

INSTRUÇÃO NORMATIVA ITI N° 17, DE 18 DE NOVEMBRO DE 2020

Aprova a versão 1.0 do documento Rede de Carimbo do Tempo na ICP-Brasil – Recursos Técnicos DOC-ICP-11.01.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9º do anexo I do Decreto nº 8.985, de 8 de fevereiro de 2017, pelo art. 1º da [Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004](#), e pelo art. 2º da [Resolução nº 163 do Comitê Gestor da ICP-Brasil, de 17 de abril de 2020](#),

CONSIDERANDO a necessidade de avanço para protocolo aberto de carimbo do tempo,

RESOLVE:

Art. 1º Aprovar a versão 1.1 do documento DOC-ICP-11.01 – Rede de Carimbo do Tempo na ICP-Brasil – Recursos Técnicos. [\(Redação dada pela Instrução Normativa ITI nº 19, de 2021\)](#)

Art. 2º Esta Instrução Normativa entra em vigor em 1º de dezembro de 2020.

CARLOS ROBERTO FORTNER



Infraestrutura de Chaves Públicas Brasileira

ANEXO

REDE DE CARIMBO DO TEMPO NA ICP-BRASIL RECURSOS TÉCNICOS

DOC-ICP-11.01

Versão 1.1

(Redação dada pela Instrução Normativa ITI nº 19, de 2021)

10 de novembro de 2021

(Redação dada pela Instrução Normativa ITI nº 19, de 2021)



Infraestrutura de Chaves Públicas Brasileira

SUMÁRIO

CONTROLE DE ALTERAÇÕES	3
LISTA DE SIGLAS E ACRÔNIMOS.....	4
1 INTRODUÇÃO	5
2 SINCRONISMO DO TEMPO.....	5
3 AUDITORIA	6
4 ASPECTOS DE SEGURANÇA.....	7
5 DOCUMENTOS DA ICP-BRASIL	8
6 REFERÊNCIAS.....	9



Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Instrução Normativa ITI nº 19, de 10.11.2021 Versão 1.1	2.1, alínea “b”	Adequação aos novos protocolos de sincronismo e auditoria da Rede de Carimbo do Tempo da ICP-Brasil.
Instrução Normativa ITI nº 17, de 18.11.2020 Versão 1.0		Aprova a versão 1.0 do documento Rede de Carimbo do Tempo na ICP-Brasil – Recursos Técnicos.



Infraestrutura de Chaves Públicas Brasileira

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
AS	Sistemas Autônomos
EAT	Entidade de Auditoria do Tempo
ETSI	<i>European Telecommunication Standard Institute</i>
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	<i>Internet Engineering Task Force</i>
MSC	Módulo de Segurança Criptográfico
RCT	Rede de Carimbo do Tempo da ICP-Brasil
RFC	<i>Request For Comments</i>
SAS	Sistemas de Auditoria e Sincronismo
SCT	Sistema de Carimbo do Tempo
TLS	<i>Transport Layer Security</i>



Infraestrutura de Chaves Públicas Brasileira

1 INTRODUÇÃO

1.1 Este documento faz parte de um conjunto de normativos criados para regulamentar a geração e uso de carimbos do tempo no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. Tal conjunto se compõe dos seguintes documentos:

- a) VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL [1];
- b) REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL [2];
- c) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [3];
- d) PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [4]; e
- e) REDE DE CARIMBO DO TEMPO NA ICP-BRASIL – RECURSOS TÉCNICOS, este documento.

1.2 Este documento foi elaborado com base nas normas da ICP-Brasil, nas RFC 3628 e 3161 do IETF e no documento TS 101861 do ETSI.

1.3 Este documento define recursos técnicos adotados para a Rede de Carimbo do Tempo da ICP-Brasil - RCT, como protocolos para sincronismo, auditoria e outros aspectos de segurança.

2 SINCRONISMO DO TEMPO

2.1 Os recursos usados para manter o sincronismo dos relógios dos equipamentos que compõem a Rede de Carimbo do tempo da ICP-Brasil são os seguintes:

- a) o sincronismo entre a FCT e o SAS deve empregar o protocolo PTPv2.1 – IEEE 1588v2-2008, com uso de estampas do tempo produzidas pelo hardware das interfaces de rede (*hardware timestamping*);
- b) o sincronismo dos relógios dos SCT com o SAS deve ocorrer permanentemente, em períodos variáveis definidos e iniciados por equipamento da EAT, utilizando o protocolo PTPv2 – IEEE 1588v2-2008. A fim de prover a autenticação de dados no Protocolo PTP, deve-se associá-lo a mecanismos que garantam a criação de conexão segura e cifrada por meio do protocolo TLS entre servidor (SAS) e cliente (SCT). O sincronismo entre SAS e SCT deve ser permitido somente para equipamentos autorizados. ([Redação dada pela Instrução Normativa ITI nº 19, de 2021](#))

2.2 Os SCT devem gerar Árvores de Encadeamento do Tempo, que é uma estrutura de encadeamento de carimbos do tempo e dados sincronismo empregando recursos criptográficos baseados em Árvores de Merkle;

2.2.1 O SCT, ao receber um novo alvará, inicia uma nova Árvore;

2.2.2 Cada Árvore, indexada por 1 (um) alvará, formará um bloco, o qual conterá:

- i. estampa do tempo de finalização do bloco;
- ii. o número sequencial do bloco [bloco gênese terá o número 0 (zero)];



Infraestrutura de Chaves Públicas Brasileira

- iii. quantos nós (transações) aconteceram no bloco;
- iv. tamanho em bits do bloco;
- v. a raiz de *Merkle* da árvore;
- vi. o resumo criptográfico do bloco anterior;
- vii. o resumo criptográfico do bloco atual, resultado das alíneas ‘i’ a ‘vi’.

2.2.3 Os nós da Árvore de Encadeamento do Tempo deverão ser construídos da seguinte forma:

- i. cada operação de sincronismo deverá ter seus dados de estampa do tempo no SCT (*timestamp*), desvio médio (offset) e atraso médio (delay), resumidos criptograficamente e registrados em 1 (um) nó da árvore;
- ii. cada carimbo do tempo emitido pelo SCT deve ser resumido criptograficamente e registrado em 1 (um) nó da árvore;
- iii. os registros acontecem sequencialmente e os nós devem ter um indexador, também sequencial, com a localização do mesmo na Árvore de Merkle.

2.2.4 O algoritmo de resumo criptográfico deve ser SHA-256, descrito no DOC-ICP-01.01 [5].

2.3 Os dados usados para gerar os resumos criptográficos da Árvore deverão ser armazenados em registros de eventos (logs), com indexador de cada nó da árvore ao qual ele pertence;

2.4 Ao receber novo alvará, a Árvore de Encadeamento do Tempo é finalizada e consolidada.

3 AUDITORIA

3.1 O processo de auditoria realizado pelo SAS deve ser composto das seguintes etapas:

- a) O SAS envia alvará ao SCT;
- b) O SCT recebe alvará e inicia, com este alvará, nova Árvore de Encadeamento do Tempo;
- c) O SAS solicita os dados usados para gerar os resumos criptográficos que compõe a árvore de encadeamento encerrada pelo SCT;
- d) O SCT envia os dados do item c) ao SAS para análise, junto a respectiva Árvore de Encadeamento do Tempo;
- e) Para emissão de alvará o SAS deve avaliar a precisão e exatidão do relógio do SCT por meio de avaliação estatística dos dados da alínea c);
- f) O resultado final do processo de auditoria é a emissão pela EAT, através do SAS, de um alvará que permite ao SCT continuar operando por mais um período de tempo, se seu relógio estiver dentro dos padrões pré-definidos, ou, caso contrário, de um alvará com prazo de validade igual a zero, o que significa que o SCT não poderá emitir carimbos do tempo até ter seu relógio novamente sincronizado com a FCT. Os principais atributos do alvará são: ano, mês, dia, hora, minuto, segundo, compensação e retardo.



Infraestrutura de Chaves Públicas Brasileira

3.2 O envio de dados de auditoria será realizado com uso do Protocolo WebSocket (RFC 6455 e atualizações) encapsulado pelo Protocolo *Transport Layer Security* (TLS) v 1.3 ou posterior (RFC 8446 e atualizações).

3.3 Os SCT deverão dispor de recurso para envio das Árvores de Encadeamento do Tempo

4 ASPECTOS DE SEGURANÇA

4.1 Aspectos Gerais de Segurança da Entidade de Auditoria do Tempo

A AC Raiz da ICP-Brasil, como Entidade de Auditoria do Tempo, obriga-se a:

- a) adotar medidas de segurança física, lógica e de pessoal compatíveis, no mínimo, com as estabelecidas para as Autoridades de Carimbo do Tempo da ICP- BRASIL;
- b) utilizar, para as operações de auditoria e sincronismo da Rede de Carimbo do Tempo da ICP-Brasil, SASs cujos MSCs associados possuam capacidade de processamento criptográfico para geração de chaves e realização de assinaturas digitais;
- c) manter os relógios de seus SASs sincronizados com a FCT;
- d) garantir que a emissão dos alvarás seja feita em conformidade com o tempo constante do relógio interno do SAS e que a assinatura digital do alvará seja realizada dentro do MSC a ele associado;
- e) manter seus SASs com disponibilidade mínima de 99% do tempo;
- f) analisar e emitir relatórios dos registros de auditoria e sincronismo dos SASs;
- g) utilizar, em seus SAS, somente certificados digitais ICP-Brasil para assinatura de alvarás;
- h) identificar e registrar as ações que executar, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil;
- i) dispor no mínimo de duas linhas de comunicação com a Internet, providas por diferentes sistemas autônomos (AS).



Infraestrutura de Chaves Públicas Brasileira

5 DOCUMENTOS DA ICP-BRASIL

5.1 Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL Aprovado pela Resolução nº 58, de 28 de novembro de 2008	DOC-ICP-11
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	DOC-ICP-12
[3]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL Aprovado pela Resolução nº 60, de 28 de novembro de 2008	DOC-ICP-13
[4]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL Aprovado pela Resolução nº 61, de 28 de novembro de 2008	DOC-ICP-14

5.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

REF.	NOME DO DOCUMENTO	CÓDIGO
[5]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL Aprovado pela Instrução Normativa nº 04, de 18 de maio de 2006	DOC-ICP-01.01



Infraestrutura de Chaves Públicas Brasileira

6 REFERÊNCIAS

- RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), august 2001.*
- RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, november 2003.*
- RFC 6455, IETF - The WebSocket Protocol, December 2011*
- RFC 8446, IETF - The Transport Layer Security (TLS) Protocol Version 1.3, august 2018*
- ETSI TS 101.861 - v 1.2.1 Technical Specification / Time Stamping Profile, march 2002.*