEFINIÇÕES

<b>e-CPF:</b>	Documento eletrônico, que permite assinar <b>digitalmente outros documentos</b> e possui validade jurídica, servindo para atestar o autor em transações eletrônicas e diversos serviços realizadas ou pedidos através de meios eletrônicos.
<b>ICP-Brasil:</b>	Cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão brasileiro.
<b>PBAD:</b>	Padrão Brasileiro de Assinatura Digital. Conjunto de padrões, estabelecidos pelo ITI.
<b>Assinatura Eletrônica:</b>	Registros de liberação eletrônico, que se dividem em Assinatura Digital e outros meios de identificação, como login/senha e biometria.
<b>Assinatura Digital:</b>	Tipo específico de assinatura eletrônica que se caracteriza pela constatação, por um terceiro e algoritmos de criptografia que o assinador é realmente quem diz ser.
<b>ITI:</b>	Instituto Nacional de Tecnologia da Informação.
<b>PDF:</b>	A sigla inglesa <b>PDF</b> significa Portable Document Format (Formato Portátil de Documento), um formato de arquivo criado pela empresa Adobe Systems para que qualquer documento seja visualizado, independente de qual tenha sido o programa que o originou.
<b>Token:</b>	Dispositivo eletrônico gerador de senhas ou de chaves criptográficas. No caso de tokens com certificado e-CPF a conexão se dará por uma porta USB.
<b>Driver:</b>	Arquivo que contém as funções a serem integradas a um sistema operacional para controlar um determinado periférico.
<b>Documento nato digital:</b>	Documento <b>nato digital</b> é o documento que nasceu em formato <b>digital</b> , tal como um documento produzido pelo Office, por uma câmera <b>digital</b> e tantos outros que nascem no formato <b>digital</b> .

## 4 PROCEDIMENTOS

### 4.1 ENTENDENDO A ASSINATURA DIGITAL

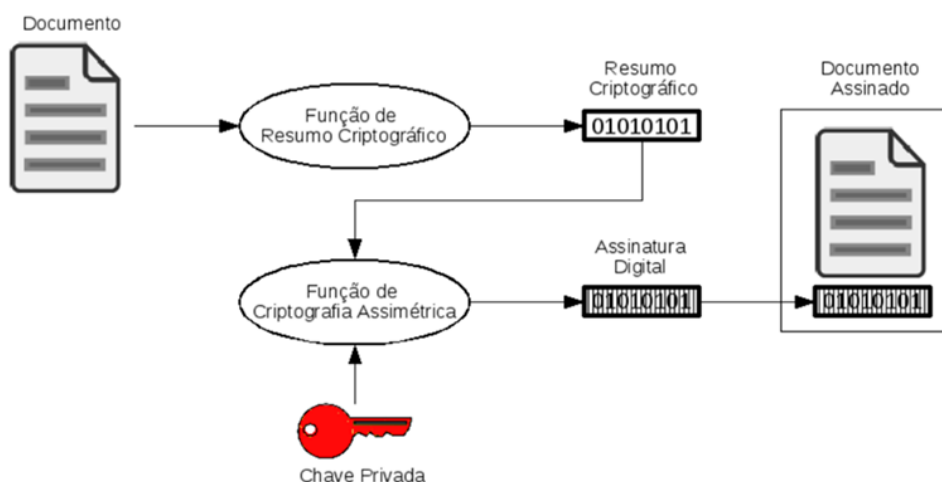
Ao receber o Token com o e-CPF o empregado estará apto para assinar digitalmente todos os documentos e se autenticar em sites que permitirem esse tipo de integração, como o site da Receita Federal (e-CAC).

A assinatura digital é um tipo de assinatura eletrônica, que utiliza um certificado digital padrão ICP-Brasil que possui chaves criptográficas de forma a atestar que o documento não foi alterado e garantir que a pessoa que assina um documento, de fato seja quem diz ser.

O Certificado Digital armazenado no Token entregue ao empregado é parte da tecnologia que permite essa assinatura. As assinaturas digitais que utilizem esse tipo de identificação possuem valor equivalente a assinatura pública e, qualquer ato jurídico realizado com ela, possui valor legal, sendo assim, é necessário que cada possuidor de um e-CPF tenha extremo cuidado com **a posse de seu Token e sua respectiva senha**. Jamais empreste seu Token e/ou divulgue sua senha.

Ao assinar um documento com um certificado digital, existe a garantia do autor da assinatura, da autenticidade do documento e valor similar, garantido por lei, da legitimidade da assinatura, desde que a mesma tenha sido feita durante a validade do certificado digital.

A Figura 1 ilustra o esquema simplificado de funcionamento da assinatura digital.



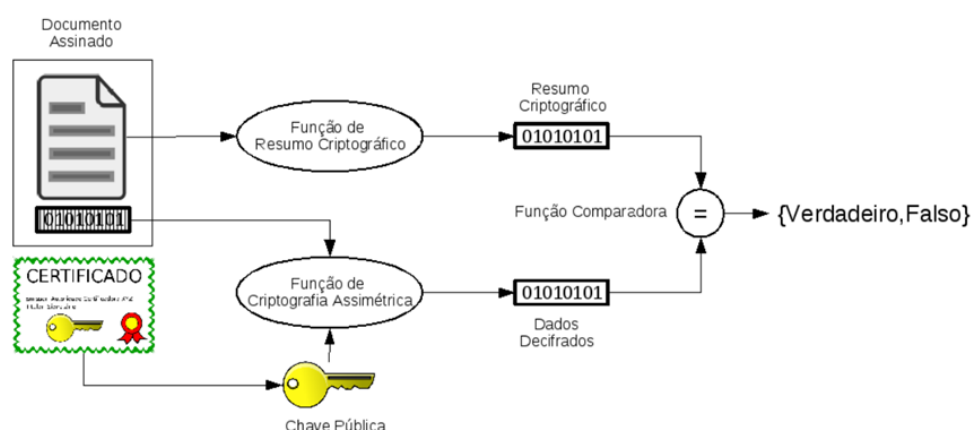
*Figura 1: Diagrama simplificado de criação de assinatura digital*

Para realizar uma Assinatura Digital, além do certificado digital padrão ICP-Brasil, o empregado necessita ter instalado em sua máquina o Driver do Token e um programa responsável pela assinatura do documento eletrônico. Esses programas são os Assinadores, que podem ser proprietários ou de terceiros. O Assinador é um programa que tem a responsabilidade de gerar a assinatura digital que pode ficar dentro do documento (como é o caso de PDFs) ou acompanhar externamente o documento, no caso de outros tipos.

Como o PBAD estabelece padrão para assinaturas dentro do documento somente para PDFs, a recomendação é que todos os documentos que precisarem ser assinados, sejam gerados em PDF-A, para então serem assinados.

Existem programas responsáveis por validarem as assinaturas, através de algoritmos de validação. A tecnologia que permite a assinatura digital também é responsável pela verificação, que pode ser feito por qualquer pessoa que tiver o arquivo assinado. O ITI fornece um verificador de conformidade on-line, onde arquivos assinados podem ser postados e serão verificados pelo seu portal de verificação.

Para realizar a verificação é necessário que seja utilizado o arquivo assinado (caso a assinatura esteja internalizada) ou o arquivo e a chave criptográfica gerada externamente. A Figura 2 ilustra como é que a tecnologia de assinatura digital realiza a verificação de integridade da assinatura digital.



*Figura 2: Verificação de um documento assinado digitalmente*

Para verificar se a assinatura digital de um documento é válida, **não é necessário** possuir o Token utilizado na geração da assinatura, visto que a chave criptográfica de origem e outras informações necessárias sobre o documento são armazenados juntamente com a assinatura.

Ressalta-se ainda que os documentos assinados digitalmente perdem valor ao serem impressos, ou seja, somente sua cópia digital tem valor de original, não tendo validade as suas reproduções em meio físico. Outra informação relevante é que o conceito de “arquivo original” se perde, visto que todas as cópias, desde que não alterado o conteúdo do arquivo, tem o valor de original, podendo ser copiados quantas vezes forem necessários.

Outra característica existente em assinatura de documentos físicos que não faz sentido em documentos assinados digitalmente é a rubrica em cada página do documento. Como a assinatura digital leva em conta todo o seu conteúdo, se qualquer parte do documento for alterada, o resumo muda e sua validade se perde, ou seja, a autenticidade do conteúdo de todas as páginas já está atestada por uma única assinatura.

Um documento assinado digitalmente, pode ser assinado por várias pessoas, desde que as demais assinaturas também sejam digitais. O documento não pode ser assinado, parcialmente digital e parcialmente fisicamente, visto que uma assinatura física ao ser digitalizada perde o valor e uma assinatura digital, ao ser impressa, também.

## 4.2 INSTALAÇÃO DO DRIVER E DOS ASSINADORES

Ao receber o seu Token, para utilizá-lo é necessário possuir instalado na estação de trabalho o Driver, responsável pela leitura dos dados armazenados no dispositivo e do programa Assinador, que

fará uso do par de chaves para gerar a assinatura digital, com o conteúdo do documento.

Para instalar o Driver do Token em sua estação de trabalho, é necessário abrir um chamado no Portal de Atendimento do Help Desk, na INB.

A instalação do Assinador da INB está disponível em <http://inbnet/instalacoes/Assinador/publish.html>. Caso não seja possível instalá-lo diretamente, registre o pedido no Portal de Atendimento do Help Desk, na INB.

Somente após a instalação do Driver do Token e do Assinador da INB que será possível assinar digitalmente documentos.

Para validar assinaturas, deve ser utilizada o validador de conformidade disponibilizado pelo ITI, através da URL: <https://verificador.iti.gov.br/verifier-2.5.2/>.

### **4.3 ASSINATURA DIGITAL EM DOCUMENTOS DA INB**

Para modernizar a Gestão Documental, os documentos tramitados internamente e externamente para atendimento desde comunicações (internas e externas) até processos de aquisição, pagamentos, formulários do recursos humanos (TEP de transferência, TEP coletivo etc.) podem ser assinados e tramitados integralmente no formato digital, sem sua transposição para o meio físico (papel).

Para os documentos assinados digitalmente, não faz sentido sua impressão, não sendo mais necessária e até mesmo sendo indesejável, visto que documentos assinados digitalmente, ao serem impressos, perdem seu valor. O documento deverá ser transmitido, via e-mail ou através de Sistemas próprios de Gestão Documental, para as partes interessadas.

Todos os documentos possíveis de serem produzidos exclusivamente em meio digital, deverão ser portados para PDF, quando em sua versão final e assinados digitalmente. Excetuam-se dessa regra os documentos que forem impossíveis de se transportar integralmente do meio físico para o meio digital, quando houver a impossibilidade de todos os atores envolvidos o assinarem digitalmente.

#### **4.3.1 Documentos de Suprimentos**

Os documentos anexados no Sistema de RMS que anteriormente eram assinados fisicamente, digitalizados e anexados, tendo os originais encaminhados via malote a GESUP.F, passam a ser integralmente digitais, sendo assinado pelos gestores responsáveis somente, com o certificado digital.

Os documentos que serão anexado no RMS serão os originais em PDF, assinado digitalmente, não existindo mais a necessidade de imprimir-los e gerar os documentos físicos, eliminando com isso o custo com a impressão do documento, transporte e armazenamento.

Outro benefício para a área de suprimentos é a eliminação da pasta física do processo, passando essa pasta a ser virtual, com a vantagem de estar acessível em qualquer lugar, organizado pelo Sistema.

É importante observar que, nos documentos em papel que possuam várias páginas, para garantir a autenticidade de todo o documento, os responsáveis rubricam página a página. Em um documento eletrônico, para garantir a autenticidade, conforme já dito anteriormente, bastará assiná-lo uma única vez, não sendo necessário assinar todas as folhas, visto que a tecnologia garante a integridade de todo o documento.

Os Anexo 1 e Anexo 2 são exemplos de documentos de suprimentos, assinados digitalmente para comporem o processo de requisição de material ou serviço.

#### 4.3.2 Documentos Técnicos e Administrativos

Os demais documentos que precisem de aprovação, precisarão ser redesenvolvidos para que, nos campos aprovação, contenham somente as assinaturas de gestores. O registro da elaboração será interno e no Software de Gestão Documental. Com o certificado sendo distribuído para todos os empregados, será possível registrar livremente assinatura de elaboradores e revisores, sendo esses registros realizados em similaridade com o papel. Para o registro da elaboração e revisão de documentos, o software de Gestão Documental da INB, Alfresco, pode ser utilizado. Caso sua área ainda não tenha acesso, solicitar a implantação a COSIG.F, via e-mail, através do gestor da área a implantação e capacitação.

As CIs, CEs, TEPs de Transferência etc., devem ser preenchidos pela área e, após seu preenchimento, gerar o PDF, para então o(s) gestor (es) responsável (eis) assinar(em) o documento digitalmente, para distribuí-lo pelos meios adequados.

#### 4.4 ASSINANDO DOCUMENTOS

Existem diversas possibilidades de programas disponíveis para a geração da Assinatura Digital. A INB, visando a integração de um aplicativo que gere a assinatura com os seus sistemas, desenvolveu o seu próprio Assinador, disponibilizado em <http://inbnet/instalacoes/Assinador/publish.html>. A recomendação interna é que todos os documentos sejam assinados no formato PDF para que a assinatura fique dentro do arquivo, não sendo necessário transportar arquivos adicionais. Essa recomendação inclui, inclusive, plantas de engenharia, que, quando necessitar da assinatura do engenheiro responsável ou do gestor da área, para garantir a integridade e autenticidade do documento, seja “plotado” em formato PDF e assinado. Para todos os casos propostos, o documento em PDF será **o correspondente eletrônico da cópia impressa em papel** e assinada fisicamente.

Para gerar o PDF a partir de um documento dentro do WORD, existem dois caminhos: exportar diretamente para PDF, conforme ilustrado na Figura 3.

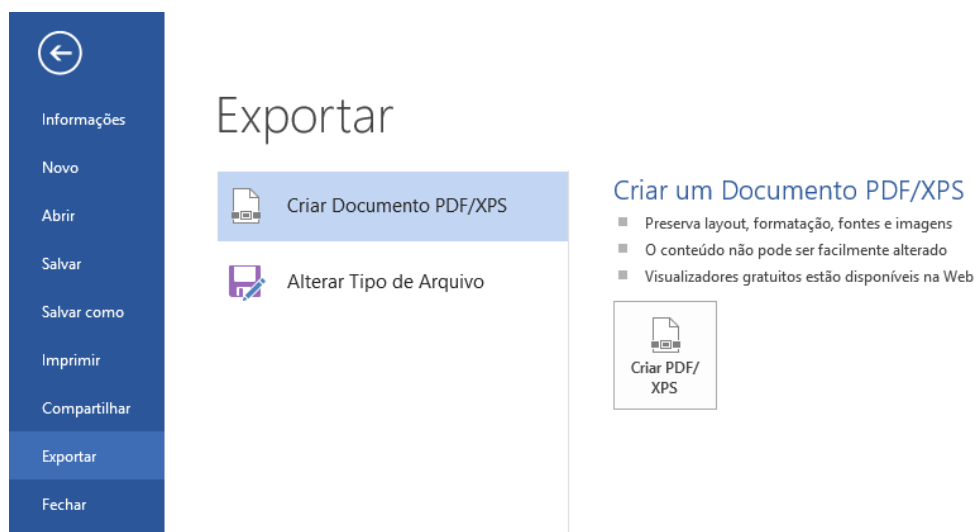
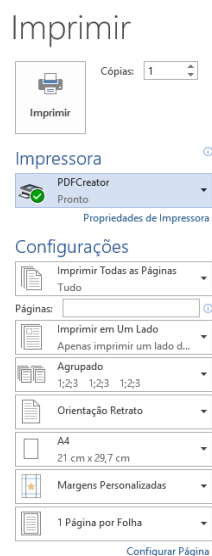


Figura 3: Exportando documento Word para PDF

Outra forma de gerar um PDF, a partir de qualquer aplicativo, é imprimi-lo em PDF, conforme ilustrado na Figura 4.

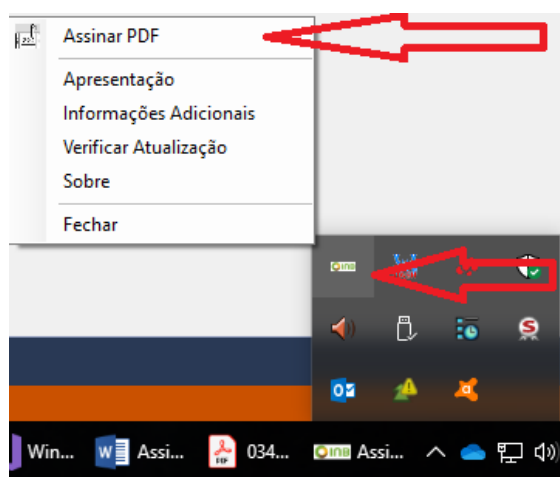


*Figura 4: Imprimindo o documento em PDF*

Após gerar o PDF o documento estará disponível para ser assinado antes de ser anexado no Sistema de RMS ou transmitido, via e-mail a(s) parte(s) interessada(s).

Fica ressaltado novamente que, independente de quantas cópias se faça do arquivo após assinado, se o mesmo não for alterado, terá sua autenticidade e integridade validada, sendo todas as suas cópias consideradas arquivos originais.

Após instalar o Assinador da INB, um ícone na barra de tarefas do Windows ficará disponível para acessá-lo, conforme ilustrado na Figura 5. Caso o ícone não esteja disponível no seu computador na empresa, solicite ao Help -Desk sua instalação através do ramal 8799. Caso seja em seu computador pessoal, o Assinador pode ser obtido diretamente do site do Serpro (ASSINADOR SERPRO, 2019).



*Figura 5: Acessando o Assinador da INB*

Para assinar documento PDF, clique no menu “Assinar PDF”. Essa ação abrirá uma janela para selecionar o PDF que deseja ser assinado. O Assinador abrirá uma visualização, que permite navegar pelas páginas do documento para posicionar o selo, com o clique do mouse, conforme ilustrado na Figura 6.

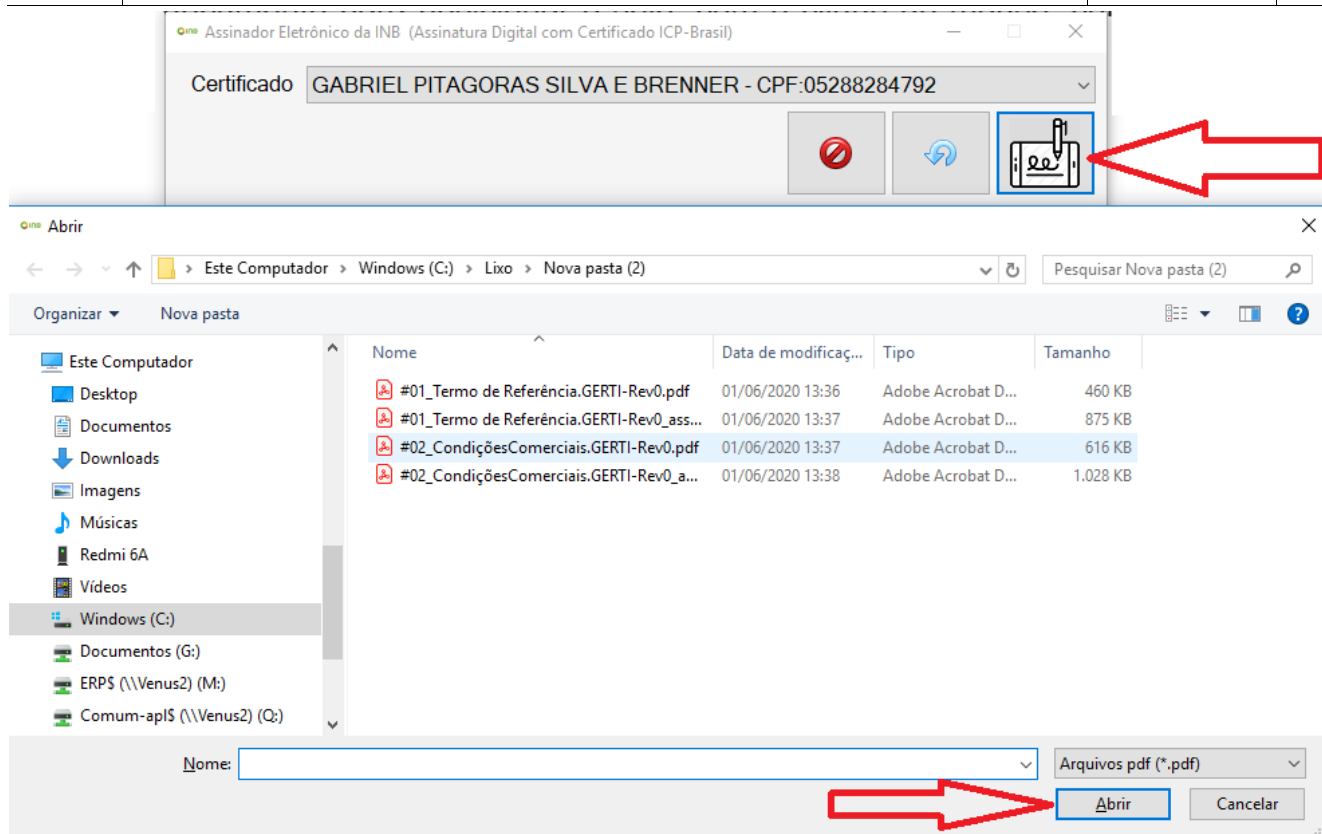


Figura 6: Assinando PDF

Após selecionar o certificado, clicar no botão “Assinar PDF”, selecionar o arquivo, abrirá a tela para posicionamento do selo da assinatura, conforme ilustrado na Figura 7. Qualquer dúvida nesse procedimento, ligar para o Help Desk no ramal 8799.

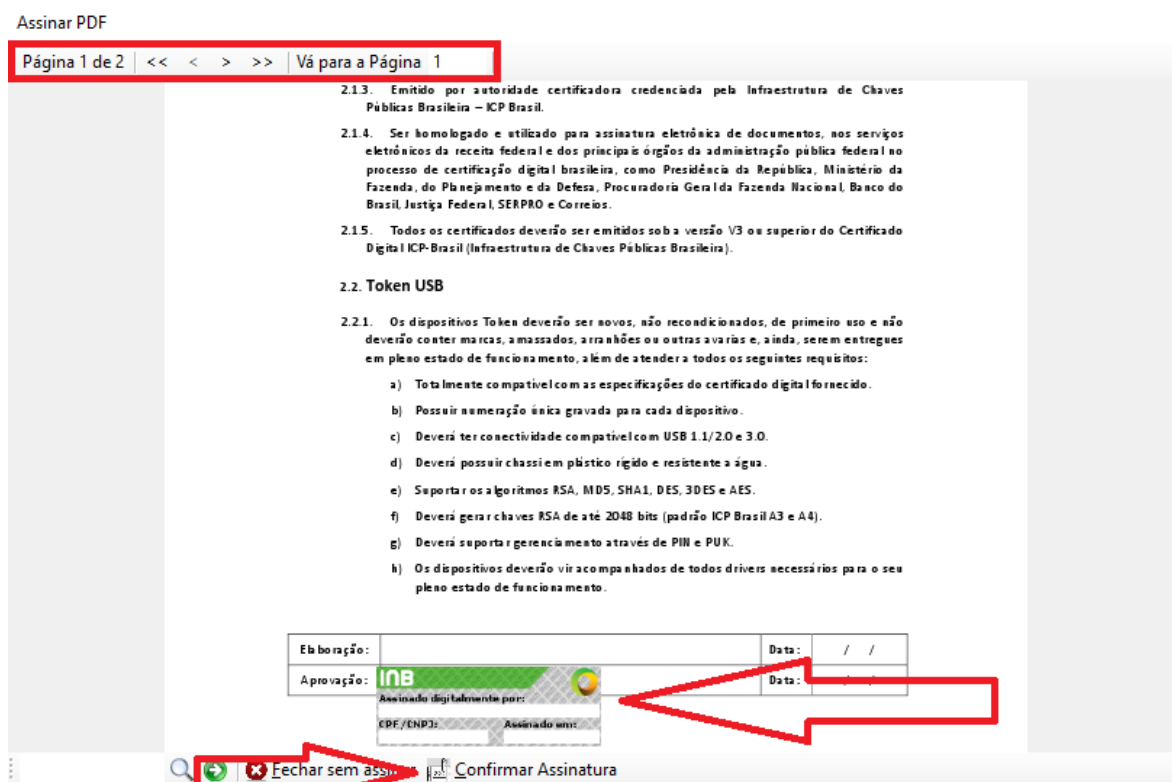
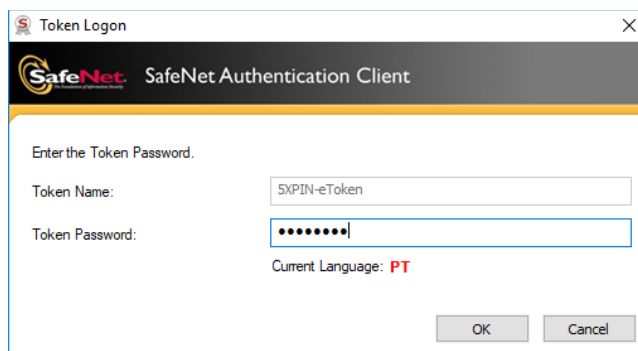


Figura 7: Tela de seleção do certificado

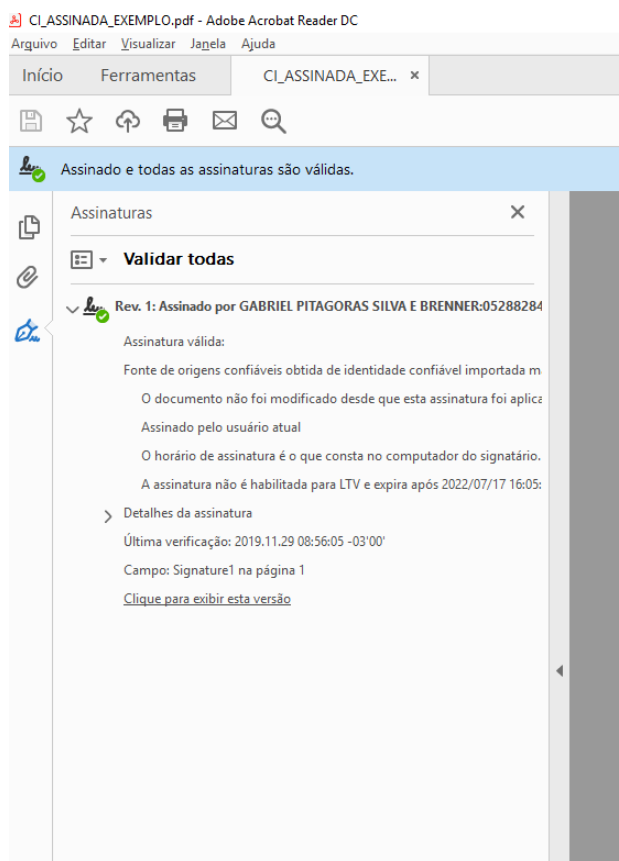


Ao selecionar o certificado, a senha cadastrada junto a unidade certificadora será solicitada. A senha é pessoal e intransferível e, em hipótese alguma, deve ser passada a outra pessoa. A seleção da senha está ilustrada na Figura 8.



*Figura 8: Tela de solicitação da senha do certificado*

Após assinar o PDF, uma cópia do arquivo será gerada, na mesma pasta do arquivo original ou, caso seja uma assinatura gerada diretamente através de uma integração com um Sistema, uma nova versão do arquivo será colocada automaticamente nos anexos. O arquivo PDF, ao ser aberto pelo software “Acrobat Reader”, permite ver na aba assinaturas, todas as assinaturas, conforme ilustrado na Figura 9.



*Figura 9: Painel de assinaturas do PDF Reader*

Para que as assinaturas sejam validadas pelo Acrobat Reader, a cadeia de certificação precisa estar instalada na máquina. Caso ocorra algum problema nessa validação é necessário acionar o Help Desk através do Ramal 8799, para que o mesmo seja resolvido.

Nas informações da assinatura, consta a data/hora que foi assinado, a identidade de quem

assinou e informações se o documento foi modificado ou não. Como o algoritmo de geração da assinatura utiliza o resumo do documento e a chave criptográfica do certificado para gerar a assinatura, **existe a garantia que o documento original não foi alterado**, enquanto as assinaturas forem válidas.

## 4.5 VALIDANDO ASSINATURAS

### 4.5.1 Validando pelo Site do ITI

O site Verificador de Conformidade do ITI (<https://verificador.iti.gov.br/>), permite a qualquer usuário conectado à Internet, independentemente de qualquer aplicativo instalado em seu computador, validar arquivos assinados digitalmente. Para isso, abra o portal de validação do Verificador de Conformidade do ITI, selecione o PDF assinado e clique no botão “VERIFICAR CONFORMIDADE”, conforme ilustrado na Figura 10.



Figura 10: Site verificador de conformidade do ITI

A Figura 11 ilustra a validação realizada pelo Site da ITI.

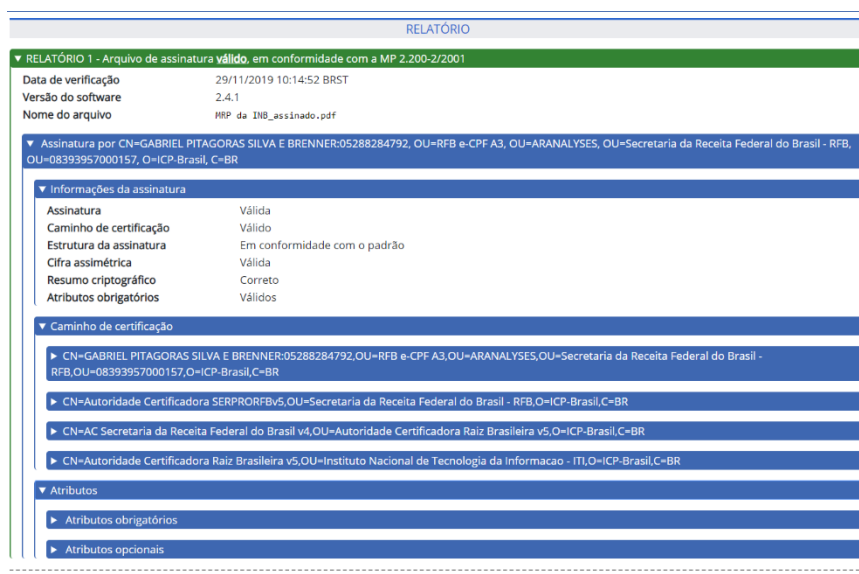


Figura 11: Validação realizada pelo Site do ITI

Cabe ressaltar que a validação do ITI leva em conta todos os aspectos definidos pela PBAD e a política definida na assinatura. Em alguns casos, como o PDF gerado não é na versão 1.7, gerará “problemas de validação” nesse portal, o que não necessariamente invalida a assinatura digital. Por via das dúvidas, valide sempre a assinatura de arquivos que receber assinado digitalmente.

A Figura 12 ilustra uma validação indevida do portal do ITI.

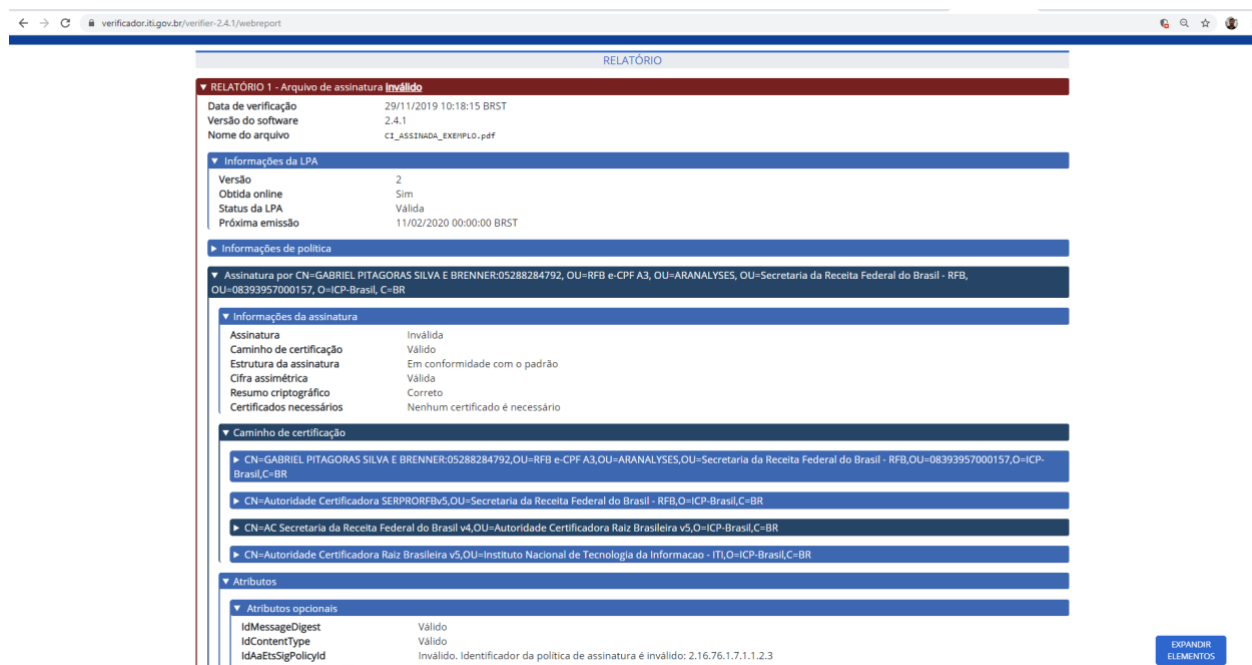


Figura 12: Problema de validação da assinatura no Portal do ITI

Nos atributos opcionais, um dos itens é inválido e, com isso, o portal não valida a assinatura.

## 5 DOCUMENTOS DE REFERÊNCIA

**RECEITA.** Site da Receita Federal. Disponível em

<https://cav.receita.fazenda.gov.br/autenticacao/login>. Acessado em 27/11/2019.

**DOC-ICP-15v3.** VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL.

[https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/15/DOC-ICP-15 - Versao 3.0 VISAO GERAL SOBRE ASSIN DIG NA ICP-BRASIL\\_25-08-2015.pdf](https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/15/DOC-ICP-15_-_Versao_3.0_VISAO_GERAL SOBRE ASSIN DIG NA ICP-BRASIL_25-08-2015.pdf), acessado em 27/11/2019.

**VERIFICADOR DE CONFORMIDADE.** Verificador de Conformidade do ITI. Disponível em:

<https://verificador.iti.gov.br/verifier-2.4.1/>. Acessado em 27/11/2019.

**ACESSO VERIFICADOR.** ITI disponibiliza verificador de assinaturas digitais para a sociedade brasileira com agilidade e segurança. Disponível em


<https://www.iti.gov.br/component/content/article?id=4048>. Acessado em 28/11/2019.

**ETSI.org.** Disponível em:

[https://www.etsi.org/deliver/etsi\\_en/319100\\_319199/31914202/01.01.01\\_60/en\\_31914202v010101p.pdf](https://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf). Acessado em: 28/11/2019.

## 6 ANEXOS

### 6.1 ANEXO 1 - TERMO DE REFERÊNCIA ASSINADO DE EXEMPLO.

	TERMO DE REFERÊNCIA PARA AQUISIÇÃO DE MATERIAIS	GERTI.F
		Rev. 0
		Pág. 1/2
RMS GERTI.F-2020/05/00029 – Adesão ao convênio SIGEP/SERPRO para emissão de Certificados Digitais e-CPF		

#### TERMO DE REFERÊNCIA

##### 1. OBJETO

- 1.1. Fornecimento de certificados digitais conforme condições, quantidades e características estabelecidas no presente Termo de Referência.

ITEM	DESCRIÇÃO	VALIDADE	QUANTIDADE
01	Certificados Digitais e-CPFs	36 MESES	4000
02	Token USB	-	1300

##### 2. ESPECIFICAÇÃO TÉCNICA

###### 2.1. Certificados digitais e-CPF A3 Token USB


- 2.1.1. Os certificados e-CPF (Autoridade Certificadora Raiz ICP-Brasil) deverão ser do tipo A3.
- 2.1.2. Validade de 03 (três) anos, contados a partir da data do aceite definitivo do certificado.
- 2.1.3. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP Brasil.
- 2.1.4. Ser homologado e utilizado para assinatura eletrônica de documentos, nos serviços eletrônicos da receita federal e dos principais órgãos da administração pública federal no processo de certificação digital brasileira, como Presidência da República, Ministério da Fazenda, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco do Brasil, Justiça Federal, SERPRO e Correios.
- 2.1.5. Todos os certificados deverão ser emitidos sob a versão V3 ou superior do Certificado Digital ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira).

###### 2.2. Token USB

- 2.2.1. Os dispositivos Token deverão ser novos, não reconicionados, de primeiro uso e não deverão conter marcas, amassados, arranhões ou outras avarias e, ainda, serem entregues em pleno estado de funcionamento, além de atender a todos os seguintes requisitos:
- a) Totalmente compatível com as especificações do certificado digital fornecido.
  - b) Possuir numeração única gravada para cada dispositivo.
  - c) Deverá ter conectividade compatível com USB 1.1/2.0 e 3.0.
  - d) Deverá possuir chassi em plástico rígido e resistente a água.
  - e) Suportar os algoritmos RSA, MD5, SHA1, DES, 3DES e AES.
  - f) Deverá gerar chaves RSA de até 2048 bits (padrão ICP Brasil A3 e A4).
  - g) Deverá suportar gerenciamento através de PIN e PUK.
  - h) Os dispositivos deverão vir acompanhados de todos drivers necessários para o seu pleno estado de funcionamento.

Elaboração:		Data:	/ /
Aprovação:		Data:	/ /

## 6.2 ANEXO 2 – JUSTIFICATIVA TÉCNICA ASSINADA DE EXEMPLO.

	<b>JUSTIFICATIVA TÉCNICA</b>	<b>NÚMERO DE RMS</b> 2020/01/00001	
		<b>Data:</b> 08/01/2020	<b>Página:</b> 1/1
Manutenção corretiva dos Relógios de Ponto			

Manutenção corretiva nos relógios de ponto de Resende, totalizando R\$ 4.615,69, sendo esse valor referente a troca das peças abaixo:

- 1) Printpoint II Nº 300037015320, Pat. 226695
  - a) placa controladora
  - b) fonte
- 2) Printpoint II Nº 3001000043201, Pat. 229088
  - a) placa controladora
  - b) fonte
- 3) Printpoint II Nº 300037015320, Pat. 226696
  - a) leitor de biometria

A manutenção foi solicitada pelo representante da área de recursos humanos, e autorizada a execução pela GERTI.F.

De acordo com a cláusula contratual 1.5.1, a REALDI está autorizada a trocar peças defeituosas visando manter o perfeito funcionamento dos equipamentos.



Gabriel Pitágoras Silva e Brenner  
 Coordenador de Sistemas de Informação, Processos e Gestão Documental – COSIG.F

---

Coordenador de Sistemas de Informação,  
Processos e Gestão Documental – COSIG.F