Infraestrutura de Chaves Públicas Brasileira

PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL

DOC-ICP-14

Versão 2.0

17 de agosto de 2020

Sumário

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
Resolução nº 174, de 17/08/2020		Revisão e consolidação do DOC-ICP 14, conforme Decreto nº 10.139, de 28 de novembro de 2019. Definição de novo protocolo aberto de carimbo do tempo para a ICP-Brasil.
Resolução nº 112, de 30/09/2015	5. Referências	Retira as referências a Lei 2.784, de 18.06.1913, e ao Decreto 10.546, de 05.11.1918.
Resolução nº 69, de 13/10/2009	3; 3.1; 3.1.1; 3.1.1.1; 3.1.1.2; 3.1.2; 3.1.2.1.	Aprova a versão 1.1 dos documentos que regulamentam a geração e uso de carimbo do tempo no âmbito da ICP-Brasil.
Resolução nº 61, de 28/11/2008		Aprova a versão 1.0 do Documento Procedimentos para Auditoria do Tempo na ICP-Brasil.

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC RAIZ	Autoridade Certificadora Raiz da ICP-BRASIL
ACT	Autoridade de Carimbo do Tempo
ASCII	*American Stardard Code for Information Interchange*
EAT	Entidade de Auditoria do Tempo
ETSI	*European Telecommunication Standard Institute*
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force*
PCT	Política de Carimbo do Tempo
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
SAS	Sistemas de Auditoria e Sincronismo
SCT	Servidor de Carimbo do Tempo
UTC	*Universal Time Coordinated*
UTF	*Unicode Tranformation Format*

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]**, documento aprovado pela Resolução nº 58, de 28 de novembro de 2008;

b) **REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL [2]**, aprovado pela Resolução nº 59, de 28 de novembro de 2008;

c) **REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [3],** documento aprovado pela Resolução nº 60, de 28 de novembro de 2008;

d) **PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL** - este documento, aprovado pela Resolução nº61, de 28 de novembro de 2008

1.2 Um carimbo do tempo aplicado a um documento eletrônico é uma evidência que ele foi criado antes da data incluída no carimbo do tempo. Os carimbos do tempo são emitidos por terceiras partes confiáveis, as Autoridades de Carimbo do Tempo (ACTs), cujas operações devem ser devidamente documentadas e periodicamente auditadas pela Entidade de Auditoria do Tempo (EAT) da ICP-Brasil.

1.3 A utilização de carimbos do tempo no âmbito da ICP-Brasil é facultativa. Documentos eletrônicos assinados digitalmente com chave privada correspondente a certificados ICP-Brasil são válidos com ou sem o carimbo do tempo.

1.4 Os relógios dos Servidores de Carimbo do Tempo (SCTs), utilizados pelas ACTs devem ser auditados e sincronizados pela EAT da ICP-Brasil. Este documento trata desse processo de auditoria, realizado pela EAT em todos os SCTs que pertencem às ACTs credenciadas junto à ICP-Brasil.

1.5 Ele tem como base as normas da ICP-Brasil, as RFC 3628 e 3161, do IETF, e o documento TS 101861 do ETSI.

1.6 Aplicam-se ainda às ACTs da ICP-Brasil e a seus Prestadores de Serviço de Suporte (PSS), no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil, entre os quais destacamos:

a) **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**, documento aprovado pela Resolução nº 02, de 25 de setembro de 2001;

b) **CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5]**, documento aprovado pela Resolução nº 06, de 22 de novembro de 2001;

c) **CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]**, documento aprovado pela Resolução nº 24, de 29 de agosto de 2003;

d) **CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7]**, documento aprovado pela Resolução nº 25, de 24 de outubro de 2003;

e) **POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [8]**, documento aprovado pela Resolução nº10, de 14 de fevereiro de 2002; e

f) **REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [9]**, documento aprovado pela Resolução nº 36 de 21 de outubro de 2004.

2 PROCESSO DE AUDITORIA E SINCRONISMO

2.1 Descrição Sumária do Processo

2.1.1 A auditoria do relógio do SCT consiste na sua avaliação periódica pela EAT, para verificar se ele está sincronizado com a Fonte Confiável do Tempo (FCT), ou se encontra-se dentro de um erro máximo pré-definido, avaliando sua precisão e exatidão em relação ao horário UTC.

2.1.2 Para sincronizar o relógio do SCT com a FCT serão realizados procedimentos especificados em regulamento editado por instrução normativa da AC Raiz.

2.1.3 Somente serão considerados aptos a emitir carimbo do tempo os equipamentos diretamente monitorados pela EAT que se mantenham dentro dos padrões de comportamento previamente estabelecidos pela Política de Carimbo do Tempo (PCT) da Autoridade de Carimbo do Tempo (ACT).

2.1.4 A EAT audita e sincroniza os relógios dos SCTs por meio dos sistemas denominados Sistemas de Auditoria e Sincronismo (SAS). A comunicação entre os SASs e os SCTs, o envio de dados e o procedimento de auditoria devem seguir as especificações descritas em regulamento editado por instrução normativa da AC Raiz.

2.2 Procedimentos da EAT

2.2.1 Nesta seção são apresentados os procedimentos realizados pela EAT para a auditoria e sincronismo dos relógios dos SCTs.

2.2.2 A EAT disponibilizará às ACTs cópia dos certificados digitais de seus SAS, para permitir a autenticação mútua SAS-SCT.

2.2.3 Após a colocação do SCT em operação, a EAT deverá:

a) auditar periodicamente os SCTs, a fim de verificar o funcionamento dentro dos parâmetros estatísticos de sincronismo estabelecidos nas PCTs;

b) emitir alvarás, respeitando o período descrito no item a) habilitando o funcionamento dos SCTs;

c) informar à ACT, por meio de mensagem eletrônica, o motivo da impossibilidade da emissão de um alvará para um SCT;

d) analisar e emitir relatórios dos registros de auditoria e sincronismo do relógio do SCT, usando os dados registrados no SAS;

e) pelo menos 2 (dois) dias úteis antes da expiração do certificado do SAS, providenciar novo certificado e disponibilizá-lo às ACTs.

2.3 Procedimentos das Autoridades de Carimbo do Tempo

2.3.1 Nesta seção são apresentados os procedimentos que devem ser realizados pela ACT para permitir a auditoria e o sincronismo dos relógios de seus SCTs.

2.3.2 Antes de colocar em operação seus SCTs, a ACT deve:

a) solicitar os serviços da Rede de Carimbo do Tempo da ICP-Brasil para cada relógio de SCT que emita carimbos do tempo no âmbito da ICP-Brasil;

b) contratar o fornecimento dos meios de comunicação e dos equipamentos necessários para ligar seus SCTs à Rede de Carimbo do Tempo da ICP-Brasil;

c) enviar à AC Raiz cópia dos certificados digitais de seus SCTs, para permitir a autenticação mútua SAS-SCT.

2.3.3 Após a colocação do SCT em operação, a ACT deverá:

a) utilizar, em seus SCTs, somente certificados digitais ICP-Brasil específicos para equipamentos de carimbo do tempo;

b) pelo menos 2 (dois) dias úteis antes da expiração do certificado do SCT, providenciar novo certificado e enviá-lo à AC Raiz.

3 REQUISITOS OPERACIONAIS

3.1 Esta seção trata do conteúdo dos arquivos que serão gerados durante as auditorias na Rede de Carimbo do Tempo da ICP-Brasil.

3.2 Arquivos Gerados nas Auditorias

3.2.1 As operações de autenticação mútua e sincronismo gerarão arquivos codificados em UTF-8 (ou ASCII) nos SASs e SCTs, contendo dados resultantes destas operações.

3.2.1.1 Dados Referentes à Autenticação Mútua

3.2.1.1.1 Os arquivos de registro do SAS devem conter no mínimo as seguintes informações:

a) data e hora de realização da autenticação;
b) endereço de rede do SAS;

c) endereço de rede do SCT;
d) identificação do certificado digital do SCT;
e) identificação do alvará;
f) mensagem de aviso ou de erro.

3.2.1.1.2 Os arquivos de registro do SCT devem conter as seguintes informações:
a) data e hora de realização da autenticação;
b) endereço de rede do SAS;
c) endereço de rede do SCT;
d) identificação do certificado digital do SAS;
e) identificação do alvará;
f) mensagem de aviso ou de erro.

3.2.1.2 Dados Referentes ao Sincronismo

3.2.1.2.1 Os arquivos de registro do SAS e do SCT devem conter no mínimo as seguintes informações:
a) data e hora de realização do sincronismo;
b) erro do relógio do SCT (*Offset*);
c) retardo (*Delay*);
d) endereço de rede do SAS;
e) endereço de rede do SCT.

4 DOCUMENTOS DA ICP-BRASIL

4.1 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**	DOC-ICP-11
[2]	**REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL**	DOC-ICP-12
[3]	**REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL**	DOC-ICP-13
[4]	**POLÍTICA DE SEGURANÇA DA ICP-BRASIL**	DOC-ICP-02
[5]	**CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL**	DOC-ICP-03
[6]	**CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL**	DOC-ICP-08
[7]	**CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL**	DOC-ICP-09
[8]	**POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL**	DOC-ICP-06
[9]	**REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL**	DOC-ICP-10

5 REFERÊNCIAS

RFC 3161, IETF - *Public Key Infrastructure Time Stamp Protocol* (TSP), agosto de 2001.
RFC 3628, IETF - *Policy Requirements for Time Stamping Authorities*, November 2003.
ETSI TS 101 861 - v 1.2.1 *Technical Specification / Time Stamping Profile*, março de 2002.