Declaração de Práticas de Carimbo de Tempo – DPCT

Autoridade de Carimbo de Tempo VALID

OID 2.16.76.1.5.5
DPCT da ACT VALID

Versão 4.1
Junho de 2023

Sumário

CONTROLE DE ALTERAÇÕES:

Versão	Data	Resolução que aprova a alteração	Item Alterado	Descrição da Alteração
1.1	25.11.2015	Resolução nº 112, de 30/09/2015	Diversos	Retira as referências a Lei 2.784, de 18.06.1918, e ao Decreto 10.546, de 05.11.1918.
2.0	10/07/2020	Resolução nº 155, de 03/12/2019	2.1.3.3, 7.2.2.2 e 9	Inclusão da referência as regras de validação do alvará.
3.0	02/09/2020	Resolução 172	Diversos	Adequação para atender a Resolução.
4.0	20/09/2022	Resolução 188	Diversos	Adequação para atender a Resolução.
4.1	16/06/2023	-	5.5.5	Detalhamento da datação de registro.

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 ICPBRASIL - este documento;
b) REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL [1];
c) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2];
d) PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3];
e) PERFIL DO ALVARÁ DO CARIMBO DO TEMPO DA ICPBRASIL [10].

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

1.1.3. A utilização de carimbos 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 VALID (ACT VALID), integrante na Infraestrutura de Chaves Públicas Brasileira ICP-Brasil na execução dos seus serviços de carimbo do tempo. De modo geral, a política de carimbo do tempo indica "o que deve ser cumprido" enquanto uma declaração de práticas da ACT indica "como cumprir", isto é, os processos que serão usados pela ACT para criar carimbos do tempo e manter a precisão do seu relógio.

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

1.1.6. A estrutura desta DPCT está baseada no DOC-ICP-12 do Comitê Gestor da ICP- Brasil - Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil. As referências a formulários presentes nesta DPCT deverão ser entendidas também como referências a outras formas que a ACT VALID ou entidades a ela vinculadas possam vir a adotar.

1.1.7. Aplicam-se ainda à ACT VALID 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. Este documento é chamado “Declaração de Práticas de Carimbo do Tempo da Autoridade de Carimbo do Tempo VALID - ACT VALID”, e comumente referido como “DPCT VALID”. O Identificador do Objeto (**OID**) desta DPCT, atribuído pela AC Raiz, após a conclusão do processo de seu credenciamento, é **2.16.76.1.5.5**.

1.3. Comunidade

1.3.1. Autoridades de Carimbo do tempo

1.3.1.1. Esta DPCT refere-se unicamente à Autoridade de Carimbo do Tempo VALID (ACT VALID) integrante da ICP-Brasil.

1.3.2. Prestador de Serviços de Suporte

1.3.2.1. A ACT VALID utiliza o seguinte Prestador de Serviço de Suporte (PSS) nas suas operações: VALID S.A. Essa informação encontra-se na página *web*: https://www.validcertificadora.com.br/index.aspx?DID=314.

1.3.2.2. PSS são entidades utilizadas pela ACT ou pela AR para desempenhar as atividades descritas abaixo:

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.

Nota: A ACT VALID utiliza o seguinte Prestador de Serviço de Suporte (PSS) nas suas operações: VALID S.A, para disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.2.3. A ACT VALID mantem as informações acima sempre atualizadas.

1.3.3. Subscritores

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

1.3.4. Partes confiáveis

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

1.4. Aplicabilidade

1.4.1. A ACT VALID implementa a seguinte Políticas de Carimbo do Tempo: Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo VALID, PCT da ACT VALID **OID 2.16.76.1.6.5**.

1.5 Política de Administração

Neste item estão incluídos o nome, o endereço e outras informações da ACT VALID responsável pela DPCT, assim como são informados o nome, os números de telefone e de fax e o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC: ACT VALID

1.5.2 Contatos

Endereço: Alameda Rio Claro, 241 - Bela Vista - São Paulo, SP
CEP: 01332-010
Telefone: (11) 2575-6800
Página Web: http://www.validcertificadora.com.br/
E-mail: pki.compliance@valid.com

1.5.3 Pessoa responsável pela adequabilidade da DPCT e PCT

Nome: Márcio Nunes da Silva
Telefone: (11) 2575-6800
E-mail: pki.compliance@valid.com

1.5.4 Procedimentos de aprovação da DPCT

Esta DPCT é aprovada pelo ITI, conforme o determinado pelo documento **CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].**

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC	RAIZ Autoridade Certificadora Raiz da ICP-BRASIL
ACT	Autoridade de Carimbo do Tempo
ASR	Autenticação e Sincronização de Relógio
CG	Comitê Gestor da ICP-BRASIL
CMM-SEI	*Capability Maturity Model - Software Engineering Institute*
CN	*Common Name*
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPCT	Declarações de Práticas de Carimbo do tempo
EAT	Entidade de Auditoria do Tempo
ETSI	*European Telecommunication Standard Institute*
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Sistemas de Detecção de Intrusão
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
ITSEC	*European infrmation Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
MSC	Módulo de Segurança Criptográfico
NBR	Norma Brasileira
OID	*Object Identifier*
PCN	Plano de Continuidade do Negócio
PCT	Política de Carimbo do Tempo
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
SAS	Sistemas de Auditoria e Sincronismo
SCT	Servidor de Carimbo do Tempo
SNMP	*Simple Network Management Protocol*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*Trusted Software Development Methodology*
TSP	*Time Stamp Protocol*
TSQ	*Time Stamp Request*
URL	*Uniform Resource Locator*
UTC	*Universal Time Coordinated*

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Publicação de informações da ACT

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

2.1.2. As seguintes informações, são publicadas pela ACT VALID em sua página web:

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

2.2. Frequência de Publicação

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

2.3. Controle de Acesso aos Repositórios

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

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

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

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

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

4. REQUISITOS OPERACIONAIS

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

4.1. Solicitação de Carimbos do Tempo

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

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

A PCT VALID da ACT VALID 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 ocorre no processo de assinatura digital que demanda esse artefato e pode ser realizada por pessoas físicas e jurídicas em aplicações mantidas pela VALID.

4.1.2 Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1 Responsabilidades da ACT

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

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

4.1.2.2 Obrigações da ACT

As obrigações da ACT VALID são as abaixo relacionadas:

a) operar de acordo com a sua DPCT e com as PCTs que implementa;
b) gerar, gerenciar e assegurar a proteção das chaves privadas dos SCTs;
c) manter os SCTs sincronizados e auditados pela EAT;
d) tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
e) monitorar e controlar a operação dos serviços fornecidos;
f) assegurar que seus relógios estejam sincronizados, com autenticação, com a Rede de Carimbo do Tempo da ICP-Brasil;
g) permitir o acesso da EAT aos SCTs de sua propriedade;
h) notificar à AC emitente do seu certificado quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;
i) notificar aos seus usuários quando ocorrer suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
j) publicar em sua página web sua DPCT, as PCTs aprovadas que implementa e os certificados de seus SCTs;
k) publicar em sua página web as informações definidas no item 2.2.2 deste documento;
l) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
m) adotar as medidas de segurança e controle previstas na DPCT, PCT e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
n) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
o) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
p) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);
q) manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, com cobertura suficiente e compatível com o risco dessas atividades;
r) informar às terceiras partes e subscritores de carimbos do tempo acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima; e
s) informar à EAT, mensalmente, a quantidade de carimbos do tempo emitidos.

4.1.2.3 Obrigações do Subscritor

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

4.2. Emissão de Carimbos do Tempo

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

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

4.2.3. O Servidor de Aplicativos pode se constituir de:

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

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

4.2.5. O Servidor de Aplicativos executa as seguintes tarefas:

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

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

a) Verificar se a requisição está de acordo com as especificações da norma RFC 3161. Caso esteja, realizar as demais operações a seguir descritas. Se a requisição estiver fora das especificações, o SCT deve responder de acordo com o item 2.4.2 da RFC 3161, com um valor de status diferente de 0 ou 1, e indicar no campo "*PKIFailureInfo*" qual foi a falha ocorrida sem emitir, neste caso, um carimbo do tempo e encerrando, sem executar as demais etapas;
b) Produzir carimbos do tempo apenas para solicitações válidas;
c) Usar uma fonte confiável do tempo;
d) Incluir um valor de tempo confiável para cada carimbo do tempo;

e) Incluir na resposta um identificador único para cada carimbo do tempo emitido;
f) Incluir em cada carimbo do tempo um identificador da política sob a qual o carimbo do tempo foi criado;
g) Somente carimbar o hash dos dados, e não os próprios dados;
h) Verificar se o tamanho do hash recebido está de acordo com a função *hash* utilizada;
i) Não examinar o hash que está sendo carimbado, de nenhuma forma, exceto para verificar seu comprimento, conforme item anterior;
j) Nunca incluir no carimbo do tempo algum tipo de informação que possa identificar o requisitante do carimbo do tempo;
k) Assinar cada carimbo do tempo com uma chave própria gerada exclusivamente para esse objetivo;
l) A inclusão de informações adicionais solicitadas pelo requerente deve ser feita nos campos de extensão suportados; caso não seja possível, responder com mensagem de erro;
m) Encadear o carimbo do tempo atual com o anterior, caso a ACT tenha adotado o mecanismo de encadeamento.

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

4.3. Aceitação de Carimbos do Tempo

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

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

o OID definido pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [10].

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

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

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

4.3.5. A PCT VALID define 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 SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

5.1. Segurança Física

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

5.1.1. Construção e localização das instalações de ACT

5.1.1.1. A operação da ACT VALID é executada dentro de um ambiente físico seguro em área de instalação altamente protegida. A localização e o sistema de certificação utilizado para a operação da ACT VALID não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados.

Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Nas instalações da ACT VALID, foram implementados, entre outros, os seguintes controles de segurança física:

a) Instalações de equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, retificadores, estabilizadores e similares;
b) Instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas; e
c) Iluminação de emergência.

5.1.2. Acesso físico nas instalações de ACT

O acesso físico às dependências da ACT VALID é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso. O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes. O sistema de certificação da ACT VALID está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.2.1 Níveis de Acesso

5.1.2.1.1. São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da ACT VALID, e mais 2 (dois) níveis relativos à proteção da chave privada de AC.

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

5.1.2.1.3. O segundo nível – ou nível 2 – é interno ao primeiro e requer a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da ACT Valid. A passagem do primeiro 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 divisórias de alvenaria. Não há janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.

5.1.2.1.5. O acesso a este nível é permitido apenas a pessoas que trabalham diretamente com as atividades de carimbo do tempo ou ao pessoal responsável pela manutenção de sistemas e equipamentos da ACT Valid, como

administradores de rede e técnicos de suporte de informática. Demais funcionários da ACT Valid ou ambiente que esta compartilha não acessam este nível.

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

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

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

5.1.2.1.9. No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: 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. Não há janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso.

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

5.1.2.1.12. Há 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. Existem na ACT Valid vários ambientes de nível 3 para abrigar e segregar:

a) equipamentos de produção e cofre de armazenamento; e
b) equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

5.1.2.1.14. Caso a ACT se situe dentro de um datacenter, com requisitos de segurança julgados adequados pela EAT, dispensa a existência de um ambiente de Nível 3 específico para a ACT.

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

c) Os SCT e equipamentos criptográficos;
d) 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) Ser feitos em aço ou material de resistência equivalente; e
b) Possuir tranca com chave.

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

5.1.2.2. Sistemas Físicos de Detecção

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmaras de vídeo ligadas a um sistema de gravação 24x7 (vinte e quatro horas por dia, sete dias por semana). O posicionamento e a capacidade dessas câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2. A segurança é realizada por:
a) Guarda armado, uniformizado, devidamente treinado e apto para a tarefa de vigilância; e
b) Circuito interno de TV, sensores de intrusão instalados em todas as portas e janelas e sensores de movimento, monitorados local ou remotamente por empresa de segurança especializada.

5.1.2.2.3. O ambiente de nível 3 possui circuito interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não deverão permitir a captura de senhas digitadas nos sistemas.

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

5.1.2.2.5. A ACT VALID possui mecanismos que permitam, em caso de falta de energia:
a) Iluminação de emergência em todos os ambientes, acionada automaticamente; e
b) Continuidade de funcionamento dos sistemas de alarme e do circuito interno de TV.

5.1.2.3. Sistema de controle de acesso

O sistema de controle de acesso 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 certificação da ACT VALID está dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da ACT VALID e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da ACT VALID.

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

5.1.3.3. Existem 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, telefonia e dados.

5.1.3.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

5.1.3.5. São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Qualquer modificação nessa rede é previamente documentada.

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 exigida pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante à falhas.

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

5.1.3.9. A capacidade de redundância de toda a estrutura de energia e ar condicionado da ACT VALID é garantida, por meio de:

a) Geradores de porte compatível;
b) Geradores de reserva;

c) Sistemas de “no-breaks” redundantes;
d) Sistemas redundantes de ar condicionado.

5.1.4. Exposição à água nas instalações de ACT

A estrutura inteiriça do ambiente de nível 3, construído na forma de célula estanque, provê proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5. Prevenção e proteção contra incêndio nas instalações de ACT

5.1.5.1. Todas as instalações da ACT VALID possuem sistemas de prevenção contra incêndio. Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2. Existem, a partir do ambiente de 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.

Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.3. Existe, a partir do ambiente de nível 3, sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre constituem eclusas, onde uma porta só abre quando a anterior estiver fechada.

5.1.5.4. Nos ambientes de nível 1 e 2 da ACT VALID, existem extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitam o seu acesso e manuseio.

5.1.5.5. Em caso de incêndio nas instalações da ACT VALID, a temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

5.1.6. Armazenamento de mídia nas instalações de ACT

5.1.6.1. A ACT VALID atende a norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”).

5.1.7. Destruição de lixo nas instalações de ACT

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo.

5.1.7.2. Todos os dispositivos eletrônicos não mais utilizáveis, e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, são fisicamente destruídos.

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

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

5.2. Controles Procedimentais

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na ACT VALID, 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 separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.2.1.2. A ACT VALID estabelece 3 (três) perfis distintos para sua operação, atribuídos às seguintes áreas:

- **Administrador do sistema** - autorizado a instalar, configurar e manter os sistemas confiáveis para gerenciamento do carimbo do tempo, bem como administrar a implementação das práticas de segurança da ACT. Autorizado a realizar backup e recuperação do sistema;
- **Operador de sistema** - responsável pela operação diária dos sistemas confiáveis da ACT. Pode configurar novos usuários (subscritores) autorizados a solicitar carimbos de tempos e seus limites de utilização.
- **Auditor de Sistema** - autorizado a ver arquivos e auditar os logs dos sistemas confiáveis da ACT.

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

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

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada dos SCT operados pela ACT VALID, conforme o descrito em 6.1.1.

5.2.2.2. Todas as tarefas executadas no ambiente onde está localizado o equipamento de SCT da ACT VALID necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da ACT VALID. As demais tarefas da ACT VALID poderão ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1 Pessoas que ocupam os perfis designados pela ACT VALID passam por um processo rigoroso de seleção. Todo funcionário da ACT VALID tem sua identidade e perfil verificados antes de:

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

5.2.3.2. Os certificados, contas e senhas utilizados para identificação e autenticação dos funcionários:

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

5.2.3.3. A ACT VALID implementa um padrão de utilização de "senhas fortes", definido 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 estão descritos requisitos e procedimentos, implementados pela ACT VALID 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 VALID, encarregados de tarefas operacionais, têm registrado em contrato ou termo de responsabilidade:

a) Os termos e as condições do perfil que ocupam;
b) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e
c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.1.1. Todo o pessoal da ACT VALID e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

5.3.2. Procedimentos de Verificação de Antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade da ACT VALID, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo, é submetido aos seguintes processos, antes do começo das atividades de:

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

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

5.3.3. Requisitos de treinamento

5.3.3.1. Todo o pessoal da ACT VALID envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e tecnologias de carimbo do tempo e sistema de carimbos do tempo em uso na ACT;
b) ICP-Brasil;
c) Princípios e tecnologias de certificação digital e de assinaturas eletrônicas;
d) Princípios e mecanismos de segurança de redes e segurança da ACT;
e) Procedimentos de recuperação de desastres e de continuidade do negócio;

f) Familiaridade com procedimentos de segurança, para pessoas com responsabilidade de Oficial de Segurança;
g) Familiaridade com procedimentos de auditorias em sistemas de informática, para pessoas com responsabilidade de Auditores de Sistema;
h) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

5.3.4.1. Todo o pessoal da ACT VALID 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 no sistema de certificação da ACT VALID.

5.3.5. Frequência e sequência de rodízios 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, realizada por pessoa responsável por processo operacional da ACT VALID, esta deverá imediatamente suspenderá o seu acesso aos SCT, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas cabíveis.

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

a) Relato da ocorrência com "*modus operandis*";
b) Identificação dos envolvidos;
c) Eventuais prejuízos causados;
d) Punições aplicadas, se for o caso; e
e) Conclusões.

5.3.6.3. Concluído o processo administrativo, a ACT VALID encaminhará suas conclusões à AC Raiz.

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

a) Advertência;
b) Suspensão por prazo determinado; ou
c) Impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

5.3.7.1. Todo o pessoal da ACT VALID envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo, é contratado conforme o estabelecido nas

POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4] e na Política de Segurança da ACT VALID.

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A ACT VALID disponibiliza para todo o seu pessoal:

a) Sua DPCT;
b) As PCTs que implementa;
c) A Política de Segurança da ICP-Brasil [8];
d) Documentação operacional relativa às suas atividades; e
e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela ACT VALID.

5.4 Procedimentos de Log de Auditoria

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

5.4.1 Tipos de eventos registrados

5.4.1.1 A ACT VALID pela DPCT registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:
a) iniciação e desligamento do SCT;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACT;
c) mudanças na configuração do SCT ou nas suas chaves;
d) mudanças nas políticas de criação de carimbos do tempo;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não-autorizadas de acesso aos arquivos de sistema;
g) geração de chaves próprias do SCT e demais eventos relacionados com o ciclo de vida destes certificados;
h) emissão de carimbos do tempo;
i) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
j) operações falhas de escrita ou leitura, quando aplicável; e
k) todos os eventos relacionados à sincronização dos relógios dos SCTs com a FCT; isso inclui no mínimo:

i. a própria sincronização;
ii. desvio de tempo ou retardo de propagação acima de um valor especificado;
iii. falta de sinal de sincronização;
iv. tentativas de autenticação malsucedidas;
v. detecção da perda de sincronização.

5.4.1.2 A ACT VALID pela DPCT também registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema, tais como:

a) registros de acessos físicos;
b) manutenção e mudanças na configuração de seus sistemas;
c) mudanças de pessoal e de perfis qualificados;
d) relatórios de discrepância e comprometimento; e
e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

5.4.1.3 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 Esta DPCT prevê que todos os registros de auditoria contem a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos contém o horário UTC. Registros manuais em papel contém a hora local desde que especificado o local.

5.4.1.5 Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da ACT VALID 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

A análise dos registros de auditoria é realizada semanalmente pela área de segurança e PKI da ACT VALID. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando-se que não foram alterados, em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3 Período de retenção para registros de auditoria

A ACT VALID mantém localmente, nas suas instalações técnicas, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento de maneira descrita no item 5.5.

5.4.4 Proteção de registro de auditoria

5.4.4.1. Os equipamentos da ACT VALID, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança. 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.

5.4.4.2. A inspeção contínua dos diversos registros dos sistemas é feita por meio de ferramentas nativas do sistema operacional e do banco de dados. Os relatórios emitidos a partir dessas ferramentas são coletados e armazenados em sala de arquivos em nível 3 de segurança.

5.4.4.3. Os registros de auditoria gerados eletrônica ou manualmente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

5.4.5 Procedimentos para cópia de segurança (Backup) de registros de auditoria

5.4.5.1. São executados semanalmente os procedimentos de backup dos registros de auditoria dos sistemas utilizados pela ACT VALID. As cópias de segurança semanais são feitas automaticamente ou pelos administradores de sistemas e enviadas as Equipe de Segurança e PKI.

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

5.4.6.1. O sistema de coleta de dados de auditoria da ACT VALID é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de ACT VALID, pelo sistema de controle de acesso e pelo pessoal operacional.

5.4.7 Notificação de agentes causadores de eventos

5.4.7.1. Eventos registrados pelo conjunto de sistemas de auditoria da ACT VALID não são notificados à pessoa, organização, dispositivo ou aplicação que causou o evento.

5.4.8 Avaliações de vulnerabilidade

5.4.8.1. Uma Avaliação de Riscos de Segurança foi realizada para a ACT VALID. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação. Eventos que indiquem possível vulnerabilidade, detectados na análise dos registros de auditoria da ACT VALID são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

5.5 Arquivamento de Registros

Nos itens seguintes da DPCT da ACT VALID é descrita a política geral de arquivamento de registros, para uso futuro, em uso pela ACT VALID.

5.5.1 Tipos de registros arquivados

5.5.1.1. Neste item da DPCT é especificados os tipos de registros arquivados, que compreendem, entre outros:

a) Notificações de comprometimento de chaves privadas do SCT;
b) Substituições de chaves privadas dos SCTs;
c) Informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo

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

Todos os registros 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 A Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da ACT VALID, protegido o mesmo tipo de proteção utilizada no arquivo principal.

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

5.5.4.3 A A ACT VALID garante que a verificação da integridade dessas cópias de Segurança, é realizada no mínimo, a cada 6 (seis) meses.

5.5.5 Requisitos para datação de registros

Os servidores da ACT Valid são sincronizados com a hora UTC fornecida pela AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em UTC, inclusive os certificados emitidos por esses equipamentos.

5.5.6 Sistema de coleta de dados de arquivo

5.5.6.1 O sistema de coleta de dados de arquivos da ACT VALID é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de ACT e pelo pessoal operacional.

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 VALID, 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 base 64 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 deve ser realizada somente por funcionários com perfis qualificados, através de duplo controle, em ambiente físico seguro.

5.7 Comprometimento e Recuperação de Desastre

5.7.1 Disposições Gerais

5.7.1.1 Nos itens seguintes desta DPCT são descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no Plano de Continuidade de Negócios (PCN) da ACT VALID, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], para garantir a continuidade dos seus serviços críticos.
5.7.1.2 A ACT VALID assegura, no caso de comprometimento de sua operação por qualquer um dos motivos relacionados nos itens abaixo, que as informações relevantes são disponibilizadas aos subscritores e às terceiras partes. A ACT VALID disponibiliza a todos os subscritores e terceiras partes uma descrição do comprometimento ocorrido.

5.7.1.3 No caso de comprometimento de uma operação do SCT (por exemplo, comprometimento da chave privada do SCT), suspeita de comprometimento ou

perda de calibração, o SCT não deverá emitir 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 VALID, sempre que possível, ela disponibiliza a todos os subscritores e terceiras partes informações que possam ser utilizadas para identificar os carimbos do tempo que podem ter sido afetados, a não ser que isso viole a privacidade dos subscritores ou comprometa a segurança dos serviços da ACT VALID.

5.7.2 Recursos computacionais, software e/ou dados corrompidos

5.7.2.1 Em caso de suspeita de corrupção de dados, *softwares* e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança da ACT VALID, 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 o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação. Caso haja necessidade, o Gerente de Segurança decretará a contingência.

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado do SCT é revogado
5.7.3.1.1 Em caso de suspeita de comprometimento de chave do SCT, após a identificação da crise, será notificado o departamento de Segurança e PKI da ACT VALID que acionam as equipes envolvidas, de forma a indispor temporariamente os serviços de autoridade certificadora. É necessário que o certificado do SCT seja revogado. O SCT deve ser desabilitado no SGACT pelo Administrador.

5.7.3.2 Chave privada do SCT é comprometida
5.7.3.2.1. Não há recuperação da chave privada no caso de comprometimento, é necessária a geração de um novo par de chaves e o Administrador deve cadastrar o novo SCT.

Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

a) O certificado do SCT será revogado e todos os carimbos do tempo subsequentes serão inválidos.

b) Cerimônias específicas serão realizadas para geração de novos pares de chaves.

5.7.3.3 Calibração e sincronismo do SCT são perdidos

5.7.3.3.1 Na hipótese de perda de calibração e de sincronismo do SCT, o fato é imediatamente comunicado aos gestores da AC RAIZ, o qual deverá entrar na interface de auditoria do SAS e executar o procedimento de calibração e sincronismo do SCT que apresentou problema. Caso ocorra um erro ao auditar

o SCT, o SCT será desabilitado na ACT VALID até que providências sejam tomadas.

5.7.4 Capacidade de continuidade de negócio após desastre

5.7.4.1 O Plano de continuidade de negócio especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza, como fogo, greves etc. e que podem ser resumidas no seguinte:

a) é feita a identificação da crise e o acionamento das equipes envolvidas;
b) é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas;
c) confirmado o desastre e constatada a impossibilidade de operação no site principal, as atividades são transferidas para o site de contingência.

5.8 Extinção dos serviços de ACT ou PSS

5.8.1 A ACT VALID observa os procedimentos no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

5.8.2. A ACT VALID assegura que possíveis rompimentos com os subscritores e terceiras partes, em consequência da cessação dos serviços de carimbo do tempo da ACT VALID 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 VALID cessar seus serviços de carimbo do tempo os seguintes procedimentos serão executados, no mínimo:

a) A ACT VALID disponibilizará a todos os subscritores e partes receptoras informações a respeito de sua extinção;
b) A ACT VALID revogará a autorização de todos os PSSs e subcontratados que atuam em seu nome para a realização de quaisquer funções que se relacionam ao processo de emissão do carimbo do tempo;
c) A ACT VALID transferirá a outra ACT, após aprovação da AC-Raiz, as obrigações relativas à manutenção de arquivos de registro e de auditoria necessários para demonstrar a operação correta da ACT, por um período razoável;
d) A ACT VALID manterá ou transferirá a outra ACT, após aprovação da AC Raiz, suas obrigações relativas a disponibilizar sua chave pública ou seus certificados a terceiras partes, por um período razoável;
e) As chaves privadas dos SCT serão destruídas de forma que não possam ser recuperadas;
f) A ACT VALID solicitará a revogação dos certificados de seus SCT;
g) A ACT VALID notificará todas as entidades afetadas.

5.8.4. A ACT VALID 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 de requisição de certificado digital;
c) Exclusão de requisição de certificado digital;
d) Instalação de certificados digitais;
e) Renovação de certificado digital (com a geração de novo par de chaves);
f) Proteção de chaves privadas.

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas da ACT VALID é gerado pela própria ACT VALID, 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 VALID 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 VALID;
b) A geração da chave de assinatura do SCT será realizada dentro de módulo criptográfico que cumpra os requisitos dispostos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [10];
c) O algoritmo de geração de chave do SCT, o comprimento da chave assinante resultante e o algoritmo de assinatura usado para assinar o carimbo do tempo constam no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [10].

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

6.1.2. Geração de Requisição de Certificado Digital

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

a) Verifica se chave privada correspondente a esse certificado encontra-se em seu módulo criptográfico interno;
b) Verifica se o certificado possui as extensões obrigatórias; e
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 VALID para usuários

6.1.6.1. A ACT VALID 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 www.validcertificadora.com.br

6.1.7. Tamanhos de chave

6.1.7.1. A PCT VALID define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

6.1.8. Geração de parâmetros de chaves assimétricas

6.1.8.1. A geração dos parâmetros de chaves assimétricas é gerada em módulo de segurança criptográfico, utilizando os padrões de segurança FIPS 140-2 nível 3, e adotarão o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

6.1.9. Verificação da qualidade dos parâmetros

6.1.9.1. Os parâmetros para geração das chaves são baseados nos padrões de segurança FIPS 140-2 nível 3, e são aplicados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

6.1.10. Geração de chave por hardware ou software

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 VALID 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.

6.2. Proteção da Chave Privada

A ACT VALID 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

6.2.1.1. 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 [10].

6.2.2. Controle “n de m’ para chave privada

Não se aplica.

6.2.3. Recuperação de chave privada

6.2.3.1. Não é permitido, no âmbito da ICP-Brasil, a recuperação de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular. 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 permitido, no Âmbito da ICP-Brasil, a geração de cópia de segurança (backup) de chaves privadas de assinatura digital de SCT.

6.2.5. Arquivamento de chave privada

6.2.5.1. A ACT VALID 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. A chave privada é ativada somente se existir um alvará válido emitido pela EAT.

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.

6.2.9. 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. A DPCT prevê que as chaves públicas dos SCT da ACT Valid, 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.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas dos SCT da ACT VALID 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 deverá rejeitar qualquer tentativa de emitir carimbos do tempo caso sua chave privada de assinatura esteja vencida ou revogada.

6.4. Dados de Ativação da Chave do SCT

Não se aplica.

6.4.2. Proteção dos dados de ativação.

Não se aplica.

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

Neste item, a DPCT 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 VALID, 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 deverão ser implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de gerenciamento do carimbo do tempo e com mecanismos de segurança física.

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

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

6.5.2. Classificação da segurança computacional

6.5.2.1. A segurança computacional da ACT VALID 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, atendendo às especificações descritas nesta seção. A responsabilidade pelo atendimento é do fabricante do SCT.

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

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

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

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

6.5.3.6. O SCT utilizado pela ACT VALID 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; autoridade de carimbo do tempo;
d) Permitir identificação e registro de todas as ações executadas e dos carimbos do tempo emitidos;
e) Garantir a irretroatividade na emissão de carimbos do tempo;
f) Prover meios para que a EAT possa auditar e sincronizar o seu relógio interno;
g) Garantir que o acesso da EAT seja realizado através de autenticação mútua entre o SCT e o SAS, utilizando certificados digitais;
h) Possuir certificado de especificações emitido pelo fabricante;
i) Somente emitir carimbo do tempo se:
    i. Possuir alvará vigente emitido pela EAT, a fim de garantir que a precisão do sincronismo do seu relógio esteja de acordo com o relógio da FCT;
    ii. For assinado por certificado digital válido emitido por AC credenciada na ICP-Brasil.

6.5.4 Ciclo de Vida de Módulo Criptográfico Associados aos SCTs

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 VALID certifica-se que seus SCT estejam sincronizados com o UTC dentro da precisão declarada nas PCT respectivas e, particularmente, que:

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

relógio do SCT está fora da precisão estabelecida na PCT correspondente;

f) a sincronização dos relógios dos SCTs seja mantida mesmo quando ocorrer a inserção de um segundo de transição (*leap second*);
g) a EAT tenha acesso com perfil de auditoria aos logs resultantes das ASRs.

6.6 Controles Técnicos do Ciclo de Vida

Nos itens seguintes desta DPCT são descritos, quando aplicáveis, os controles implementados pela ACT VALID e pelos PSSs a ela vinculados no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1 Controles de desenvolvimento de sistema

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.

6.6.2 Controles de gerenciamento de segurança

6.6.2.1. A ACT VALID 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 VALID utiliza método formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3 Classificações de segurança de ciclo de vida

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 da DPCT são descritos os controles relativos à segurança da rede da ACT VALID, 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 intrusos (IDS), localizados no segmento de rede que hospeda o sistema de certificação estão localizados e operam em ambiente de nível 4.

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

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

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

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

a) pela AC RAIZ 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 AC RAIZ;
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 AC RAIZ;
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 VALID.

.

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

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

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1 O sistema de detecção de intrusão está 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 aos firewalls ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas ou ainda a reconfiguração dos firewalls.

.

6.7.3.2. O sistema de detecção de intrusão reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com atualização da sua base de reconhecimento.

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

6.7.4 Registro de acessos não autorizados à rede

As tentativas de acesso não-autorizado – em roteadores, firewalls ou IDS – são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é diária 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 VALID implementa serviço de proxy, restringindo o acesso, a partir de todas suas estações de trabalho, a serviços que possam comprometer a segurança do ambiente ACT VALID.

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

6.7.5.3 Os relógios dos SCTs são 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

O módulo criptográfico utilizado para armazenamento da chave privada da ACT VALID está em conformidade com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

7. PERFIS DOS CARIMBOS DO TEMPO

7.1. Diretrizes Gerais

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

7.2. Perfil do Carimbo do tempo

Todos os carimbos do tempo emitidos pela ACT VALID 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 [10].

7.2.1.2. Perfil do formato da resposta

a) Parâmetros a serem suportados:
    i. O campo *accuracy* deve ser suportado e compreendido;
    ii. Mesmo quando inexistente ou configurado como FALSO, o campo ordering deve ser suportado;
    iii. O campo *nonce* deve ser suportado e verificado com o valor constante da requisição correspondente para que a resposta seja corretamente validada;
    iv. Nenhuma extensão necessita ser tratada ou suportada

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

7.2.2. Requisitos para um servidor TSP

7.2.2.1. Perfil para o formato do pedido
a) Parâmetros a serem suportados
   i. Não necessita suportar nenhuma extensão;
   ii. Deve ser capaz de tratar os campos opcionais reqPolicy, nonce, certReq.
b) Algoritmos a serem suportados: Consultar documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

7.2.2.2. Perfil do formato da resposta
a) Parâmetros a serem suportados
   i. O campo *genTime* deve ser representado até a unidade especificada na PCT;
   ii. Deve haver uma precisão mínima, conforme definido na PCT;
   iii. O campo *ordering* deve ser configurado como falso ou não deve ser incluído na resposta;
   iv. Extensão, não crítica, contendo informação sobre o encadeamento de carimbos do tempo, caso a ACT adote esse mecanismo;
   v. Outras extensões, se incluídas, não devem ser marcadas como críticas;
   vi. Campo de identificação do alvará vigente no momento da emissão do Carimbo do Tempo e válido conforme descrito no DOC-ICP-12.01.
a) Algoritmos a serem suportados: Consultar documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].
b) Tamanhos de chave a serem suportados: Consultar documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

7.2.3. Perfil do Certificado do SCT

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

7.2.3.2. O certificado correspondente contém apenas uma instância do campo de extensão, conforme definido na RFC 3280, com o 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-kptimeStamping: 1.3.6.1.5.5.7.3.8.

7.2.4. Formatos de nome

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

C = BR
O = ICP-Brasil
OU = Autoridade de Carimbo do Tempo VALID
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: HTTP/HTTPS**.**

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. Políticas de publicação e notificação

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

a) quanto aos procedimentos operacionais, pela AC RAIZ, por meio de pessoal de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].
b) quanto 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 VALID recebeu auditoria prévia da AC RAIZ para fins de credenciamento na ICP-Brasil e que é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.4.3. A ACT VALID recebeu auditoria prévia da AC RAIZ 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 VALID informa que as entidades da ICPBrasil a ela diretamente vinculadas também receberam auditoria prévia, para fins de credenciamento, e que a ACT VALID pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo 8.2.2.

8.5 Ações tomadas como resultado de uma deficiência

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

8.6 Comunicação dos resultados

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

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 Tarifas de Serviço

Nos itens a seguir, é especificada pela ACT VALID pela DPCT a política tarifária e de reembolso aplicáveis.

9.1.1 Tarifas de emissão de carimbos do tempo

Não se aplica.

9.1.2 Tarifas de acesso ao carimbo do tempo

Não se aplica.

9.1.3 Tarifas de revogação ou de acesso à informação de status

Não há tarifa de revogação ou de acesso à informação de status.

9.1.4 Tarifas para outros serviços

Tarifas para outros serviços da AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [8].

9.1.5 Política de reembolso

Não se aplica.

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 Todas as informações coletadas, geradas, transmitidas e mantidas pela ACT VALID e pelas ARs vinculadas são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.3. Essas informações serão arquivadas de acordo com sua classificação, especificada na Política de Segurança

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

9.3.2 Informações fora do escopo de informações confidenciais

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

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

9.3.3 Responsabilidade em proteger a informação confidencial

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

9.3.3.2 A chave privada de assinatura digital dos SCTs será gerada e mantida pela ACT VALID, que será responsável pelo seu sigilo.

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

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

9.4.2 Tratamento de informação como privadas

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

9.4.3 Informações não consideradas privadas

9.4.3.1. Não aplicável.

9.4.4 Responsabilidade para proteger a informação privadas

9.4.4.1 A ACT VALID 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 VALID poderão ser utilizadas ou divulgadas a terceiras mediantes expressas 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 VALID 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 VALID 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.

9.4.6.2 Não aplicável.

9.4.7 Outras circunstâncias de divulgação de informação

9.4.7.1 Em nenhuma outra circunstância, que não esteja prevista nesta DPCT, serão divulgadas informações sigilosas.

9.4.8 Informações a terceiros

9.4.8.1 Como diretriz geral, nenhum documento, informação ou registro sob a guarda da ACT VALID, será fornecido a terceiros, exceto quando o requerente o solicite por meio de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado

9.5 Direitos de Propriedade Intelectual

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

9.6 Declarações e Garantias

9.6.1 Declarações e garantias das terceiras partes

9.6.1.1 Constituem direitos da terceira parte:

a) recusar a utilização do carimbo do tempo para fins diversos dos previstos na PCT correspondente;
b) verificar, a qualquer tempo, a validade do carimbo do tempo.

9.6.1.2 Um carimbo emitido por ACT VALID 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 VALID e do subscritor.

9.7 Isenção de garantias

Não se aplica.

9.8 Limitações de responsabilidades

9.8.1 A ACT VALID 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 VALID 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 A ACT VALID realiza as notificações, as solicitações ou quaisquer outras comunicações necessárias com os participantes, relativas às práticas descritas na DPCT, por meio de comunicado interno e externo e e-mail.

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 VALID.

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. É estabelecido que a DPCT da ACT VALID 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 VALID 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 VALID. 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 REFERENCIADOS

Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-11
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-13
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[4]	POLITICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[5]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

[6]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[8]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO AMBITO DA ICP-BRASIL	DOC-ICP-10
[10]	PERFIL DO ALVARÁ DO CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12.01
[11]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

11.REFERÊNCIAS

RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.
RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, november 2003.
RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.
ETSI TS 101861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.