



**Infraestrutura de Chaves Públicas Brasileira**

**REQUISITOS MÍNIMOS PARA AS  
POLÍTICAS DE CARIMBO DO TEMPO  
DA ICP-BRASIL**

**DOC-ICP-13**

**Versão 2.0**

**17 de agosto de 2020**

## Sumário

CONTROLE DE ALTERAÇÕES.....	2
1 INTRODUÇÃO.....	3
1.1 Visão Geral.....	3
1.2 Identificação.....	4
1.3 Participantes da ICP-Brasil.....	4
1.4 Usabilidade do Certificado.....	5
1.5 Política de Administração.....	5
1.6 Definições e Acrônimos.....	6
2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO.....	7
3 IDENTIFICAÇÃO E AUTENTICAÇÃO.....	7
4 REQUISITOS OPERACIONAIS.....	7
4.1 Solicitação de Carimbos do Tempo.....	7
4.2 Emissão de Carimbos do Tempo.....	7
4.3 Aceitação de Carimbos do Tempo.....	8
4.4 Características do carimbo do tempo.....	8
5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES.....	8
6 CONTROLES TÉCNICOS DE SEGURANÇA.....	10
7 PERFIS DOS CARIMBOS DO TEMPO.....	10
8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES.....	10
9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	10
10 DOCUMENTOS DA ICP-BRASIL.....	13
11 REFERÊNCIAS.....	14

## CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	Item Alterado	Descrição da Alteração
Resolução nº 173, de 17/08/2020		Revisão e consolidação do DOC-ICP-13, conforme Decreto nº 10.139, de 28 de novembro de 2019. Adequação da estrutura do documento à RFC 3647.
Resolução nº 112, de 30/09/2015	5. Referências	Retira as referências à Lei nº 2.784, de 18.06.1918, e ao Decreto nº 10.546, de 05.11.1918.
Resolução nº 69, de 13/10/2009	2.2; 2.2.1; 2.2.2; 2.2.3.	Aprova a versão 1.1 dos documentos que regulamentam a geração e uso de carimbo do tempo no âmbito da ICP-Brasil:
Resolução nº 60, de 28/11/2008		Aprova a versão 1.0 do documento Requisitos mínimos para as políticas de carimbo do tempo da ICP-Brasil.

## 1 INTRODUÇÃO

### 1.1 Visão Geral

1.1.1 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]**, documento aprovado pela Resolução nº 59, de 28 de novembro de 2008;
- c) **REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL** - este documento, aprovado pela Resolução nº 60, de 28 de novembro de 2008;
- d) **PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3]**, documento aprovado pela Resolução nº 61, de 28 de novembro de 2008.

1.1.2 Um carimbo do tempo aplicado a uma assinatura digital ou a um documento prova que ele já existia na data incluída no carimbo do tempo. Os carimbos do tempo são emitidos por terceiras partes confiáveis, as Autoridades de Carimbo do Tempo - ACT, cujas operações devem ser devidamente documentadas e periodicamente auditadas pela própria AC Raiz da ICP-Brasil.

1.1.3 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.

1.1.4 O presente documento especifica os requisitos mínimos que devem constar de uma política de carimbo do tempo de um ACT credenciada na ICP-Brasil. O subscritor e as terceiras partes devem consultar a Declaração de Práticas de Carimbo do Tempo (DPCT) da ACT para obter detalhes adicionais sobre precisamente como esta Política de Carimbo do Tempo (PCT) é implementada pela ACT. De modo geral, a política de carimbo do tempo indica "o que deve ser cumprido" enquanto uma declaração de práticas da ACT indica "como cumprir", isto é, os processos que serão usados pela ACT para criar carimbos do tempo e manter a precisão do seu relógio.

1.1.5 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.

1.1.6 Toda PCT elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.

1.1.7 Aplicam-se ainda às entidades que compõem a estrutura de carimbo do tempo na ICP-Brasil, 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 nº 10, 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.

## 1.2 Identificação

1.2.1 Neste item deve ser identificada a PCT e indicado o seu *Object Identifier* (OID). No âmbito da ICP-Brasil, um OID no formato 2.16.76.1.6.n será atribuído à PCT na conclusão do processo de credenciamento da ACT responsável.

1.2.2 Neste item deve ser identificada a DPCT que estabelece os procedimentos adotados pela ACT para emissão de carimbos do tempo emitidos segundo a PCT. Deve também ser indicado o seu OID, no formato 2.16.76.1.5.n, o qual será atribuído à DPCT na conclusão do processo de credenciamento da ACT responsável.

## 1.3 Participantes da ICP-Brasil

### 1.3.1 Autoridades de Carimbo do tempo

Neste item deve ser identificada a ACT integrante da ICP-Brasil a que se refere esta PCT.

### 1.3.2 Prestador de Serviços de Suporte

1.3.2.1 Neste item deve ser identificado o endereço da página web (URL) onde está publicada a relação de todos os PSSs vinculados à ACT responsável, se houver.

1.3.2.2 PSS são entidades utilizadas pela ACT para desempenhar atividade descrita nesta DPCT ou

na PCT e se classificam em três categorias, conforme o tipo de atividade prestada:

- a) disponibilização de infraestrutura física e lógica;
- b) disponibilização de recursos humanos especializados; ou
- c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.2.3 A ACT responsável deverá manter as informações acima sempre atualizadas.

### **1.3.3 Subscritores**

1.3.3.1 Neste item devem ser caracterizadas as entidades - pessoas físicas ou jurídicas - que poderão solicitar carimbos do tempo emitidos segundo esta PCT.

### **1.3.4 Partes confiáveis**

1.3.4.1 Considera-se terceira parte aquela que confia no teor, validade e aplicabilidade do carimbo do tempo.

## **1.4 Usabilidade do Certificado**

1.4.1 Este item da PCT deve relacionar as aplicações para as quais são adequados os carimbos emitidos pela ACT e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses carimbos.

## **1.5 Política de Administração**

Neste item devem ser incluídos nome, endereço e outras informações da ACT responsável pela PCT. Devem ser também informados o nome, os números de telefone e endereço eletrônico de uma pessoa para contato.

### **1.5.1 Organização administrativa do documento**

Nome da ACT.

### **1.5.2 Contatos**

Endereço:

Telefone:

Fax:

Página web:

E-mail:

Outros:

### **1.5.3 Pessoa responsável pela adequabilidade da DPCT e PCT**

Nome:

Telefone:

E-mail:

Outros:

#### 1.5.4 Procedimentos de aprovação da PCT

1.5.4.1 Toda PCT deverá ser submetida à aprovação, durante o processo de credenciamento da ACT responsável, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

#### 1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC RAIZ	Autoridade Certificadora Raiz
ACT	Autoridade de Carimbo do Tempo
DPCT	Declarações de Práticas de Carimbo do Tempo
ETSI	<i>European Telecommunication Standard Institute</i>
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	<i>Internet Engineering Task Force</i>
OID	<i>Object Identifiers</i>
PCT	Política de Carimbo do Tempo
PSS	Prestador de Serviço de Confiança
RFC	<i>Request For Comments</i>
SCT	Servidor de Carimbo do Tempo

## **2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO**

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

- 2.1 Publicação de informações da ACT
- 2.2 Frequência de Publicação
- 2.3 Controle de Acesso aos Repositórios

## **3 IDENTIFICAÇÃO E AUTENTICAÇÃO**

Neste item devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

## **4 REQUISITOS OPERACIONAIS**

Neste item devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

### **4.1 Solicitação de Carimbos do Tempo**

Neste item da PCT devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela ACT responsável para as solicitações de emissão carimbo do tempo. Esses requisitos e procedimentos, que deverão ser atendidos e executados pelos subscritores, deverão compreender, no mínimo:

- a) o protocolo de solicitação do carimbo do tempo (http, e-mail, etc.);
- b) os algoritmos de *hash* que poderão ser utilizados pelos subscritores para solicitação do carimbo.

#### **4.1.1 Quem pode submeter uma solicitação de carimbo do tempo**

Neste item devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

#### **4.1.2 Processo de registro e responsabilidades**

Neste item devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

### **4.2 Emissão de Carimbos do Tempo**

Neste item devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

#### 4.3 Aceitação de Carimbos do Tempo

Neste item da PCT devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela ACT responsável para verificação de um carimbo do tempo. Esses requisitos e procedimentos deverão compreender, no mínimo:

- a) forma de conferência do carimbo tempo, pelo subscritor e pela terceira parte, inclusive após a expiração do certificado que o assinou;
- b) algoritmo do *hash* inserido no carimbo do tempo.

#### 4.4 Características do carimbo do tempo

Neste item devem ser informadas as características dos carimbos do tempo que serão emitidos segundo a PCT, contendo, no mínimo:

- a) a exatidão ou precisão mínima do tempo registrado no carimbo;
- b) a unidade utilizada no campo *genTime* do carimbo do tempo (segundos, milissegundos ou microssegundos).

### 5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

- 5.1 Segurança Física
  - 5.1.1 Construção e localização das instalações de ACT
  - 5.1.2 Acesso físico nas instalações de ACT
  - 5.1.3 Energia e ar-condicionado do ambiente de nível 3 da ACT
  - 5.1.4 Exposição à água nas instalações de ACT
  - 5.1.5 Prevenção e proteção contra incêndio nas instalações de ACT
  - 5.1.6 Armazenamento de mídia nas instalações de ACT
  - 5.1.7 Destruição de lixo nas instalações de ACT
  - 5.1.8 Sala externa de arquivos (*off-site*) para ACT
- 5.2 Controles Procedimentais
  - 5.2.1 Perfis qualificados
  - 5.2.2 Número de pessoas necessário por tarefa
  - 5.2.3 Identificação e autenticação para cada perfil
- 5.3 Controles de Pessoal
  - 5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade
  - 5.3.2 Procedimentos de verificação de antecedentes



## Infraestrutura de Chaves Públicas Brasileira

- 5.3.3 Requisitos de treinamento
- 5.3.4 Frequência e requisitos para reciclagem técnica
- 5.3.5 Frequência e sequência de rodízio de cargos
- 5.3.6 Sanções para ações não autorizadas
- 5.3.7 Requisitos para contratação de pessoal
- 5.3.8 Documentação fornecida ao pessoal
- 5.4 Procedimentos de Log de Segurança
  - 5.4.1 Tipos de eventos registrados
  - 5.4.2 Frequência de auditoria de registros (*logs*)
  - 5.4.3 Período de retenção para registros (*logs*) de auditoria
  - 5.4.4 Proteção de registro (*log*) de auditoria
  - 5.4.5 Procedimentos para cópia de segurança (backup) de registro (*log*) de auditoria
  - 5.4.6 Sistema de coleta de dados de auditoria
  - 5.4.7 Notificação de agentes causadores de eventos
  - 5.4.8 Avaliações de vulnerabilidade
- 5.5 Arquivamento de Registros
  - 5.5.1 Tipos de registros arquivados
  - 5.5.2 Período de retenção para arquivo
  - 5.5.3 Proteção de arquivo
  - 5.5.4 Procedimentos para cópia de segurança (backup) de arquivo
  - 5.5.5 Requisitos para datação de registros
  - 5.5.6 Sistema de coleta de dados de arquivo
  - 5.5.7 Procedimentos para obter e verificar informação de arquivo
- 5.6 Troca de chave
- 5.7 Comprometimento e Recuperação de Desastre
  - 5.7.1 Disposições Gerais
  - 5.7.2 Recursos computacionais, software e dados corrompidos
  - 5.7.3 Certificado do SCT é revogado
  - 5.7.4 Chave privada do SCT é comprometida
  - 5.7.5. Calibração e sincronismo do SCT são perdidos
  - 5.7.6. Segurança dos recursos após desastre natural ou de outra natureza

- 5.8 Extinção dos serviços de ACT ou PSS

## **6 CONTROLES TÉCNICOS DE SEGURANÇA**

Neste item devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

## **7 PERFIS DOS CARIMBOS DO TEMPO**

Neste item devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

## **8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES**

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver.

- 8.1 Frequência e circunstâncias das avaliações
- 8.2 Identificação/Qualificação do avaliador
- 8.3 Relação do avaliador com a entidade avaliada
- 8.4 Tópicos cobertos pela avaliação
- 8.5 Ações tomadas como resultado de uma deficiência
- 8.6 Comunicação dos resultados

## **9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS**

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPCT da ACT responsável ou detalhados aspectos específicos para a PCT, se houver. Os itens seguintes com requisitos especificados devem ser atendidos.

- 9.1 Tarifas de Serviço
  - 9.1.1 Tarifas de emissão de carimbos do tempo
  - 9.1.2 Tarifas de acesso ao carimbo do tempo
  - 9.1.3 Tarifas de revogação ou de acesso à informação de status
  - 9.1.4 Tarifas para outros serviços
  - 9.1.5 Política de reembolso
- 9.2 Responsabilidade Financeira
  - 9.2.1 Cobertura do seguro

- 9.3 Confidencialidade da informação do negócio
  - 9.3.1 Escopo de informações confidenciais
  - 9.3.2 Informações fora do escopo de informações confidenciais
  - 9.3.3 Responsabilidade em proteger a informação confidencial
- 9.4 Privacidade da informação pessoal
  - 9.4.1 Plano de privacidade
  - 9.4.2 Tratamento de informação como privadas
  - 9.4.3 Informações não consideradas privadas
  - 9.4.4 Responsabilidade para proteger a informação privadas
  - 9.4.5 Aviso e consentimento para usar informações privadas
  - 9.4.6 Divulgação em processo judicial ou administrativo
  - 9.4.7 Outras circunstâncias de divulgação de informação
  - 9.4.8 Informações a terceiros
- 9.5 Direitos de Propriedade Intelectual
- 9.6 Declarações e Garantias-
  - 9.6.1 Declarações e garantias das terceiras partes
- 9.7 Isenção de garantias
- 9.8 Limitações de responsabilidades
- 9.9 Indenizações
- 9.10 Prazo e Rescisão
  - 9.10.1 Prazo
  - 9.10.2 Término
  - 9.10.3 Efeito da rescisão e sobrevivência
- 9.11 Avisos individuais e comunicações com os participantes
- 9.13 Procedimentos de solução de disputa
- 9.14 Lei aplicável
- 9.15 Conformidade com a Lei aplicável
- 9.16 Disposições Diversas
  - 9.16.1 Acordo completo

- 9.16.2 Cessão
- 9.16.3 Independência de disposições

## **9.12 Alterações**

### **9.12.1 Procedimento para emendas**

9.12.1.1 Neste item devem ser descritos a política e os procedimentos utilizados para realizar alterações na PCT. Qualquer alteração na PCT deverá ser submetida à aprovação da AC Raiz. Como parte desse processo, além da conformidade com este documento, deverá ser verificada a compatibilidade entre a PCT e a DPCT da ACT responsável.

### **9.12.2 Mecanismo de notificação e períodos**

9.12.2.1 Neste item devem ser descritos os mecanismos empregados para a distribuição da PCT à comunidade envolvida.

9.12.3 Circunstâncias na qual o OID deve ser alterado.

## 10 DOCUMENTOS DA ICP-BRASIL

10.1 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.

<b>Ref</b>	<b>Nome do documento</b>	<b>Código</b>
[1]	<b>VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL</b>	DOC-ICP-11
[2]	<b>REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL</b>	DOC-ICP-12
[3]	<b>PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL</b>	DOC-ICP-14
[4]	<b>POLÍTICA DE SEGURANÇA DA ICP-BRASIL</b>	DOC-ICP-02
[5]	<b>CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL</b>	DOC-ICP-03
[6]	<b>CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL</b>	DOC-ICP-08
[7]	<b>CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL</b>	DOC-ICP-09
[8]	<b>POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL</b>	DOC-ICP-06
[9]	<b>REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL</b>	DOC-ICP-10

## 11 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.

RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.

ETSI TS 101.861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.