DECLARAÇÃO DE PRÁTICAS DA AUTORIDADE DE CARIMBO DO TEMPO ACT ONR

Versão 1.2 – novembro de 2024

(Elaborada conforme DOC-ICP-12, Versão 2.1, de 18 de maio de 2021)

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
1.0	12.04.2023	-	-	Criação do documento
1.1	20.10.2023	-	1.5.2	Mudança de email
1.2	04.11.2024	-	1.5.3	Mudança de pessoa responsável pela adequação da DPCT

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 são devidamente documentadas e periodicamente auditadas pela própria EAT da ICP-Brasil. Os relógios dos Servidores de Carimbo do Tempo - SCTs são 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 Este documento que descreve as práticas e os procedimentos empregados pela ACT ONR na execução de seus serviços. De modo geral, a política de carimbo do tempo indica "o que deve ser cumprido" enquanto uma declaração de práticas da ACT indica "como cumprir", isto é, os processos que serão usados pela ACT para criar carimbos do tempo e manter a precisão do seu relógio.

1.1.5 Este documento tem como base as normas da ICP-Brasil, as RFC 3628 e 3161, do IETF e o documento TS 101861 do ETSI.

1.1.6 A estrutura desta DPCT está baseada no DOC-ICP-12 do Comitê Gestor da ICP-Brasil –

Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil. As referências a formulários presentes nesta DPCT são entendidas também como referências a outras formas que a ACT ONR possa vir a adotar.

1.1.7 Aplicam-se ainda à ACT ONR 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 ICP-BRASIL [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 ONR, a seguir designada simplesmente por DPCT da ACT ONR.

1.2.2. O OID deste documento é 2.16.76.1.5.14

1.3 Comunidade

1.3.1 Autoridades de Carimbo do tempo

1.3.1.1 Esta DPCT refere-se à ACT ONR, integrante da ICP-Brasil.

1.3.2 Prestador de Serviços de Suporte

1.3.2.1 O endereço da página web (URL) onde está publicada a relação de todos os PSSs vinculados à ACT ONR é: https://www.act.onr.org.br

1.3.2.2 PSS são entidades utilizadas pela ACT para desempenhar atividade descrita nesta DPCT ou na PCT e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infraestrutura física e lógica;

b) disponibilização de recursos humanos especializados; ou

c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.2.3 A ACT ONR mantém as informações acima sempre atualizadas.

1.3.3 Subscritores

1.3.3.1 Todas as pessoas físicas ou jurídicas poderão solicitar carimbos do tempo emitidos segundo esta DPCT.

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 ONR implementa a seguinte PCT:

Política de Carimbo do Tempo	Nome conhecido	OID
Política de Carimbo do Tempo da ACT ONR	PCT ACT ONR	2.16.76.1.6.14

1.4.2 A PCT define como os carimbos do tempo emitidos devem ser utilizados pela comunidade e relaciona as aplicações para as quais são adequados os carimbos emitidos pela ACT e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses carimbos. De forma resumida:

1.4.2.1. Os carimbos do tempo emitidos pela ACT ONR podem ser utilizados como referência temporal por aplicações ou processos de negócio que necessitem provar a existência de um determinado documento em relação a uma data específica.

1.4.2.2 Ao entrar no site http://www.oficioeletronico.com.br é necessário fazer um cadastro de pessoa física, deve utilizar seu certificado digital emitido por uma das Autoridades Certificadoras no âmbito da ICP-Brasil. No momento da assinatura do documento eletrônico o certificado digital deve estar válido.

1.4.2.3 Podem ser assinados: Contratos de qualquer natureza, Atas, Atestados, Apólices de seguro, Balanços, Diplomas, Laudos médicos ou técnicos, Notificações, Petições, Procurações, Relatórios, Certidões, Transcrições, Translado ou qualquer documento do Registro de imóveis, Tabelionato de notas ou registro civil entre outros documentos.

1.4.2.4 Todos os documentos eletrônicos assinados digitalmente no site Central Nacional do Documento Eletrônico estão no padrão de assinatura AD-RT (assinatura digital com carimbo de tempo).

1.4.2.5 Todos os participantes do fluxo de assinaturas: administrador, signatários e visualizadores receberão um e-mail com o link para acesso ao documento.

1.4.2.6 Uma assinatura digital com carimbo do tempo emitido pela ACT ONR, após consultada a LCR, garante a irretratabilidade da sua geração, pois o carimbo do tempo serve como evidência de que o certificado do signatário não estava revogado ou expirado no momento da assinatura.

1.5 Política de Administração

1.5.1 Organização administrativa do documento

Nome do responsável pela ACT: Operador Nacional Do Sistema De Registro Eletrônico De Imóveis - ONR,

1.5.2 Contatos

Endereço: st srtvs quadra 701 conjunto d bloco a, sn, sala 221 centro empresarial, asa sul, Brasília

Telefone: 11 2780-0328

Página web: https://www.act.onr.org.br

E-mail: actonr@onr.org.br

1.5.3 Pessoa responsável pela adequabilidade da DPCT e PCT

Nome: Diego Igor Fiorini

Telefone: +55 11 98751-1024

E-mail: diego.fiorini@onr.org.br

1.5.4 Procedimentos de aprovação da DPCT

Esta DPCT foi submetida à aprovação, durante o processo de credenciamento da ACT ONR, conforme 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	Declarações 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 ACT ONR publicará todas as informações obrigatórias em seu repositório, na página da internet https://act.onr.org.br/. A disponibilidade das informações publicadas pela ACT ONR 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, são publicadas pela ACT em página web:

a) os certificados dos SCTs que opera;
b) esta DPCT;
c) a PCT que implementa;
d) as condições gerais mediante as quais são prestados os serviços de carimbo do tempo;
e) a exatidão do carimbo do tempo com relação à FCT;
f) algoritmos de *hash* que poderão ser utilizados pelos subscritores e o algoritmo de *hash* utilizado pela ACT ONR;
g) uma relação, regularmente atualizada, dos PSSs vinculados.

2.2 Frequência de Publicação

2.2.1 As novas versões ou alterações desta DPCT e da PCT são publicadas no website da ACT ONR após aprovação da AC Raiz da ICP-Brasil. As demais informações de que trata o item anterior serão imediatamente atualizadas no repositório, sempre que sofrerem alterações, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

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 ONR.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 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.

3.2 No caso da ACT ONR, o serviço de Carimbo do Tempo será disponibilizado por meio do protocolo TSP (conforme descrito na RFC 3161). O cliente deve enviar uma solicitação de carimbo (timestamp query). O protocolo TSP é disponibilizado utilizando como meio de transporte protocolo HTTPS com autenticação cliente e HTTP com IP de origem. A autenticação do cliente é necessária para que o Servidor de Aplicativos identifique o subscritor e qual a sua modalidade de contabilidade.

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 deverá gerar 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 sistema do subscritor (oficioeletronico.com.br) e por meio da integração de aplicações que utilizem assinatura digital de documentos. A requisição de carimbo do tempo deverá estar no formato TSQ (conforme descrito na RFC 3161). O serviço de Carimbo do Tempo será disponibilizado por meio do protocolo TSP, conforme descrito na RFC 3161. O cliente deve enviar uma solicitação de carimbo (timestamp query). O protocolo TSP é disponibilizado pela internet, utilizando como meio de transporte protocolo HTTPS com autenticação cliente e HTTP com IP de origem.

O Servidor de Aplicativos da ACT ONR aceitará as solicitações de emissão de carimbo do tempo cujo certificado digital do subscritor esteja válido. O Servidor de Aplicativos da ACT ONR acessa o serviço de carimbo do tempo por meio do protocolo TCP/IP, no qual o cliente envia uma solicitação de carimbo de tempo e a ACT ONR envia uma resposta para a entidade solicitante.

A conferência do carimbo é feita pelo Servidor de Aplicativos da ACT ONR. Antes de a resposta ser enviada para o subscritor, é analisado o status de erro retornado na resposta. Caso nenhum erro tenha ocorrido, são verificados os vários campos contidos na resposta. Em particular, deve-se verificar se o que foi carimbado corresponde ao que foi solicitado. O próprio subscritor deve fazer uma segunda conferência ao receber o carimbo do tempo.

A PCT da ACT ONR define 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 Qualquer pessoa física ou jurídica poderá solicitar carimbos do tempo emitidos segundo esta DPCT.

4.1.2 Processo de registro e responsabilidades

Nos itens a seguir são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1 Responsabilidades da ACT

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

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

4.1.2.2 Obrigações da ACT

As obrigações da ACT ONR são as abaixo relacionadas:

a) operar de acordo com a sua DPCT e com as PCTs que implementa;

b) gerar, gerenciar e assegurar a proteção das chaves privadas dos SCTs;

c) manter os SCTs sincronizados e auditados pela 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, com a Rede de Carimbo do Tempo da ICP-Brasil;

g) permitir o acesso da EAT aos SCTs de sua propriedade;

h) notificar à AC emitente do seu certificado quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

i) notificar aos seus usuários quando ocorrer suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

j) publicar em sua página web sua DPCT, as PCTs aprovadas que implementa e os certificados de seus SCTs;

k) publicar em sua página web as informações definidas no item 2.2.2 deste documento;

l) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

m) adotar as medidas de segurança e controle previstas na DPCT, PCT e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

n) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

o) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

p) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);

q) manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, com cobertura suficiente e compatível com o risco dessas atividades;

r) informar às terceiras partes e subscritores de carimbos do tempo acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima; e

s) informar à 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 Neste item 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 ONR dispõe aos subscritores o acesso a um Servidor de Aplicativos (SA), encaminha as TSQs recebidas ao SCT e em seguida devolve ao subscritor os valores de hash devidamente carimbados.

4.2.3 O Servidor de Aplicativos se constitui de um sistema instalado em equipamento da ACT ONR, distinto do SCT.

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

4.2.5 O Servidor de Aplicativos executa as seguintes tarefas:

a) identifica e valida, se necessário, o usuário 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 *hashes* 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, realiza a seguinte sequência:

a) verifica se a requisição está de acordo com as especificações da norma RFC 3161. Caso esteja, realizar as demais operações a seguir descritas. Se a requisição estiver fora das especificações, o SCT responde de acordo com o item 2.4.2 da RFC 3161, com um valor de status diferente de 0 ou 1, e indicar no campo "PKIFailureInfo" qual foi a falha ocorrida sem emitir, neste caso, um carimbo do tempo e encerrando, sem executar as demais etapas;

b) produz carimbos do tempo apenas para solicitações válidas;

c) usa uma fonte confiável do tempo;

d) inclui um valor de tempo confiável para cada carimbo do tempo;

e) inclui na resposta um identificador único para cada carimbo do tempo emitido;

f) inclui em cada carimbo do tempo um identificador da política sob a qual o carimbo do tempo foi criado;

g) somente carimba o *hash* dos dados, e não os próprios dados;

h) verifica se o tamanho do *hash* recebido está de acordo com a função *hash* utilizada;

i) não examina o *hash* que está sendo carimbado, de nenhuma forma, exceto para verificar seu comprimento, conforme item anterior;

j) nunca inclui no carimbo do tempo algum tipo de informação que possa identificar o requisitante do carimbo do tempo;

k) assina 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) encadeia o carimbo do tempo atual com o anterior, caso a ACT tenha adotado o mecanismo de encadeamento.

4.2.7 A disponibilidade dos serviços de carimbo do tempo da ACT ONR é de, no mínimo, de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

4.3 Aceitação de Carimbos do Tempo

4.3.1 A solicitação de carimbo do tempo pelo subscritor ocorre por meio do uso de aplicação que faz a interface com a ACT ONR. 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 esteja presente, isto é, o status esteja 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.

4.3.2 Uma vez recebida a resposta (que é ou inclui um TimeStampResp, que normalmente contém um carimbo do tempo), a aplicação utilizada pelo 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 a aplicação utilizada pelo subscritor deve verificar se o que foi carimbado corresponde ao que foi enviado para carimbar. O Subscritor deve verificar também se o carimbo do tempo foi assinado pela ACT ONT e se estão corretos o *hash* dos dados e o OID do algoritmo de hash. Ela deve então verificar a tempestividade da resposta, analisando ou o tempo incluído na resposta, comparando-o com uma fonte local confiável de tempo, se existir, ou o valor do número de controle incluído na resposta, comparando-o com o número incluído no pedido. Se qualquer uma das verificações acima falhar, o carimbo do tempo deve ser rejeitado.

4.3.4 Além disso, o certificado do SCT pode ter sido revogado, o status do certificado é verificado para confirmar se ainda está válido. A seguir o subscritor deve checar também o campo policy para determinar se a política sob a qual o carimbo foi emitido é aceitável ou não para a aplicação.

4.3.5 Os processos acima são requisitos aplicáveis para aceitação dos carimbos do tempo da ACT ONR.

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

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

5.1 Segurança Física

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

5.1.1 Construção e localização das instalações de ACT

5.1.1.1 A ACT ONR não disponibiliza acesso físico ao público, uma vez que presta serviços de carimbo do tempo apenas pela Internet ou outro tipo de acesso por rede de dados.

A operação da ACT ONR está instalada em Data Center, em um ambiente segregado, com case totalmente fechado por grade, o acesso é somente por biometria e cartão de aproximação, monitorado por câmeras e na porta do rack B o acesso com cartão de aproximação nas duas portas no rack A está a ACT REGISTADORES com acesso com cartão de aproximação nas duas portas.

5.1.2 Acesso físico nas instalações de ACT

A ACT ONR implanta um sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a **POLÍTICA DE SEGURANÇA DA ICP- BRASIL [4]** e os requisitos que seguem.

5.1.2.1 Níveis de acesso

5.1.2.1.1 Existem (três) níveis de acesso físico aos diversos ambientes da ACT ONR e mais 1 (um) quarto nível relativo à proteção do SCT.

5.1.2.1.2 O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da ACT. O ambiente de nível 1 desempenha a função de interface com eventuais pessoas que necessitem comparecer à ACT.

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. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da ACT. A passagem do primeiro para o segundo nível 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 escritório, alvenaria ou pré-moldadas de gesso acartonado. Não existem 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 trabalhem diretamente com as atividades de carimbo do tempo ou ao pessoal responsável pela manutenção de sistemas e equipamentos da ACT, como administradores de rede e técnicos de suporte de informática. Demais funcionários da ACT ou do possível ambiente que esta compartilhe não possuem acesso a este nível.

5.1.2.1.6 *No-breaks*, geradores e outros componentes da infraestrutura física estão abrigados neste nível, para evitar acessos ao ambiente de nível 3 por parte de prestadores de serviços de manutenção.

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

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

5.1.2.1.9 No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: cartão magnético para identificação e ativação do sistema e identificação biométrica para abrir a porta.

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

5.1.2.1.11 Como o ambiente de Nível 3 possui forro ou piso falsos, para impedir o acesso ao ambiente por meio desses, são adotadas grades de ferro estendendo-se das paredes até as lajes de concreto superior e inferior.

5.1.2.1.12 Existe uma porta única de acesso ao ambiente de nível 3, que abre somente depois que o funcionário se autenticou 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, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário.

5.1.2.1.13 NA ACT ONR existe um único ambiente de nível 3 que abriga:

a) equipamentos de produção e cofre de armazenamento; e

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

5.1.2.1.14 Embora a ACT ONR se situe dentro de um datacenter, optou-se por criar um ambiente de Nível 3 específicos para a ACT.

5.1.2.1.15 O quarto nível, ou nível 4, interior ao ambiente de nível 3, gabinetes reforçados trancados com cartão de aproximação e chave física nas duas portas, que abrigam.

a) os SCT e equipamentos criptográficos;

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

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

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

b) possuem tranca com chave.

5.1.2.1.17 O gabinete que abriga os SCTS é trancado de forma que sua abertura seja possível somente com a presença de dois funcionários de confiança da ACT. Ele é trancado com duas fechaduras: uma é comum e a outra é um cartão magnético das pessoas autorizadas a abrir.

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:

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

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

5.1.2.2.3 O ambiente de nível 3 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 2.

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 3.

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

5.1.3.1 A infraestrutura do ambiente de nível 3 da ACT está dimensionada com sistemas e dispositivos que garantam 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 São 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. São 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 aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente.

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

5.1.3.9 A capacidade de redundância de toda a estrutura de energia e ar-condicionado do ambiente de nível 3 da ACT é garantida por meio de nobreaks e geradores de porte compatível.

5.1.4 Exposição à água nas instalações de ACT

5.1.4.1 O ambiente de nível 3 da ACT 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

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

5.1.5.2 A prevenção de incendido do nível 2 possui um sistema de detecção e monitoramento de partículas no ar. Qualquer anomalia é notificada ao monitoramento. No combate ao incêndio é utilizado um gás chamado agente extinto rde incêndio HFC-125, que atua de duas formas:

- Reação física que esfria as chamas;
- Reação química, onde a substância reage com o fogo eliminando as chamas.

O prédio também tem um sistema de sprinklers a seco e ativado apenas na região em que um eventual incêndio esteja ocorrendo de forma a minimizar os danos aos equipamentos

5.1.5.3 Todos os ambientes possuem sistema de prevenção contra incêndios, que acionam alarmes preventivos uma vez detectadas partículas no ar ou fumaça no ambiente.

5.1.5.4 Nos demais ambientes da ACT existem extintores de incêndio para as classes de fogo B e C, dispostos em locais que facilitam o seu acesso e manuseio.

5.1.5.5 Mecanismos específicos foram implantados pela ACT para garantir a segurança de seu pessoal 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 de ACT

5.1.6.1 A ACT ONR armazena as mídias no cofre instalado dentro do gabinete e 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 de ACT

5.1.7.1 Todos os documentos em papel que contenham informações classificadas como sensíveis 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

5.1.8.1 Os backups são armazenados em sala externa ao ambiente da ACT ONR e atendem aos requisitos mínimos estabelecidos por esse documento. A sala tem câmeras de monitoramento dentro e fora, biometria na porta, armário e um cofre acionado por senha ou chave.

5.2 Controles Procedimentais

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

5.2.1 Perfis qualificados

5.2.1.1 A ACT ONR 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 estão limitadas de acordo com seu perfil.

5.2.1.2 A ACT estabelece seis perfis distintos para sua operação, a saber:

a) **Administrador de ACT**-Autorizado a instalar, configurar e manter os sistemas confiáveis para gerenciamento do carimbo do tempo, bem como administrar a implementação das práticas de segurança da ACT, realizar as renovações dos certificados dos SCTs. O Administrador de ACT também tem as funções de Gerente da ACT.

b) **Operador de ACT**-Autorizado a realizar tarefas operacionais no Servidor de Carimbo do tempo dentre elas as configurações do sistema, rotinas de backup, análise de logs;

c) **Auditor de ACT**-Autorizado a ver arquivos e auditar os logs de todos os sistemas confiáveis da ACT.

d) **Analista de Infraestrutura**– Responsável pelas instalações de equipamentos da ACT. Autorizado a realizar tarefas operacionais nos equipamentos de rede (firewall, switches, etc.), como configuração, rotinas de backup, coleta de logs e análise de logs. Autorizado a realizar tarefas operacionais nos demais equipamentos da ACT (servidor de arquivos, servidor de controle de acesso, servidor de

CFTV e outros) dentre elas as configurações dos servidores, execução de rotinas de backup, coleta e análise de logs.

e) **Analista de segurança/Redes** - Autorizado a realizar tarefas operacionais nos equipamentos de rede (firewall, switches etc.), como configuração, rotinas de backup, coleta de logs e análise de logs.

f) **Analista de Plataforma** - Autorizado a realizar tarefas operacionais nos demais equipamentos da ACT (servidor de arquivos, servidor de controle de acesso, servidor de CFTV e outros) dentre elas as configurações dos servidores, execução de rotinas de backup, coleta e análise de logs.

5.2.1.3 Todos os empregados da ACT 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 desliga da ACT, suas permissões de acesso são revogadas imediatamente. Quando ocorre mudança na posição ou função que o empregado ocupa dentro da ACT, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à ACT no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1 Existe controle multiusuário para a geração da chave privada dos SCTs operados pela ACT ONR, na forma definida no item 6.1.1.

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

5.2.3 Identificação e autenticação para cada perfil

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

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

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

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

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

a) diretamente atribuídos a um único empregado;

b) não compartilhados; e

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

5.2.3.3 A ACT 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 requisitos e procedimentos, implementados pela ACT ONR 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 ONR e PSS vinculados, encarregados de tarefas operacionais terão registrado em contrato ou termo de responsabilidade:

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

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 ONR e dos PSSs 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 ONR poderá definir requisitos adicionais para a admissão.

5.3.2 Procedimentos de verificação de antecedentes

5.3.2.1 Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da ACT ONR 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 ONR poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

5.3.3.1 Todo o pessoal da ACT ONR e dos PSSs vinculados envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados 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;

b) ICP-Brasil;

c) princípios e tecnologias de certificação digital e de assinaturas eletrônicas;

d) princípios e mecanismos de segurança de redes e segurança da ACT;

e) procedimentos de recuperação de desastres e de continuidade do negócio;

f) familiaridade com procedimentos de segurança, para pessoas com responsabilidade de Oficial de Segurança;

g) familiaridade com procedimentos de auditorias em sistemas de informática, para pessoas com responsabilidade de Auditores de Sistema;

h) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

5.3.4.1 Todo o pessoal da ACT ONR 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.

5.3.5 Frequência e sequência de rodízio de cargos

5.3.5.1 Não estabelecido.

5.3.6 Sanções para ações não autorizadas

5.3.6.1 Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa encarregada de processo operacional da ACT ONR ou de um PSS vinculado, a ACT, 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 contém, 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 ONR encaminha 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 ONR 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]**.

5.3.8 Documentação fornecida ao pessoal

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

a) sua DPCT;

b) as PCTs que implementa;

c) a PS da AC ONR;

d) documentação operacional relativa às suas atividades; e

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

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

5.4 Procedimentos de Log de Auditoria

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela ACT ONR com o objetivo de manter um ambiente seguro.

5.4.1 Tipos de eventos registrados

5.4.1.1 A ACT ONR registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos estão 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 ONR 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 Além dos já citados, a ACT ONR registra todos os logs das carimbadoras, os de emissão dos carimbos bem como os logs do acesso ao SCT e os logs de auditoria do Sistema operacional, logs dos firewalls, switch, logs de aplicação, logs de acesso ao case no data center, câmeras de monitoramento.

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 contêm 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 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 O pessoal operacional da ACT ONR analisa os registros de auditoria em periodicidade não superior a uma semana. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve 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 são documentadas.

5.4.3 Período de retenção para registros de auditoria

5.4.3.1 A ACT ONR mantém localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena-os da 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.

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 ONR têm cópias de segurança semanais, feitas pelos administradores de sistemas. Estas cópias são enviadas ao departamento de segurança.

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

5.4.6.1 . O sistema interno de coleta de dados de auditoria da ACT ONR é 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 ONR, 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 ONR, serão analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela ACT e registradas para fins de auditoria.

5.5 Arquivamento de Registros

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

5.5.1 Tipos de registros arquivados

5.5.1.1 Os tipos de registros arquivados compreendem, entre outros:

a) notificações de comprometimento de chaves privadas do SCT;

b) substituições de chaves privadas dos SCTs;

c) informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo

5.5.2.1 O período de retenção para cada registro arquivado, incluindo os carimbos do tempo emitidos e as demais informações, inclusive arquivos de auditoria, é 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 ONR, recebendo o mesmo tipo de proteção utilizada por ela 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 ONR 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, 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 ONR 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 ONR ou ao Prestador de Serviço de Suporte (PSS), 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, é necessário adicionar um novo TSA, informando os atributos de configuração relativos a TSA como: Nome, OID da Política, Algoritmos de hash aceitos, encoding do TAC e tipo de source audit. zW pelo equipamento e nele armazenada. Após concluída geração da chave, o administrador deverá solicitar geração da CSR preenchendo os campos solicitados. O sistema retornará a CSR em formato Base64 RSA 2048 String, que será enviada à AC para que possa ser gerado o certificado.

5.6.2. Na existência de uma chave privada em uso pelo SCT, ela não será substituída pela nova chave gerada. Ela continuará armazenada até que o administrador do sistema decida que o seu uso será descontinuado e será substituída pela nova chave privada.

5.6.3. 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 A seguir são descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no Plano de Continuidade de Negócios (PCN) da ACT ONR, estabelecido conforme a **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**, para garantir a continuidade dos seus serviços críticos.

5.7.1.2 A ACT ONR assegura, no caso de comprometimento de sua operação por qualquer um dos

motivos relacionados nos itens abaixo, que as informações relevantes são disponibilizadas aos subscritores e às terceiras partes. A ACT ONR disponibiliza 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 ONR, sempre que possível, ela disponibilizará 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 ONR.

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 de segurança da ACT ONR, 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 funcionários, devidamente treinados para essa situação. Caso haja necessidade, o gerente de segurança 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. Não há recuperação do certificado do SCT no caso de revogação. É necessária a geração de um novo par de chaves e o Administrador deve cadastrar o novo certificado do 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 de segurança do ACT ONR que acionam as equipes envolvidas, de forma a indispor temporariamente os serviços. É necessário que o certificado do SCT seja revogado. O SCT deve ser desabilitado no SGACT pelo Administrador. Não há recuperação da chave privada no caso de comprometimento, é necessária a geração de um novo par de chaves e o Administrador deve cadastrar o novo certificado de 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 aos gestores da 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 ONR 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 ONR, o gerente de operações da instalação operacional, responsável pela contingência, notifica o gerente de segurança 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 ONR;

b) monitorar e controlar o foco da contingência;

c) diminuir ao máximo os danos aos ativos de processamento da ACT ONR, 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 da DPCT descreve os requisitos e os procedimentos que serão adotados nos casos de extinção dos serviços da ACT ONR ou de um PSS a ela vinculado.

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

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

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

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

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

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

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

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

g) a ACT notificará todas as entidades afetadas.

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

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPCT define as medidas de segurança implantadas pela ACT ONR para proteger suas chaves criptográficas e manter o sincronismo de seus SCTs. Também são definidos outros controles técnicos de segurança utilizados pela ACT e pelos PSSs vinculados na execução de suas funções operacionais.

6.1 Ciclo de Vida de Chave Privada do SCT

O SCT permite:

a) geração do par de chaves criptográficas;

b) geração de requisição de certificado digital;

c) exclusão de requisição de certificado digital;

d) instalação de certificados digitais;

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

f) proteção de chaves privadas.

6.1.1 Geração do par de chaves

6.1.1.1 O par de chaves criptográficas dos SCTs da ACT ONR é gerado pela própria ACT, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP- Brasil.

6.1.1.2 A ACT assegura que quaisquer chaves criptográficas são geradas em circunstâncias controladas. Em particular:

a) 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 é limitado àqueles que receberam essa responsabilidade de acordo com as práticas da ACT;

b) a geração da chave de assinatura do SCT é 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 são aqueles constantes no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [11]. O tamanho das chaves criptográficas associadas ao certificado da ACT ONR é de 2048 bits.

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

6.1.2 Geração de Requisição de Certificado Digital

6.1.2.1 O SCT possui mecanismo para geração de requisição de certificado digital correspondente à chave privada gerada no módulo criptográfico associado ao SCT, que atende ao formato definido pela 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 implica a exclusão da chave privada correspondente.

6.1.4 Instalação de Certificado Digital

6.1.4.1 O SCT realiza, no mínimo, a conferência dos itens descritos a seguir antes da instalação do certificado:

a) verifica se chave privada correspondente a esse certificado se encontra 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 par de chaves. Os procedimentos a serem seguidos são os mesmos da geração de um novo par de chaves, com a única diferença que os dados do certificado são apenas conferidos pelo usuário administrador com acesso à interface segura e controlada, não podendo ser mudados e um novo par de chaves é gerado.

6.1.6 Disponibilização de chave pública da ACT para usuários

6.1.6.1. A ACT ONR disponibiliza o certificado de seus SCT e todos os certificados da cadeia de certificação para os usuários da ICP-Brasil, por meio do endereço de Internet http://act.onr.org.br/repositorio/.

6.1.7 Tamanhos de chave

6.1.7.1 A PCT implementada pela ACT ONR 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]**. O tamanho das chaves criptográficas associadas ao certificado da ACT ONR é de 2048 bits.

6.1.8 Geração de parâmetros de chaves assimétricas

6.1.8.1 Os parâmetros de geração de chaves assimétricas da ACT ONR 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 ONR é feito por hardware.

6.1.11 Propósitos de uso de chave

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

6.2 Proteção da Chave Privada

Nos itens seguintes, estão definidos os procedimentos de segurança que a ACT ONR adota para a proteção da chave privada de seus SCTs.

6.2.1 Padrões para módulo criptográfico

6.2.1.1 O módulo criptográfico de geração e guarda de chaves assimétricas da ACT ONR 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 permitida, 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 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 em hardware criptográfico é ativada mediante identificação dos operadores responsáveis por meio de login/senha ou certificado digital.

6.2.7.2. A chave privada é ativada somente se existir um alvará válido emitido pela EAT responsável.

6.2.8 Método de desativação de chave privada

6.2.8.1. A chave privada do SCT em hardware criptográfico é desativada mediante identificação dos operadores responsáveis por meio de login/senha ou de 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 SCT da ACT ONR, após a expiração dos certificados correspondentes, serão guardadas pela AC que emitiu os certificados, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas dos SCTs da ACT ONR 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

Não se aplica.

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

A seguir estão indicados os mecanismos utilizados para prover a segurança de suas estações de trabalho, servidores e demais sistemas e equipamentos, observado o disposto no item 9.3 da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.1.1 Os SCTs e os equipamentos da ACT ONR, 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;

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

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

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

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

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

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

6.5.1.4 Qualquer equipamento incorporado à ACT é 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 ONR 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 deverá estar instalado e operando no mesmo nível 4 de acesso físico do SCT.

6.5.3.5 O SCT deve garantir 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 As características dos SCTs utilizados pela ACT ONR são:

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. Para a geração de chaves é necessária a autenticação com certificado digital para acessar a interface administrativa.

6.5.5 Auditoria e Sincronização de Relógio de SCT

6.5.5.1 A ACT ONR certifica-se que seus SCTs estejam sincronizados com a FCT dentro da precisão declarada nas PCTs respectivas e, particularmente, que:

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

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

c) os relógios dos SCTs estejam protegidos contra-ataques, incluindo violações e imprecisões

causadas por sinais elétricos ou sinais de rádio, evitando que sejam descalibrados e permitindo que qualquer modificação possa ser detectada;

d) a ocorrência de perda de sincronização do valor do tempo indicado em um carimbo do tempo com 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

Nos itens seguintes estão descritos os controles implementados pela ACT ONR e pelos PSSs a ela vinculados no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1 Controles de desenvolvimento de sistema

6.6.1.1. O desenvolvimento do sistema utilizado na ACT ONR baseia-se na metodologia SCRUM – um framework (caixa de ferramentas) de desenvolvimento iterativo e incremental utilizado no gerenciamento de projetos e desenvolvimento de software ágil. O processo de desenvolvimento pode ser dividido em: planejamento, produção e delivery. Cada uma dessas fases é executada em pequenos *sprints*, compostos pelas seguintes práticas:

- Planejamento de Sprint *(SprintPlanning)*: Avaliação da relevância e complexidade de cada atividade para a definição de prioridades e seus executores –aqui os requisitos são melhor detalhados;
- Líder Técnico (*coach*): A arquitetura das soluções égerida por um líder técnico;
- Reunião rápida diária (*Daily Meeting*): Diariamente os executores das atividades se reportam aos seus colegas e superiores compartilhando o status e as dificuldades da atividade;
- Padrão de codificação (*Coding Style*): Normalização dos métodos de codificação e documentação de código;
- Inspeção de Código (*Code Review*): Cada atividade gera um resultado que precisa ser revisado por outro executor antes de ser marcada como pronta;
- Testes (*Tests*): A equipe de qualidade produz testes diversos, inclusive testes automáticos nas atividades de código. Em caso de não conformidade, o desenvolvimento é reiniciado até que todos os critérios sejam aprovados.
- Homologação (*UAT*): As entregas são homologadas pelo cliente antes de enviadas ao ambiente de produção.

6.6.1.1 Os processos de projeto e desenvolvimento conduzidos pela ACT ONR proveem documentação suficiente para suportar avaliações externas de segurança dos componentes da ACT ONR.

6.6.2 Controles de gerenciamento de segurança

6.6.2.1. A ACT ONR e seus Prestadores de Serviço de Suporte, verificam 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.

6.6.2.1 A ACT ONR utiliza o disposto no item "Requisito de segurança do ambiente físico" e "Requisito de segurança do ambiente lógico" da POLÍTICA DE SEGURANÇA DA ICP-BRASIL para 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 Não se aplica.

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

6.7 Controles de Segurança de Rede

6.7.1 Diretrizes Gerais

6.7.1.1 Neste item da DPCT estão descritos os controles relativos à segurança da rede da ACT ONR, incluindo *firewall* 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*, *firewall* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda os SCT, estão localizados e operam em ambiente nível 3.

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

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

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

6.7.2 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 subredes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à ACT.

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

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

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1 O sistema de detecção de intrusão possui 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 de intrusão possui 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 de 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

As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – são registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro é, no mínimo, 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 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 é 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 ONR utiliza os padrões de referência definidos no documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11]**.

6.8.2 O tamanho das chaves criptográficas associadas ao certificado da ACT ONR é de 2048 bits.

7 PERFIS DOS CARIMBOS DO TEMPO

7.1 Diretrizes Gerais

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

7.2 Perfil do Carimbo do tempo

Todos os carimbos do tempo emitidos pela ACT ONR 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: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11]**.

7.2.1.2 Perfil do formato da resposta

a) Parâmetros a serem suportados:

i. o campo *accuracy* deve ser suportado e compreendido;

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

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

iv. nenhuma extensão necessita ser tratada ou suportada.

b) Algoritmos a serem suportados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11]**.

c) Tamanhos de chave a serem suportados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11]**.

7.2.2 Requisitos para um servidor TSP

7.2.2.1 Perfil para o formato do pedido

a) Parâmetros a serem suportados:

i. não necessita suportar nenhuma extensão;

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

b) Algoritmos a serem suportados: Consultar documento **PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11]**.

7.2.2.2 Perfil do formato da resposta

a) Parâmetros a serem suportados:

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

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

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

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

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

vi. campo de identificação do alvará vigente no momento da emissão do 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 suportados: Consultar **documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11]**.

c) Tamanhos de chave a serem suportados: Consultar **documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].**

7.2.3 Perfil do Certificado do SCT

7.2.3.1 A ACT assina cada mensagem de carimbo do tempo com uma chave privada específica para esse uso.

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-kp- timeStamping. 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 o SCT da ACT adota o “Distinguished Name” (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = Autoridade de Carimbo do Tempo ONR

CN = < nome do Servidor de Carimbo do tempo >

7.3 Protocolos de transporte

7.3.1. O serviço é disponibilizado por meio do protocolo TSP (conforme descrito na RFC 3161), onde o cliente deve enviar uma solicitação de carimbo. O protocolo TSP é disponibilizado utilizando como meio de transporte o protocolo HTTPS com autenticação cliente.

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 ONR recebeu auditoria prévia da EAT para fins de credenciamento na ICP-Brasil 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 ONR 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 ONR também receberam auditoria prévia, para fins de credenciamento, e a ACT é responsável pela realização de auditorias anuais nessas 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

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

9.1.1 Tarifas de emissão de carimbos do tempo

Variável conforme definição interna da ACT ONR.

9.1.2 Tarifas de acesso ao carimbo do tempo

Não são cobradas tarifas de acesso ao carimbo de tempo emitido.

9.1.3 Tarifas de revogação ou de acesso à informação de status

Variável conforme definição interna da ACT ONR.

9.1.4 Tarifas para outros serviços

Variável conforme definição interna da ACT ONR.

9.1.5 Política de reembolso

Variável conforme definição interna da ACT ONR.

9.2 Responsabilidade Financeira

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

9.2.1 Cobertura do seguro

Conforme item 9.6. Declarações e Garantias da DPCT.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

9.3.1.1 Como princípio geral, todo documento, informação ou registro fornecido à ACT ONR é considerado sigiloso pela ACT ONR, de acordo com as normas, critérios, práticas e procedimentos da ICP- Brasil.

9.3.1.2 Como princípio geral, nenhum documento, informação ou registro fornecido pelo subscritor à ACT ou aos PSSs vinculados é 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 ONR e pelos PSSs a ela vinculados compreendem, entre outros:

a) os certificados dos SCTs;

b) as PCTs implementadas pela ACT;

c) a DPCT da ACT;

d) versões públicas de PS; e

e) a conclusão dos relatórios de auditoria.

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 será gerada e mantida pela ACT, que será responsável pelo seu sigilo.

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

9.4.1.1 A ACT assegurará 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 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

9.3.1.3 Não se aplica.

9.4.4 Responsabilidade para proteger a informação privadas

9.4.4.1 A ACT 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 poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável. O titular de certificado 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 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 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 Nenhum documento, informação ou registro sob a guarda do PSS ou da ACT ONR 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, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas são tratados de acordo com a legislação

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 por ACT integrante da ICP-Brasil é considerado válido quando:

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

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

c) caso o alvará seja integrado no 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 ONR e do subscritor.

9.7 Isenção de garantias

Não se aplica

9.8 Limitações de responsabilidades

9.8.1 A ACT 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 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 Toda a comunicação necessária, relativas às práticas descritas nesta DPCT, serão enviadas através de e-mails aos participantes.

9.12 Alterações

9.12.1 Procedimento para emendas

Qualquer alteração nesta DPCT é submetida à AC Raiz.

9.12.2 Mecanismo de notificação e períodos

Mudança nesta DPCT será publicado no site da ACT.

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 ONR não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.13.3 Os casos omissos são 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 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. 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-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[8]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL	DOC-ICP-10
[10]	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 101861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.