Infraestrutura de Chaves Públicas Brasileira

REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL

DOC-ICP-12
versão 1.2

30 de setembro de 2015

Infraestrutura de Chaves Públicas Brasileira

Sumário

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
Resolução nº 112, de 30/09/2015	Referências	Retira as referências a Lei 2.784, de 18.06.1918, e ao Decreto 10.546, de 05.11.1918.
Resolução nº 69, de 13/10/2009	6.10.1; 6.10.1.1; 6.10.1.2;6.10.1.3; 6.10.1.4; 6.10.1.5; 6.10.1.6; 6.10.5.3; tem 11	Aprova a versão 1.1 dos Documentos que Regulamentam a Geração e Uso de Carimbo do Tempo no Âmbito da ICP-Brasil:
Resolução Nº 59, de 01/12/2008		Aprova a versão 1.0 do Documento Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC-RAIZ	Autoridade Certificadora Raiz da ICP-BRASIL
ACT	Autoridade de Carimbo do Tempo
ASR	Autenticação e Sincronização de Relógio
CG	Comitê Gestor da ICP-BRASIL
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CN	*Common Name*
CT	Carimbo do Tempo
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPCT	Declarações de Práticas de Carimbo do tempo
EAT	Entidade de Auditoria do Tempo
ETSI	*European Telecommunication Standard Institute*
FCT	Fonte Confiável de Tempo
HSM	*Hardware Security Module*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Sistemas de Detecção de Intrusão*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*

IP	*Internet Protocol*
ITI	Instituto Nacional de Tecnologia da Informação
ITSEC	*European infrmation Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
NBR	Norma Brasileira
LCR	Lista de Certificados Revogados
OID	*Internet Engineering Task Force*
PCN	*Network Time Protocol*
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
SAS	Sistemas de Auditoria e Sincronismo
SCT	Sistema de Carimbo de Tempo
SNMP	*Simple Network Management Protocol*
TCSEC	*Trutes Software Development Methodology*
TSP	*Time Stamp Protocol*
TSQ	*Time Stamp Request*
TSDM	*Trusted Software Development Methodology*
UTC	*Universal Time Coordinated*
URL	*Uniform Resource Locator*

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** - este documento;

c) **REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2];**

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. Os relógios dos SCTs devem ser auditados e sincronizados por Sistemas de Auditoria e Sincronismo (SASs).

1.1.3. A utilização de carimbos de 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. Este documento estabelece os requisitos mínimos a serem obrigatoriamente observados pelas ACTs integrantes da ICP-Brasil na elaboração de suas Declarações de Práticas de Carimbo do tempo (DPCTs). A DPCT é o documento que descreve as práticas e os procedimentos empregados pela ACT na execução de seus serviços. 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. Toda DPCT elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.

1.1.7. Aplicam-se ainda às ACT 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];**

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

Neste item deve ser identificada a DPCT e indicado o seu Object Identifier (OID). No âmbito da ICP-Brasil, um OID no formato 2.16.76.1.5.n será atribuído à DPCT na conclusão do processo de credenciamento da ACT responsável.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades de Carimbo do tempo

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

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

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

1.3.4. Aplicabilidade

Este item da DPCT deve relacionar e identificar as PCTs implementadas pela ACT, que definem como os carimbos do tempo emitidos devem ser utilizados pela comunidade. Nas PCTs estarão relacionadas 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.

1.4. Dados de Contato

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

2. DISPOSIÇÕES GERAIS

2.1. Obrigações e direitos

Nos itens a seguir devem ser descritas as obrigações gerais das entidades envolvidas. Caso haja obrigações específicas para as PCTs implementadas, as mesmas devem ser descritas.

2.1.1. Obrigações da ACT

Neste item devem ser incluídas as obrigações da ACT responsável pela DPCT, contendo, no mínimo, 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 EAT;

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, à Rede de Carimbo do Tempo da ICP-Brasil;

g) permitir o acesso da EAT 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 as 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 2.6.1.2 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.

2.1.2. 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.

2.1.3. Direitos da terceira parte (Relying Party)

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

2.1.3.2. Constituem direitos da terceira parte:

a) recusar a utilização do carimbo do tempo para fins diversos dos previstos na PCT correspondente;

b) verificar, a qualquer tempo, a validade do carimbo do tempo.

2.1.3.3. Um carimbo emitido por ACT integrante da ICP-Brasil é considerado válido quando:

a) tiver sido assinado corretamente, usando certificado ICP-Brasil específico para equipamentos de carimbo do tempo;

b) a chave privada usada para assinar o carimbo do tempo não foi comprometida até o momento da verificação;

c) caso o alvará seja integrado no CT, ele deverá também estar válido para o período do CT.

2.1.3.4. O não exercício desses direitos não afasta a responsabilidade da ACT responsável e do subscritor.

2.2. Responsabilidades

2.2.1. Responsabilidades da ACT

2.2.1.1. A ACT responsável responde pelos danos a que der causa.

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

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (Relying Party)

Neste item deve ser estabelecida a inexistência de responsabilidade da terceira parte (relying party) perante a ACT, exceto na hipótese de prática de ato ilícito.

2.3.2. Relações Fiduciárias

Neste item deve constar que a ACT responsável indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o subscritor for pessoa jurídica.

2.3.3. Processos Administrativos

Neste item devem ser relacionados os processos administrativos cabíveis, relativos às operações da ACT responsável pela DPCT e dos PSSs vinculados.

2.4. Interpretação e Execução

2.4.1. Legislação

Neste item deve ser indicada a legislação que ampara a DPCT.

2.4.2. Forma de interpretação e notificação

2.4.2.1. Neste item devem ser relacionadas as providências a serem tomadas na hipótese de uma ou mais das disposições da DPCT ser, por qualquer razão, considerada inválida, ilegal ou não aplicável.

2.4.2.2. Deve também ser definida a forma pela qual serão realizadas as notificações, as solicitações ou quaisquer outras comunicações necessárias, relativas às práticas descritas na DPCT.

2.4.3. Procedimentos de solução de disputa

2.4.3.1. Neste item devem ser definidos os procedimentos a serem adotados em caso de conflito entre a DPCT e outras declarações, políticas, planos, acordos, contratos ou documentos que a ACT adotar.

2.4.3.2. Deve também ser estabelecido que a DPCT da ACT responsável não prevaleça sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.
2.4.3.3. Os casos omissos deverão ser encaminhados para apreciação da AC-Raiz.

2.5. Tarifas de Serviço

Nos itens a seguir, deve ser especificada pela ACT responsável pela DPCT a política tarifária e de reembolso aplicáveis.

2.5.1. Tarifas de emissão de carimbos do tempo
2.5.2. Tarifas de acesso ao carimbo do tempo
2.5.3. Tarifas de revogação ou de acesso à informação de status
2.5.4. Tarifas para outros serviços
2.5.5. Política de reembolso

2.6. Publicação

2.6.1. Publicação de informação da ACT

2.6.1.1. Neste item devem ser definidas as informações a serem publicadas pela ACT responsável pela DPCT, o modo pelo qual serão disponibilizadas e a sua disponibilidade.
2.6.1.2. 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.

2.6.2. Freqüência de publicação

Neste item deve ser informada a freqüência de publicação das informações de que trata o item anterior, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

2.6.3. Controles de acesso

Neste item devem ser descritos os 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.

2.7. Fiscalização e Auditoria de Conformidade

2.7.1. As fiscalizações e auditorias realizadas nas ACTs da ICP-Brasil e em seus PSSs têm por objetivo verificar se seus processos, procedimentos e atividades estão em conformidade com suas respectivas DPCT, PCTs, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

2.7.2. As fiscalizações das ACTs da ICP-Brasil e de seus PSSs são realizadas pela AC-Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento **CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7]**.

2.7.3. As auditorias das ACTs da ICP-Brasil e de seus PSS são realizadas:

a) quanto aos procedimentos operacionais, pela AC-Raiz, por meio de pessoal de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento **CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].**

b) quanto a autenticação e ao sincronismo dos SCTs pela Entidade de Auditoria do Tempo (EAT) observado o disposto no documento **PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS DO TEMPO NA ICP-BRASIL [3].**

2.7.4. Neste item da DPCT, a ACT responsável deve informar que recebeu auditoria prévia da AC-Raiz para fins de credenciamento na ICP-Brasil e que é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento **CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]**. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5. Neste item da DPCT, a ACT responsável deve informar que recebeu auditoria prévia da EAT quanto aos aspectos de autenticação e sincronismo, sendo regularmente auditada, para fins de continuidade de operação, com base no disposto no documento

PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS DO TEMPO NA ICP-BRASIL [3].

2.7.6. Neste item da DPCT, a ACT responsável deve informar que as entidades da ICP-Brasil a ela diretamente vinculadas também receberam auditoria prévia, para fins de credenciamento, e que a ACT é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo 2.7.3.

2.8. Sigilo

2.8.1. Disposições Gerais

2.8.1.1. A chave privada de assinatura digital dos SCTs serão geradas e mantidas pela ACT, que será responsável pelo seu sigilo.

2.8.2. Tipos de informações sigilosas

2.8.2.1. Neste item devem ser identificados os tipos de informações consideradas sigilosas pela ACT responsável pela DPCT, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.8.2.2. A DPCT deve estabelecer, como princípio geral, que nenhum documento, informação ou registro fornecido pelo subscritor à ACT ou aos PSSs vinculados deverá ser divulgado, exceto quando for estabelecido um acordo com o subscritor para sua publicação mais ampla.

2.8.3. Tipos de informações não sigilosas

Neste item devem ser indicados os tipos de informações consideradas não sigilosas pela ACT responsável pela DPCT e pelos PSSs a ela vinculados, os quais deverão compreender, entre outros:

a) os certificados dos SCTs;
b) as PCTs implementadas pela ACT;
c) a DPCT da ACT;
d) versões públicas de PS; e
e) a conclusão dos relatórios de auditoria.

2.8.4. Quebra de sigilo por motivos legais

Este item deve estabelecer o dever da ACT responsável pela DPCT de fornecer documentos, informações ou registros sob sua guarda, mediante ordem judicial.

2.8.5. Informações a terceiros

Este item da DPCT deve estabelecer como diretriz geral que nenhum documento, informação ou registro sob a guarda do PSS ou da ACT responsável pela DPCT deverá ser fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

2.8.6. Outras circunstâncias de divulgação de informação Neste item da DPCT devem ser descritas, quando cabíveis, quaisquer outras circunstâncias em que poderão ser divulgadas informações sigilosas.

2.9. Direitos de Propriedade Intelectual

Neste item da DPCT devem ser tratadas as questões referentes aos direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, de acordo com a legislação vigente.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Neste item a ACT responsável deve descrever a forma utilizada para identificar e autenticar os solicitantes de carimbos do tempo, caso necessária a realização de tais procedimentos.

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.

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. Como segunda mensagem, a ACT responde enviando uma resposta (que é ou inclui um Carimbo do Tempo) para o subscritor.

4.1. Solicitação de Carimbos do Tempo

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

4.1.2. Neste item devem ser descritos todos os requisitos e procedimentos operacionais referentes à solicitação de um carimbo do tempo e indicado o protocolo a ser implementado para envio do TSQ, entre aqueles definidos na RFC 3161.

4.1.3. Cada PCT implementada pela ACT responsável deve definir os procedimentos específicos para solicitação dos carimbos do tempo emitidos segundo a PCT, com base

nos requisitos aplicáveis estabelecidos pelo documento **REQUISITOS MÍNIMOS PARA POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2].**

4.2. Emissão de Carimbos do Tempo

4.2.1. Neste item devem ser 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 deve disponibilizar aos subscritores o acesso a um Servidor de Aplicativos, encaminhar as TSQs recebidas ao SCT e em seguida devolver 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;

d) uma combinação das soluções anteriores.

4.2.4. Em qualquer dos casos acima, o fornecimento e correto funcionamento do Servidor de Aplicativos é de responsabilidade da ACT.

4.2.5. O Servidor de Aplicativos deve executar, pelo menos, as seguintes tarefas:

a) identificar e validar, se necessário, o usuário que está acessando o sistema;

b) receber os *hash*es que serão carimbados;

c) enviar ao SCT os *hash*es que serão carimbados;

d) receber de volta os *hash*es 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;

i)emitir alarmes por email 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 ACT responsável deverá informar na PCT a disponibilidade dos seus serviços de carimbo do tempo. Essa disponibilidade deverá ser, no mínimo, de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

4.3. Aceitação de Carimbos do Tempo

4.3.1. Neste item devem ser descritos todos os requisitos e procedimentos operacionais referentes à aceitação de um carimbo do tempo recebido pelo subscritor.

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. Além disso, 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 o 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.

4.3.5. Cada PCT implementada pela ACT responsável deve definir os procedimentos específicos para aceitação dos carimbos do tempo emitidos segundo a PCT, 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. Procedimentos de Auditoria de Segurança

Nos itens seguintes da DPCT devem ser descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela ACT responsável com o objetivo de manter um ambiente seguro.

4.4.1. Tipos de eventos registrados

4.4.1.1. A ACT responsável pela DPCT deverá registrar em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

a) iniciação e desligamento do SCT;

b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACT;

c) mudanças na configuração do SCT ou nas suas chaves;

d) mudanças nas políticas de criação de carimbos do tempo;

e) tentativas de acesso (login) e de saída do sistema (logoff);

f) tentativas não-autorizadas de acesso aos arquivos de sistema;

g) geração de chaves próprias do SCT e demais eventos relacionados com o ciclo de vida destes certificados;

h) emissão de carimbos do tempo;

i) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;

j) operações falhas de escrita ou leitura, quando aplicável; e

k) todos os eventos relacionados à sincronização dos relógios dos SCTs com a FCT; isso inclui no mínimo:

i. a própria sincronização;

ii. desvio de tempo ou retardo de propagação acima de um valor especificado;

iii. falta de sinal de sincronização;

iv. tentativas de autenticação mal-sucedidas;

v. detecção da perda de sincronização.

4.4.1.2. A ACT responsável pela DPCT deverá também registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema, tais como:

a) registros de acessos físicos;

b) manutenção e mudanças na configuração de seus sistemas;

c) mudanças de pessoal e de perfis qualificados;

d) relatórios de discrepância e comprometimento; e

e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

4.4.1.3. Neste item, a DPCT deve especificar todas as informações que deverão ser registradas pela ACT responsável.

4.4.1.4. A DPCT deve prever que todos os registros de auditoria deverão conter a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos deverão conter o horário UTC. Registros manuais em papel poderão conter a hora local desde que especificado o local

4.4.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da ACT deverá ser armazenada, eletrônica ou manualmente, em local único, conforme a **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].**

4.4.2. Frequência de auditoria de registros (logs)

A DPCT deve estabelecer a periodicidade, não superior a uma semana, com que os registros de auditoria da ACT responsável serão analisados pelo seu pessoal operacional. Todos os eventos significativos deverão ser explicados em relatório de auditoria de registros. Tal análise deverá envolver uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise deverão ser documentadas.

4.4.3. Período de retenção para registros (logs) de auditoria

Neste item, a DPCT deve estabelecer que a ACT responsável mantenha localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, deverá armazená-los da maneira descrita no item 4.5.

4.4.4. Proteção de registro (log) de auditoria

4.4.4.1. Neste item, a DPCT deve descrever os mecanismos obrigatórios incluídos no sistema de registro de eventos da ACT responsável para proteger os seus registros de auditoria contra leitura não autorizada, modificação e remoção.

4.4.4.2. Também devem ser descritos os mecanismos obrigatórios de proteção de informações manuais de auditoria contra a leitura não autorizada, modificação e remoção.

4.4.4.3. Os mecanismos de proteção descritos neste item devem obedecer à **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].**

4.4.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria

Neste item da DPCT devem ser descritos os procedimentos adotados pela ACT responsável para gerar cópias de segurança (backup) de seus registros de auditoria e a sua periodicidade, que não deve ser superior a uma semana.

4.4.6. Sistema de coleta de dados de auditoria

Neste item da DPCT devem ser descritos e localizados os recursos utilizados pela ACT responsável para a coleta de dados de auditoria.

4.4.7. Notificação de agentes causadores de eventos

A DPCT deve observar que quando um evento for registrado pelo conjunto de sistemas de auditoria da ACT responsável, nenhuma notificação deverá ser enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.4.8. Avaliações de vulnerabilidade

A DPCT deve assegurar que os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da ACT responsável, serão analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes deverão ser implementadas pela ACT e registradas para fins de auditoria.

4.5. Arquivamento de Registros

Nos itens seguintes da DPCT deve ser descrita a política geral de arquivamento de registros, para uso futuro, implementada pela ACT responsável e pelos PSSs a ela vinculados.

4.5.1. Tipos de registros arquivados

Neste item da DPCT devem ser especificados os tipos de registros arquivados, que deverão compreender, entre outros:

a) notificações de comprometimento de chaves privadas do SCT;
b) substituições de chaves privadas dos SCTs;
c) informações de auditoria previstas no item 4.4.1.

Neste item, a DPCT deve estabelecer os períodos de retenção para cada registro arquivado, observando que os carimbos do tempo emitidos e as demais informações, inclusive arquivos de auditoria, deverão ser retidos por, no mínimo, 6 (seis) anos.

4.5.3. Proteção de arquivo

A DPCT deve estabelecer que todos os registros arquivados devem ser classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].**

4.5.4. Procedimentos para cópia de segurança (backup) de arquivo

4.5.4.1. A DPCT deve estabelecer que uma segunda cópia de todo o material arquivado deverá ser armazenada em local externo às instalações principais da ACT responsável, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

4.5.4.2. As cópias de segurança deverão seguir os períodos de retenção definidos para os registros dos quais são cópias.

4.5.4.3. A ACT responsável pela DPCT deverá verificar a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.5.5. Requisitos para datação de registros

Neste item, a DPCT deve estabelecer os formatos e padrões de data e hora contidos em cada tipo de registro.

4.5.6. Sistema de coleta de dados de arquivo

Neste item da DPCT devem ser descritos e localizados os recursos de coleta de dados de arquivo utilizados pela ACT responsável.

4.5.7. Procedimentos para obter e verificar informação de arquivo

Neste item da DPCT devem ser detalhadamente descritos os procedimentos definidos pela ACT responsável e pelos PSSs vinculados para a obtenção ou a verificação de suas informações de arquivo.

4.6. Troca de chave

4.6.1. Neste item, a DPCT deve descrever os procedimentos técnicos e operacionais que serão usados pela ACT responsável para garantir que um novo par de chaves será gerado e instalado no SCT quando o ciclo de vida do par de chaves que estiver em utilização chegar ao fim.

4.6.2. A geração de um novo par de chaves e instalação do respectivo certificado no SCT deve ser realizada somente por funcionários com perfis qualificados, através de duplo controle, em ambiente físico seguro.

4.7. Comprometimento e Recuperação de Desastre

4.7.1. Disposições Gerais

4.7.1.1. Nos itens seguintes da DPCT devem ser descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no Plano de Continuidade de Negócios (PCN) da ACT responsável, estabelecido conforme a **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**, para garantir a continuidade dos seus serviços críticos.

4.7.1.2. A ACT deve assegurar, no caso de comprometimento de sua operação por qualquer um dos motivos relacionados nos itens abaixo, que as informações relevantes sejam disponibilizadas aos subscritores e às terceiras partes. A ACT deve disponibilizar a todos os subscritores e terceiras partes uma descrição do comprometimento ocorrido

4.7.1.3. No caso de comprometimento de uma operação do SCT (por exemplo, comprometimento da chave privada do SCT), suspeita de comprometimento ou perda de calibração, o SCT não deverá emitir carimbo do tempo até que sejam tomadas medidas para recuperação do comprometimento.

4.7.1.4. Em caso de comprometimento grave da operação da ACT, sempre que possível, ela deve disponibilizar a todos os subscritores e terceiras partes informações que possam ser utilizadas para identificar os carimbos do tempo que podem ter sido afetados, a não ser que isso viole a privacidade dos subscritores ou comprometa a segurança dos serviços da ACT.

4.7.2. Recursos computacionais, software, e dados corrompidos

Neste item da DPCT devem ser descritos os procedimentos de recuperação utilizados pela ACT responsável quando recursos computacionais, software ou dados estiverem corrompidos ou houver suspeita de corrupção.

4.7.3. Certificado do SCT é revogado

Neste item da DPCT devem ser descritos os procedimentos de recuperação utilizados na circunstância de revogação do certificado do SCT da ACT responsável.

4.7.4. Chave privada do SCT é comprometida

4.7.4.1. Neste item da DPCT devem ser descritos os procedimentos de recuperação utilizados na circunstância de comprometimento da chave privada do SCT, e, caso existam, os meios que podem ser usados para distinguir entre carimbos genuínos e carimbos com datas e horários adulterados.

4.7.5. Calibração e sincronismo do SCT são perdidos

Neste item a DPCT deve descrever os procedimentos de recuperação previstos pela ACT para utilização nas hipóteses de perda de calibração e de sincronismo do SCT.

4.7.6. Segurança dos recursos após desastre natural ou de outra natureza

Neste item da DPCT devem ser descritos os procedimentos de recuperação utilizados pela ACT responsável após a ocorrência de um desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro.

4.8. Extinção dos serviços de ACT ou PSS

4.8.1. Observado o disposto no item 4 do documento **CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5]**, este item da DPCT deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços da ACT responsável ou de um PSS a ela vinculado.

4.8.2. A ACT deve assegurar que possíveis rompimentos com os subscritores e terceiras partes, em conseqüência da cessação dos serviços de carimbo do tempo da ACT sejam minimizados e, em particular, assegurar a manutenção continuada da informação necessária para verificar a precisão dos carimbos do tempo que emitiu.

4.8.3. Antes de a ACT cessar seus serviços de carimbo do tempo os seguintes procedimentos serão executados, no mínimo:

a) a ACT disponibilizará a todos os subscritores e partes receptoras informações a respeito de sua extinção;

b) a ACT revogará a autorização de todos os PSSs e subcontratados que atuam em seu nome para a realização de quaisquer funções que se relacionam ao processo de emissão do carimbo do tempo;

c) a ACT transferirá a outra ACT, após aprovação da AC-Raiz, as obrigações relativas à manutenção de arquivos de registro e de auditoria necessários para demonstrar a operação correta da ACT, por um período razoável;

d) a ACT manterá ou transferirá a outra ACT, após aprovação da AC-Raiz, suas obrigações relativas a disponibilizar sua chave pública ou seus certificados a terceiras partes, por um período razoável;

e) as chaves privadas dos SCT serão destruídas de forma que não possam ser recuperadas;

f) a ACT solicitará a revogação dos certificados de seus SCT;

g) A ACT notificará todas as entidades afetadas.

4.8.4. A ACT providenciará os meios para cobrir os custos de cumprimento destes requisitos mínimos no caso de falência ou se por outros motivos se ver incapaz de arcar com os seus custos.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes devem ser descritos os controles de segurança implementados pela ACT responsável pela DPCT e pelos PSSs a ela vinculados para executar de modo seguro suas funções.

5.1. Segurança Física

Nos itens seguintes da DPCT devem ser descritos os controles físicos referentes às instalações que abrigam os sistemas da ACT responsável e das PSS vinculadas.

5.1.1. Construção e localização das instalações de ACT

5.1.1.1. Uma ACT pode ser acessível ao público, uma vez que pode prestar serviços de carimbo do tempo em documentos digitais entregues pelo subscritor em mídias magnéticas, e não apenas pela Internet ou outro tipo de acesso por rede de dados.

5.1.2. Acesso físico nas instalações de ACT

Toda ACT integrante da ICP-Brasil deverá implantar um sistema de controle de acesso físico que garanta a segurança de suas instalações, conforme a **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]** e os requisitos que seguem.

5.1.2.1. Níveis de acesso

5.1.2.1.1. A DPC deve definir pelo menos 3 (três) níveis de acesso físico aos diversos ambientes da ACT responsável e mais 1 (um) quarto nível relativo à proteção do SCT.

5.1.2.1.2. O primeiro nível – ou nível 1 – deverá situar-se após a primeira barreira de acesso às instalações da ACT. O ambiente de nível 1 das ACTs da ICP-Brasil desempenha a função de interface com o cliente que deseja utilizar o serviço de carimbo do tempo e necessita comparecer pessoalmente à ACT.

5.1.2.1.3. O segundo nível – ou nível 2 – será interno ao primeiro e deverá requerer a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da ACT. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico e o uso de crachá.

5.1.2.1.4. O ambiente de nível 2 deverá ser separado do nível 1 por paredes divisórias de escritório, alvenaria ou pré-moldadas de gesso acartonado. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.

5.1.2.1.5. O acesso a este nível deverá ser permitido apenas a pessoas que trabalhem diretamente com as atividades de carimbo do tempo ou ao pessoal responsável pela manutenção de sistemas e equipamentos da ACT, como administradores de rede e técnicos de suporte de informática. Demais funcionários da ACT ou do possível ambiente que esta compartilhe não deverão acessar este nível.

5.1.2.1.6. Preferentemente, no-breaks, geradores e outros componentes da infraestrutura física deverão estar abrigados neste nível, para evitar acessos ao ambiente de nível 3 por parte de prestadores de serviços de manutenção.

5.1.2.1.7. Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da ACT, a partir do nível 2. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua

entrada controlada e somente poderão ser utilizados mediante autorização formal e sob supervisão.

5.1.2.1.8. O terceiro nível – ou nível 3 – deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação da ACT. Qualquer atividade relativa à emissão de carimbos do tempo deverá ser realizada nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível.

5.1.2.1.9. No terceiro nível deverão ser controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica ou digitação de senha.

5.1.2.1.10. As paredes que delimitam o ambiente de nível 3 deverão ser de alvenaria ou material de resistência equivalente ou superior. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.

5.1.2.1.11. Caso o ambiente de Nível 3 possua forro ou piso falsos, devem ser adotados recursos para impedir o acesso ao ambiente por meio desses, tais como grades de ferro estendendo-se das paredes até as lajes de concreto superior e inferior.

5.1.2.1.12. Deve haver uma porta única de acesso ao ambiente de nível 3, que abra somente depois que o funcionário tenha se autenticado eletronicamente no sistema de controle de acesso. A porta deve ser dotada de dobradiças que permitam a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário.

5.1.2.1.13. Poderão existir na ACT vários ambientes de nível 3 para abrigar e segregar, quando for o caso:

a) equipamentos de produção e cofre de armazenamento; e

b) equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

5.1.2.1.14. Caso a ACT se situe dentro de um datacenter, com requisitos de segurança julgados adequados pela AC-Raiz, poderá ser dispensada a existência de um ambiente de Nível 3 específico para a ACT.

5.1.2.1.15. O quarto nível, ou nível 4, interior ao ambiente de nível 3, deverá compreender pelo menos 2 cofres ou gabinetes reforçados trancados, que abrigarão, separadamente:

a) os SCT e equipamentos criptográficos;

b) outros materiais criptográficos, tais como cartões, chaves, dados de ativação e suas cópias.

5.1.2.1.16. Para garantir a segurança do material armazenado, os cofres ou os gabinetes deverão obedecer às seguintes especificações mínimas:

a) ser feitos em aço ou material de resistência equivalente; e

b) possuir tranca com chave.

5.1.2.1.17. O cofre ou gabinete que abrigará os SCTs deverá ser trancado de forma que sua abertura seja possível somente com a presença de dois funcionários de confiança da ACT.

5.1.2.2. Sistemas físicos de detecção

5.1.2.2.1. A segurança de todos os ambientes da ACT deverá ser feita em regime de vigilância 24 x 7 (vinte e quatro horas por dia, sete dias por semana).

5.1.2.2.2. A segurança poderá ser realizada por:

a) guarda armado, uniformizado, devidamente treinado e apto para a tarefa de vigilância; ou

b) Circuito interno de TV, sensores de intrusão instalados em todas as portas e janelas e sensores de movimento, monitorados local ou remotamente por empresa de segurança especializada.

5.1.2.2.3. O ambiente de nível 3 deverá ser dotado, adicionalmente, de Circuito Interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não deverão permitir a captura de senhas digitadas nos sistemas.

5.1.2.2.4. As mídias resultantes dessa gravação deverão ser armazenadas por, no mínimo, 1 (um) ano, em ambiente de nível 2.

5.1.2.2.5. A ACT deverá possuir mecanismos que permitam, em caso de falta de energia:

a) iluminação de emergência em todos os ambientes, acionada automaticamente;

b) continuidade de funcionamento dos sistemas de alarme e do circuito interno de TV.

5.1.2.3. Sistema de controle de acesso

O sistema de controle de acesso deverá estar baseado em um ambiente de nível 3.

5.1.3. Energia e ar condicionado do ambiente de nível 3 da ACT

5.1.3.1. A infraestrutura do ambiente de nível 3 da ACT deverá ser dimensionada com sistemas e dispositivos que garantam o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia devem ser mantidas de forma a atender os requisitos de disponibilidade dos sistemas da ACT e seus respectivos serviços. Um sistema de aterramento deverá ser implantado.

5.1.3.2. Todos os cabos elétricos deverão estar protegidos por tubulações ou dutos apropriados.
5.1.3.3. Deverão ser utilizados tubulações, dutos, calhas, quadros e caixas de passagem, distribuição e terminação projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. Deverão ser utilizados dutos separados para os cabos de energia, de telefonia e de dados.
5.1.3.4. Todos os cabos deverão ser catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 (seis) meses, na busca de evidências de violação ou de outras anormalidades.
5.1.3.5. Deverão ser mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**. Qualquer modificação nessa rede deverá ser documentada e autorizada previamente.
5.1.3.6. Não deverão ser admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.
5.1.3.7. O sistema de climatização deverá atender aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente.
5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização deverá ser permanentemente monitorada.
5.1.3.9. A capacidade de redundância de toda a estrutura de energia e ar condicionado do ambiente de nível 3 da ACT deverá ser garantida por meio de nobreaks e geradores de porte compatível.

5.1.4. Exposição à água nas instalações de ACT

O ambiente de Nível 3 da ACT deve estar instalado em local protegido contra a exposição à água, infiltrações e inundações.

5.1.5. Prevenção e proteção contra incêndio nas instalações de ACT

5.1.5.1. Nas instalações da ACT não será permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do nível 2.
5.1.5.2. Deverão existir no interior do ambiente nível 3 extintores de incêndio das classes B e C, para apagar incêndios em combustíveis e equipamentos elétricos, dispostos no ambiente de forma a facilitar o seu acesso e manuseio. Em caso da existência de sistema de sprinklers no prédio, o ambiente de nível 3 da ACT não deverá possuir saídas de água, para evitar danos aos equipamentos.

5.1.5.3. O ambiente de nível 3 deve possuir sistema de prevenção contra incêndios, que acione alarmes preventivos uma vez detectada fumaça no ambiente.
5.1.5.4. Nos demais ambientes da ACT deverão existir extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitem o seu acesso e manuseio
5.1.5.5. Mecanismos específicos deverão ser implantados pela ACT para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.

5.1.6. Armazenamento de mídia nas instalações de ACT

A ACT responsável deverá atender à norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”).

5.1.7. Destruição de lixo nas instalações de ACT

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis deverão ser triturados antes de ir para o lixo.
5.1.7.2. Todos os dispositivos eletrônicos não mais utilizáveis e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, deverão ser fisicamente destruídos.

5.1.8. Sala externa de arquivos (off-site) para ACT

Uma sala de armazenamento externa à instalação técnica principal da ACT deve ser usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala deverá estar disponível a pessoal autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e deverá atender aos requisitos mínimos estabelecidos por este documento para um ambiente de nível 2.

5.2. Controles Procedimentais

Nos itens seguintes da DPCT devem ser descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na ACT responsável e nos PSSs a ela vinculados, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

5.2.1.1. A ACT responsável pela DPCT deverá garantir a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente o SCT sem ser detectado. As ações de cada empregado deverão estar limitadas de acordo com seu perfil.

5.2.1.2. A ACT deverá estabelecer um mínimo de 3 (três) perfis distintos para sua operação, a saber:

a) Administrador do sistema – autorizado a instalar, configurar e manter os sistemas confiáveis para gerenciamento do carimbo do tempo, bem como administrar a implementação das práticas de segurança da ACT;

b) Operador de sistema – responsável pela operação diária dos sistemas confiáveis da ACT. Autorizado a realizar backup e recuperação do sistema.

c) Auditor de Sistema - autorizado a ver arquivos e auditar os logs dos sistemas confiáveis da ACT.

5.2.1.3. Todos os empregados da ACT deverão receber treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso serão determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4. Quando um empregado se desligar da ACT, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da ACT, deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à ACT no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. A DPCT deve estabelecer o requisito de controle multiusuário para a geração da chave privada dos SCTs operados pela ACT responsável, na forma definida no item 6.1.1.

5.2.2.2. Todas as tarefas executadas no cofre ou gabinete onde se localizam os SCT deverão requerer a presença de, no mínimo, 2 (dois) empregados com perfis qualificados. As demais tarefas da ACT poderão ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. A DPCT deve garantir que todo empregado da ACT responsável terá sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso físico às instalações da ACT;

b) ser incluído em uma lista para acesso lógico aos sistemas confiáveis da ACT;

c) ser incluído em uma lista para acesso lógico aos SCTs da ACT.

5.2.3.2. Os certificados, contas e senhas utilizadas para identificação e autenticação dos empregados deverão:

a) ser diretamente atribuídos a um único empregado;

b) não ser compartilhados; e

c) ser restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A ACT deverá implementar um padrão de utilização de "senhas fortes", definido na sua PS e em conformidade com a **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**, juntamente com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Nos itens seguintes da DPCT devem ser descritos requisitos e procedimentos, implementados pela ACT responsável e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. A DPCT deve garantir que todos os empregados da ACT responsável e PSS vinculados, encarregados de tarefas operacionais terão registrado em contrato ou termo de responsabilidade:

a) os termos e as condições do perfil que ocuparão;

b) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e

c) o compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da ACT responsável e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo deverá ser admitido conforme o estabelecido na **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**. A ACT responsável poderá definir requisitos adicionais para a admissão.

5.3.2. Procedimentos de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da ACT responsável e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo deverá ser submetido a:

a) verificação de antecedentes criminais;
b) verificação de situação de crédito;
c) verificação de histórico de empregos anteriores; e
d) comprovação de escolaridade e de residência.

5.3.2.2. A ACT responsável poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

Todo o pessoal da ACT responsável e dos PSSs vinculados envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverão receber treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e tecnologias de carimbo do tempo e sistema de carimbos do tempo em uso na ACT;
b) ICP-Brasil;
c) princípios e tecnologias de certificação digital e de assinaturas eletrônicas;
d) princípios e mecanismos de segurança de redes e segurança da ACT;
e) procedimentos de recuperação de desastres e de continuidade do negócio;
f) familiaridade com procedimentos de segurança, para pessoas com responsabilidade de Oficial de Segurança;
g) familiaridade com procedimentos de auditorias em sistemas de informática, para pessoas com responsabilidade de Auditores de Sistema;
h) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal da ACT responsável e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo deverá ser mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da ACT.

5.3.5. Frequência e sequência de rodízio de cargos

Neste item, a DPCT pode definir uma política a ser adotada pela ACT responsável e pelos PSSs vinculados para o rodízio de pessoal entre os diversos cargos e perfis por elas estabelecidos. Essa política não deverá contrariar os propósitos estabelecidos no item 5.2.1 para a definição de perfis qualificados.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. A DPCT deve prever que na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da ACT responsável ou de um PSS vinculado, a ACT deverá, de imediato, suspender o acesso dessa pessoa aos SCT, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.

5.3.6.2. O processo administrativo referido acima deverá conter, no mínimo, os seguintes itens:

a) relato da ocorrência com "modus operandis";
b) identificação dos envolvidos;
c) eventuais prejuízos causados;
d) punições aplicadas, se for o caso; e
e) conclusões.

5.3.6.3. Concluído o processo administrativo, a ACT responsável deverá encaminhar suas conclusões à AC-Raiz.

5.3.6.4. As punições passíveis de aplicação, em decorrência de processo administrativo, são:

a) advertência;
b) suspensão por prazo determinado; ou
c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da ACT responsável e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo deverá ser contratado conforme o estabelecido na **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**. A ACT responsável poderá definir requisitos adicionais para a contratação.

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A DPCT deve garantir que a ACT responsável tornará disponível para todo o seu pessoal e para o pessoal dos PSSs vinculados, pelo menos:

a) sua DPCT;
b) as PCTs que implementa;
c) a **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**;
d) documentação operacional relativa à suas atividades; e

e) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação fornecida ao pessoal deverá estar classificada segundo a política de classificação de informação definida pela ACT e deverá ser mantida atualizada.

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPCT deve definir as medidas de segurança implantadas pela ACT responsável para proteger suas chaves criptográficas e manter o sincronismo de seus SCTs. Devem também ser definidos outros controles técnicos de segurança utilizados pela ACT e pelos PSSs vinculados na execução de suas funções operacionais.

6.1. Ciclo de Vida de Chave Privada do SCT

O SCT deve permitir:

a) geração do par de chaves criptográficas;

b) geração de requisição de certificado digital;

c) exclusão de requisição de certificado digital;

d) instalação de certificados digitais;

e) renovação de certificado digital (com a geração de novo par de chaves);

f) proteção de chaves privadas.

6.1.1. Geração do par de chaves

6.1.1.1. Neste item, a DPCT deve descrever os requisitos e procedimentos referentes ao processo de geração do par de chaves criptográficas da ACT responsável. O par de chaves criptográficas dos SCTs da ACT responsável pela DPCT deverá ser gerado pela própria ACT, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2 A ACT assegurar-se-á de que quaisquer chaves criptográficas sejam geradas em circunstâncias controladas. Em particular:

a) a geração da chave de assinatura do SCT será realizada em um ambiente físico seguro, por pessoal em funções de confiança sob, pelo menos, controle duplo. O pessoal autorizado para realizar essa função será limitado àqueles que receberam essa responsabilidade de acordo com as práticas da ACT;

b) a geração da chave de assinatura do SCT será realizada dentro de módulo criptográfico que cumpra os requisitos dispostos no documento

PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [10];

c) o algoritmo de geração de chave do SCT, o comprimento da chave assinante resultante e o algoritmo de assinatura usado para assinar o carimbo do tempo serão aqueles constantes no documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [10].**

6.1.1.3. A ACT deverá garantir que as chaves privadas serão geradas de forma a não serem exportáveis.

6.1.2. Geração de Requisição de Certificado Digital

Neste item, a DPCT deve informar que o SCT deve possuir mecanismo para geração de requisição de certificado digital correspondente à chave privada gerada no módulo criptográfico interno ao SCT, que atende ao formato definido pela ICP-Brasil.

6.1.3. Exclusão de Requisição de Certificado Digital

O SCT deve garantir que a exclusão de uma requisição de certificado digital, por desistência de emissão do certificado, obrigatoriamente implicará a exclusão da chave privada correspondente.

6.1.4. Instalação de Certificado Digital

O SCT deve realizar no mínimo a conferência dos itens descritos a seguir antes da instalação do certificado:

a) verificar se chave privada correspondente a esse certificado encontra-se em seu módulo criptográfico interno;

b) verificar se o certificado possui as extensões obrigatórias;

c) validar o caminho de certificação.

6.1.5. Renovação de Certificado Digital

O SCT deve permitir a renovação do seu certificado digital, através da geração de requisição de certificado digital desde que seja gerado novo par de chaves, diferente do atual.

6.1.6. Disponibilização de chave pública da ACT para usuários

Neste item, a DPCT deve definir as formas para a disponibilização do certificado da ACT responsável, e de todos os certificados da cadeia de certificação para os usuários da ICP-Brasil. Essas formas poderão compreender, entre outras:

a) a disponibilização de um carimbo do tempo para o subscritor, contendo a cadeia de certificação, conforme formato definido no documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10];**
b) página web da ACT; e
c) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.7. Tamanhos de chave

Neste item, a DPCT deve observar que cada PCT implementada pela ACT responsável definirá o tamanho das chaves criptográficas dos SCTs que opera, com base nos requisitos aplicáveis estabelecidos pelo documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10]**.

6.1.8. Geração de parâmetros de chaves assimétricas

A DPCT deve prever que os parâmetros de geração de chaves assimétricas da ACT responsável adotarão o padrão definido no documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

6.1.9. Verificação da qualidade dos parâmetros

Os parâmetros deverão ser verificados de acordo com as normas estabelecidas pelo padrão definido no documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

6.1.10. Geração de chave por hardware ou software

A DPCT deve indicar que o processo de geração do par de chaves da ACT responsável é feito por hardware.

6.1.11. Propósitos de uso de chave

Neste item, a DPCT deve especificar que as chaves privadas dos SCTs operados pela ACT responsável somente poderão ser utilizadas para assinatura dos carimbos do tempo por ela emitidos.

6.2. Proteção da Chave Privada

Nos itens seguintes, a DPCT deve estabelecer os procedimentos de segurança que adotará para a proteção da chave privada de seus SCTs.

6.2.1. Padrões para módulo criptográfico

A DPCT deve prever que o módulo criptográfico de geração e guarda de chaves assimétricas da ACT responsável adotará o padrão definido no documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

6.2.2. Controle "n de m" para chave privada

Não se aplica.

6.2.3. Recuperação de chave privada

Neste item, a DPCT deve observar que não é permitido, no âmbito da ICP-Brasil, a recuperação de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4. Cópia de segurança (backup) de chave privada

Neste item, a DPCT deve observar que não é permitido, no âmbito da ICP-Brasil, a geração de cópia de segurança (backup) de chaves privadas de assinatura digital de SCT.

6.2.5. Arquivamento de chave privada

Neste item da DPCT, deve ser definido que a ACT não arquivará chaves privadas de assinatura digital de seus SCTs, entendendo-se como arquivamento o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6. Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7. Método de ativação de chave privada

Neste item da DPCT devem ser descritos os requisitos e os procedimentos necessários para a ativação da chave privada da ACT responsável. Devem ser definidos os agentes autorizados a ativar essa chave, o método de confirmação da identidade desses agentes (senhas, tokens ou biometria) e as ações necessárias para a ativação.

6.2.8. Método de desativação de chave privada

Neste item da DPCT devem ser descritos os requisitos e os procedimentos necessários para desativação da chave privada da ACT responsável. Devem ser definidos os agentes

autorizados, o método de confirmação da identidade desses agentes e as ações necessárias.

6.2.9. Método de destruição de chave privada

Neste item da DPCT devem ser descritos os requisitos e os procedimentos necessários para destruição da chave privada do SCT. Devem ser definidos os agentes autorizados, o método de confirmação da identidade desses agentes e as ações necessárias, tais como destruição física, sobrescrita ou apagamento da mídia de armazenamento.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

A DPCT deve prever que as chaves públicas dos SCT da ACT responsável, após a expiração dos certificados correspondentes, serão guardadas pela AC que emitiu os certificados, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas dos SCTs da ACT responsável pela DPCT deverão ser utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. O sistema de geração de carimbos do tempo deverá rejeitar qualquer tentativa de emitir carimbos do tempo caso sua chave privada de assinatura esteja vencida ou revogada.

6.4. Dados de Ativação da Chave do SCT

Não se aplica.

6.4.2. Proteção dos dados de ativação

Não se aplica.

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Características do SCT

6.5.1. O Servidor de Carimbo do tempo é um sistema de hardware e software que executa a geração de carimbos do tempo, atendendo às especificações descritas nesta seção. A responsabilidade pelo atendimento é do fabricante do SCT.
6.5.2. O SCT deve manter o relógio interno do HSM sincronizado com a fonte confiável de tempo (FCT) mantida pela AC-Raiz. A avaliação da manutenção desse sincronismo é realizada pela Entidade Auditora do Tempo (EAT).
6.5.3. O SCT deve garantir que a emissão dos carimbos do tempo será feita em conformidade com o tempo constante do relógio interno do HSM e que a assinatura digital do carimbo do tempo será feita dentro do HSM.
6.5.4. Neste item da DPCT, devem ser definidas as características dos SCTs utilizados pela ACT. O SCT deve possuir como características mínimas:

a) emitir os carimbos do tempo na mesma ordem em que são recebidas as requisições;
b) permitir gerenciamento e proteção de chaves privadas;
c) utilizar certificado digital válido emitido por AC credenciada pelo Comitê Gestor da ICP-Brasil; autoridade de carimbo do tempo
d) permitir identificação e registro de todas as ações executadas e dos carimbos do tempo emitidos;
e) permitir que o relógio interno de seu HSM se mantenha sincronizado com a FCT;
f) garantir a irretroatividade na emissão de carimbos do tempo;
g) prover meios para que a EAT possa auditar e sincronizar o relógio interno do seu HSM;
h) garantir que o acesso da EAT seja realizado através de autenticação mútua entre o SCT e o SAS, utilizando certificados digitais;
i) possuir certificado de especificações emitido pelo fabricante;
j) somente emitir carimbo do tempo se:
   i. possuir alvará vigente emitido pela EAT, a fim de garantir que a precisão do sincronismo do relógio do seu HSM esteja de acordo com o relógio da FCT;
   ii. possuir certificado digital dentro do período de validade e não revogado, emitido por AC credenciada na ICP-Brasil;
   iii. possuir certificado de especificações emitido e assinado pelo fabricante do SCT.

6.6. Ciclo de Vida de Módulo Criptográfico de SCT

Neste item da DPCT, devem ser descritos os requisitos e procedimentos necessários à segurança do módulo criptográfico dos SCTs durante todo o seu ciclo de vida. Particularmente, a ACT deve garantir que a instalação e ativação do módulo criptográfico sejam feitas somente pelo pessoal formalmente designado, envolvendo mais de uma pessoa simultaneamente, em ambiente seguro.

6.7. Auditoria e Sincronização de Relógio de SCT

A ACT deve certificar-se que seus SCTs estejam sincronizados com o UTC dentro da precisão declarada nas PCTs respectivas e, particularmente, que:

a) os valores de tempo utilizados pelo SCT na emissão de carimbos do tempo sejam rastreáveis até a hora UTC;

b) a calibração dos relógios dos SCTs seja mantida de tal forma que não se afaste da precisão declarada na PCT;

c) os relógios dos SCTs estejam protegidos contra ataques, incluindo violações e imprecisões causadas por sinais elétricos ou sinais de rádio, evitando que sejam descalibrados e permitindo que qualquer modificação possa ser detectada;

d) a ocorrência de perda de sincronização do valor do tempo indicado em um carimbo do tempo com o UTC seja detectada pelos controles do sistema;

e) o SCT deixe de emitir carimbos do tempo, caso receba da EAT alvará com validade igual a zero, situação que ocorrerá se a EAT constatar que o relógio do SCT está fora da precisão estabelecida na PCT correspondente;

f) a sincronização dos relógios dos SCTs seja mantida mesmo quando ocorrer a inserção de um segundo de transição (leap second);

g) a EAT tenha acesso com perfil de auditoria aos logs resultantes das ASRs.

6.8. Controles de Segurança Computacional

6.8.1. Disposições Gerais

Neste item, a DPCT deve indicar os mecanismos utilizados para prover a segurança de suas estações de trabalho, servidores e demais sistemas e equipamentos, observado o disposto no item 9.3 da **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].**

6.8.2. Requisitos técnicos específicos de segurança computacional

6.8.2.1. A DPCT deve prever que os SCTs e os equipamentos da ACT responsável, usados nos processos de emissão, expedição, distribuição ou gerenciamento de carimbos do tempo deverão implementar, entre outras, as seguintes características:

a) controle de acesso aos serviços e perfis da ACT;

b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da ACT;

c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

d) geração e armazenamento de registros de auditoria da ACT;

e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e

f) mecanismos para cópias de segurança (backup).

6.8.2.2. Essas características deverão ser implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de gerenciamento do carimbo do tempo e com mecanismos de segurança física.

6.8.2.3. Qualquer equipamento, ou parte desse, ao ser enviado para manutenção deverá ter apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da ACT, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, deverão ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da ACT. Todos esses eventos deverão ser registrados para fins de auditoria.

6.8.2.4. Qualquer equipamento incorporado à ACT deverá ser preparado e configurado como previsto na PS implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.8.3. Classificação da segurança computacional

Neste item da DPCT deve ser informada, quando disponível, a classificação atribuída à segurança computacional da ACT responsável, segundo critérios como: Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC) ou o Common Criteria.

6.9. Controles Técnicos do Ciclo de Vida

Nos itens seguintes da DPCT devem ser descritos, quando aplicáveis, os controles implementados pela ACT responsável e pelos PSSs a ela vinculados no desenvolvimento de sistemas e no gerenciamento de segurança.

6.9.1. Controles de desenvolvimento de sistema

6.9.1.1. Neste item da DPCT devem ser abordados aspectos tais como: segurança do ambiente e do pessoal de desenvolvimento, práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros, aplicados ao software do sistema da ACT ou a qualquer outro software desenvolvido ou utilizado pela ACT responsável.

6.9.1.2. Os processos de projeto e desenvolvimento conduzidos pela ACT deverão prover documentação suficiente para suportar avaliações externas de segurança dos componentes da ACT.

6.9.2. Controles de gerenciamento de segurança

6.9.2.1. Neste item da DPCT devem ser descritas as ferramentas e os procedimentos empregados pela ACT responsável e pelos PSSs vinculados para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

6.9.2.2. Uma metodologia formal de gerenciamento de configuração deverá ser usada para a instalação e a contínua manutenção do sistema da ACT.

6.9.3. Classificações de segurança de ciclo de vida

Neste item da DPCT deve ser informado, quando disponível, o nível de maturidade atribuído ao ciclo de vida de cada sistema, com base em critérios como: Trusted Software Development Methodology (TSDM) ou o Capability Maturity Model do Software Engineering Institute (CMM-SEI).

6.10. Controles de Segurança de Rede

6.10.1. Diretrizes Gerais

6.10.1.1. Neste item da DPCT devem ser descritos os controles relativos à segurança da rede da ACT responsável, incluindo *firewall* e recursos similares, observado o disposto no item 9.3.3 da **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**.

6.10.1.2. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como: roteadores, *hubs*, *switches*, *firewall* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda os SCT, deverão estar localizados e operar em ambiente de, no mínimo, nível 3.

6.10.1.3. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos

respectivos fabricantes deverão ser implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

6.10.1.4. O acesso lógico aos elementos de infraestrutura e proteção de rede deverá ser restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas deverão implementar filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.10.1.5. O acesso à Internet deverá ser provido por no mínimo duas linhas de comunicação de sistemas autônomos (AS) distintos.

6.10.1.6. O acesso via rede aos SCTs e sistemas de gestão da ACT deverá ser permitido somente para os seguintes serviços:

a) pela EAT da ICP-Brasil, para o sincronismo e auditoria de relógios dos SCTs;

b) pela ACT, para a administração dos SCTs e sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;

c) pelo PSS da ACT, para a administração dos SCTs e sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;

d) pelo subscritor, para a solicitação e recebimento de carimbos do tempo.

6.10.2. Firewall

6.10.2.1. Mecanismos de firewall deverão ser implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Os firewalls deverão ser dispostos e configurados de forma a promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à ACT.

6.10.2.2. O software de firewall, entre outras características, deverá implementar registros de auditoria.

6.10.2.3. O Oficial de Segurança deve verificar periodicamente as regras dos firewalls, para assegurar-se que apenas o acesso aos serviços realmente necessários é permitido e que está bloqueado o acesso a portas desnecessárias ou não utilizadas.

6.10.3. Sistema de detecção de intrusão (IDS)

6.10.3.1. O sistema de detecção de intrusão deverá ter capacidade de ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar traps SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao firewall ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do firewall.

6.10.3.2. O sistema de detecção de intrusão deverá ter capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

6.10.3.3. O sistema de detecção de intrusão deverá prover o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.10.4. Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, firewalls ou IDS – deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada. A freqüência de exame dos arquivos de registro deverá ser, no mínimo, semanal e todas as ações tomadas em decorrência desse exame deverão ser documentadas.

6.10.5. Outros controles de segurança de rede

6.10.5.1. A ACT deve implementar serviço de proxy, restringindo o acesso, a partir de todas suas estações de trabalho, a serviços que possam comprometer a segurança do ambiente da ACT.

6.10.5.2. As estações de trabalho e servidores devem estar dotadas de antivírus, antispyware e de outras ferramentas de proteção contra ameaças provindas da rede a que estão ligadas.

6.10.5.3. Os relógios dos SCTs devem estar protegidos contra ataques, incluindo violações e imprecisões causadas por sinais elétricos ou sinais de rádio, para evitar que sejam descalibrados. Qualquer modificação ocorrida nestes relógios deverá ser registrada e detectada.

6.11. Controles de Engenharia do Módulo Criptográfico

Este item da DPCT deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada dos SCTs da ACT responsável. Poderão ser indicados padrões de referência, como aqueles definidos no documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

7. PERFIS DOS CARIMBOS DO TEMPO

7.1. Diretrizes Gerais

Nos seguintes itens da DPCT devem ser descritos os aspectos dos carimbos do tempo emitidos pela ACT responsável, bem como das requisições que lhes são enviadas.

7.2. Perfil do Carimbo do tempo

Todos os carimbos do tempo emitidos pela ACT responsável deverão estar em conformidade com o formato definido pelo Perfil de Carimbo do tempo constante da European Telecommunications Stardards Institute Technical Specification 101 861 (ETSI TS 101 861) e devem seguir as definições constantes da RFC 3161.

7.2.1. Requisitos para um cliente TSP

7.2.1.1. Perfil para o formato do pedido

a) Parâmetros a serem suportados: nenhuma extensão precisa estar presente.

b) Algoritmos a serem usados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

7.2.1.2. Perfil do formato da resposta

a) Parâmetros a serem suportados:

i. o campo accuracy deve ser suportado e compreendido;

ii. mesmo quando inexistente ou configurado como FALSO, o campo ordering deve ser suportado;

iii. o campo nonce deve ser suportado e verificado com o valor constante da requisição correspondente para que a resposta seja corretamente validada;

iv. nenhuma extensão necessita ser tratada ou suportada.

b) Algoritmos a serem suportados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

c) Tamanhos de chave a serem suportados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

7.2.2. Requisitos para um servidor TSP

7.2.2.1. Perfil para o formato do pedido

a) Parâmetros a serem suportados

i. não necessita suportar nenhuma extensão;

ii. deve ser capaz de tratar os campos opcionais reqPolicy, nonce, certReq.

b) Algoritmos a serem suportados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

7.2.2.2. Perfil do formato da resposta

a) Parâmetros a serem suportados

i. o campo genTime deve ser representado até a unidade especificada na PCT;

ii. deve haver uma precisão mínima, conforme definido na PCT;

iii. o campo ordering deve ser configurado como falso ou não deve ser incluído na resposta;

iv. extensão, não crítica, contendo informação sobre o encadeamento de carimbos do tempo, caso a ACT adote esse mecanismo;

v. outras extensões, se incluídas, não devem ser marcadas como críticas;

vi. campo de identificação do alvará vigente no momento da emissão do CT.

b) Algoritmos a serem suportados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

c) Tamanhos de chave a serem suportados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].**

7.2.3. Perfil do Certificado do SCT

7.2.3.1. A ACT precisa assinar cada mensagem de carimbo do tempo com uma chave privada específica para esse uso. A ACT pode usar chaves distintas para acomodar, por exemplo, diferentes políticas, diferentes algoritmos, diferentes tamanhos de chaves privadas ou para aumentar a performance.

7.2.3.2. O certificado correspondente deve conter apenas uma instância do campo de extensão, conforme definido na RFC 3280, com o sub-campo KeyPurposeID contendo o valor id-kp-timeStamping. Essa extensão deve ser crítica.

7.2.3.3. O seguinte OID identifica o KeyPurposeID, contendo o valor id-kp-timeStamping: 1.3.6.1.5.5.7.3.8.

7.2.4. Formatos de nome

O certificado digital emitido para o SCT da ACT deverá adotar o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR
O = ICP-Brasil
OU = < nome da Autoridade de Carimbo do Tempo >
CN = < nome do Servidor de Carimbo do tempo >

7.3. Protocolos de transporte No mínimo o seguinte protocolo definido na RFC 3161 deve ser suportado: Time Stamp Protocol via HTTP.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes devem definir como será mantida e administrada a DPCT.

8.1. Procedimentos de mudança de especificação

Neste item devem ser descritos a política e os procedimentos utilizados para realizar alterações na DPCT. Qualquer alteração na DPCT deverá ser submetida à aprovação da AC-Raiz.

A DPCT deverá ser atualizada sempre que uma nova PCT implementada pela ACT responsável o exigir.

8.2. Políticas de publicação e notificação

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

8.3. Procedimentos de aprovação

Toda DPCT 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].**

9. 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 POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL**	DOC-ICP-13
[3]	**PROCEDIMENTOS PARA AUDITORIA DO TEMPO 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 DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL**	DOC-ICP-10

10. REFERÊNCIAS

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.