



Infraestrutura de Chaves Públicas Brasileira

**PROCEDIMENTOS PARA
AUDITORIA DO TEMPO
NA ICP-BRASIL**

DOC-ICP-14

versão 1.1

13 de outubro de 2009

Sumário

1. INTRODUÇÃO.....	4
2. PROCESSO DE AUDITORIA E SINCRONISMO.....	5
3. REQUISITOS OPERACIONAIS.....	7
4. DOCUMENTOS DA ICP-BRASIL.....	7
5. REFERÊNCIAS.....	9



Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

<i>Resolução ou IN que aprovou alteração</i>	<i>Item Alterado</i>	<i>Descrição da Alteração</i>
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.



Infraestrutura de Chaves Públicas Brasileira

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC-RAIZ	Autoridade Certificadora Raiz da ICP-BRASIL
ACT	Autoridade de Carimbo do Tempo
ASCII	<i>American Standard Cod for Information Interchange</i>
CG	Comitê Gestor da ICP-BRASIL
EAT	Entidade de Auditoria do Tempo
ETSI	<i>European Telecommunication Standard Institute</i>
FCT	Fonte Confiável de Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	<i>Internet Engineering Task Force</i>
ITI	Instituto Nacional de Tecnologia da Informação
NCT	<i>Internet Engineering Task Force</i>
NTP	Network Time Protocol
PCT	Política de Carimbo do Tempo
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
SAS	Sistemas de Auditoria e Sincronismo
SCT	Sistemas de Carimbo do Tempo



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 - este documento.**

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 AC-Raiz 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 Sistemas de Carimbo do Tempo (SCTs), utilizados pelas ACTs devem ser auditados e sincronizados pela AC Raiz, que é a Entidade de Auditoria do Tempo (EAT), no âmbito da ICP-Brasil. Este documento trata desse processo de auditoria, realizado pela AC Raiz 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];**
- b) **CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5];**
- c) **CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6];**



Infraestrutura de Chaves Públicas Brasileira

- d) **CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7];**
- e) **POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [8];**
- f) **REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [9].**

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 AC Raiz, para verificar se ele está sincronizado com a Fonte Confiável de Tempo (FCT), ou se se encontra dentro de um erro máximo pré-definido. Caso não esteja, serão realizadas tentativas de re-sincronizar o relógio do SCT.

2.1.2. Somente serão considerados sincronizados os equipamentos diretamente monitorados pela AC Raiz que se mantenham dentro dos padrões de comportamento previamente estabelecidos pela Política de Carimbo do Tempo (PCT) da Autoridade de Carimbo do Tempo (ACT).

2.1.3. O resultado final do processo de auditoria e sincronismo é a emissão, pela AC Raiz, 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 de tempo até ter seu relógio novamente sincronizado com a FCT.

2.1.4. A AC Raiz audita e sincroniza os relógios dos SCTs através de equipamentos denominados Sistemas de Auditoria e Sincronismo (SAS). A comunicação entre os SASs e os SCTs deve ser feita através de um protocolo que prevê a autenticação mútua baseada em certificados digitais e o uso de protocolos para o sincronismo do relógio tal como o Network Time Protocol (NTP).

2.1.5. Adicionalmente, a AC Raiz tem acesso a uma interface de auditoria dos SCTs para verificação dos registros produzidos.

2.2. Procedimentos da AC Raiz

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

2.2.2. A AC Raiz 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 AC Raiz deverá:



Infraestrutura de Chaves Públicas Brasileira

- a) auditar periodicamente o relógio dos SCTs, em período tal que o erro máximo acumulado não ultrapasse o valor especificado na PCT correspondente;
- b) emitir alvarás, respeitando o período descrito no item a) habilitando o funcionamento dos SCTs;
- c) informar à ACT, através 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 de tempo no âmbito da ICP-Brasil;
- b) contratar o fornecimento dos meios de comunicação e dos equipamentos necessários para ligar seus SCTs à rede Rede de Carimbo do Tempo da ICP-Brasil;
- c) utilizar somente equipamentos homologados pela ICP-Brasil ou por entidades por ela autorizadas;
- d) 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.

2.4. Auditoria e Sincronismo

2.4.1. A AC Raiz, por intermédio dos seus SASs, deverá realizar auditorias automáticas nos relógios dos SCTs, verificando o seu correto funcionamento. No final dessas auditorias, o SCT recebe um alvará que autorizará ou não o seu funcionamento.

2.4.2. O intervalo entre auditorias será fixado pela AC Raiz, de forma que o erro máximo acumulado pelo relógio do SCT não ultrapasse o valor máximo estabelecido na



Infraestrutura de Chaves Públicas Brasileira

PCT da ACT. Se a correção ou o atraso de rede ultrapassar esse valor, o SCT não receberá permissão para funcionar.

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. Dados Referentes à Autenticação Mútua

3.2.1.1. 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.

3.2.1.2. 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.

3.1.2. Dados Referentes ao Sincronismo

3.1.2.1 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;
- c) retardo;
- d) endereço de rede do SAS;
- e) endereço de rede do SCT.



Infraestrutura de Chaves Públicas Brasileira

4. DOCUMENTOS DA ICP-BRASIL

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.itl.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

BRASIL, Lei nº 2.784, de 18 de junho de 1913 – determina a Hora Legal no Brasil.

BRASIL, Decreto nº 10.546, de 05 de novembro de 1918 - aprova o Regulamento da Lei nº 2.784.

BRASIL, Decreto nº 4.264, de 10 de junho de 2002 - Restabelece e Modifica o Regulamento anterior.

BRASIL, Lei nº 9.933, de 20 de dezembro de 1999 - Dispõe sobre o Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (CONMETRO) e sobre o Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO).

RFC 1305, IETF - Network Time Protocol version 3.0.

RFC 2030, IETF - Simple Network Time Protocol (SNTP) version 4.0.

RFC 2527, IETF - Internet X-509 Public Key Infrastructure Certificate Policy and Certifications Practices Frame work, março de 1999.

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.

ETSI TS 102.023 - v 1.1.1 Technical Specification / Policy Requirements for Time Stamping Authorities, abril de 2002.