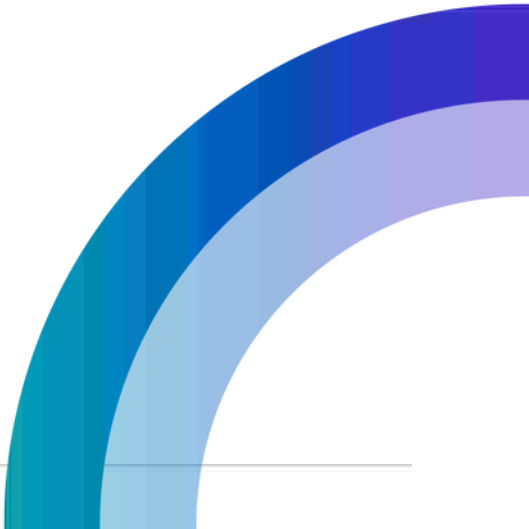
Políticas de Carimbo do Tempo

SERPRO

(PCT SERPRO)

Versão 3.1 de Outubro 2022



Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Responsável	Motivo	Descrição
1.0	Outubro/ 2013	Versão Inicial	Versão Inicial	
2.0	22/07/2020	Lucia Castelli	Revisão	Alterações conforme resolução 112 e 155
2.0	22/07/2020	Alice Vasconcellos	Aprovação	
3.0	18/11/2020	Lucia Castelli	Revisão	Alterações conforme resolução 173
3.0	18/11/2020	Alice Vasconcellos	Aprovação	
3.1	14/10/2021	Fernando Morgado	Revisão	Alterado nome de PC ACT Serpro para PCT Serpro – Apontamento auditoria operacional.
3.1	14/10/2021	Alice Vasconcellos	Aprovação	

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 pela Autoridade de Carimbo do Tempo SERPRO 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, 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 da ACT SERPRO, credenciada na ICP-Brasil. O subscritor e as terceiras partes devem consultar a Declaração de Práticas de Carimbo do Tempo (DPCT) da ACT SERPRO 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. Este documento adota obrigatoriamente, a mesma estrutura empregada nos Requisitos Mínimos para as Políticas de Carimbo do Tempo da ICP-Brasil – DOC-ICP-13.

1.1.7. Aplicam-se ainda à PCT SERPRO, no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil, dentre os quais se destacam:

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];

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].

1.2. Identificação

1.2.1. A Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo SERPRO, a seguir designada simplesmente PCT SERPRO, é identificada pelo **OID (Object Identifier) 2.16.76.1.6.2.**

1.2.2. Os carimbos do tempo emitidos pela ACT SERPRO, segundo esta PCT, seguem os procedimentos descritos na DECLARAÇÃO DE PRÁTICAS DE CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO SERPRO (DPCT SERPRO), cujo **OID 2.16.76.1.5.2.**

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades de Carimbo do tempo

Essa Política de Carimbo de Tempo se refere à Autoridade de Carimbo do Tempo do Serpro;

1.3.2. Prestador de Serviços de Suporte

1.3.2.1. A ACT SERPRO utiliza como Prestador de Serviço de Suporte (PSS) o SERPRO (Serviço Federal de Processamento de Dados).

O endereço(url) da página da ACT SERPRO: http://carimbodotempo.serpro.gov.br/act

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 SERPRO mantêm as informações acima sempre atualizadas.

1.3.3. Subscritores

1.3.3.1. A solicitação de carimbos do tempo poderá ser realizada por clientes externos e funcionários do Serviço Federal de Processamento de Dados, previamente autorizados no sistema da ACT SERPRO.

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. Neste item estão relacionados abaixo as aplicações as quais são adequados os carimbos emitidos pela ACT SERPRO

a) Os carimbos do tempo emitidos pela ACT SERPRO no âmbito desta PCT podem ser utilizados como referência temporal por aplicações ou processos de negócio que necessitem provar a existência de um determinado documento em relação a uma data específica;

b) Uma assinatura digital com carimbo do tempo emitido pela ACT SERPRO garante a irretratabilidade da sua geração, pois o carimbo do tempo serve como evidência de que o certificado do signatário não estava revogado ou expirado no momento da assinatura;

c) Não há proibição de uso de carimbo do tempo por sistemas aplicativos.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

ACT SERPRO – Autoridade de Carimbo do Tempo do SERPRO

1.5.2. Contatos

Administrativo:

Nome: Pedro Moacir Rigo Motta

Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

E-mail: certificados@serpro.gov.br

Telefone: (61) 2021-7957

Suporte / Fraudes

Nome: Central de Serviços SERPRO

Página Web: https://atendimento.serpro.gov.br/certificacaodigital

E-mail: css.serpro@serpro.gov.br

Telefone: 0800 7282323

1.5.3. Pessoa responsável pela adequabilidade da DPCT e PCT

Nome: Pedro Moacir Rigo Motta

E-mail: certificados@serpro.gov.br

Telefone: (61) 2021-7957

1.5.4. Procedimentos de aprovação da PCT

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

1.6. Definições e Acrônimos

AC-RAIZ Autoridade Certificadora Raiz da ICP-BRASIL
ACT Autoridade de Carimbo do Tempo
DPCT Declarações de Práticas de Carimbo do tempo
ETSI European Telecommunication Standard Institute
ICP-Brasil Infraestrutura de Chaves Públicas Brasileira
IETF Internet Engineering Task Force
OID Object Identifier
PCT Política de Carimbo do tempo
PSS Prestadores de Serviço de Suporte
RFC Request For Comments
SCT Servidor de Carimbo do Tempo

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Os itens seguintes estão descritos da DPACT da ACT.

2.1. Publicação de informações da ACT

2.2. Frequência de Publicação

2.3. Controle de Acesso aos Repositórios

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Este item está descrito da DPCT da ACT SERPRO.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Carimbos do Tempo

Neste item da PCT estão descritos todos os requisitos e procedimentos operacionais estabelecidos pela ACT SERPRO para as solicitações de emissão carimbo do tempo. Estes requisitos e procedimentos, que deverão ser atendidos e executados pelos subscritores, compreendem:

a) Para solicitar um carimbo do tempo o subscritor deverá entrar em contato com a ACT SERPRO através dos contatos descritos no item 1.5.2.

b) Após a habilitação do subscritor no sistema da ACT SERPRO o mesmo deverá acessar o endereço *https://www.frameworkdemoiselle.gov.br/v3/signer/docs/timestamp-master.html* e solicitar o carimbo do tempo.

c) Para solicitar um carimbo do tempo num documento original, o subscritor deverá gerar uma requisição de carimbo do tempo (TSQ) contendo o hash a ser carimbado. Para geração do hash, deverá ser utilizado algoritmo SHA2;

d) A requisição de carimbo do tempo TSQ (Time Stamp Request) deverá estar assinada pelo certificado do subscritor utilizando o padrão de assinatura CMS definido na RFC 3852;

e) O Servidor de Aplicativos da ACT SERPRO não aceitará as solicitações de emissão de carimbo do tempo cujo certificado do subscritor esteja expirado ou revogado.

f) O Servidor de Aplicativos da ACT SERPRO disponibiliza o serviço de carimbo do tempo através do protocolo TCP utilizando a porta 318, de acordo com a RFC 3161.

4.1.1. Quem pode submeter uma solicitação de carimbo do tempo

Esse item está descrito na DPCT da ACT.

4.1.2. Processo de registro e responsabilidades

Esse item está descrito na DPCT da ACT.

4.2. Emissão de Carimbos do Tempo

Esse item está descrito na DPCT da ACT.

4.3. Aceitação de Carimbos do Tempo

Esse item está descrito na DPCT da ACT.

4.4. Características do carimbo do tempo

4.4.1. Os carimbos do tempo emitidos segundo esta PCT implementam a versão 1 do padrão X.509, de acordo com perfil estabelecido na RFC 3161. Apresentam as seguintes características;

a) O campo accuracy apresenta a precisão do tempo presente no campo *genTime* do carimbo do tempo. A precisão mínima é determinada pelo Sistema de Auditoria e Sincronismo (SAS) que realiza periodicamente a auditoria e sincronismo dos relógios dos SCT desta ACT;

b) O campo genTime é representado até a unidade de microssegundos;

c) O campo *policy* indica o OID da política do SCT utilizada na geração do carimbo do tempo;

d) O campo *ordering* marcado como falso;

e) O campo *nounce* apresenta um valor que permite verificar se a resposta do SCT corresponde à requisição que foi enviada;

f) O campo *serialNumber* possui um número sequencial e único gerado para cada carimbo do tempo emitido por um SCT;

g) O campo *messageImprint* possui o hash do conteúdo carimbado;

h) O campo *version* apresenta a versão do *timestamp tokem* utilizado. O valor para este campo é 1;

O campo *TSA* apresenta os valores do *Distinguished Name* do certificado digital que assina os carimbos do tempo.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os itens seguintes estão descritos na DPCT da ACT.

5.1. Segurança Física

5.2. Controles Procedimentais

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Os itens seguintes estão descritos na DPCT da ACT.

9.1. Tarifas de serviço

9.2. Responsabilidade Financeira

9.3 Confidencialidade da informação do negócio

9.4. Privacidade da informação pessoal

9.5. Direitos de Propriedade Intelectual

9.6. Declarações e Garantias

9.7. Isenção de garantias

9.8. Limitações de responsabilidades

9.9 Indenizações

9.10 Prazo e Rescisão

9.11. Avisos individuais e comunicações com os participantes

9.12. Alterações

9.13. Solução de conflitos

9.14 Lei aplicável

9.15 Conformidade com a Lei aplicável

9.16 Disposições Diversas

9.12. Alterações

9.12.1. Procedimento para emendas

9.12.1.1. Qualquer alteração nesta PCT deverá ser submetida à AC Raiz.

9.12.2. Mecanismo de notificação e períodos

9.12.2.1. Mudança nesta PCT será publicada no site da ACT.

9.12.3. Circunstâncias na qual o OID deve ser alterado.

Não se aplica.

10. 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.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]	PROCEDIMENTOS PARA AUDITORIA DOTEMPO NA ICP-BRASIL	DOC-ICP-14
[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 DA ICP-BRASIL	DOC-ICP-10

11. REFERÊNCIAS

RFC 3161 https://tools.ietf.org/	IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001
RFC 3628 https://tools.ietf.org/	IETF - Policy Requirements for Time Stamping Authorities, November 2003
RFC 3647 https://tools.ietf.org/	IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.
ETSI TS 101.861 - v 1.2.1 https://www.etsi.org/	Technical Specification / Time Stamping Profile, março de 2002.