IMPRENSA OFICIAL DO ESTADO SA IMESP

(ACT IMPRENSA OFICIAL)

DECLARAÇÃO DE PRÁTICAS DE CARIMBO DO TEMPO

VERSÃO 1.0 –23/11/2020

Histórico de Versões

Data	*Versão*	*Observações*
23/11/2020	1.0	Redação Inicial

AVISO LEGAL

Qualquer dúvida ou pedido de informação relativamente ao conteúdo deste documento deverá ser dirigido a certificacao@imprensaoficial.com.br.

Sumário

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 ICPBRASIL [3], documento aprovado pela Resolução nº 61, de 28 de novembro de 2008; e

e) PERFIL DO ALVARÁ DO CARIMBO DO TEMPO DA ICPBRASIL [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 de tempo são emitidos por terceiras partes confiáveis, as Autoridades de Carimbo do tempo – ACT, cujas operações devem ser devidamente documentadas e periodicamente auditadas pela própria EAT da ICP-Brasil. Os relógios dos servidores de Carimbo do Tempo- SCTs devem ser auditados e sincronizados por Sistemas de Auditoria e Sincronismo (SASs).

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

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

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

1.1.6 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 deverão ser entendidas também como referências a outras formas que a ACT IMPRENSA OFICIAL ou entidades a ela vinculadas possam vir a adotar.

1.1.7 Aplicam-se ainda à ACT IMPRENSA OFICIAL os regulamentos dispostos nos demais documentos da ICP-Brasil, entre os quais destacamos:

a) POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4];

b) CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5];

c) CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6];

d) CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7];

e) POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [8];

f) REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [9].

g) PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICPBRASIL [11].

1.2 Identificação

1.2.1 Esta DPCT é chamada Declaração de Práticas de Carimbo do Tempo da Autoridade de Carimbo do Tempo IMPRENSA OFICIAL, a seguir designada simplesmente por DPCT da ACT IMPRENSA OFICIAL.

1.2.2 O OID deste documento é 2.16.76.1.5.10.

1.3 Comunidade

1.3.1 Autoridade de Carimbo de Tempo

1.3.1.1 Esta DPCT refere-se à Autoridade de Carimbo do Tempo IMPRENSA OFICIAL – ACT IMPRENSA OFICIAL.

1.3.2 Prestador de Serviço de Suporte

1.3.2.1. A relação com o(s) PSS(s) vinculado(s) à ACT Imprensa Oficial está publicado no seguinte endereço https://certificadodigital.imprensaoficial.com.br/repositorio/.

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 IMPRENSA OFICIAL deverá manter as informações acima sempre atualizadas

1.3.3 Subscritores

1.3.3.1 A solicitação de carimbos do tempo poderá ser realizada por pessoa física ou jurídica que seja previamente cadastrada como usuário da ACT IMPRENSA OFICIAL e realize as solicitações de carimbo do tempo de forma remota conforme especificado na RFC3161. As requisições de carimbo do tempo deverão utilizar encapsulamento CMS utilizando certificado digital conforme recomendado na RFC-3161 item 2.4.1.

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 IMPRENSA OFICIAL implementa a seguinte Política de Carimbo do Tempo:

Política de Carimbo do Tempo	Nome conhecido	OID
Política de Carimbo do Tempo da ACT IMPRENSA OFICIAL	PCT IMPRENSA OFICIAL	2.16.76.1.6.10

1.5 Política de Administração

1.5.1 Organização administrativa do documento

ACT Imprensa Oficial

1.5.2 Contatos

Endereço: Rua da Mooca, 1921 – Mooca – São Paulo, SP

Telefone: (55 11) 0800 0123401

Fax: (55 11) 2799 9887

Pagina Web: https://certificadodigital.imprensaoficial.com.br/

Email: certificacao@imprensaoficial.com.br

1.5.3 Pessoa que determina a adequabilidade da DPCT com a PCT

Nome: Roseli Ramalho de Jesus Caccaos

Telefone: (55 11) 2799 9805

E-mail: certificacao@imprensaoficial.com.br

1.5.4 Procedimentos de aprovação da DPCT

Esta DPCT foi submetida à aprovação, durante o processo de credenciamento da ACT IMPRENSA OFICIAL, conforme o determinado pelo documento CRITÉRIOS E

PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC-RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
ASR	Autenticação e Sincronização de Relógio
CG	Comitê Gestor da ICP-BRASIL
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CN	*Common Name*
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPCT	Declaração de Práticas de Carimbo do tempo
EAT	Entidade de Auditoria do Tempo
ETSI	*European Telecommunication Standard Institute*
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infra-Estrutura 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 de 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 de Tempo
SNMP	Simple Network management Protocol
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
TSQ	Time Stamp Request
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

2.RESPONSABILIDADES DE PUBLICAÇÃO E RESPOSITÓRIO

2.1 Publicação de informação da ACT

2.1.1 A disponibilidade das informações publicadas pela ACT IMPRENSA OFICIAL na página da Internet https://certificadodigital.imprensaoficial.com.br/repositorio/ de 99,5% (noventa e nove e cinco décimos percentuais) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.2 As seguintes informações, no mínimo, são publicadas pela ACT IMPRENSA OFICIAL em sua página de Internet https://certificadodigital.imprensaoficial.com.br/repositorio/

a) os certificados dos SCTs que opera;
b) esta DPCT;
c) a PCT IMPRENSA OFICIAL;
d) as condições gerais mediante as quais são prestados os serviços de carimbo do tempo;
e) a exatidão do carimbo do tempo com relação ao UTC;
f) algoritmos de hash que poderão ser usados pelos subscritores e o algoritmo de hash utilizado pela ACT IMPRENSA OFICIAL;
g) uma relação, regularmente atualizada, dos PSS vinculados.

2.2 Frequência de Publicação

2.2.1 Os certificados dos SCT são publicados imediatamente após a sua emissão. As versões ou alterações desta DPCT e da PCT são atualizadas na página de Internet da ACT IMPRENSA OFICIAL após aprovação da AC Raiz da ICP-Brasil.

2.3 Controles 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 IMPRENSA OFICIAL.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

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

3.1.1 O padrão de assinatura é CMS do tipo Attached.

3.1.2 Após a identificação do subscritor, o TSQ é extraído da assinatura e é utilizado para dar andamento na emissão do carimbo de tempo.

3.2 Não se aplica.

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 de 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 resumo criptográfico da informação a ser carimbada. Para geração do resumo criptográfico, deverá ser utilizado o algoritmo SHA-256.

As solicitações de carimbo do tempo serão realizadas através de software específico disponibilizado ao subscritor ou através da integração de aplicações que utilizem assinatura digital de documentos.

Quando o subscritor utilizar o protocolo TCP, a requisição de carimbo do tempo TSQ deverá estar assinada pelo certificado do subscritor, utilizando-se o padrão de assinatura CMS definido na RFC 3852. O Servidor de Aplicativos da ACT IMPRENSA OFICIAL não aceitará as solicitações de emissão de carimbo do tempo cujo certificado do subscritor esteja expirado ou revogado.

Quando o subscritor utilizar os protocolos HTTP ou HTTPS, o cabeçalho da requisição deverá possuir as credenciais fornecidas pela ACT.

O Servidor de Aplicativos da ACT IMPRENSA OFICIAL dispõe o serviço de carimbo do tempo por meio dos protocolos TCP/IP utilizando a porta 318, HTTP utilizando a porta 80 e HTTPS utilizando a porta 443 de acordo com a RFC 3161.

A PCT IMPRENSA OFICIAL da ACT IMPRENSA OFICIAL 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 A solicitação de carimbos do tempo poderá ser realizada por pessoa física ou jurídica que seja previamente cadastrada como usuário da ACT IMPRENSA OFICIAL e realize as solicitações de carimbo do tempo de forma remota conforme especificado na RFC3161. As requisições de carimbo do tempo deverão utilizar encapsulamento CMS utilizando certificado digital conforme recomendado na RFC-3161 item 2.4.1.

4.1.2 Processo de registro e responsabilidades

4.1.2.1 Responsabilidades da ACT

4.1.2.1.1.A ACT IMPRENSA OFICIAL responde pelos danos a que der causa.

4.1.2.1.2 Não se aplica.

4.1.2.2 Obrigações da ACT

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. Os requisitos específicos associados a essas obrigações estão detalhados na PCT implementada pela ACT IMPRENSA OFICIAL.

a) operar de acordo com esta DPCT e com as PCT que implementa;
b) gerar, gerenciar e assegurar a proteção das chaves privadas dos SCTs;
c) manter os SCTs sincronizados e auditados pela EAT;
d) tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
e) monitorar e controlar a operação dos serviços fornecidos;
f) assegurar que seus relógios estejam sincronizados, com autenticação, à Rede de Carimbo do Tempo da ICP-Brasil;
g) permitir o acesso da EAT aos SCT de sua propriedade;
h) notificar a Autoridade Certificadora emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;
i) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
j) publicar em sua página de Internet a sua DPCT, as PCT aprovadas que implementa e os certificados de seus SCT;
k) publicar, em sua página web, as informações definidas no item 2.1.2 deste documento;
l) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
m) adotar as medidas de segurança e controle previstas na DPCT, PCT e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
n) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
o) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
p) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);
q) manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, com cobertura suficiente e compatível com o risco dessas atividades;
r) informar às terceiras partes e subscritores de carimbos do tempo acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
s) informar à EAT, mensalmente, a quantidade de carimbos do tempo emitidos.

4.1.2.3 Obrigações do Subscritor

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

4.2 Emissão de Carimbos do Tempo

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

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

4.2.3 O Servidor de Aplicativos se constitui de:

a) sistema instalado no próprio equipamento que realiza as funções de SCT;

b) sistema instalado em equipamento da ACT distinto do SCT;

c) Não se aplica;

d) uma combinação das soluções anteriores.

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

4.2.5 O Servidor de Aplicativos executa as seguintes tarefas:

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

b) receber os hashes que serão carimbados;

c) enviar ao SCT os hashes que serão carimbados;

d) receber de volta os hashes devidamente carimbados;

e) conferir a assinatura digital do SCT;

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

g) devolver ao usuário o hash devidamente carimbado;

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

i) emitir alarmes por e-mail aos responsáveis quando ocorrerem problemas de acesso aos SCTs.

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

a) Verifica se a requisição está de acordo com as especificações da norma RFC 3161. Caso esteja de acordo, realizar as demais operações a seguir descritas.

Se a requisição estiver fora das especificações, o SCT 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) produzir carimbos do tempo apenas para solicitações válidas;

c) usar uma fonte confiável de tempo;

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

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

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

g) somente carimbar o resumo criptográfico (rash) dos dados, e não os próprios dados;

h) verificar se o tamanho do rash recebido está de acordo com a função rash utilizada;

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

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

k) assinar cada carimbo do tempo com uma chave própria gerada exclusivamente para esse objetivo;

l) a inclusão de informações adicionais solicitadas pelo requerente deve ser feita nos campos de extensão suportados; caso não seja possível, responder com mensagem de erro;

m) encadear o carimbo do tempo atual com o anterior, caso a ACT tenha adotado o mecanismo de encadeamento.

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

4.3 Aceitação de Carimbos do Tempo

4.3.1 Os requisitos e procedimentos operacionais estabelecidos pela ACT IMPRENSA OFICIAL para aceitação de um carimbo do tempo recebido pelo subscritor são:

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), deverão ser verificados os próximos itens;

b) Comparar se o resumo criptográfico 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 resume criptográfico no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT;
d) Comparar se o número de controle (valor do campo nonce) presente no carimbo do tempo é igual ao da requisição (TSQ) enviada para ACT;
e) Verificar a validade da assinatura digital do SCT que emitiu o carimbo do tempo;
f) Verificar se o certificado do SCT é válido e não está revogado;
g) Verificar se o certificado do SCT possui o uso adequado para este objetivo, isto é, o certificado deve possuir o valor id-kp-timeStamping com o OID definido pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [11].

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

4.3.3 Em especial ele deve verificar se o que foi carimbado corresponde ao que foi enviado para carimbar. O subscritor deve verificar também se o carimbo do tempo foi assinado pela ACT IMPRENSA OFICIAL e se estão corretos o resumo criptográfico dos dados e o OID do algoritmo de resumo criptográfico. Ele deve então verificar a tempestividade da resposta, analisando ou o tempo incluído na resposta, comparando-o com uma fonte local confiável de tempo, se existir, ou o valor do número de controle incluído na resposta, comparando-o com o número incluído no pedido. Se qualquer uma das verificações acima falhar, o carimbo do tempo deve ser rejeitado.

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

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

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1 Segurança Física

Nos itens seguintes desta DPCT são descritos os controles de segurança usados pela ACT IMPRENSA OFICIAL, responsável pela DPCT, para executar de modo seguro as suas funções.

5.1.1 Construção e localização das instalações da ACT

5.1.1.1.1 A localização e o sistema de carimbo do tempo utilizado para a operação da ACT IMPRENSA OFICIAL não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de carimbo do tempo. Essas operações são segregadas em compartimentos fechados e fisicamente protegidas.

5.1.2 Acesso físico nas instalações da ACT

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

5.1.2.1 Níveis de acesso

5.1.2.1.1. Esta DPCT define três (3) níveis de acesso físico aos diversos ambientes da ACT IMPRENSA OFICIAL e mais um (1) quarto nível relativo à proteção do SCT.

5.1.2.1.2. O primeiro nível – ou nível 1 – deverá situar-se após a primeira barreira de acesso às instalações da ACT IMPRENSA OFICIAL. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da ACT IMPRENSA OFICIAL transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC é executado nesse nível.

5.1.2.1.3. O segundo nível – ou nível 2 – é interno ao primeiro e requer, da mesma forma que o primeiro, 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 IMPRENSA OFICIAL. A passagem para o segundo nível exige identificação por meio eletrônico e uso de crachá.

5.1.2.1.4 O ambiente de nível 2 é separado do nível 1 por paredes. Não há janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.

5.1.2.1.5. O acesso a este nível será 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 IMPRENSA OFICIAL, como administradores de rede e técnicos de suporte de informática. Demais funcionários da ACT IMPRENSA OFICIAL ou do possível ambiente que esta compartilhe não deverão acessar 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 por parte de prestadores de serviços de manutenção.

5.1.2.1.7. Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da ACT IMPRENSA OFICIAL, a partir do nível 1. 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 será o primeiro nível a abrigar material e atividades sensíveis da operação da ACT IMPRENSA OFICIAL. Qualquer atividade relativa à emissão de carimbos do tempo será realizada nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível.

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

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

5.1.2.1.11. Não se aplica.

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

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

a) equipamentos de produção;
b) equipamentos de rede e infra-estrutura (firewall, roteadores, switches e servidores).

5.1.2.1.14. Não se aplica.

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

a) os SCT e equipamentos criptográficos;
b) outros materiais criptográficos, tais como cartões, chaves, dados de ativação e suas cópias.

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

a) serem feitos em aço ou material de resistência equivalente; e possuírem tranca com chave.

5.1.2.1.17. O cofre ou gabinete que abrigará os SCT é trancado de forma que sua abertura seja possível somente com a presença de dois funcionários de confiança da ACT IMPRENSA OFICIAL.

5.1.2.2 Sistemas físicos de detecção

5.1.2.2.1 A segurança de todos os ambientes da ACT IMPRENSA OFICIAL será feita em regime de vigilância 24x7 (vinte e quatro horas por dia, sete dias por semana).

5.1.2.2.2 A segurança poderá ser realizada por:

a. Guarda armado, uniformizado, devidamente treinado e apto para a tarefa de vigilância;
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 permitirão 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 IMPRENSA OFICIAL possui mecanismos que permitam, em caso de falta de energia:

a) iluminação de emergência em todos os ambientes, acionada automaticamente;
b) continuidade de funcionamento dos sistemas de alarme e do circuito interno de TV.

5.1.2.3 Sistema de controle de acesso

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 IMPRENSA OFICIAL é 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 IMPRENSA OFICIAL 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 ICPBRASIL [4]. Qualquer modificação nessa rede deverá ser 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 IMPRENSA OFICIAL é garantida por meio de no-breaks 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 da ACT

5.1.5.1 Nas instalações da ACT IMPRENSA OFICIAL não é permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do nível 1.

5.1.5.2 Existe no interior do ambiente nível 3 extintores de incêndio das classes B e C, para apagar incêndios em combustíveis e equipamentos elétricos, dispostos no ambiente de forma a facilitar o seu acesso e manuseio. Em caso da existência de sistema de sprinklers no prédio, o ambiente de nível 3 da ACT IMPRENSA OFICIAL não deverá possuir saídas de água, para evitar danos aos equipamentos.

5.1.5.3 O ambiente de nível 3 possui sistema de prevenção contra incêndios, que aciona alarmes preventivos uma vez detectada fumaça no ambiente.

5.1.5.4 Nos demais ambientes da ACT IMPRENSA OFICIAL existem extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitem o seu acesso e manuseio.

5.1.5.5 Mecanismos específicos foram implantados pela ACT IMPRENSA OFICIAL 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 da ACT

5.1.6.1 A ACT IMPRENSA OFICIAL atende à norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7 Destruição de lixo nas instalações da ACT

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. Quando aplicável, as mídias de armazenamento passam pelo processo de sanitização que tem a finalidade de impossibilitar eventuais tentativas de recuperação de informações mesmo que parciais.

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

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

5.2 Controles Procedimentais

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

5.2.1 Perfis qualificados

5.2.1.1 A ACT IMPRENSA OFICIAL garante a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente o SCT sem ser detectado. As ações de cada empregado são limitadas de acordo com seu perfil.

5.2.1.2 A ACT IMPRENSA OFICIAL estabelece seis perfis distintos para sua operação, à 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;
b) Comercial – tem a função de cadastrar departamentos e seus respectivos gerentes. Gerar e visualizar relatórios sobre transações efetuadas pelos departamentos;
c) Auditor - autorizado a ver arquivos e auditar os logs dos sistemas confiáveis da ACT;
d) Gerente de Departamento – Pode ser um titular ou subtitular departamento, e pode executar certas funções administrativas no

departamento(s) ao(s) qual(is) esteja vinculado. Um departamento é uma entidade que concentra usuários dos serviços de carimbo de tempo;

e) Administrador de SCT – autorizado a administrar o Servidor de Carimbo do Tempo bem como suas configurações de funcionamento, tais como: rede, cadastro de usuários, gerencia de certificados digitais;
f) Operador de SCT – autorizado a realizar tarefas operacionais no Servidor de Carimbo do tempo dentre elas as configurações de firewall, rotinas de backup, analise de logs.

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

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

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1 A DPCT estabelece o requisito de controle multiusuário para a geração da chave privada dos SCTs operados pela ACT IMPRENSA OFICIAL, 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 IMPRENSA OFICIAL poderão ser executadas por um único empregado.

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1 Todo empregado da ACT IMPRENSA OFICIAL terá sua identidade e perfil verificados antes de:

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

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

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

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

5.3 Controles de Pessoal

Nos itens seguintes são descritos os requisitos e procedimentos, implementados pela ACT IMPRENSA OFICIAL 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 IMPRENSA OFICIAL encarregados de tarefas operacionais terão registrado em contrato ou termo de responsabilidade:

a) os termos e as condições do perfil que ocuparão;
b) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
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 IMPRENSA OFICIAL envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo será admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]. A ACT IMPRENSA OFICIAL 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 IMPRENSA OFICIAL 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;
d) comprovação de escolaridade e de residência.

5.3.2.2 A ACT IMPRENSA OFICIAL poderá definir, caso necessário, requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

5.3.3.1 Todo o pessoal da ACT IMPRENSA OFICIAL envolvido em atividades diretamente relacionadas com os processos de emissão de carimbo do tempo e gerenciamento de Autoridade de Carimbo do Tempo recebem 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 IMPRENSA OFICIAL;

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 IMPRENSA OFICIAL;
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 IMPRENSA OFICIAL 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 IMPRENSA OFICIAL.

5.3.5 Frequência e sequência de rodízio de cargos

Não se aplica.

5.3.6 Sanções para ações não autorizadas

5.3.6.1 Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da ACT IMPRENSA OFICIAL, esta deverá, de imediato, suspender o acesso dessa pessoa aos SCT, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.

5.3.6.2 O processo administrativo referido acima conterá, no mínimo, os seguintes itens:

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

5.3.6.3 Concluído o processo administrativo, a ACT IMPRENSA OFICIAL encaminhará suas conclusões à EAT.

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

a) advertência;
b) suspensão por prazo determinado;
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 IMPRENSA OFICIAL envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo é contratado conforme o estabelecido na

POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]. A ACT IMPRENSA OFICIAL poderá definir requisitos adicionais para a contratação.

5.3.8 Documentação fornecida ao pessoal

5.3.8.1 A ACT IMPRENSA OFICIAL disponibiliza para todo o seu pessoal:

a) a DPCT da ACT IMPRENSA OFICIAL;
b) as PCTs da ACT IMPRENSA OFICIAL;
c) a PS da ACT IMPRENSA OFICIAL;
d) documentação operacional relativa à suas atividades;
e) contratos, normas e políticas relevantes para suas atividades.

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

5.4 Procedimentos de Logs de Auditoria

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

5.4.1 Tipos de eventos registrados

5.4.1.1 A ACT IMPRENSA OFICIAL registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos obrigatoriamente são incluídos em arquivos de auditoria:

a) iniciação e desligamento do SCT;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACT;
c) mudanças na configuração do SCT ou nas suas chaves;
d) mudanças nas políticas de criação de carimbos do tempo;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não autorizadas de acesso aos arquivos de sistema;
g) geração de chaves próprias do SCT e demais eventos relacionados com o ciclo de vida destes certificados;
h) emissão de carimbos do tempo;
i) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
j) operações falhas de escrita ou leitura, quando aplicável; e
k. todos os eventos relacionados à sincronização dos relógios dos SCT com a FCT; isso inclui no mínimo:
i. a própria sincronização;
ii. desvio de tempo ou retardo de propagação acima de um valor especificado;
iii. falta de sinal de sincronização;

iv. tentativas de autenticação mal sucedidas;
v. detecção da perda de sincronização.

5.4.1.2 A ACT IMPRENSA OFICIAL 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) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

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

5.4.1.4 Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da ACT IMPRENSA OFICIAL 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 (logs)

5.4.2.1 A periodicidade com que os registros de auditoria são analisados pelo pessoal responsável é de uma semana. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolverá uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise deverão ser documentadas.

5.4.3 Período de retenção para registros (logs) de auditoria

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

5.4.4 Proteção de registro (log) de auditoria

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

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

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

5.4.5 Procedimentos para cópia de segurança (backup) de registro (log) de auditoria

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

5.4.6 Sistema de coleta de dados de auditoria

5.4.6.1 O sistema interno de coleta de dados de auditoria da ACT IMPRENSA OFICIAL 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 IMPRENSA OFICIAL, nenhuma notificação deverá ser 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 IMPRENSA OFICIAL serão analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes serão implementadas pela ACT IMPRENSA OFICIAL 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, em uso pela ACT IMPRENSA OFICIAL.

5.5.1 Tipos de registros arquivados

5.5.1.1 Os tipos de registros arquivados compreendem:

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

5.5.2 Período de retenção para arquivo

5.5.2.1 Os períodos de retenção para cada registro arquivado, de carimbos do tempo emitidos e das demais informações, inclusive arquivos de auditoria, são retidos por, 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 IMPRENSA OFICIAL, 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 IMPRENSA OFICIAL verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5 Requisitos para datação de registros

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

5.5.6 Sistema de coleta de dados de arquivo

5.5.6.1 Todos os sistemas de coleta de dados de arquivo utilizados pela ACT IMPRENSA OFICIAL 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 IMPRENSA OFICIAL, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

5.6 Troca de chave

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

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

5.7 Comprometimento e Recuperação de Desastre

5.7.1 Disposições Gerais

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

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

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

5.7.1.4 Em caso de comprometimento grave da operação da ACT IMPRENSA OFICIAL, sempre que possível, ela disporá a todos os subscritores e terceiras partes informações que possam ser usadas 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 IMPRENSA OFICIAL.

5.7.2 Recursos computacionais, software e 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 IMPRENSA OFICIAL, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as consequências que ele pode gerar. Esse procedimento é realizado por um grupo pré-determinado de empregados devidamente treinados para essa situação. Caso haja necessidade, o gerente de segurança declarará a contingência.

5.7.3 Procedimento no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado do SCT é revogado

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

5.7.3.2 Chave privada do SCT é comprometida

5.7.3.2.1 Em caso de suspeita de comprometimento de chave do SCT, após a identificação da crise, são notificados os gestores de segurança do ACT IMPRENSA OFICIAL que acionam as equipes envolvidas, de forma a indispor temporariamente os serviços de emissão de carimbo do tempo. É necessário que o certificado do SCT seja revogado. O

SCT deve ser desabilitado no SGACT pelo Administrador. É necessária a geração de um novo par de chaves e o Administrador deve cadastrar o novo SCT. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

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

5.7.3.3 Calibração e sincronismo do SCT são perdidos

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

5.7.3.3.1.2 Caso ocorra um erro ao auditar o SCT, o SCT será desabilitado na ACT IMPRENSA OFICIAL 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 IMPRENSA OFICIAL, 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 IMPRENSA OFICIAL;
b) monitorar e controlar o foco da contingência;
c) diminuir ao máximo os danos aos ativos de processamento da ACT IMPRENSA OFICIAL, de forma a evitar a descontinuidade dos serviços.

5.8 Extinção dos serviços de ACT ou PSS

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

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

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

a) a ACT IMPRENSA OFICIAL disporá a todos os subscritores e partes receptoras informações a respeito de sua extinção;
b) não se aplica;
c) a ACT IMPRENSA OFICIAL transferirá a outra ACT, após aprovação da AC Raiz, as obrigações relativas à manutenção de arquivos de registro e de auditoria necessários para demonstrar a operação correta da ACT IMPRENSA OFICIAL, por um período razoável;
d) a ACT IMPRENSA OFICIAL manterá ou transferirá a outra ACT, após aprovação da AC Raiz, suas obrigações relativas a dispor 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 IMPRENSA OFICIAL solicitará a revogação dos certificados de seus SCT;
g) a ACT IMPRENSA OFICIAL notificará todas as entidades afetadas.

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

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 Ciclo de Vida de Chave Privada do SCT

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

a) geração do par de chaves criptográficas;
b) geração da requisição de certificado digital;
c) exclusão da requisição de certificado digital;
d) instalação de certificados digitais;
e) renovação de certificado digital (com a geração de novo par de chaves);
f) proteção das chaves privadas em módulo de segurança criptográfica.

Todo o processo de controle do ciclo de vida da chave privada é feito através de uma interface de usuário final de acesso controlado e seguro, com comunicação em SSL.

6.1.1 Geração do par de chaves

6.1.1.1 Neste item, são descritos os requisitos e procedimentos referentes ao processo de geração do par de chaves criptográficas da ACT IMPRENSA OFICIAL. O par de chaves criptográficas dos SCT da ACT IMPRENSA OFICIAL é gerado pela própria ACT IMPRENSA OFICIAL, 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 IMPRENSA OFICIAL assegura que quaisquer chaves criptográficas são geradas em circunstâncias controladas. Em particular:

a) geração da chave de assinatura do SCT é realizada em um ambiente físico seguro, por pessoal em funções de confiança sob, pelo menos, controle

duplo. O pessoal autorizado para realizar essa função será limitado àqueles que receberam essa responsabilidade de acordo com as práticas da ACT IMPRENSA OFICIAL;

b) a geração da chave de assinatura do SCT será realizada dentro de módulo criptográfico que cumpra os requisitos dispostos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [11];
c) o algoritmo de geração de chave do SCT, o comprimento da chave assinante resultante e o algoritmo de assinatura usado para assinar o carimbo do tempo constam no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [11]:

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

6.1.2 Geração de Requisição de Certificado Digital

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

6.1.3 Exclusão de Requisição de Certificado Digital

6.1.3.1 O SCT garante que a exclusão de uma requisição de certificado digital obrigatoriamente implica na exclusão da chave privada correspondente.

6.1.4 Instalação de Certificado Digital

6.1.4.1 A instalação do certificado digital se dá através da interface segura e controlada do SCT. São informados, além do certificado digital, os certificados intermediários e o certificado raiz do caminho de certificação do certificado gerado.

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

a) verifica se a chave privada correspondente do certificado encontra-se em seu módulo de segurança criptográfico;
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 mesmo 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 IMPRENSA OFICIAL dispõe 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 https://certificadodigital.imprensaoficial.com.br/repositorio/.

6.1.7 Tamanhos de chave

6.1.7.1 A ACT IMPRENSA OFICIAL define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2].

6.1.8 Geração de parâmetros de chaves assimétricas

6.1.8.1 A geração dos parâmetros de chaves assimétricas é feita no módulo de segurança criptográfica, com padrão de segurança FIPS 140-2 nível 3, e estão em conformidade com o documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

6.1.9 Verificação da qualidade dos parâmetros

6.1.9.1 A verificação dos parâmetros para geração das chaves é feita no módulo de segurança criptográfica, com padrão de segurança FIPS 140-2 nível 3, e está em conformidade com o 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 da chave privada é executado internamente ao módulo de segurança criptográfica do equipamento.

6.1.11 Propósitos de uso de chave

6.1.11.1 As chaves privadas dos SCT operados pela ACT IMPRENSA OFICIAL somente serão utilizadas para assinatura dos carimbos do tempo por ela emitidos em conformidade com o documento Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil [11].

6.2 Proteção da Chave Privada

A ACT IMPRENSA OFICIAL implementa uma combinação de controles físicos lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas. Controles Lógico e Procedimental estão descritos no item 5.2. Controle de acesso físico está descrito no item 5.1.

6.2.1 Padrões para módulo criptográfico

6.2.2.1 Para o controle do ciclo de vida de vida e armazenamento da chave privada do SCT, o equipamento utiliza um módulo de segurança criptográfica que obedece aos requisitos definidos 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. Além disso, não é possível recuperar as chaves privadas do SCT. As mesmas ficam armazenadas no módulo de segurança criptográfica.

6.2.4 Cópia de segurança (backup) de chave privada

6.2.4.1 Não é possível a geração de cópia de segurança (backup) de chaves privadas do SCT.

6.2.5 Arquivamento de chave privada

6.2.5.1 A ACT IMPRENSA OFICIAL não arquivará chaves privadas com validade vencida ou de uso descontinuado de seus SCT, 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 após a autenticação de usuário com perfil de qualificado na interface de gerenciamento.

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

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas dos SCT da ACT IMPRENSA OFICIAL serão utilizadas apenas durante o período de validade dos certificados correspondentes. As chaves públicas correspondentes 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

Neste item, indica 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 A DPCT prevê que os SCT e os equipamentos da ACT IMPRENSA OFICIAL, 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 serão implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de gerenciamento do carimbo do tempo e com mecanismos de segurança física.

6.5.1.3 Qualquer equipamento, ou parte desses, ao ser enviado para manutenção 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 IMPRENSA

OFICIAL, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, deverão ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da ACT IMPRENSA OFICIAL. Todos esses eventos deverão ser registrados para fins de auditoria.

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

6.5.2 Classificação da segurança computacional

6.5.2.1 A segurança computacional da ACT IMPRENSA OFICIAL segue as recomendações Common Criteria.

6.5.3 Características do SCT

6.5.3.1 O Servidor de Carimbo do tempo é um sistema de hardware e software que executa a geração de carimbos do tempo, com monitoramento de execução de seus processos por entidades credenciadas confiáveis e acessos protegidos e controlados, atendendo às especificações descritas nesta seção. A responsabilidade pelo atendimento é do fabricante do SCT.

6.5.3.2 Seu relógio interno utilizado é o relógio interno do MSC, que se mantém sincronizado com a fonte confiável de tempo (FCT) mantida pela AC-Raiz. O controle da sincronização é feito através de auditoria por uma EAT, que controla se a diferença de tempo entre o relógio do SCT e o relógio do servidor de auditoria e sincronismo que o controla está dentro de parâmetros aceitáveis. O tempo do relógio interno do MSC e do SCT é homologado ou revogado através de emissão de alvará de funcionamento pelo SAS com base nas medições realizadas na auditoria. Quando o tempo do SCT está com um alvará de revogação emitido por um SAS, o SCT não emite carimbos do tempo até que seu relógio interno esteja novamente sincronizado. Todo o processo de auditoria entre SCT e SAS por uma EAT é feito com autenticação mútua por certificação digital através de canal seguro SSL. A EAT tem acesso à interface administrativa do SCT, através de autenticação por certificação digital, com permissões para visualização das informações correspondente ao tempo do relógio do MSC e dos registros de logs que tenham relação com o tempo utilizado pelo SCT para os carimbos do tempo.

6.5.3.3 A assinatura digital do carimbo de tempo é realizada dentro do MSC do SCT. Seus carimbos de tempo não permitem irretroatividade e são emitidos sempre em uma ordem crescente. Os carimbos de tempo para as requisições são emitidos sempre na ordem de recebimento das requisições pelo SCT.

6.5.3.4 O SCT utilizado pela ACT IMPRENSA OFICIAL possui como características:

a. emitir os carimbos do tempo na mesma ordem em que são recebidas as requisições;
b. permitir gerenciamento e proteção de chaves privadas;

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

6.5.4 Ciclo de Vida de Módulo Criptográfico de SCT

6.5.4.1 A instalação e a ativação do MSC 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 IMPRENSA OFICIAL certifica-se que seus SCT estejam sincronizados com o FCT dentro da precisão declarada nas PCT respectivas e, particularmente, que:

a) os valores de tempo utilizados pelo SCT na emissão de carimbos do tempo são rastreáveis até a hora UTC;
b) a calibração dos relógios dos SCT é mantida de tal forma que não se afaste da precisão declarada na PCT;
c) os relógios dos SCT são protegidos contra ataques, incluindo violações e imprecisões causadas por sinais elétricos ou sinais de rádio, evitando que sejam descalibrados e permitindo que qualquer modificação possa ser detectada;
d) a ocorrência de perda de sincronização do valor do tempo indicado em um carimbo do tempo com o UTC seja detectada pelos controles do sistema;
e) o SCT deixa de emitir carimbos do tempo, caso receba da EAT alvará de revogação, 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 SCT 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 ASR.

6.6 Controles Técnicos do Ciclo de Vida

Nos itens seguintes são descritos, quando aplicáveis, os controles implementados pela ACT IMPRENSA OFICIAL no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1 Controles de desenvolvimento de sistema

6.6.1.1 O desenvolvimento desses sistemas basear-se-á na metodologia RUP – uma abordagem iterativa baseada em disciplinas para atribuir tarefas e responsabilidades dentro de uma organização de desenvolvimento. O processo é baseado em 3 fases: concepção, iteração e finalização.

a) Na etapa de concepção é definida a visão geral do sistema, a lista de requisitos e a lista de casos de uso. Com base nestas informações é gerado o plano de projetos. Este plano contém informações sobre o projeto, estimativas de esforço, tamanho e custos do projeto, riscos associados, cronograma e dados a serem gerenciados.
b) Para cada iteração, são realizadas 3 etapas: análise, desenvolvimento e finalização. Esta é uma fase dinâmica, após a finalização da iteração, volta-se para a análise. Na fase de análise são estimados o esforço e tamanho da iteração juntamente com um prazo para finalização.
c) Após a execução de todas as iterações realiza-se a fase de finalização do projeto. Esta é a fase de organização da documentação gerada pelo projeto. Nesta etapa, também, são gerados os executáveis e é elaborado o manual de instruções de uso referente ao programa desenvolvido.

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

6.6.2 Controles de gerenciamento de segurança

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

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

6.6.3 Classificações de segurança de ciclo de vida

6.6.3.1 A maturidade do ciclo de vida do Servidor de Aplicativo (SA) e a do Sistema de Carimbo do TEMPO (SCT) atendem ao nível do Capability Maturity Model do Software Engineering Institute (CMMSEI).

6.7 Controles de Segurança de Rede

6.7.1 Diretrizes Gerais

6.7.1.1 Neste item são descritos os controles relativos à segurança da rede da ACT IMPRENSA OFICIAL, incluindo firewalls e recursos similares, observado o disposto no item 9.3.3 da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

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

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

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

6.7.1.5 O acesso à Internet deverá ser 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 deverá ser permitido somente para os seguintes serviços:

a) pela EAT da ICP-Brasil, para o sincronismo e auditoria de relógios dos SCTs;
b) pela ACT, para a administração dos SCTs e sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;
c) pelo PSS da ACT, para a administração dos SCTs e sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;
d) pelo subscritor, para a solicitação e recebimento de carimbos do tempo

6.7.2 Firewall

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

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

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

6.7.3.3 O sistema de detecção de intrusão prove 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, 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 deve implementar serviço de proxy, restringindo o acesso, a partir de todas suas estações de trabalho, a serviços que possam comprometer a segurança do ambiente da ACT.

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

6.8 Controles de Engenharia do Módulo Criptográfico

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

7 PERFIS DOS CARIMBOS DO TEMPO

7.1 Diretrizes Gerais

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

7.2 Perfil do Carimbo do tempo

Todos os carimbos do tempo emitidos pela ACT IMPRENSA OFICIAL estão em conformidade com o formato definido pelo Perfil de Carimbo do tempo constante da European Telecommunications Stardards Institute Technical Specification 101 861 (ETSI TS 101 861) e 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 IMPRENSA OFICIAL assina cada mensagem de carimbo do tempo com uma chave privada específica para esse uso. A ACT IMPRENSA OFICIAL pode usar chaves distintas para acomodar, por exemplo, diferentes políticas, diferentes algoritmos, diferentes tamanhos de chaves privadas ou para aumentar o desempenho.

7.2.3.2 O certificado correspondente contém apenas uma instância do campo de extensão, conforme definido na RFC 3280, com o sub-campo KeyPurposeID contendo o valor id-kp-timeStamping. Essa extensão 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 IMPRENSA OFICIAL adotará o “Distinguished Name” (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = < nome da Autoridade de Carimbo do Tempo >

CN = < nome do Servidor de Carimbo do Tempo >

7.3 Protocolos de transporte

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

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 ICPBRASIL [6].

8.2 Identificação/Qualificação do avaliador

8.2.1s 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 ICPBRASIL [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 ICPBRASIL [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 IMPRENSA OFICIAL 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 IMPRENSA OFICIAL 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 A ACT IMPRENSA OFICIAL informa que as entidades da ICP-Brasil a ela diretamente vinculadas também receberam auditoria prévia, para fins de credenciamento, e a ACT IMPRENSA OFICIAL é responsável pela realização de auditorias anuais dessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo 8.2.2.

8.5 Ações tomadas como resultado de uma deficiência

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

8.6 Comunicação dos resultados

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

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 Tarifas de Serviço

Nos itens a seguir, é especificado pela ACT IMPRENSA OFICIAL a política tarifária e de reembolso aplicáveis.

9.1.1 Tarifas de emissão de carimbos do tempo

9.1.2 Tarifas de acesso ao carimbo do tempo

9.1.3 Tarifas de revogação ou de acesso à informação de status

9.1.4 Tarifas para outros serviços

9.1.5 Política de reembolso

9.2 Responsabilidade Financeira

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

9.2.1 Cobertura do seguro

Conforme item 4 desta DPCT.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

9.3.1.1 São consideradas sigilosas as seguintes informações:

a. As chaves privadas dos SCTs;
b. as senhas e demais credenciais de acesso aos ambientes operacionais;
c. os dossiês dos funcionários do PSS;
d. o PCN da ACT;
e. conteúdo dos relatórios de auditorias (exceto a sua conclusão).

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

9.3.2 Informações fora do escopo de informações confidenciais

9.3.2.1 São consideradas informações não sigilosas pela ACT IMPRENSA OFICIAL e pelos PSSs a ela vinculados, os quais deverão compreender, entre outros:

a) os certificados dos SCTs;

b) as PCTs implementadas pela ACT;

c) a DPCT da ACT;

d) versões públicas de PS; e

e) a conclusão dos relatórios de auditoria.

9.3.3 Responsabilidade em proteger a informação confidencial

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

9.3.3.2 A chave privada de assinatura digital dos SCTs serão geradas e mantidas pela ACT IMPRENSA OFICIAL, 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

9.4.3.1 Descrever quais são as informações não consideradas privadas, se for o caso.

9.4.4 Responsabilidade para proteger a informação privadas

9.4.4.1 A ACT IMPRENSA OFICIAL 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 Como diretriz geral nenhum documento, informação ou registro sob a guarda do PSS ou da ACT IMPRENSA OFICIAL será 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 Não se aplica.

9.6 Declarações e Garantias

9.6.1 Declarações e garantias das terceiras partes

9.6.1.1 Constituem direitos da terceira parte:

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

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

9.6.1.2 Um carimbo emitido pela ACT IMPRENSA OFICIAL 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 IMPRENSA OFICIAL 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 Todas as notificações relevantes relativas às práticas descritas nesta DPCT serão enviadas através de e-mails aos participantes.

9.12 Alterações

9.12.1 Procedimento para emendas
Qualquer alteração nesta DPCT deverá ser 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 Deve também ser estabelecido que a DPCT da ACT IMPRENSA OFICIAL não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.13.3 Os casos omissos deverão ser 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

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 ICPBRASIL	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 ICPBRASIL	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-ICP12.01
[11]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOCP-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.