DECLARAÇÃO DE PRÁTICAS DE CARIMBO DO TEMPO DA AUTORIDADE DE CARIMBO DO TEMPO SAFEWEB

DPCT – ACT SAFEWEB

Versão 2.1

Novembro 2022

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado
1.0	16/12/2014		Versão inicial
2.0	22/11/2021	Resolução nº 112, de 30/09/2015	Referências
		Resolução nº 155, de 03/12/2019	1.1, 2.1.3.3, 7.2.2.2 e 9
		Resolução nº 172, de 17/08/2020	Diversos - consolidação
		Resolução nº 188, de 18/05/2021	2.1.2, 6.5.3, 6.5.3.1, 6.5.3.2, 6.5.3.3, 6.5.3.4, 6.5.3.5, 6.5.3.6, 6.5.4, 6.5.4.1 e 6.5.5.1
2.1	28/11/2022	Revisão geral	1.6, 4.3.3, 6.6.3.1, 7.2.1.1, 7.2.1.2 e 7.2.2.2

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Este documento faz parte de um conjunto de normativos criados para regulamentar a geração e uso de carimbos do tempo no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Tal conjunto se compõe dos seguintes documentos:

a) VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL [1], documento aprovado pela Resolução nº 58, de 28 de novembro de 2008;

b) REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL - este documento, aprovado pela Resolução nº 59, de 28 de novembro de 2008;

c) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2], documento aprovado pela Resolução nº 60, de 28 de novembro de 2008;

d) PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3], documento aprovado pela Resolução nº 61, de 28 de novembro de 2008; e

e) PERFIL DO ALVARÁ DO CARIMBO DO TEMPO DA ICP-BRASIL [10], documento aprovado pela Resolução nº 155, de 03 de dezembro de 2019.

1.1.2 Um carimbo do tempo aplicado a uma assinatura digital ou a um documento prova que ele já existia na data incluída no carimbo do tempo. Os carimbos do tempo são emitidos por terceiras partes confiáveis, as Autoridades de Carimbo do Tempo - ACT, cujas operações devem ser devidamente documentadas e periodicamente auditadas pela própria EAT da ICP-Brasil. Os relógios dos Servidores de Carimbo do Tempo - SCTs devem ser auditados e sincronizados por Sistemas de Auditoria e Sincronismo (SASs).

1.1.3 A utilização de carimbos do tempo no âmbito da ICP-Brasil é facultativa. Documentos eletrônicos assinados digitalmente com chave privada correspondente a certificados ICP-Brasil são válidos com ou sem o carimbo do tempo.

1.1.4 Esta Declaração de Práticas de Carimbo do Tempo (DPCT) descreve as práticas e os procedimentos empregados pela Autoridade de Carimbo do Tempo Safeweb (ACT Safeweb), integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços de carimbo do tempo.

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 Esta DPCT adota a mesma estrutura empregada no DOC-ICP-12 - Requisitos Mínimos para as Declarações de Práticas das ACT da ICP-Brasil.

1.1.7 Aplicam-se ainda às ACTs 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], documento aprovado pela Resolução nº 02, de 25 de setembro de 2001;

b) CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5], documento aprovado pela Resolução nº 06, de 22 de novembro de 2001;

c) CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], documento aprovado pela Resolução nº 24, de 29 de agosto de 2003;

d) CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7], documento aprovado pela Resolução nº 25, de 24 de outubro de 2003;

e) POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICPBRASIL [8], documento aprovado pela Resolução nº 10, de 14 de fevereiro de 2002;

f) REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [9], documento aprovado pela Resolução nº 36, de 21 de outubro de 2004; e

g) PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [11], documento aprovado pela Instrução Normativa nº 04, de 18 de maio de 2006.

1.2 IDENTIFICAÇÃO

1.2.1 Esta DPCT é chamada Declaração de Práticas de Carimbo do Tempo da Autoridade de Carimbo do Tempo Safeweb, a seguir designada simplesmente por DPCT da ACT Safeweb. O OID deste documento é **2.16.76.1.5.4.**

1.3 COMUNIDADE

1.3.1 Autoridades de Carimbo do Tempo

1.3.1.1 Esta DPCT refere-se à Autoridade de Carimbo do Tempo Safeweb (ACT Safeweb), integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.3.2 Prestador de Serviço de Suporte

1.3.2.1 A relação com os PSSs vinculados à ACT Safeweb está publicado em https://safeweb.com.br/repositorio.

1.3.2.2 PSS são entidades utilizadas pela ACT para desempenhar atividade descritas nesta DPCT 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 Safeweb mantém as informações acima sempre atualizadas.

1.3.3 Subscritores

1.3.3.1 A solicitação de carimbos do tempo poderá ser realizada por pessoa física ou jurídica que seja previamente cadastrada como usuário da ACT Safeweb e realize as solicitações de carimbo do tempo de forma remota conforme especificado na RFC 3161.

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 APLICABILIDADE

1.4.1 A ACT Safeweb implementa as seguintes Políticas de Carimbo do Tempo:

Política de Carimbo do Tempo	Nome conhecido	OID
Política de Carimbo de Tempo da ACT Safeweb	PCT da ACT Safeweb	2.16.76.1.6.4

Tabela 1: Política de Carimbo do Tempo Fonte: Safeweb, 2021.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 Organização administrativa do documento

Nome da ACT: ACT Safeweb

1.5.2 Contatos

Endereço: Av. Princesa Isabel, 828, Santana, Porto Alegre/RS, CEP 90620-000.
Telefones: +55 (51) 3018-0300 / 0800-728-5900
Página web: www.safeweb.com.br
E-mail: compliance@safeweb.com.br

1.5.3 Pessoa responsável pela adequabilidade da DPCT e PCT

Nome: Roseli Zanquim
Telefone: +55 (51) 3018-0300/ 0800-728-5900
E-mail: compliance@safeweb.com.br
Outros: Compliance

1.5.4 Procedimentos de aprovação da DPCT

Esta DPCT foi submetida à aprovação, durante o processo de credenciamento da ACT Safeweb e é submetida à aprovação sempre que houver alteração, 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	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 Software Engineering Institute
CN	Common Name
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPCT	Declaração de Práticas de Carimbo do Tempo
EAT	Entidade de Auditoria do Tempo
ETSI	European Telecommunication Standard Institute
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Sistemas de Detecção de Intrusão
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
MSC	Módulo de Segurança Criptográfico
NBR	Norma Brasileira
OID	Object Identifier
PCN	Plano de Continuidade do Negócio
PCT	Política de Carimbo do Tempo
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
SAS	Sistemas de Auditoria e Sincronismo
SCT	Servidor de Carimbo do Tempo
SNMP	Simple Network Management Protocol
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
TSP	Time Stamp Protocol
TSQ	Time Stamp Request

URL	Uniform Resource Locator
UTC	Universal Time Coordinated

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 PUBLICAÇÃO DE INFORMAÇÕES DA ACT

2.1.1 A disponibilidade das informações publicadas pela ACT Safeweb em sua página de Internet no endereço https://safeweb.com.br/repositorio é de 99,5% (noventa e nove e cinco décimos percentuais) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.2 As seguintes informações, no mínimo, são publicadas pela ACT Safeweb em sua página web https://safeweb.com.br/repositorio:

a) os certificados dos SCTs que opera;

b) esta DPCT;

c) a PCT da ACT Safeweb;

d) as condições gerais mediante as quais são prestados os serviços de carimbo do tempo;

e) a exatidão do carimbo do tempo com relação à FCT;

f) algoritmos de *hash* que poderão ser utilizados pelos subscritores e o algoritmo de *hash* utilizado pela ACT Safeweb;

g) uma relação, regularmente atualizada, dos PSSs vinculados.

2.2 FREQUÊNCIA DE PUBLICAÇÃO

2.2.1 Os certificados dos SCTs são publicados imediatamente após a sua emissão. As versões ou alterações desta DPCT e da PCT são atualizadas na página web da ACT Safeweb após aprovação da AC Raiz da ICP-Brasil.

2.3 CONTROLE DE ACESSO AOS REPOSITÓRIOS

2.3.1 Não há qualquer restrição ao acesso para consulta a esta DPCT e à PCT implementada. São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado pela gestão da ACT Safeweb.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 A identificação e autenticação do solicitante são feitas através de certificado digital contendo o CNPJ do subscritor (e-CNPJ, e-Servidor, etc.). Este deve estar previamente cadastrado

no banco de dados da ACT Safeweb. Após a identificação do subscritor, o TSQ (Time Stamp Request) é utilizado para dar andamento na emissão do carimbo do tempo.

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 da utilização de certificado digital.

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

Para solicitar um carimbo do tempo num documento digital, o subscritor gera uma requisição de carimbo do tempo (TSQ – *Time Stamp Request*) contendo o *hash* a ser carimbado.

As solicitações de carimbo do tempo serão realizadas através de *software* específico disponibilizado ao subscritor ou através da integração de aplicações que utilizem assinatura digital de documentos. A ACT Safeweb dispõe o serviço de carimbo do tempo por meio do protocolo HTTP, de acordo com a RFC 3161.

A PCT da ACT Safeweb tem definidos 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].

4.1.1 Quem pode submeter uma solicitação de carimbo do tempo

4.1.1.1 A solicitação de carimbos do tempo poderá ser realizada por pessoa física ou jurídica que seja previamente cadastrada como usuário da ACT Safeweb e realize as solicitações de carimbo do tempo de forma remota conforme especificado na RFC 3161.

4.1.2 Processo de registro e responsabilidades

4.1.2.1 Responsabilidades da ACT Safeweb

4.1.2.1.1 A ACT Safeweb responde pelos danos a que der causa.

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

4.1.2.2 Obrigações da ACT Safeweb

a) operar de acordo com esta DPCT e com a PCT 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 a AC emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

i) notificar os 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 a DPCT e PCT aprovadas que implementa e os certificados de seus SCT;

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 EAT, 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

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 Safeweb disponbiliza aos subscritores o acesso a um Servidor de Aplicativos (SA), que 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 se constitui de um sistema instalado em equipamento da ACT Safeweb distinto do SCT.

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

4.2.5 O Servidor de Aplicativos executa as seguintes tarefas:

a) identifica e valida o subscritor que está acessando o sistema;

b) recebe os *hashes* que serão carimbados;

c) envia ao SCT os *hashes* que serão carimbados;

d) recebe de volta os *hashs* devidamente carimbados;

e) confere a assinatura digital do SCT;

f) confere o *hash* recebido de volta do SCT com o *hash* enviado ao SCT;

g) devolve ao usuário o *hash* devidamente carimbado;

h) comuta automaticamente para o SCT reserva, em caso de pane no SCT principal;

i) emite 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 de acordo, realizar as demais operações a seguir descritas. Se a requisição estiver fora das especificações, o SCT deve respondes de acordo com o item 2.4.2 da RFC 3161, com um valor de *status* diferente de 0 ou 1, e indica 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 Safeweb provê 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 aplicação que faz a interface com a ACT Safeweb. Esta aplicação realiza automaticamente a conferência dos dados do carimbo e deve observar os seguintes requisitos e procedimentos:

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 o subscritor deve verificar se o que foi carimbado corresponde ao que foi enviado para carimbar. Ele deve verificar também se o carimbo do tempo foi assinado pela ACT Safeweb 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 do 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. O 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 Safeweb 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].

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1 SEGURANÇA FÍSICA

Nos itens seguintes desta DPCT são descritos os controles físicos referentes às instalações que abrigam os sistemas da ACT Safeweb e dos PSS vinculados.

5.1.1 Construção e Localização das Instalações da ACT Safeweb

5.1.1.1 A ACT Safeweb 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 da ACT Safeweb

A ACT Safeweb implanta um sistema de controle de acesso físico que garante a segurança de suas instalações operacionais, 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 ACT Safeweb definiu 4 (quatro) níveis de acesso físico aos diversos ambientes da ACT Safeweb e 2 (dois) níveis relativos à proteção das chaves privada dos SCTs da ACT Safeweb.

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

5.1.2.1.3 O segundo nível - ou nível 2 - é interno ao primeiro e requer a identificação individual das pessoas que nele entram. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá.

5.1.2.1.4 O ambiente de nível 2 é separado do nível 1 por paredes divisórias de alvenaria. Não há 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 é permitido apenas a pessoas que trabalham diretamente com as atividades de carimbo do tempo ou o pessoal responsável pela manutenção de sistemas e equipamentos da ACT Safeweb, como administradores de rede e técnicos de suporte de informática. Demais funcionários da ACT Safeweb não devem acessar este nível.

5.1.2.1.6 No terceiro nível - ou nível 3, ficam as estações de trabalho dos vigilantes que monitoram as operações.

5.1.2.1.7 Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da ACT Safeweb, a partir do nível 2. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente são utilizados mediante autorização formal e sob supervisão.

5.1.2.1.8 O terceiro nível - ou nível 3 situa-se após o segundo. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da ACT Safeweb. Somente pessoas autorizadas permanecem nesse nível.

5.1.2.1.9 No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Nesse nível dois tipos de mecanismos de controle são requeridos para o acesso: senha individual e identificação biométrica.

5.1.2.1.10 As paredes que delimitam o ambiente de nível 3 são de alvenaria. Não há janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.

5.1.2.1.11 Não se aplica.

5.1.2.1.12 Há uma porta única de acesso ao ambiente de nível 3, que somente abre com biometria e senha do funcionário autorizado. A porta é de vidro, com abertura para o lado externo. Possui alarme de quebra de vidro e alarme sonoro, que acusa se a porta ficar aberta por mais de 15 segundos.

5.1.2.1.13 Existe apenas um ambiente de nível 3 na ACT Safeweb.

5.1.2.1.14 As operações da ACT Safeweb situam-se dentro de datacenter, quarto nível – ou nível 4,

com requisitos de segurança julgados adequados pela EAT e certificado pela ABNT.

5.1.2.1.14.1 No quarto nível - ou nível 4, interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da ACT Safeweb, tais como: emissão de carimbos do tempo. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência no mínimo de duas pessoas autorizadas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.14.2 No quarto nível todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. No quarto nível, os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 possuem proteção contra interferência eletromagnética externa.

5.1.2.1.14.3 O nível 4 posui uma porta única de acesso que abre somente depois que as pessoas tenham se autenticado eletronicamente no sistema de controle de acesso. A porta é dotada de dobradiças que permitem a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente.

5.1.2.1.15 O quinto nível – ou nível 5, interior ao ambiente de nível 4, compreende um cofre ou gabinete reforçado trancado. OS SCTs e os materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos estão armazenados em ambiente de nível 5 ou superior.

5.1.2.1.16 Para garantir a segurança do material armazenado, o cofre ou o gabinete obedecem às seguintes especificações mínimas:

a) É feito em aço ou material de resistência equivalente;
b) Possui tranca com chave e segredo.

5.1.2.1.16.1 O sexto nível – ou nível 6, consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de duas fechaduras, sendo uma comum a todos os depósitos e uma individual. Os dados de ativação da chave privada dos SCTs da ACT Safeweb são armazenados nesses depósitos.

5.1.2.1.17 O cofre ou gabinete que abriga os SCTs é trancado, e sua abertura só é possível com a presença de dois funcionários autorizados e de confiança da ACT Safeweb.

5.1.2.2 Sistemas Físicos de Detecção

5.1.2.2.1 A segurança de todos os ambientes da ACT é 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 é realizada por circuito interno de TV, sensores de intrusão instalados em todas as portas e janelas e sensores de movimento, monitorados localmente por guarda

uniformizado, devidamente treinado e apto para a tarefa de vigilância.

5.1.2.2.3 Todo o ambiente é dotado, adicionalmente, de circuito interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não permitem a captura de senhas digitadas nos sistemas.

5.1.2.2.4 As mídias resultantes dessa gravação são armazenadas por, no mínimo, 1 (um) ano, em ambiente de nível 4.

5.1.2.2.5 A ACT possui mecanismos que permitem, 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

5.1.2.3.1 O sistema de controle de acesso está baseado em um ambiente de nível 4.

5.1.3 Energia e Ar-Condicionado nos ambientes da ACT Safeweb

5.1.3.1 A infraestrutura do ambiente de nível 4 da ACT é dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da ACT e seus respectivos serviços. Um sistema de aterramento está implantado.

5.1.3.2 Todos os cabos elétricos estão protegidos por tubulações ou dutos apropriados.

5.1.3.3 Foram 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. Foram utilizados dutos separados para os cabos de energia, de telefonia e de dados.

5.1.3.4 Todos os cabos são 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 São 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 é documentada e autorizada previamente.

5.1.3.6 Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

5.1.3.7 O sistema de climatização atende os requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente.

5.1.3.8 A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada.

5.1.3.9 A capacidade de redundância de toda a estrutura de energia e ar-condicionado do ambiente de nível 4 da ACT Safeweb é garantida, por meio de:

a) Geradores de porte compatível;
b) Geradores de reserva;
c) Sistemas de no-breaks redundantes;
d) Sistemas redundantes de ar-condicionado.

5.1.4 Exposição à Água nas Instalações da ACT Safeweb

5.1.4.1 O ambiente de Nível 4 da ACT Safeweb está instalado em local protegido contra a exposição à água, infiltrações e inundações.

5.1.5 Prevenção e Proteção Contra Incêndio nas Instalações de ACT Safeweb

5.1.5.1 Nas instalações da ACT Safeweb não é permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do nível 2.

5.1.5.2 Existem 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.

5.1.5.3 O ambiente de nível 4 deve possuir sistema de prevenção contra incêndios, que aciona alarmes preventivos uma vez detectada fumaça no ambiente.

5.1.5.4 Nos demais ambientes da ACT Safeweb existem 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 estão implantados para garantir a segurança do pessoal da ACT Safeweb e de seus equipamentos em situações de emergência. Esses mecanismos permitem 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 aciona imediatamente os alarmes de abertura de portas.

5.1.6 Armazenamento de Mídia nas Instalações da ACT Safeweb

5.1.6.1 A ACT Safeweb atende 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 da ACT Safeweb

5.1.7.1 Todos os documentos em papel que contenham informações classificadas como sensíveis ou confidenciais são 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, são fisicamente destruídos.

5.1.8 Sala Externa de Arquivos (*Off-Site*) para ACT Safeweb

5.1.8.1 Uma sala de armazenamento externa à instalação técnica da ACT Safeweb é usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala está disponível ao pessoal

autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e atende aos requisitos mínimos estabelecidos por este documento para um ambiente de nível 3.

5.2 CONTROLES PROCEDIMENTAIS

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

5.2.1 Perfis Qualificados

5.2.1.1 A ACT Safeweb garante 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 são limitadas de acordo com seu perfil.

5.2.1.2 A ACT Safeweb estabelece 20 (vinte) perfis distintos, agrupados em 6 (seis) equipes, para manter o princípio de segregação de tarefas na sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. As responsabilidades e níveis de acesso estão descritas em documentação interna. As equipes e os perfis estabelecidos são:

a) GERÊNCIA
   a.1) Gerente da AC

b) COMPLIANCE
   b.1) Coordenador de Compliance
   b.2) Operador de Compliance

c) SISTEMAS
   c.1) Coordenador de Sistemas
   c.2) Administrador de Sistemas
   c.3) Desenvolvedor de Sistemas

d) INFRAESTRUTURA
   d.1) Coordenador de Infraestrutura
   d.2) Administrador de Domínio
   d.3) Administrador de Infraestrutura
   d.4) Administrador de Rede
   d.5) Administrador de Banco de Dados
   d.6) Administrador de *Backup*
   d.7) Operador de Infraestrutura

e) OPERACIONAL
   e.1) Coordenador Operacional
   e.2) Detentor de chaves de HSM

e.3) Operador de Recursos Humanos
e.4) Operador de Serviços
e.5) Vigilante

f) SEGURANÇA DA INFORMAÇÃO
f.1) Coordenador de Segurança da Informação
f.2) Auditor Interno

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

5.2.1.4 Quando um empregado se desligar da ACT Safeweb, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da ACT Safeweb, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deve devolver à ACT Safeweb no ato de seu desligamento.

5.2.2 Número de Pessoas Necessário por Tarefa

5.2.2.1 Esta DPCT estabelece o requisito de controle multiusuário para a geração da chave privada dos SCTs operados pela ACT Safeweb, na forma definida no item 6.1.1.

5.2.2.2 Todas as tarefas executadas no ambiente onde se localizam os SCTs requerem a presença de, no mínimo, 2 (dois) empregados com perfis qualificados. As demais tarefas da ACT Safeweb podem ser executadas por um único empregado.

5.2.3 Identificação e Autenticação para Cada Perfil

5.2.3.1 Todo empregado da ACT Safeweb tem sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso físico às instalações da ACT Safeweb;
b) ser incluído em uma lista para acesso lógico aos sistemas confiáveis da ACT Safeweb;
c) ser incluído em uma lista para acesso lógico aos SCTs da ACT Safeweb.

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

a) diretamente atribuídos a um único empregado;
b) não compartilhados;
c) restritos às ações associadas ao perfil para o qual foram criados.

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

5.3 CONTROLES DE PESSOAL

Nos itens seguintes são descritos os requisitos e procedimentos, implementados pela ACT Safeweb 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. Todos os empregados da ACT Safeweb encarregados de tarefas operacionais tem registrado em contrato e/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

5.3.1.1 Todo o pessoal da ACT Safeweb e dos PSS vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]. A ACT Safeweb não define 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 Safeweb e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo é 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 Safeweb não definiu requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de Treinamento

5.3.3.1 Todo o pessoal da ACT Safeweb e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de carimbo do tempo recebe 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 Safeweb;

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 Safeweb;

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

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

5.3.5 Frequência e Sequência de Rodízio de Cargos

5.3.5.1 A ACT Safeweb não definiu uma política de rodízio de cargos.

5.3.6 Sanções para Ações Não Autorizadas

5.3.6.1 Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da ACT Safeweb ou de um PSS vinculado, esta deverá, de imediato, suspender o acesso dessa pessoa aos SCTs, 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 conterá, 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 Safeweb encaminhará suas conclusões à EAT.

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

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

5.3.8 Documentação fornecida ao pessoal

5.3.8.1 A ACT Safeweb disponibiliza para todo o seu pessoal e para o pessoal dos PSSs vinculados:

a) a DPCT da ACT Safeweb;
b) a PCT da ACT Safeweb;
c) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4];
d) a PS da ACT Safeweb;
e) documentação operacional relativa à suas atividades; e
f) contratos, normas e políticas relevantes para suas atividades.

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

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA

Nos itens seguintes desta DPCT estão descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela ACT Safeweb com o objetivo de manter um ambiente seguro.

5.4.1 Tipos de Eventos Registrados

5.4.1.1 A ACT Safeweb registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos obrigatoriamente são 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 malsucedidas;
v. detecção da perda de sincronização.

5.4.1.2 A ACT Safeweb também registra, 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.

5.4.1.3 A ACT Safeweb registra apenas as informações descritas nos itens 5.4.1.1 e 5.4.1.2.

5.4.1.4 Todos os registros de auditoria contêm a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos contêm o horário UTC. Registros manuais em papel poderão conter a hora local desde que especificado o local.

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

5.4.2 Frequência de Auditoria de Registros

5.4.2.1 A periodicidade com que os registros de auditoria são analisados pelo pessoal responsável é de uma semana. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolverá 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.

5.4.3 Período de Retenção para Registros de Auditoria

5.4.3.1 A ACT Safeweb mantém localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena de maneira descrita no item 5.5.

5.4.4 Proteção de Registro de Auditoria

5.4.4.1 O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção através das funcionalidades nativas dos sistemas operacionais. As ferramentas disponíveis no sistema operacional liberam os acessos lógicos aos registros de auditoria somente a usuários ou aplicações autorizadas, por meio de permissões de acesso dadas pelo administrador do sistema de acordo com o cargo dos usuários ou aplicações e orientação da área de segurança. O próprio sistema operacional também registra os acessos aos arquivos onde estão armazenados os registros de auditoria.

5.4.4.2 Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção através de controles de acesso aos ambientes físicos onde são armazenados estes registros.

5.4.4.3 Os mecanismos de proteção descritos estão em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

5.4.5 Procedimentos para Cópia de Segurança (*Backup*) de Registros de Auditoria

5.4.5.1 Os registros de eventos de log e sumários de auditoria dos equipamentos utilizados pela ACT Safeweb têm cópias de segurança semanais, feitas automaticamente pelo sistema ou manualmente pelos administradores de sistemas.

5.4.6 Sistema de Coleta de Dados de Auditoria (Interno e Externo)

5.4.6.1 O sistema interno de coleta de dados de auditoria da ACT Safeweb possui uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

5.4.7 Notificação de Agentes Causadores de Eventos

5.4.7.1 Quando um evento é registrado pelo conjunto de sistemas de auditoria da ACT Safeweb, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

5.4.8 Avaliações de Vulnerabilidade

5.4.8.1 Os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da ACT Safeweb são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela ACT Safeweb e registradas para fins de auditoria.

5.5 ARQUIVAMENTO DE REGISTROS

Nos itens seguintes desta DPCT é descrita a política geral de arquivamento de registros, para uso futuro, implementada pela ACT Safeweb e pelos PSSs vinculados.

5.5.1 Tipos de Registros Arquivados

5.5.1.1 Os tipos de registros arquivados compreendem:

a) notificações de comprometimento de chaves privadas do SCT;
b) substituições de chaves privadas dos SCTs;
c) informações de auditoria previstas no item 5.4.1.

5.5.2 Período de Retenção para Arquivo

5.5.2.1 Os períodos de retenção para cada registro arquivado, de carimbos do tempo emitidos e das demais informações, inclusive arquivos de auditoria, são de no mínimo, 6 (seis) anos.

5.5.3 Proteção de Arquivo

5.5.3.1 Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

5.5.4 Procedimentos de Cópia de Arquivo

5.5.4.1 Uma segunda cópia de todo o material arquivado é armazenada em local externo às instalações principais da ACT Safeweb, recebendo o mesmo tipo de proteção utilizada no arquivo principal.

5.5.4.2 As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.

5.5.4.3 A ACT Safeweb verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5 Requisitos para Datação de Registros

5.5.5.1 Informações de data e hora nos registros baseiam-se no horário *Greenwich Mean Time* (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos for zero. Nos casos em que por algum motivo os documentos formalizem o uso de outro formato, ele será aceito.

5.5.6 Sistema de Coleta de Dados de Arquivo

5.5.6.1 Todos os sistemas de coleta de dados de arquivo utilizados pela ACT Safeweb em seus procedimentos operacionais são automatizados, manuais e internos.

5.5.7 Procedimentos para Obter e Verificar Informação de Arquivo

5.5.7.1 A verificação de informação de arquivo deve ser solicitada formalmente à ACT Safeweb e PSSs vinculados, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

5.6 TROCA DE CHAVE

5.6.1 Por intermédio da interface de administração do SCT, na área destinada à administração do par de chaves, é necessário confirmar os dados de renovação do certificado para na sequência iniciar o processo de geração de uma nova chave. A nova chave é gerada internamente ao MSC do equipamento e nele armazenada. O sistema retornará, por meio da interface com o usuário, a requisição em base64 para ser gerado o certificado na AC. Na existência de uma chave privada em uso pelo SCT, ela ainda não será substituída pela nova chave privada gerada. Ela continuará armazenada até que a sua chave pública correspondente seja cadastrada no sistema, sendo que quando ocorrer esse fato, seu uso será descontinuado e será substituída pela nova chave privada.

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

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

5.7.1 Disposições Gerais

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

5.7.1.2 A ACT Safeweb assegura, no caso de comprometimento de sua operação por qualquer um dos motivos relacionados nos itens abaixo, que as informações relevantes serão dispostas aos subscritores e às terceiras partes. A ACT Safeweb disporá a todos os subscritores e terceiras partes uma descrição do comprometimento ocorrido.

5.7.1.3 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 emitirá carimbo do tempo até que sejam tomadas medidas para recuperação do comprometimento.

5.7.1.4 Em caso de comprometimento grave da operação da ACT Safeweb, sempre que possível, ela disporá 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 Safeweb.

5.7.2 Recursos Computacionais, *Software* e/ou Dados Corrompidos

5.7.2.1 Em caso de suspeita de corrupção de dados, *softwares* e ou recursos computacionais, o fato é comunicado ao gerente da ACT Safeweb, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as consequências que ele pode gerar. Esse procedimento é realizado por um grupo pré-determinado de empregados devidamente treinados para essa situação. Caso haja necessidade, o gerente da ACT Safeweb declarará a contingência.

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado do SCT é revogado

5.7.3.1.1 Em caso de revogação do certificado do SCT todos os carimbos do tempo subsequentes estarão automaticamente inválidos. O SCT deve ser desabilitado no SGACT pelo Administrador. É necessária a geração de um novo par de chaves e o Administrador deve cadastrar o novo SCT.

5.7.3.2 Chave Privada do SCT é Comprometida

5.7.3.2.1 Em caso de suspeita de comprometimento de chave do SCT, após a identificação da crise, são notificados os gestores da ACT Safeweb que acionam as equipes envolvidas, de forma a indispor temporariamente os serviços de carimbo do tempo. É necessário que o certificado do SCT seja revogado. O SCT deve ser desabilitado no SGACT pelo Administrador. É necessária a geração de um novo par de chaves e o Administrador deve cadastrar o novo SCT. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

a) O certificado do SCT será revogado e todos os carimbos do tempo subsequentes serão inválidos;
b) Cerimônias específicas serão realizadas para geração de novos pares de chaves.

5.7.3.3 Calibração e Sincronismo do SCT são Perdidos

5.7.3.3.1 Na hipótese de perda de calibração e de sincronismo do SCT, o fato é imediatamente comunicado ao responsável pela operação no SAS na EAT, o qual deverá entrar na interface de auditoria do SAS e executar o procedimento de calibração e sincronismo do SCT que apresentou problema.

5.7.3.3.2 Caso ocorra um erro ao auditar o SCT, o SCT será desabilitado na ACT Safeweb até que providências sejam tomadas.

5.7.4 Capacidade de Continuidade de Negócio após Desastre

5.7.4.1 Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso às instalações operacionais da ACT Safeweb, o responsável pela instalação operacional notifica o gerente e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:

a) garantir a integridade física das pessoas que se encontram nas instalações da ACT Safeweb;

b) monitorar e controlar o foco da contingência; e

c) diminuir ao máximo os danos aos ativos de processamento da ACT Safeweb, de forma a evitar a descontinuidade dos serviços.

5.8 EXTINÇÃO DOS SERVIÇOS DE ACT OU PSS

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

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

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

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

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

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

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

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

g) a ACT Safeweb notificará todas as entidades afetadas.

5.8.4 A ACT Safeweb 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.

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 CICLO DE VIDA DE CHAVE PRIVADA DO SCT

O SCT permite um controle completo do ciclo de vida de sua chave privada. Controles tais como:

a) geração do par de chaves criptográficas;

b) geração da requisição de certificado digital;

c) exclusão da requisição de certificado digital;

d) instalação de certificados digitais;

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

f) proteção das chaves privadas.

6.1.1 Geração do Par de Chaves

6.1.1.1 O par de chaves criptográficas dos SCTs da ACT Safeweb é gerado pela própria ACT Safeweb, 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 Safeweb assegura que quaisquer chaves criptográficas são geradas em circunstâncias controladas. Em particular:

a) geração da chave de assinatura do SCT é 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 Safeweb;

b) a geração da chave de assinatura do SCT será realizada dentro de MSC que cumpra os requisitos dispostos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [11];

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 constam no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [11].

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

6.1.2 Geração de Requisição de Certificado Digital

6.1.2.1 A geração da chave privada é realizada internamente em um módulo de segurança criptográfica do SCT que atende ao formato da ICP-Brasil. A requisição é retornada em base64 ao usuário cadastrado com acesso seguro e controlado através de interface do sistema para que seja feita a geração do certificado digital em uma AC integrante da ICP-Brasil.

6.1.3 Exclusão de Requisição de Certificado Digital

6.1.3.1 O SCT garante 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

6.1.4.1 O SCT realiza a conferência dos itens descritos a seguir antes da instalação do certificado:

a) verifica se a chave privada correspondente a esse certificado encontra-se em seu módulo criptográfico associado;

b) verifica se o certificado possui as extensões obrigatórias;

c) valida o caminho de certificação.

6.1.5 Renovação de Certificado Digital

6.1.5.1 O SCT permite 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 Disposição de Chave Pública da ACT para Usuários

6.1.6.1 A ACT Safeweb dispõe o certificado de seus SCTs e todos os certificados da cadeia de certificação para os usuários da ICP-Brasil, por meio do endereço de Internet https://safeweb.com.br/repositorio.

6.1.7 Tamanhos de Chave

6.1.7.1 A PCT implementada pela ACT Safeweb define o tamanho das chaves criptográficas dos SCTs que opera, com base nos requisitos aplicáveis estabelecidos pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

6.1.8 Geração de Parâmetros de Chaves Assimétricas

6.1.8.1 Os parâmetros de geração de chaves assimétricas da ACT Safeweb adotam o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

6.1.9 Verificação da Qualidade dos Parâmetros

6.1.9.1 Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

6.1.10 Geração de Chave por *Hardware* ou *Software*

6.1.10.1 O processo de geração do par de chaves da ACT Safeweb é feito por hardware.

6.1.11 Propósitos de Uso De Chave

6.1.11.1 As chaves privadas dos SCTs operados pela ACT Safeweb são utilizadas somente para assinatura dos carimbos do tempo por ela emitidos.

6.2 Proteção da Chave Privada

6.2.1 Padrões para Módulo Criptográfico

6.2.1.1 O módulo criptográfico de geração e guarda de chaves assimétricas da ACT Safeweb adota o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

6.2.2 Controle "N de M" para Chave Privada

Não se aplica.

6.2.3 Custódia *(escrow)* de chave privada

6.2.3.1 Não é permitida, 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 de Chave Privada

6.2.4.1 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

6.2.5.1 A ACT Safeweb não arquiva 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

6.2.7.1 A chave privada do SCT está armazenada em módulo criptográfico e é ativada somente após a autenticação de usuário com perfil qualificado na interface de gerenciamento por meio de login/senha ou certificado digital.

6.2.8 Método de Desativação de Chave Privada

6.2.8.1 A chave privada do SCT está armazenada em módulo criptográfico e é desativada mediante a autenticação de usuário com perfil qualificado na interface de gerenciamento por

meio de login/senha ou certificado digital no momento da instalação de um novo certificado digital.

6.2.8.2 Quando a chave privada do SCT for desativada, em decorrência de renovação ou revogação, esta é eliminada da memória do módulo criptográfico.

6.2.9 Método de Destruição de Chave Privada

6.2.9.1 A destruição da chave privada é realizada por processos internos ao módulo de segurança criptográfica e necessita a presença de no mínimo dois operadores do sistema. A destruição é feita somente na criação de uma nova chave privada.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de Chave Pública

6.3.1.1 As chaves públicas dos SCTs da ACT Safeweb, após a expiração dos certificados correspondentes, são guardadas pela AC que emitiu os certificados, permanentemente, para verificação de assinaturas geradas durante seu período de validade. Adicionalmente, as chaves públicas também continuam armazenadas no SCT, mesmo após a destruição de sua chave privada correspondente do MSC.

6.3.2 Períodos de Uso para as Chaves Pública e Privada

6.3.2.1 As chaves privadas dos SCTs da ACT Safeweb serão 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 rejeitará 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

6.4.1 Geração e instalação dos dados de ativação

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 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 Requisitos Técnicos Específicos de Segurança Computacional

6.5.1.1 Os SCTs e os equipamentos da ACT Safeweb, usados nos processos de emissão, expedição, distribuição ou gerenciamento de carimbos do tempo implementam, entre outras, as seguintes características:

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

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

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 Safeweb;

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

f) mecanismos para cópias de segurança (*backup*).

6.5.1.2 Essas características serão 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.

6.5.1.3 Qualquer equipamento, ou parte desses, ao ser enviado para manutenção terá 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 Safeweb, o equipamento que passou por manutenção será inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, serão destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da ACT Safeweb. Todos esses eventos serão registrados para fins de auditoria.

6.5.1.4 Qualquer equipamento incorporado à ACT Safeweb será 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.

6.5.2 Classificação da Segurança Computacional

6.5.2.1 A segurança computacional da ACT Safeweb segue as recomendações *Common Criteria*.

6.5.3 Características do SCT

6.5.3.1 O Sistema 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.

6.5.3.2 O SCT mantém sincronizado o seu relógio interno com a fonte confiável do tempo (FCT). A avaliação da manutenção desse sincronismo é realizada pela Entidade Auditoria do Tempo (EAT).

6.5.3.3 MSC associado ao SCT é aquele que, conectado de forma segura ao SCT, seja situado internamente ou externamente a este, armazena as chaves criptográficas usadas para assinaturas digitais, como por exemplo em carimbos do tempo.

6.5.3.4 Qualquer MSC associado externamente a um SCT está instalado e operando no mesmo nível 4 de acesso físico do SCT.

6.5.3.5 O SCT garante que a emissão dos carimbos do tempo será feita em conformidade com o tempo constante do seu relógio interno e que a assinatura digital do carimbo do tempo será feita por um MSC associado.

6.5.3.6 O SCT utilizado pela ACT Safeweb possui como características:

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;

d) permitir identificação e registro de todas as ações executadas e dos carimbos do tempo emitidos;

e) garantir a irretroatividade na emissão de carimbos do tempo;

f) prover meios para que a EAT possa auditar e sincronizar o seu relógio interno;

g) garantir que o acesso da EAT seja realizado através de autenticação mútua entre o SCT e o SAS, utilizando certificados digitais;

h) possuir certificado de especificações emitido pelo fabricante;

i) somente emitir carimbo do tempo se:

i. possuir alvará vigente emitido pela EAT, a fim de garantir que a precisão do sincronismo do seu relógio esteja de acordo com o relógio da FCT;

ii. for assinado por certificado digital válido emitido por AC credenciada na ICP-Brasil.

6.5.4 Ciclo de Vida de Módulos Criptográficos Associados aos SCTs

6.5.4.1 A instalação e a ativação do HSM no SCT são realizadas sempre com a presença de no mínimo duas pessoas formalmente designadas para a tarefa em ambiente seguro e controlado.
6.5.4.2 Para a geração de chaves é necessária a autenticação para acessar a interface administrativa.

6.5.5 Auditoria e Sincronização de Relógio de SCT

6.5.5.1 A ACT Safeweb certifica-se que seus SCTs estejam sincronizados com o FCT dentro da precisão declarada na PCT respectiva e, particularmente, que:

a) os valores de tempo utilizados pelo SCT na emissão de carimbos do tempo são rastreáveis até a hora da FCT;

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

c) os relógios dos SCTs são 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 a FCT 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.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 Controles de Desenvolvimento de Sistema

6.6.1.1 O desenvolvimento de sistemas baseia-se em metodologia ágil – uma abordagem iterativa, dividida em ciclos chamados de *sprints*. Ao final de cada ciclo é feita uma entrega com novas funcionalidades até a aprovação final do sistema.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela ACT Safeweb provêem documentação suficiente para suportar avaliações externas de segurança dos componentes da ACT.

6.6.2 Controles de Gerenciamento de Segurança

6.6.2.1 A ACT Safeweb verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2 A ACT Safeweb utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3 Classificações de Segurança de Ciclo de Vida

6.6.3.1 A maturidade do ciclo de vida do Servidor de Aplicativo (SA) e a do Sistema de Carimbo do Tempo (SCT) atendem ao nível do *Capability Maturity Model Software Engineering Institute* (CMM-SEI).

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 Diretrizes Gerais

6.7.1.1 Neste item da DPCT são descritos os controles relativos à segurança da rede da ACT Safeweb, incluindo *firewalls* e recursos similares, observado o disposto no item sobre "redes das entidades da ICP-Brasil" da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.7.1.2 Todos os servidores e elementos de infraestrutura e proteção de rede, tais como: roteadores, *hubs*, *switches*, *firewalls* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o SCT, estão localizados e operam em ambiente de nível 4.

6.7.1.3 As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

6.7.1.4 O acesso lógico aos elementos de infraestrutura e proteção de rede é restrito por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.1.5 O acesso à Internet é provido por no mínimo duas linhas de comunicação de sistemas autônomos (AS) distintos.

6.7.1.6 O acesso via rede aos SCTs e sistemas de gestão da ACT é permitido somente para os seguintes serviços:

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

b) pela ACT Safeweb, 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 Safeweb, 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.

6.7.2 *Firewall*

6.7.2.1 Mecanismos de *firewall* são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Os *firewalls* são 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 Safeweb.

6.7.2.2 O *software* de *firewall*, entre outras características, implementa registros de auditoria.

6.7.2.3 As regras dos *firewalls* são revisadas periodicamente, 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.

6.7.3 Sistema de Detecção e Prevenção de Intrusão (IDS/IPS)

6.7.3.1 O sistema de detecção e prevenção de intrusão tem a 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*.

6.7.3.2 O sistema de detecção e prevenção de intrusão tem a capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

6.7.3.3 O sistema de detecção e prevenção de intrusão provê o registro dos eventos em *logs* recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4 Registro de Acessos Não Autorizados à Rede

6.7.4.1 As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS/IPS – são registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro é semanal e todas as ações tomadas em decorrência desse exame são documentadas.

6.7.5 Outros Controles de Segurança de Rede

6.7.5.1 A ACT Safeweb implementa 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.

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

6.7.5.3 Os relógios dos SCTs estão 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 será registrada e detectada.

6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

6.8.1 O módulo criptográfico utilizado para armazenamento da chave privada dos SCTs da ACT Safeweb está em conformidade com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

7 PERFIS DOS CARIMBOS DO TEMPO

7.1 DIRETRIZES GERAIS

7.1.1 Nos seguintes itens são descritos os aspectos dos carimbos do tempo emitidos pela ACT Safeweb, bem como das requisições que lhes são enviadas.

7.2 PERFIL DO CARIMBO DO TEMPO

Todos os carimbos do tempo emitidos pela ACT Safeweb estão em conformidade com o formato definido pelo Perfil de Carimbo do tempo constante da *European Telecommunications Stardards Institute Technical Specification* 101861 (*ETSI TS* 101861) e seguem 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: SHA1, SHA256 e SHA512

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 usados: SHA1, SHA256 e SHA512

c) Tamanhos de chave a serem suportados: 2.048 bits e 4096 bits

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 usados: SHA256, SHA384 e SHA512

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. não se aplica;

v. não se aplica;

vi. campo de identificação do alvará vigente no momento da emissão do Carimbo do Tempo e válido conforme descrito em regulamento editado por instrução normativa da AC Raiz que defina o perfil do alvará do carimbo do tempo da ICP-Brasil.

b) Algoritmos a serem usados: SHA256 e SHA512

c) Tamanhos de chave a serem suportados: 2048 bits e 4096 bits

7.2.3 Perfil do Certificado do SCT

7.2.3.1 A ACT Safeweb assina cada mensagem de carimbo do tempo com uma chave privada específica para esse uso. A ACT Safeweb 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 contém apenas uma instância do campo de extensão, conforme definido na RFC 3280, com o subcampo *KeyPurposeID* contendo o valor *id-kptimeStamping*. Essa extensão é 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

7.2.4.1 O certificado digital emitido para os SCTs da ACT Safeweb adota o *"Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = ACT Safeweb

CN = < nome do Servidor de Carimbo do Tempo >

7.3 PROTOCOLOS DE TRANSPORTE

7.3.1 O seguinte protocolo definido na RFC 3161 é suportado: *Time Stamp Protocol* via HTTP.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

8.1.1 Conforme o documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

8.2.1 As fiscalizações das ACTs da ICP-Brasil e de seus PSSs são realizadas pela EAT, 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].

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

a) quanto aos procedimentos operacionais, pela EAT, 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 à autenticação e ao sincronismo dos SCTs, pela Entidade de Auditoria do Tempo (EAT) observado o disposto no documento PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3].

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

8.3.1 Em acordo com o documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO

8.4.1 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.

8.4.2 A ACT Safeweb recebeu auditoria prévia da EAT para fins de credenciamento na ICP-Brasil em 2014, e 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.

8.4.3 A ACT Safeweb 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 AUDITORIA DO TEMPO NA ICP-BRASIL [3].

8.4.4 As entidades da ICP-Brasil diretamente vinculadas à ACT Safeweb também receberam auditoria prévia, para fins de credenciamento, e a ACT Safeweb é responsável pela realização de auditorias anuais dessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo 8.2.2.

8.5 AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

8.5.1 Em acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[7] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

8.6 COMUNICAÇÃO DOS RESULTADOS

8.6.1 Em acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[7] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 TARIFAS DE SERVIÇO

9.1.1 Tarifas de emissão de carimbos do tempo

Pelo carimbo de tempo emitido será cobrado o valor estabelecido contratualmente.

9.1.2 Tarifas de acesso ao carimbo do tempo

Pelo acesso ao carimbo de tempo será cobrado o valor estabelecido contratualmente.

9.1.3 Tarifas de revogação ou de acesso à informação de status.

Não se aplica.

9.1.4 Tarifas para outros serviços

Para outros serviços será cobrado o valor estabelecido contratualmente.

9.1.5 Política de reembolso

Em caso de emissão imprópria ou defeituosa, imputável à ACT Safeweb, não haverá reembolso de tarifa, todavia será emitido outro carimbo do tempo em substituição, sem ônus adicional.

9.2 RESPONSABILIDADE FINANCEIRA

A responsabilidade da ACT Safeweb será verificada conforme previsto na legislação brasileira.

9.2.1 Cobertura do Seguro

Conforme item 4 desta DPCT.

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1 Escopo de Informações Confidenciais

9.3.1.1 São consideradas confidenciais as seguintes informações:

a) As chaves privadas dos SCTs;

b) as senhas e demais credenciais de acesso aos ambientes operacionais;

c) os dossiês dos funcionários da ACT Safeweb;

d) o PCN da ACT Safeweb;

e) conteúdo dos relatórios de auditorias (exceto a sua conclusão).

9.3.1.2 Nenhum documento, informação ou registro fornecido pelo subscritor à ACT Safeweb ou aos PSSs vinculados será divulgado, exceto quando for estabelecido um acordo com o subscritor para sua publicação mais ampla.

9.3.2 Informações fora do Escopo de Informações Confidenciais

9.3.2.1 As informações consideradas não sigilosas pela ACT Safeweb e pelos PSSs a ela vinculados, compreendem:

a) os certificados dos SCTs;

b) a PCT implementada pela ACT Safeweb;

c) esta DPCT;

d) versões públicas de PS; e

e) a conclusão dos relatórios de auditoria.

9.3.3 Responsabilidade em Proteger a Informação Confidencial

9.3.3.1 Os participantes que receberem ou tiverem acesso a informações confidenciais devem possuir mecanismos para assegurar a proteção e a confidencialidade, evitando o seu uso ou divulgação a terceiros, sob pena de responsabilização, na forma da lei.

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

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1 Plano de privacidade

9.4.1.1 A ACT Safeweb assegura a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2 Tratamento de Informação como Privadas

9.4.2.1 Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à ACT Safeweb será considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

9.4.3 Informações não Consideradas Privadas

9.4.3.1 Não se aplica.

9.4.4 Responsabilidade para Proteger a Informações Privadas

9.4.4.1 A ACT Safeweb é responsável pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5 Aviso e Consentimento para Usar Informações Privadas

9.4.5.1 As informações privadas obtidas pela ACT Safeweb poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável. O titular de certificado ou carimbo do tempo e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas. Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou

b) por meio de pedido escrito com firma reconhecida.

9.4.6 Divulgação em Processo Judicial ou Administrativo

9.4.6.1 Como diretriz geral, nenhum documento, informação ou registro sob a guarda da ACT Safeweb será fornecido a qualquer pessoa, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.

9.4.6.2 As informações privadas ou confidenciais sob a guarda da ACT Safeweb poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7 Outras Circunstâncias de Divulgação de Informação

9.4.7.1 Não se aplica.

9.4.8 Informações a terceiros

9.4.8.1 Como diretriz geral, nenhum documento, informação ou registro sob a guarda do PSS ou da ACT Safeweb é 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.

9.5 DIREITOS DE PROPRIEDADE INTELECTUAL

9.5.1 Os direitos de propriedade intelectual de certificados, carimbos do tempo, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas são tratados de acordo com a legislação vigente.

9.6 DECLARAÇÕES E GARANTIAS

9.6.1 Declarações e Garantias das Terceiras Partes

9.6.1.1 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.

9.6.1.2 Um carimbo emitido pela ACT Safeweb, ou qualquer outra 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 carimbo do tempo, ele deverá estar vigente no momento em que o carimbo do tempo foi emitido e estar aderente aos requisitos previstos em regulamento editado por instrução normativa da AC Raiz que defina o perfil do alvará do carimbo do tempo da ICP-Brasil.

9.6.1.3 O não exercício desses direitos não afasta a responsabilidade da ACT Safeweb e do subscritor.

9.7 Isenção de Garantias

Não se aplica.

9.8 Limitações de Responsabilidades

9.8.1 A ACT Safeweb não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação vigente.

9.9 Indenizações

9.9.1 A ACT Safeweb responde pelos danos que der causa, e lhe sejam imputáveis, na forma da legislação vigente, assegurado o direito de regresso contra o agente ou entidade responsável.

9.10 Prazo e Rescisão

9.10.1 Prazo

9.10.1.1 Esta DPCT entra em vigor a partir da publicação que a aprovar, e permanecerá válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.2 Término

9.10.2.1 Esta DPCT vigorará por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.3 Efeito da Rescisão e Sobrevivência

9.10.3.1 Os atos praticados na vigência desta DPCT são válidos e eficazes para todos os fins de direito, produzindo efeitos mesmo após a sua revogação ou substituição.

9.11 Avisos Individuais e Comunicações com os Participantes

9.11.1 Todas as notificações relevantes relativas às práticas descritas nesta DPCT serão enviadas através de e-mails aos participantes.

9.12 Alterações

9.12.1 Procedimento para Emendas

9.12.1.1 Qualquer alteração nesta DPCT é submetida à AC Raiz.

9.12.2 Mecanismo de Notificação e Períodos

9.12.2.1 Mudança nesta DPCT é publicada no repositório da ACT Safeweb.

9.12.3 Circunstâncias na Qual o OID Deve ser Alterado.

Não se aplica.

9.13 Solução de Conflitos

9.13.1 Os litígios decorrentes desta DPCT serão solucionados de acordo com a legislação vigente.

9.13.2 A DPCT da ACT Safeweb não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.13.3 Os casos omissos serão encaminhados para apreciação da EAT.

9.14 Lei Aplicável

9.14.1 Esta DPCT é regida pela legislação da República Federativa do Brasil, notadamente a Medida Provisória Nº 2.200-2, de 24.08.2001, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas em vigor no Brasil.

9.15 Conformidade com a Lei Aplicável

9.15.1 A ACT Safeweb está sujeita à legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em lei.

9.16 Disposições Diversas

9.16.1 Acordo Completo

9.16.1.1 Esta DPCT representa as obrigações e deveres aplicáveis à ACT Safeweb. Havendo conflito entre esta DPCT e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2 Cessão

9.16.2.1 Os direitos e obrigações previstos nesta DPCT são de ordem pública e indisponíveis, não podendo ser cedidos ou transferidos a terceiros.

9.16.3 Independência de Disposições

9.16.3.1 A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPCT não prejudicará as demais disposições, as quais permanecerão plenamente válidas e eficazes. Neste caso a disposição inválida, nula ou ineficaz será considerada como não escrita, de forma que esta DPCT será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes

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]	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-IPC-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 DIFITAL NO ÂMBITO DA ICP-BRASIL	DOC-ICP-10
[10]	PERFIL DO ALVARÁ DO CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12.01
[11]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

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.