



AC DEFESA
Autoridade Certificadora de Defesa

Ministério da Defesa
Autoridade Certificadora de Defesa

POLÍTICA DE CARIMBO DO TEMPO

DA

AUTORIDADE DE CARIMBO DO TEMPO DE DEFESA

(PCT ACT DEFESA)

Versão 1.0

Março de 2025

Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)



Sumário

CONTROLE DE ALTERAÇÕES	7
1 INTRODUÇÃO	8
1.1 Visão Geral	8
1.2 Identificação	9
1.3 Participantes da ICP-Brasil	9
1.3.1 Autoridades de Carimbo do Tempo	9
1.3.2 Prestador de Serviços de Suporte	10
1.3.3 Subscritores	10
1.3.4 Partes confiáveis	10
1.4 Usabilidade do certificado	10
1.5 Política de Administração	11
1.5.1 Organização administrativa do documento	11
1.5.2 Contatos	11
1.5.3 Pessoa responsável pela adequabilidade da DPCT e PCT	11
1.5.4 Procedimentos de aprovação da PCT	11
1.6 Definições e Acrônimos	11
2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	12
2.1 Publicação de informações da ACT Defesa	12
2.2 Frequência de Publicação	12
2.3 Controles de acesso aos repositórios	12
3 IDENTIFICAÇÃO E AUTENTICAÇÃO	12
4 REQUISITOS OPERACIONAIS	12
4.1 Solicitação de Carimbos do Tempo	12
4.1.1 Quem pode submeter uma solicitação de carimbo do tempo	12
4.1.2 Processo de registro e responsabilidades	12
4.2 Emissão de Carimbos do Tempo	13
4.3 Aceitação de Carimbos do Tempo	13
4.4 Características do Carimbo do Tempo	13
5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES	13
5.1 Segurança Física	14
5.1.1 Construção e localização das instalações da ACT Defesa	14
5.1.2 Acesso físico nas instalações de ACT Defesa	14



5.1.3	Energia e ar condicionado do ambiente de nível 4 da ACT	14
5.1.4	Exposição à água nas instalações de ACT	14
5.1.5	Prevenção e proteção contra incêndio nas instalações da ACT	14
5.1.6	Armazenamento de mídia nas instalações de ACT Defesa	14
5.1.7	Destruição de lixo nas instalações da ACT	14
5.1.8	Sala externa de arquivos (<i>off-site</i>) para ACT	14
5.2	Controles Procedimentais	14
5.2.1	Perfis qualificados	14
5.2.2	Número de pessoas necessário por tarefa	14
5.2.3	Identificação e autenticação para cada perfil	14
5.3	Controles de Pessoal	14
5.3.1	Antecedentes, qualificação, experiência e requisitos de idoneidade	14
5.3.2	Procedimentos de verificação de antecedentes	14
5.3.3	Requisitos de treinamento	14
5.3.4	Frequência e requisitos para reciclagem técnica	14
5.3.5	Frequência e sequência de rodízios de cargos	14
5.3.6	Sanções para ações não autorizadas	14
5.3.7	Requisitos para designação de pessoal	14
5.3.8	Documentação fornecida ao pessoal	14
5.4	Procedimentos de Log de Auditoria	14
5.4.1	Tipos de Evento Registrados	14
5.4.2	Frequência de auditoria de registros (logs)	14
5.4.3	Período de retenção para registros de auditoria	14
5.4.4	Proteção de registros de Auditoria	15
5.4.5	Procedimentos para cópia de segurança (<i>Backup</i>) de registros de auditoria	15
5.4.6	Sistema de coleta de dados de auditoria (interno ou externo)	15
5.4.7	Notificação de agentes causadores de eventos	15
5.4.8	Avaliações de vulnerabilidade	15
5.5	Arquivamento de registros	15
5.5.1	Tipos de registros arquivados	15
5.5.2	Período de retenção para arquivo	15
5.5.3	Proteção de arquivo	15
5.5.4	Procedimentos de cópia de segurança (backup) de arquivo	15
5.5.5	Requisitos para datação de registros	15
5.5.6	Sistema de coleta de dados de arquivo (interno e externo)	15
5.5.7	Procedimentos para obter e verificar informação de arquivo	15
5.6	Troca de chave	15
5.7	Comprometimento e Recuperação de Desastre	15



5.7.1	Disposições Gerais	15
5.7.2	Recursos computacionais, <i>software</i> e dados corrompidos	15
5.7.3	Procedimentos no caso de comprometimento de chave privada de entidade	15
5.7.4	Capacidade de continuidade de negócio após desastre	15
5.8	Extinção dos serviços de ACT ou PSS	15
6	CONTROLES TÉCNICOS DE SEGURANÇA	15
6.1	Ciclo de Vida de Chave Privada do SCT	15
6.1.1	Geração do par de chaves criptográfica	16
6.1.2	Geração de Requisição de Certificado Digital.	16
6.1.3	Exclusão de Requisição de Certificado Digital	16
6.1.4	Instalação de Certificado Digital	16
6.1.5	Renovação de Certificado Digital	16
6.1.6	Disponibilização de chave pública da ACT para usuários	16
6.1.7	Tamanhos de chave	16
6.1.8	Geração de parâmetros de chaves assimétricas	16
6.1.9	Verificação da qualidade dos parâmetros	16
6.1.10	Geração de chave por hardware ou software	16
6.1.11	Propósitos de uso de chave	16
6.2	Proteção da Chave Privada	16
6.2.1	Padrões para módulo criptográfico	16
6.2.2	Controle "n" de "m" para chave privada	16
6.2.3	Custódia (<i>escrow</i>) de chave privada	16
6.2.4	Cópia de segurança da chave privada	16
6.2.5	Arquivamento de chave privada	16
6.2.6	Inserção de chave privada em módulo criptográfico	16
6.2.7	Método de ativação de chave privada	16
6.2.8	Método de desativação de chave privada	16
6.2.9	Método de destruição de chave privada	16
6.3	Outros Aspectos do Gerenciamento do Par de Chaves	16
6.3.1	Arquivamento de chave pública	16
6.3.2	Períodos de uso para as chaves pública e privada	16
6.4	Dados de Ativação da Chave do SCT.	16
6.4.1	Geração e instalação dos dados de ativação	16
6.4.2	Proteção dos dados de ativação	17
6.4.3	Outros aspectos dos dados de ativação	17
6.5	Controles de Segurança Computacional	17
6.5.1	Requisitos técnicos específicos de segurança computacional	17



6.5.2	Classificação da segurança computacional	17
6.5.3	Características do SCT	17
6.5.4	Ciclo de Vida de Módulo Criptográfico Associados aos SCTs	17
6.5.5	Auditoria e Sincronização de Relógio de SCT	17
6.6	Controles Técnicos do Ciclo de Vida	17
6.6.1	Controles de desenvolvimento de sistema	17
6.6.2	Controles de gerenciamento de segurança	17
6.6.3	Classificações de segurança de ciclo de vida	17
6.7	Controles de Segurança de Rede	17
6.7.1	Diretrizes Gerais	17
6.7.2	Firewall	17
6.7.3	Sistema de detecção de intrusão (IDS)	17
6.7.4	Registro de acessos não autorizados à rede	17
6.7.5	Outros controles de segurança de rede	17
6.8	Controles de Engenharia do Módulo Criptográfico	17
7	PERFIS DOS CARIMBOS DO TEMPO	17
7.1	Diretrizes Gerais	17
7.2	Perfil do Carimbo do Tempo	17
7.2.1	Requisitos para um cliente TSP	17
7.2.2	Requisitos para um servidor TSP	18
7.2.3	Perfil do Certificado do SCT	18
7.2.4	Formatos de Nome	18
7.3	Protocolos de Transporte	18
8	AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	18
8.1	Frequência e circunstâncias das avaliações	18
8.2	Identificação/Qualificação do avaliador	18
8.3	Relação do avaliador com a entidade avaliada	18
8.4	Tópicos cobertos pela avaliação	18
8.5	Ações tomadas como resultado de uma deficiência	18
8.6	Comunicação dos resultados	18
9	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS	18
9.12	Alterações	20
9.12.1	Procedimento para emendas	20
9.12.2	Mecanismo de notificação e períodos	20
9.12.3	Circunstâncias na qual o OID deve ser alterado	20



AC DEFESA
Autoridade Certificadora de Defesa

Ministério da Defesa
Autoridade Certificadora de Defesa

10 DOCUMENTOS DA ICP-BRASIL	21
11 REFERÊNCIAS	22



CONTROLE DE ALTERAÇÕES

Versão	Data	Motivo	Descrição da Alteração
1.0	06/03/2025	Versão Inicial	Versão inicial, de acordo com o DOC-ICP-13 versão 2.0



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 de Defesa (ACT Defesa), 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; e
- d) **PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [4]**, 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 Esta Política de Carimbo do Tempo (PCT) especifica os requisitos mínimos que devem constar da política de carimbo do tempo da ACT Defesa, integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na execução dos seus serviços de carimbo do tempo. O subscritor e as terceiras partes devem consultar a Declaração de Práticas de Carimbo do Tempo (DPCT) da ACT Defesa para obter detalhes adicionais sobre precisamente como esta Política de Carimbo do Tempo (PCT) é implementada pela ACT Defesa. 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 tem como base as normas da ICP-Brasil, as RFC 3628 e 3161 do IETF e o documento TS 101861 do ETSI.



- 1.1.6** A estrutura desta PCT, obrigatoriamente está baseada no DOC-ICP-13 - Requisitos Mínimos para as Políticas de Carimbo do Tempo da ICP-Brasil.
- 1.1.7** Aplicam-se ainda à ACT Defesa os regulamentos dispostos nos demais documentos da ICP-Brasil, entre os quais destacamos:
- a) **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [5]**, documento aprovado pela Resolução nº 02, de 25 de setembro de 2001;
 - b) **CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]**, documento aprovado pela Resolução nº 06, de 22 de novembro de 2001;
 - c) **CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITÓRIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7]**, documento aprovado pela Resolução nº 24, de 29 de agosto de 2003;
 - d) **CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [8]**, documento aprovado pela Resolução nº 25, de 24 de outubro de 2003;
 - e) **POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP- BRASIL [9]**, 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 [10]**, documento aprovado pela Resolução nº 36, de 21 de outubro de 2004.

1.2 Identificação

- 1.2.1** Esta PCT é chamada Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo de Defesa (PCT ACT Defesa) e possui o Identificador de Objeto (OID) 2.16.76.1.6.15, atribuído pela ICP-Brasil.
- 1.2.2** Os carimbos do tempo emitidos pela ACT Defesa, segundo esta PCT, seguem os procedimentos descritos na DECLARAÇÃO DE PRÁTICAS DE CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO DE DEFESA (DPCT ACT Defesa), cujo OID é 2.16.76.1.5.15

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades de Carimbo do Tempo

Esta PCT refere-se à Autoridade de Carimbo do Tempo de Defesa (ACT Defesa).



1.3.2 Prestador de Serviços de Suporte

1.3.2.1 A ACT Defesa não utiliza Prestador de Serviços de Suporte (PSS).

O endereço da página *web* (URL) da ACT Defesa é:

<https://www.acdefesa.mil.br/carimbodotempo>

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 Defesa mantém as informações acima sempre atualizadas.

1.3.3 Subscritores

1.3.3.1 A solicitação de carimbo do tempo pode ser realizada por pessoa física ou jurídica vinculada ao Ministério da Defesa (MD), à Marinha do Brasil (MB), ao Exército Brasileiro (EB) ou à Força Aérea Brasileira (FAB), por meio de aplicações ou sistemas.

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 a seguir as aplicações as quais são adequados o uso dos carimbos do tempo emitidos pela ACT Defesa:

- a) Os carimbos do tempo emitidos pela ACT Defesa 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 Defesa 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 Defesa - Autoridade de Carimbo do Tempo de Defesa.

1.5.2 Contatos

Nome: Mauro Monteiro Soares

Endereço: Centro Integrado de Telemática do Exército - CITEx, Av. Duque de Caxias, s/n, Setor Militar Urbano, CEP 70630-100 - Brasília-DF

Telefone: (61) 2035-1687

Página web: <https://www.acdefesa.mil.br>

E-mail: contato@acdefesa.mil.br

1.5.3 Pessoa responsável pela adequabilidade da DPCT e PCT

Nome: André Luiz Cibin Ribeiro

Telefone: (61) 2035-1680

E-mail: andre@acdefesa.mil.br

1.5.4 Procedimentos de aprovação da PCT

Esta PCT foi aprovada pelo ITI, durante o processo de credenciamento da ACT Defesa, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridades de Carimbo do Tempo
ASR	Autenticação e Sincronização de Relógio
CCD	Centro de Certificação Digital
CG	Comitê Gestor
DPCT	Declaração 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 DPCT da ACT Defesa.

2.1 Publicação de informações da ACT Defesa

2.2 Frequência de Publicação

2.3 Controles de acesso aos repositórios

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Este item está descrito na DPCT da ACT Defesa.

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 Defesa para as solicitações de emissão carimbo do tempo.

Para solicitar um carimbo do tempo num documento digital o subscritor deverá gerar uma requisição de carimbo do tempo TSQ (*Time Stamp Request*) contendo o *hash* a ser carimbado. Para geração do *hash*, deverá ser utilizado o algoritmo SHA-256.

À solicitação de um carimbo do tempo será atendida pela ACT Defesa segundo os requisitos e procedimentos operacionais a seguir:

- a) as solicitações de carimbo do tempo serão realizadas através de sistema ou aplicações utilizadas pelo subscritor;
- b) A requisição de carimbo do tempo deverá estar no formato TSQ conforme RFC 3161;
- c) O envio do TSQ deverá ser realizado por meio do protocolo HTTP, utilizando a porta 80, ou HTTPS, utilizando a porta 443, 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 token* 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 OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Os itens seguintes estão descritos na DPCT da ACT Defesa.



5.1 Segurança Física

5.1.1 Construção e localização das instalações da ACT Defesa

5.1.2 Acesso físico nas instalações de ACT Defesa

5.1.3 Energia e ar condicionado do ambiente de nível 4 da ACT

5.1.4 Exposição à água nas instalações de ACT

5.1.5 Prevenção e proteção contra incêndio nas instalações da ACT

5.1.6 Armazenamento de mídia nas instalações de ACT Defesa

5.1.7 Destruição de lixo nas instalações da 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

5.3.3 Requisitos de treinamento

5.3.4 Frequência e requisitos para reciclagem técnica

5.3.5 Frequência e sequência de rodízios de cargos

5.3.6 Sanções para ações não autorizadas

5.3.7 Requisitos para designação de pessoal

5.3.8 Documentação fornecida ao pessoal

5.4 Procedimentos de Log de Auditoria

5.4.1 Tipos de Evento Registrados

5.4.2 Frequência de auditoria de registros (logs)

5.4.3 Período de retenção para registros de auditoria



5.4.4 Proteção de registros de Auditoria

5.4.5 Procedimentos para cópia de segurança (*Backup*) de registros de auditoria

5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)

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 de cópia de segurança (backup) de arquivo

5.5.5 Requisitos para datação de registros

5.5.6 Sistema de coleta de dados de arquivo (interno e externo)

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 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.4 Capacidade de continuidade de negócio após desastre

5.8 Extinção dos serviços de ACT ou PSS

6 CONTROLES TÉCNICOS DE SEGURANÇA

Os itens seguintes estão descritos da DPCT da ACT Defesa.

6.1 Ciclo de Vida de Chave Privada do SCT



- 6.1.1 Geração do par de chaves criptográfica
- 6.1.2 Geração de Requisição de Certificado Digital.
- 6.1.3 Exclusão de Requisição de Certificado Digital
- 6.1.4 Instalação de Certificado Digital
- 6.1.5 Renovação de Certificado Digital
- 6.1.6 Disponibilização de chave pública da ACT para usuários
- 6.1.7 Tamanhos de chave
- 6.1.8 Geração de parâmetros de chaves assimétricas
- 6.1.9 Verificação da qualidade dos parâmetros
- 6.1.10 Geração de chave por hardware ou software
- 6.1.11 Propósitos de uso de chave
- 6.2 Proteção da Chave Privada**
 - 6.2.1 Padrões para módulo criptográfico
 - 6.2.2 Controle "n" de "m" para chave privada
 - 6.2.3 Custódia (*escrow*) de chave privada
 - 6.2.4 Cópia de segurança da chave privada
 - 6.2.5 Arquivamento de chave privada
 - 6.2.6 Inserção de chave privada em módulo criptográfico
 - 6.2.7 Método de ativação de chave privada
 - 6.2.8 Método de desativação de chave privada
 - 6.2.9 Método de destruição de chave privada
- 6.3 Outros Aspectos do Gerenciamento do Par de Chaves**
 - 6.3.1 Arquivamento de chave pública
 - 6.3.2 Períodos de uso para as chaves pública e privada
- 6.4 Dados de Ativação da Chave do SCT.**
 - 6.4.1 Geração e instalação dos dados de ativação



6.4.2 Proteção dos dados de ativação

6.4.3 Outros aspectos dos dados de ativação

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.2 Classificação da segurança computacional

6.5.3 Características do SCT

6.5.4 Ciclo de Vida de Módulo Criptográfico Associados aos SCTs

6.5.5 Auditoria e Sincronização de Relógio de SCT

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistema

6.6.2 Controles de gerenciamento de segurança

6.6.3 Classificações de segurança de ciclo de vida

6.7 Controles de Segurança de Rede

6.7.1 Diretrizes Gerais

6.7.2 Firewall

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.4 Registro de acessos não autorizados à rede

6.7.5 Outros controles de segurança de rede

6.8 Controles de Engenharia do Módulo Criptográfico

7 PERFIS DOS CARIMBOS DO TEMPO

Os itens a seguir relacionados estão descritos na DPCT da ACT Defesa

7.1 Diretrizes Gerais

7.2 Perfil do Carimbo do Tempo

7.2.1 Requisitos para um cliente TSP



7.2.2 Requisitos para um servidor TSP

7.2.3 Perfil do Certificado do SCT

7.2.4 Formatos de Nome

7.3 Protocolos de Transporte

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Os itens a seguir relacionados estão descritos na DPCT da ACT Defesa.

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

Os itens a seguir relacionados estão descritos na DPCT da ACT Defesa.

- 9.1 Tarifas de Serviço
 - 9.1.1 Tarifas de emissão de carimbos do tempo
 - 9.1.2 Tarifas de acesso ao de 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 Qualquer alteração nesta PCT será submetida à aprovação da AC Raiz. Como parte desse processo, além da conformidade com o documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [3], deverá ser verificada a compatibilidade entre a PCT e a DPCT da ACT Defesa.

9.12.2 Mecanismo de notificação e períodos

9.12.2.1 Mudanças nesta PCT serão publicadas no site da ACT Defesa.

9.12.3 Circunstâncias na qual o OID deve ser alterado

Não se aplica.



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.

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]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[5]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[8]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[9]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[10]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DA ICP-BRASIL	DOC-ICP-10



11 REFERÊNCIAS

RFC 3161 - IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001, disponível em <https://tools.ietf.org/>

RFC 3628 - IETF - Policy Requirements for Time Stamping Authorities, November 2003, disponível em <https://tools.ietf.org/>

RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003, disponível em <https://tools.ietf.org/>

ETSI TS 101.861 - v 1.2.1 - Technical Specification / Time Stamping Profile, março de 2002, disponível em <https://www.etsi.org/>