Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo VALID (PCT da ACT VALID)

OID: 2.16.76.1.6.5.

Versão 3.0
Agosto de 2020

Sumário

CONTROLE DE ALTERAÇÕES:

Versão	Data	Resolução que aprova a alteração	Item Alterado	Descrição da Alteração
1.1	19/12/2017	DOC-ICP-13	1.1; 1.6; 3.2; 3.3; 5	Adequação à versão 1.2 do DOC-ICP-13
2.0	10/07/2020	Resolução nº 155, de 03/12/2019	-	Atualização Layout
3.0	02/09/2020	Resolução 173	-	Adequação para atender a Resolução.

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];
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 - este documento;
d) PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3].

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 de 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 VALID para obter detalhes adicionais sobre precisamente como esta Política de Carimbo do Tempo (PCT) é implementada pela ACT VALID. 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. Esta PCT adota a mesma estrutura empregada no documento Requisitos Mínimos para as Políticas de Carimbo do Tempo da ICP-Brasil - DOC-ICP-13.

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];
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 ICPBRASIL[9].

1.2. Identificação

1.2.1. Esta PCT é chamada “Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo VALID” e referida como “PCT da ACT VALID”. Esta PCT descreve os usos relacionados ao certificado de Carimbo do Tempo. O OID (object identifier) atribuído a esta PCT é **2.16.76.1.6.5.**

1.2.2. Os carimbos do tempo emitidos pela ACT VALID, segundo esta PCT, seguem os procedimentos descritos na DECLARAÇÃO DE PRÁTICAS DE CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO VALID (DPCT da ACT VALID), cujo OID dessa DPCT é **2.16.76.1.5.5**.

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1 Autoridades de Carimbo do tempo

As práticas e procedimentos de certificação usados para emissão dos carimbos do tempo descritos nesta PCT encontram-se em conformidade com as práticas declaradas na DPCT da ACT VALID.

1.3.2 Prestador de Serviços de Suporte

1.3.2.1 A PCT ACT VALID está publicada no endereço de web: https://www.validcertificadora.com.br/index.aspx?DID=314 contendo a relação de todos os PSSs vinculados à ACT VALID.

1.3.2.2 PSS são entidades utilizadas pela ACT para desempenhar atividade descrita nesta 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 VALID mantém as informações acima sempre atualizadas.

1.3.3 Subscritores

1.3.3.1 A solicitação de carimbos do tempo ocorre no processo de assinatura digital que demanda esse artefato e pode ser realizada por pessoas físicas e jurídicas em aplicações mantidas pela VALID

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. As características dos carimbos do tempo que serão emitidos segundo a PCT, contem, no mínimo:

a) A exatidão ou precisão mínima do tempo registrado no carimbo é de 1 a 10 milissegundos;
b) A unidade utilizada no campo genTime do carimbo do tempo é definida em milissegundos.

1.5 Política de Administração

1.5.1. Organização administrativa do documento

Nome da ACT: ACT VALID

1.5.2. Contatos

Endereço: Avenida Paulista, 2064 -15º Andar - Bela Vista - São Paulo/SP CEP: 01310-928.
Telefone: (11) 2575-6800
Página Web: http://www.validcertificadora.com.br/
E-mail: pki.compliance@valid.com

1.5.3 Pessoa responsável pela adequabilidade da DPCT e PCT

Nome: Márcio Nunes da Silva

Telefone: (11) 2575-6800
E-mail: pki.compliance@valid.com

1.5.4 Procedimentos de aprovação da DPCT

Esta DPC é aprovada pelo ITI, 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	*European Telecommunication Standard Institute*
ICP	Brasil Infraestrutura de Chaves Públicas Brasileira
IETF	*Internet Engineering Task Force*
OID	*Object Identifiers*
PCT	Política de Carimbo do Tempo
PSS	Prestador de Serviço de Confiança
RFC	*Request For Comments*
SCT	Servidor de Carimbo do Tempo

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Publicação de informações da ACT

2.1.1. A ACT VALID mantém as informações obrigatórias publicadas em seu repositório o modo pelo qual serão disponibilizadas e a sua disponibilidade.

2.1.2. As seguintes informações, no mínimo, deverão ser publicadas pela ACT em página web:

a) os certificados dos SCTs que opera;
b) sua DPCT;
c) as PCTs que implementa;
d) as condições gerais mediante as quais são prestados os serviços de

carimbo do tempo;
e) a exatidão do carimbo do tempo com relação ao UTC;
f) algoritmos de hash que poderão ser utilizados pelos subscritores e o algoritmo de hash utilizado pela ACT;
g) uma relação, regularmente atualizada, dos PSSs vinculados.

2.2. Frequência de Publicação

2.2.1. As informações descritas são publicadas em serviço de diretório e/ou em página web da ACT VALID (https://www.validcertificadora.com.br/index.aspx?DID=314), obedecendo as regras e os critérios estabelecidos nesta DPCT. A disponibilidade das informações publicadas pela AC VALID RFB em serviço de diretório e/ou página web é de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.3. Disponibilidade dos Serviços de Carimbo do Tempo

2.3.1. De modo a assegurar a disponibilização dos controles e as eventuais restrições para acesso, leitura e escrita das informações publicadas pela ACT, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil, a ACT VALID mantem sempre atualizada de seus conteúdos:

- As versões ou alterações desta DPC e da PC são atualizadas na web site da AC VALID RFB após aprovação da AC Raiz da ICP-Brasil.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. A requisição de carimbo do tempo TSQ (Time Stamp Request) deverá estar assinada pela chave privada do certificado do subscritor utilizando o padrão de assinatura CMS definido na RFC 3852. Este procedimento é necessário para que o Servidor de Aplicativos identifique o subscritor e qual a sua modalidade de contabilidade

3.2. A requisição do carimbo do tempo (TSQ) não identifica o solicitante, por isso, em situações onde a ACT precisa conhecer a identidade do solicitante devem ser usados meios alternativos de identificação e autenticação. Sendo assim o subscritor é identificado por meio do certificado digital utilizado na autenticação cliente/servidor apresentado na camada HTTPS.

4. REQUISITOS OPERACIONAIS

Como primeira mensagem deste mecanismo, o subscritor solicita um carimbo do tempo enviando um pedido (que é ou inclui uma Requisição de Carimbo do Tempo) para a ACT VALID. Como segunda mensagem, a ACT VALID responde enviando uma resposta (que é ou inclui um Carimbo do Tempo) para o subscritor.

4.1 Solicitação de Carimbos do Tempo

Para solicitar um carimbo do tempo num documento digital, o subscritor deve enviar um TSQ (Time Stamp Request) contendo o hash a ser carimbado.

As solicitações de carimbo do tempo serão realizadas através de sistema do subscritor. A requisição de carimbo do tempo deverá estar no formato TSQ conforme RFC 3161. O Servidor de Aplicativos da ACT VALID dispõe o serviço de carimbo do tempo por meio dos protocolos HTTP/HTTPS, de acordo com a RFC 3161.

4.1.1 Quem pode submeter uma solicitação de carimbo do tempo

A solicitação de carimbos do tempo ocorre no processo de assinatura digital que demanda esse artefato e pode ser realizada por pessoas físicas e jurídicas em aplicações mantidas pela VALID.

4.1.2 Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1 Responsabilidades da ACT

4.1.2.1.1 A ACT VALID é responsável responde pelos danos a que der causa.

4.1.2.1.2 A ACT VALID responde solidariamente pelos atos dos PSSs por ela contratados.

4.1.2.2 Obrigações da ACT

As obrigações da ACT VALID são as abaixo relacionadas:

a) operar de acordo com a sua DPCT e com as PCTs que implementa;
b) gerar, gerenciar e assegurar a proteção das chaves privadas dos SCTs;
c) manter os SCTs sincronizados e auditados pela AC RAIZ;
d) tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
e) monitorar e controlar a operação dos serviços fornecidos;
f) assegurar que seus relógios estejam sincronizados, com autenticação, com a Rede de Carimbo do Tempo da ICP-Brasil;
g) permitir o acesso da AC RAIZ aos SCTs de sua propriedade;
h) notificar à AC emitente do seu certificado quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;
i) notificar aos seus usuários quando ocorrer suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

j) publicar em sua página web sua DPCT, as PCTs aprovadas que implementa e os certificados de seus SCTs;
k) publicar em sua página web as informações definidas no item 2.2.2 deste documento;
l) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
m) adotar as medidas de segurança e controle previstas na DPCT, PCT e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
n) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
o) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
p) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);
q) manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, com cobertura suficiente e compatível com o risco dessas atividades;
r) informar às terceiras partes e subscritores de carimbos do tempo acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima; e
s) informar à AC RAIZ, mensalmente, a quantidade de carimbos do tempo emitidos.

4.1.2.3 Obrigações do Subscritor

Ao receber um carimbo do tempo, o subscritor deve verificar se o carimbo do tempo foi assinado corretamente e se a chave privada usada para assinar o carimbo do tempo não foi comprometida.

4.2 Emissão de Carimbos do Tempo

As práticas e procedimentos de certificação usados para emissão dos carimbos do tempo descrito nesta PCT encontram-se em conformidade com as práticas declaradas na DPCT da ACT VALID.

4.2.1. Nos itens abaixo são descritos todos os requisitos e procedimentos operacionais referentes à emissão de um carimbo do tempo e o protocolo a ser implementado, entre aqueles definidos na RFC 3161.

4.2.2. Como princípio geral, a ACT VALID dispõe aos subscritores o acesso a um Servidor de Aplicativos (SGACT), encaminha as TSQs recebidas ao SCT e em seguida devolve ao subscritor os carimbos do tempo recebidos em resposta às TSQs.

4.2.3. O Servidor de Aplicativos pode se constituir de:

a) Sistema instalado no próprio equipamento que realiza as funções de SCT;
b) Sistema instalado em equipamento da ACT distinto do SCT;
c) Sistema instalado na estação de trabalho do subscritor; e
d) Uma combinação das soluções anteriores.

4.2.4. O fornecimento e o correto funcionamento do Servidor de Aplicativos são de responsabilidade da ACT VALID.

4.2.5. O Servidor de Aplicativos executa as seguintes tarefas:

a) Identificar e validar, se necessário, o usuário que está acessando o sistema;
b) Receber os *hashes* que serão carimbados;
c) Enviar ao SCT os *hashes* que serão carimbados;
d) Receber de volta os *hashes* devidamente carimbados;
e) Conferir a assinatura digital do SCT;
f) Conferir o *hash* recebido de volta do SCT com o *hash* enviado ao SCT;
g) Devolver ao usuário o *hash* devidamente carimbado;
h) Comutar automaticamente para o SCT reserva, em caso de pane no SCT principal; e
i) Emitir alarmes por e-mail aos responsáveis quando ocorrerem problemas de acesso aos SCTs.

4.2.6. O SCT, ao receber a TSQ, deve realizar a seguinte sequência:

a) Verificar se a requisição está de acordo com as especificações da norma RFC 3161. Caso esteja, realizar as demais operações a seguir descritas. Se a requisição estiver fora das especificações, o SCT deve responder de acordo com o item 2.4.2 da RFC 3161, com um valor de status diferente de 0 ou 1, e indicar no campo "*PKIFailureInfo*" qual foi a falha ocorrida sem emitir, neste caso, um carimbo do tempo e encerrando, sem executar as demais etapas;
b) Produzir carimbos do tempo apenas para solicitações válidas;
c) Usar uma fonte confiável de tempo;
d) Incluir um valor de tempo confiável para cada carimbo do tempo;
e) Incluir na resposta um identificador único para cada carimbo do tempo emitido;
f) Incluir em cada carimbo do tempo um identificador da política sob a qual o carimbo do tempo foi criado;
g) Somente carimbar o hash dos dados, e não os próprios dados;
h) Verificar se o tamanho do hash recebido está de acordo com a função *hash* utilizada;
i) Não examinar o hash que está sendo carimbado, de nenhuma forma, exceto para verificar seu comprimento, conforme item anterior;
j) Nunca incluir no carimbo do tempo algum tipo de informação que possa identificar o requisitante do carimbo do tempo;
k) Assinar cada carimbo do tempo com uma chave própria gerada exclusivamente para esse objetivo;

l) A inclusão de informações adicionais solicitadas pelo requerente deve ser feita nos campos de extensão suportados; caso não seja possível, responder com mensagem de erro;
m) Encadear o carimbo do tempo atual com o anterior, caso a ACT tenha adotado o mecanismo de encadeamento.

4.2.7. A PCT VALID informa a disponibilidade dos seus serviços de no mínimo 99,5% (noventa e nove e cinco décimos percentuais) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

4.3 Aceitação de Carimbos do Tempo

4.3.1. A solicitação de carimbo do tempo pelo subscritor ocorre por meio do uso de uma aplicação que s e comunica com o servidor de aplicação (SGACT) através de um dos protocolos estabelecidos nesta DPCT e que envia a solicitação de carimbo TSQ conforme RFC 3161 e recebe a resposta com o carimbo do tempo TST e tem por responsabilidade:

a) Verificar o valor do status indicado no campo *PKIStatusInfo* do carimbo do tempo. Caso nenhum erro estiver presente, isto é, o status estiver com o valor 0 (sucesso) ou 1 (sucesso com restrições), devem ser verificados os próximos itens;
b) Comparar se o hash presente no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT;
c) Comparar se o OID do algoritmo de hash no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT;
d) Comparar se o número de controle (valor do campo *nounce*) presente no carimbo do tempo é igual ao da requisição (TSQ) enviada para ACT;
e) Verificar a validade da assinatura digital do SCT que emitiu o carimbo do tempo;
f) Verificar se o certificado do SCT é válido e não está revogado;
g) Verificar se o certificado do SCT possui o uso adequado para este objetivo, isto é, o certificado deve possuir o valor *id-kp-timeStamping* com o OID definido pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [10].

4.3.2. Uma vez recebida a resposta (que é ou inclui um *TimeStampResp*, que normalmente contém um carimbo do tempo), o subscritor deve verificar o status de erro retornado pela resposta e, se nenhum erro estiver presente, ele deve verificar os vários campos contidos no carimbo do tempo e a validade da assinatura digital do carimbo do tempo.

4.3.3. Em especial ele deve verificar se o que foi carimbado corresponde ao que foi enviado para carimbar. O subscritor deve verificar também se o carimbo do tempo foi assinado por uma ACT credenciada e se estão corretos o *hash* dos dados e o OID do algoritmo de *hash*. Ele deve então verificar a tempestividade

da resposta, analisando ou o tempo incluído na resposta, comparando-o com uma fonte local confiável de tempo, se existir, ou o valor do número de controle incluído na resposta, comparando-o com o número incluído no pedido. Se qualquer uma das verificações acima falhar, o carimbo do tempo deve ser rejeitado.

4.3.4. Como o certificado do SCT pode ter sido revogado, o status do certificado deve ser verificado (ex.: analisando a LCR apropriada) para verificar se o certificado ainda está válido. A seguir a aplicação utilizada pelo subscritor deve checar também o campo *policy* para determinar se a política sob a qual o carimbo foi emitido é aceitável ou não para a aplicação. A aplicação utilizada pelo subscritor deve comparar se o valor do campo *nounce* presente no carimbo do tempo é igual ao da TSQ enviada para a ACT.

4.3.5. A PCT VALID deverá definir os procedimentos específicos para aceitação dos carimbos do tempo, com base nos processos acima e nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2].

4.4 Características do carimbo do tempo

Neste item é informada 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 são referidos os itens correspondentes da DPCT da ACT VALID.

• 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

6 CONTROLES TÉCNICOS DE SEGURANÇA

Neste item são referidos os itens correspondentes da DPCT da ACT VALID ou detalhados aspectos específicos para a PCT.

6.1. Ciclo de Vida de Chave Privada do SCT

6.1.1. Geração do par de chaves

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 VALID 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. Recuperação de chave privada

6.2.4. Cópia de segurança (backup) de chave privada

6.2.5. Arquivamento de chave privada

6.2.6. Inserção de chave privada em módulo criptográfico

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

6.4.2. 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 de SCT

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

Neste item são referidos os itens correspondentes da DPCT da ACT VALID detalhados aspectos específicos para a PCT.

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

Nos itens correspondentes à lista são referidos os itens correspondentes da DPCT da ACT VALID ou detalhados aspectos específicos para a PCT.

- 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 são referidos os itens correspondentes da DPCT da ACT VALID detalhados aspectos específicos para a PCT.

- 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. Qualquer alteração na PCT é submetida à aprovação da AC Raiz. Como parte desse processo, além da conformidade com este documento, são verificadas a compatibilidade entre a PCT e a DPCT da ACT VALID.

9.12.2 Mecanismo de notificação e períodos

9.12.2.1 Mudança da PCT será publicada no site da ACT VALID no endereço de web: https://www.validcertificadora.com.br/index.aspx?DID=314

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 POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-13
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[4]	POLITICA 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 ICPBRASIL	DOC-ICP-06
[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO AMBITO DA ICP-BRASIL	DOC-ICP-10
[10]	PERFIL DO ALVARÁ DO CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12.01

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.