DECLARAÇÃO DE PRÁTICAS DE CARIMBO DO TEMPO

DA

AUTORIDADE DE CARIMBO DO TEMPO DE DEFESA

(DPCT ACT DEFESA)

Versão 1.0
Março de 2025

Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Motivo	Descrição da Alteração
1.0	06/03/2025	Versão Inicial	Versão inicial, de acordo com o DOC-ICP-12 versão 2.1

1 INTRODUÇÃO

1.1 Visão Geral

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

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

b) **REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL** [**12**], aprovado pela Resolução nº 59, de 28 de novembro de 2008;

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

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

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

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

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

1.1.4 Esta Declaração de Práticas de Carimbo do Tempo (DPCT) descreve as práticas e os procedimentos empregados pela Autoridade de Carimbo do Tempo de Defesa (ACT Defesa), integrante da 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 são 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 - Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil.

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

a) **POLÍTICA DE SEGURANÇA DA ICP-BRASIL** [4], documento aprovado pela Resolução nº 02, de 25 de setembro de 2001;

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

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

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

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

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

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

1.2 Identificação

1.2.1 Esta DPCT é chamada Declaração de Práticas de Carimbo do Tempo da Autoridade de Carimbo do Tempo de Defesa (DPCT ACT DEFESA) e possui o Identificador de Objeto (OID) 2.16.76.1.5.15, atribuído pela ICP-Brasil para a ACT Defesa.

1.3 Comunidade

1.3.1 Autoridades de Carimbo do Tempo

1.3.1.1 Esta DPCT refere-se à Autoridade de Carimbo do Tempo de Defesa (ACT Defesa).

1.3.2 Prestador de Serviços de Suporte

1.3.2.1 A ACT Defesa não utiliza Prestador de Serviços de Suporte (PSS).
O endereço da página *web* (URL) da ACT Defesa é:
https://www.acdefesa.mil.br/carimbodotempo

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

a) disponibilização de infraestrutura física e lógica;

b) disponibilização de recursos humanos especializados; ou

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

1.3.2.3 A ACT Defesa mantêm as informações acima sempre atualizadas.

1.3.3 Subscritores

1.3.3.1 A solicitação de carimbo do tempo pode ser realizada por pessoa física ou jurídica vinculada ao Ministério da Defesa (MD), à Marinha do Brasil (MB), ao Exército Brasileiro (EB) ou à Força Aérea Brasileira (FAB), por meio de aplicações ou sistemas.

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 Defesa implementa a seguinte Política de Carimbo de Tempo (PCT), que define como os carimbos do tempo emitidos devem ser utilizados e sua aplicação e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses carimbos:

Política	Nomeclatura	OID
Política de Carimbo do Tempo da ACT Defesa	PCT ACT Defesa	2.16.76.1.6.15

1.5 Política de Administração

Esta DPCT é administrada pela ACT Defesa, conforme dados informados a seguir.

1.5.1 Organização administrativa do documento

ACT Defesa - Autoridade de Carimbo do Tempo de Defesa.

1.5.2 Contatos

Nome: Mauro Monteiro Soares
Endereço: Centro Integrado de Telemática do Exército - CITEx, Av. Duque de Caxias, s/n, Setor Militar Urbano, CEP 70630-100 - Brasília-DF
Telefone: (61) 2035-1687
Página web: https://www.acdefesa.mil.br
E-mail: contato@acdefesa.mil.br

1.5.3 Pessoa responsável pela adequabilidade da DPCT e PCT

Nome: André Luiz Cibin Ribeiro
Telefone: (61) 2035-1680
E-mail: andre@acdefesa.mil.br

1.5.4 Procedimentos de aprovação da DPCT

Esta DPCT foi aprovada pelo ITI, durante o processo de credenciamento da ACT Defesa, 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	Autoridades de Carimbo do Tempo
ASR	Autenticação e Sincronização de Relógio
CCD	Centro de Certificação Digital
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CN	Common Name
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPCT	Declaração de Práticas de Carimbo do Tempo
EAT	Entidade de Auditoria do Tempo
EB	Exército Brasileiro
ETSI	European Telecommunication Standard Institute
FAB	Força Aérea Brasileira
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

SIGLA	DESCRIÇÃO
ISO	International Organization for Standardization
ITSEC	European infrmation Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
MB	Marinha do Brasil
MD	Ministério da Defesa
MSC	Módulo de Segurança Criptográfico
NBR	Norma Brasileira
OID	Object Identifier
PCN	Plano de Continuidade de Negócio
PCT	Política de Carimbo do Tempo
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request for Comments
SAS	Sistemas de Auditoria e Sincronismo
SCT	Servidor de Carimbo 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 Location
UTC	Universal Time Coordinated

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Publicação de informações da ACT Defesa

2.1.1 A ACT Defesa publicará e manterá disponível no endereço da página web (URL) *https://www.acdefesa.mil.br/carimbodotempo* as informações descritas no item 2.1.2, ressaltando que a disponibilidade desta página é de no mínimo 99,5% (noventa e nove vírgula cinco por cento) do tempo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.2 As seguintes informações, são publicadas na página *web:*

a) os certificados dos SCTs que opera;

b) a DPCT ACT Defesa;

c) a PCT ACT Defesa ;

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 Defesa;e

g) não se aplica.

2.2 Frequência de Publicação

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

2.3 Controles de acesso aos repositórios

2.3.1 Não há quaisquer restrições para acesso, leitura e consulta às informações publicadas por esta ACT Defesa, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil. Acessos para escrita nos locais de armazenamentos e publicações são permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 A ACT Defesa identifica a Organização (MD, MB, EB ou FAB) a qual o solicitante de carimbo do tempo pertence através do endereço IP de origem da respectiva requisição do carimbo do tempo TSQ (Time Stamp Request). Esse IP é previamente cadastrado na ACT Defesa para solicitar o carimbo do tempo.

3.2 A requisição do carimbo do tempo TSQ *(Time Stamp Request)* não identifica o solicitante, por isso, em situações onde a ACT precisa conhecer a identidade do solicitante, são usados meios alternativos de identificação e autenticação.

4 REQUISITOS OPERACIONAIS

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

4.1 Solicitação de Carimbos do Tempo

Para solicitar um carimbo do tempo num documento digital o subscritor gera uma requisição de carimbo do tempo TSQ *(Time Stamp Request)* contendo o *hash* a ser carimbado. Para geração do *hash*, é utilizado o algoritmo SHA-256.

À solicitação de um carimbo do tempo será atendida pela ACT Defesa segundo os requisitos e procedimentos operacionais a seguir:

a) As solicitações de carimbo do tempo são realizadas através de sistema ou aplicações utilizadas pelo subscritor;

b) A requisição de carimbo do tempo é no formato TSQ conforme RFC 3161;

c) O envio do TSQ é realizado por meio do protocolo HTTP, utilizando a porta 80, ou HTTPS, utilizando a porta 443, de acordo com a RFC 3161.

A PCT ACT Defesa, implementada pela ACT Defesa, 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 As solicitações de carimbos do tempo são realizadas por pessoas físicas ou jurídicas vinculadas ao MD ou às Forças Singulares (MB, EB, FAB).

4.1.2 Processo de registro e responsabilidades

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

4.1.2.1 Responsabilidades da ACT Defesa

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

4.1.2.1.2 Não se aplica

4.1.2.2 Obrigações da ACT Defesa

As obrigações da ACT Defesa 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) a ACT Defesa, por ser mantida por órgão da Administração Direta da União, não cabe a contratação de seguro de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, conforme previsto no DOC-ICP-03 - CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5];

r) não se aplica.; 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 principio geral, a ACT DEFESA receberá as requisições de Carimbo do Tempo dos subscritores, que utilizarão um aplicativo para encaminhar as TSQs ao SCT, e em seguida receber os carimbos de tempo em resposta às TSQs, seguindo o formato definido na RFC 3161.

4.2.3 O aplicativo utilizado para encaminhar as TSQs ao SCT é constituído de um sistema disponibilizado na rede corporativa acessada pelo subscritor. As solicitações de carimbo do tempo apenas serão encaminhadas aos SCT da ACT DEFESA caso sejam oriundas de endereços IPs vinculados às redes corporativas do MD, MB, EB ou FAB previamente cadastrados junto à ACT DEFESA.

4.2.4 O controle do acesso da comunicação entre o aplicativo do subscritor e o SCT é de responsabilidade da ACT DEFESA.

4.2.5 O aplicativo utilizado pelo subscritor executa as seguintes tarefas:

a) encaminha as TSQ utilizando os protocolos HTTPS ou HTTP para os endereços https://sct.acdefesa.mil.br:443/timestamp ou http://sct.acdefesa.mil.br:80/timestamp

b) identifica e valida, se necessário, o usuário que está acessando o sistema;

c) receber os *hashes* que serão carimbados;

d) enviar ao SCT os *hashes* que serão carimbados;

e) receber de volta os *hashes* devidamente carimbados;

f) confere a assinatura digital do SCT;

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

h) devolver ao usuário o *hash* devidamente carimbado;

A comutação para o SCT de contingência, em caso de pane do SCT principal, será realizada por infraestrutura da ACT Defesa, sendo transparente para os subscritores solicitantes de carimbos do tempo.

4.2.6 O SCT, ao receber a TSQ, realiza a seguinte sequência de tarefas:

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

b) produz carimbos do tempo apenas para solicitações válidas;

c) usa uma fonte confiável do tempo;

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

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

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

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

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

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

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

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

l) inclui informações adicionais solicitadas pelo requerente nos campos de extensão suportados e, caso não seja possível, responde com mensagem de erro;

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

4.2.7 A ACT Defesa informa na sua PCT a disponibilidade dos seus serviços de carimbo do tempo. A disponibilidade 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 de aplicativo disponibilizado na rede corporativa do subscritor que faz a interface com o serviço da ACT DEFESA. Esse aplicativo realiza automaticamente a conferência dos dados do carimbo, observando os requisitos e procedimentos operacionais estabelecidos pela ACT DEFESA para aceitação de um carimbo do tempo, que são os seguintes:

a) Verifica o valor do status indicado no campo *PKIStatusInfo* do carimbo do tempo. Caso nenhum erro esteja presente, isto é, o status esteja com o valor 0 (sucesso) ou 1 (sucesso com restrições), são verificados os próximos itens;

b) Compara se o *hash* presente no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT;

c) Compara se o OID do algoritmo de *hash* no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT;

d) Compara se o número de controle (valor do campo *nounce*) presente no carimbo do tempo é igual ao da requisição (TSQ) enviada para ACT;

e) Verifica a validade da assinatura digital do SCT que emitiu o carimbo do tempo;

f) Verifica se o certificado do SCT é válido e não está revogado;

g) Verifica se o certificado do SCT possui o uso adequado para este objetivo, isto é, se o certificado possui o valor *id-kp-timeStamping* com o OID definido pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [13].

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

4.3.3 Em especial, o aplicativo utilizado pelo subscritor, verifica se o que foi carimbado corresponde ao que foi enviado para carimbar. Ele verifica também se o carimbo do tempo foi assinado pela ACT Defesa e se estão corretos o *hash* dos dados e o OID do algoritmo de *hash*. O aplicativo verifica ainda 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 número de controle incluído na resposta, comparando-o com o número incluído no pedido. Se qualquer uma das verificações acima falhar, o carimbo do tempo deve ser rejeitado.

4.3.4 Além disso, como o certificado do SCT pode ter sido revogado, o status do certificado é verificado (ex: analisando a LCR apropriada) para confirmar se o certificado ainda está válido. A seguir o aplicativo utilizado pelo subscritor verifica também o campo *policy* para determinar se a política sob a qual o carimbo foi emitido é aceitável ou não para o aplicativo. O aplicativo utilizado pelo subscritor compara se o valor do campo *nounce* presente no carimbo do tempo é igual ao da TSQ enviada para a ACT.

4.3.5 Cada PCT implementada pela ACT Defesa define os procedimentos específicos para aceitação dos carimbos do tempo emitidos segundo a PCT, com base nos processos acima e nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2].

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1 Segurança Física

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

5.1.1 Construção e localização das instalações da ACT Defesa

5.1.1.1 A localização e o sistema de carimbo do tempo utilizado para a operação da ACT Defesa não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.2 Acesso físico nas instalações de ACT Defesa

A ACT Defesa dispõe de um sistema de controle de acesso físico para garantir a segurança de suas instalações operacionais, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4] e os requisitos que seguem.

5.1.2.1 Níveis de acesso

5.1.2.1.1 São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da ACT Defesa.

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

5.1.2.1.3 O segundo nível - ou nível 2 - é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da ACT Defesa. A passagem para o segundo nível exige identificação por meio eletrônico e o uso de crachá.

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

5.1.2.1.5 O acesso a este nível será permitido apenas a pessoas que trabalhem diretamente no CCD AC Defesa ou ao pessoal responsável pela manutenção de sistemas

e equipamentos administrados pelo CCD AC Defesa, como administradores de rede e técnicos de suporte de informática.

5.1.2.1.6 Geradores estão situados em área externa ao ambiente da ACT Defesa. No--breaks e outros componentes da infraestrutura física estão abrigados neste nível, para evitar acessos ao ambiente por parte de prestadores de serviços de manutenção.

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

5.1.2.1.8 **O terceiro nível - ou nível 3** - situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da ACT Defesa. Qualquer atividade relativa à emissão de carimbos do tempo poderá ser realizada a partir desse nível. Somente pessoas autorizadas poderão permanecer nesse nível. Pessoas que não possuem permissão de acesso não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

5.1.2.1.9 No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Três tipos de mecanismos de controle são requeridos para a entrada nesse nível: a identificação individual (com o cartão eletrônico), a identificação biométrica e senha de acesso.

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

5.1.2.1.11 Não se aplica.

5.1.2.1.12 Há uma porta única de acesso ao ambiente de nível 3, que abrirá 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 Não se aplica

5.1.2.1.14 O SCT se encontram no ambiente de nível 4.

5.1.2.1.15 O quarto nível - ou nível 4 - é interno ao terceiro nível e as paredes, piso e o teto são inteiriços e revestidos de aço e concreto, constituindo uma célula estanque (sala cofre) contra ameaças de acesso indevido, água, vapor, gases e fogo. É onde ocorrem as atividades especialmente sensíveis de operação da ACT DEFESA. Todos os sistemas e equipamentos necessários as atividades da ACT estão localizados a partir desse nível, inclusive os SCTs. São dois (02) os ambientes de quarto nível localizados na sala cofre, abrigando os seguintes itens:

a) sala de equipamentos de suporte (ar-condicionado e quadros de distribuição);

b) sala de equipamentos de produção *on-line*, equipamentos de rede e infraestrutura (*firewall, switches,* roteadores e servidores) e cofre de armazenamento.

O quarto nível, ou nível 4, compreende pelo menos 2 cofres ou gabinetes reforçados trancados, que abrigam, separadamente, os SCTs e equipamentos criptográficos e 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 e os gabinetes obedecem as seguintes especificações mínimas:

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

b) possuem trancas com chave.

5.1.2.1.17 O acesso ao gabinete que abriga o SCTs se encontra em uma sala cofre onde sua abertura exige, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas pela ACT Defesa. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

5.1.2.2 Sistemas físicos de detecção

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

5.1.2.2.2 A segurança é realizada por:

a) um militar armado, integrante do CCD AC Defesa, 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 localmente.

5.1.2.2.3 Os ambiente de nível 3 e 4 são dotados, adicionalmente, de circuito Interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não permitirão a captura de senhas digitadas nos sistemas.

5.1.2.2.4 As mídias resultantes dessa gravação são armazenadas por, no mínimo, 1 (um) ano, em ambiente não inferior ao nível 2.

5.1.2.2.5 A ACT Defesa possui mecanismos que permitam, em caso de falta de energia:

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

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

5.1.2.3 Sistema de controle de acesso

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

5.1.3 Energia e ar condicionado do ambiente de nível 4 da ACT

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

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

5.1.3.3 São utilizados tubulações, dutos, calhas, quadros e caixas de passagem, distribuição e terminação projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, de telefonia e de dados.

5.1.3.4 Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 (seis) meses, na busca de evidências de violação ou de outras anormalidades.

5.1.3.5 São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP- BRASIL [4]. Qualquer modificação nessa rede deve ser documentada e autorizada previamente.

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

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

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

5.1.3.9 A capacidade de redundância de toda a estrutura de energia e ar condicionado do ambiente de nível 4 da ACT Defesa é garantida por meio de no-breaks e geradores de porte compatível.

5.1.4 Exposição à água nas instalações de ACT

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

5.1.5 Prevenção e proteção contra incêndio nas instalações da ACT

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

5.1.5.2 Existem no interior do ambiente nível 3 extintores de incêndio das classes B e C, para apagar incêndios em combustíveis e equipamentos elétricos, dispostos no ambiente de forma a facilitar o seu acesso e manuseio.

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

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

5.1.5.5 Mecanismos específicos são implantados pela ACT Defesa para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.6 Armazenamento de mídia nas instalações de ACT Defesa

5.1.6.1 A ACT Defesa 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 da ACT

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

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

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 Defesa é usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala está disponível ao pessoal autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e atende aos requisitos mínimos estabelecidos por este documento para um ambiente de nível 2.

5.2 Controles Procedimentais

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na ACT Defesa, 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 militar ou funcionário utilize indevidamente o sistema de carimbo do tempo sem ser detectado. As ações de cada integrante da ACT estão limitadas de acordo com o seu perfil.

5.2.1.2 A ACT Defesa estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. Os perfis estabelecidos são os seguintes:

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

b) Operador de Sistema - responsável pela operação diária dos sistemas confiáveis da ACT Defesa. Autorizado a realizar backup e recuperação de sistema;

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

5.2.1.3 Todos os integrantes da ACT Defesa 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 integrante se desliga da ACT Defesa, suas permissões de acesso são revogadas imediatamente. Quando há mudança na função que ocupa dentro da ACT, são revistas suas permissões de acesso. Existe uma lista de revogação com todos os recursos inicialmente disponibilizados, que o empregado deve devolver à ACT Defesa no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

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

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

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1 Todos as pessoas que ocupam os perfis designados pela ACT Defesa passam por um processo rigoroso de seleção. Todo integrante da ACT Defesa tem sua identidade e perfil verificados antes de:

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

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 utilizadas para identificação e autenticação dos integrantes atendem as seguintes regras:

a) são diretamente atribuídos a um único operador (integrante) da ACT DEFESA devidamente qualificado;

b) não são compartilhados; e

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

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

5.3 Controles de Pessoal

Nos itens seguintes são descritos requisitos e procedimentos, implementados pela ACT Defesa 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 integrantes da ACT Defesa, encarregados de tarefas operacionais, tem registrado no termo de responsabilidade:

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

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

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

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.1.1 Todo o pessoal da ACT DEFESA envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição e gerenciamento de carimbos do tempo, é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4] e na Política de Segurança da ACT DEFESA.

5.3.2 Procedimentos de verificação de antecedentes

5.3.2.1 Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da ACT DEFESA envolvido em atividades diretamente relacionadas com os processos de emissão, expedição e gerenciamento de carimbos do tempo, são submetidos aos seguintes processos, antes do começo das atividades:

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 Defesa poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

5.3.3.1 Todo o pessoal da ACT Defesa, envolvido em atividades diretamente relacionadas com os processos de emissão, expedição e gerenciamento de carimbos do tempo, recebem treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e tecnologias de carimbo do tempo e sistema de carimbos do tempo em uso na ACT;

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 DEFESA envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo, é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas de certificação da ACT.

5.3.5 Frequência e sequência de rodízios de cargos

5.3.5.1 A ACT Defesa não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

5.3.6.1 Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da ACT DEFESA, ou de um PSS vinculado se houver, a ACT DEFESA suspenderá, de imediato, o acesso dessa pessoa aos SCT e instaurará processo administrativo para apurar os fatos e, se for o caso, adotará as medidas legais cabíveis.

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

a) relato da ocorrência com *"modus operandi"*;

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 Defesa encaminhará suas conclusões à EAT.

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

a) advertência;

b) suspensão por prazo determinado; ou

c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 Requisitos para designação de pessoal

5.3.7.1 Todo pessoal da ACT Defesa e dos PSS vinculados se houver, envolvidos no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo, é designado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]. A ACT Defesa pode definir requisitos adicionais para a designação de pessoal.

5.3.8 Documentação fornecida ao pessoal

5.3.8.1 A ACT DEFESA disponibiliza para todo o seu pessoal e o pessoal dos PSS vinculados se houver, no mínimo:

a) esta DPCT;

b) a PCT que implementa;

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

d) a Política de Segurança da ACT DEFESA;

e) documentação operacional relativa à suas atividades;

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

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

5.4 Procedimentos de Log de Auditoria

Descrever-se-á no itens seguintes os aspectos dos sistemas de auditoria e de registro de eventos implementados pela ACT Defesa com o objetivo de manter o ambiente seguro.

5.4.1 Tipos de Eventos Registrados

5.4.1.1 Todas as ações executadas pelo pessoal da ACT Defesa, no desempenho de suas atribuições, são registradas em arquivos de auditoria de modo que cada ação esteja associada à pessoa que a realizou.

A ACT Defesa registra em arquivos para fins de auditoria os seguintes eventos relacionados à segurança do seu sistema de carimbo do tempo:

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 caribos do tempo;

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

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

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

h) emissão de carimbos do tempo;

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

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

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

   i. a própria sincronização;

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

   iii. falta de sinal de sincronização;

   iv. tentativas de autenticação mal sucedidas;

   v. detecção da perda de sincronização.

5.4.1.2 A ACT Defesa também registra, eletrônica ou manualmente, as seguintes 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 Todas as informações que são registradas pela ACT estão descritas nos itens 5.4.1.1 e 5.4.1.2.

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

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

5.4.2 Frequência de auditoria de registros (logs)

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

5.4.3 Período de retenção para registros de auditoria

5.4.3.1 A ACT Defesa mantém localmente, em suas próprias instalações, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 5.5.

5.4.4 Proteção de registros de Auditoria

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

5.4.4.2 As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção, através de controles de acesso aos ambientes físicos onde são armazenados esses registros.

5.4.4.3 Os mecanismos de proteção descritos neste item obedecem a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

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

5.4.5.1 A ACT Defesa executa procedimentos de *backup*, dos registros de eventos de log e sumários de auditoria dos equipamentos utilizados pela ACT, de duas formas:

a) diariamente: cópia de segurança;

b) semanalmente: cópia armazenada em ambiente seguro para processos de auditoria.

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 interno à ACT Defesa compreende a combinação de processos automatizados e manuais executados pelos sistemas da ACT, pelo sistema de controle de acesso e pelo pessoal operacional da AC.

5.4.7 Notificação de agentes causadores de eventos

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

5.4.8 Avaliações de vulnerabilidade

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

5.5 Arquivamento de registros

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

5.5.1 Tipos de registros arquivados

5.5.1.1 Os tipos de registros arquivados compreendem, entre outros:

a) notificações de comprometimento de chaves privadas do SCT;

b) substituições de chaves privadas dos SCTs;

c) informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo

5.5.2.1 Os períodos de retenção para cada registro arquivado, são os seguintes:

a) carimbos do tempo emitidos, são retidos, no mínimo, por 6 (seis) anos; e

b) demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 6 (seis) anos.

5.5.3 Proteção de arquivo

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

5.5.4 Procedimentos de cópia de arquivo

5.5.4.1 Uma segunda cópia de segurança *(backup)* de todo o material arquivado é armazenada em ambiente externo às instalações principais da ACT Defesa, recebendo o mesmo tipo de proteção utilizada para o arquivo principal.

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

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

5.5.5 Requisitos para datação de registros

5.5.5.1 Os servidores de dados utilizados pela ACT Defesa são sincronizados com a hora GMT fornecida pela Fonte Confiável de Tempo da AC Raiz. Informações de data e hora nos registros baseiam-se no horário Greenwich Mean Time (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos for zero. Nos casos em que por algum motivo os documentos formalizem o uso de outro formato, ele será aceito.

5.5.6 Sistema de coleta de dados de arquivo

5.5.6.1 Todos os sistemas de coleta de dados de arquivos utilizados pela ACT Defesa são internos, sendo uma combinação de procedimentos operacionais automatizados e manuais, executados pelo sistema operacional, pelos sistemas de certificação de AC 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 Defesa, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação será devidamente identificado.

5.6 Troca de chave

5.6.1 O par de chaves criptográficas da ACT Defesa é gerado pela própria ACT Defesa. Acessando a interface de administração do SCT, na área destinada à administração do par de chaves, será necessário confirmar os dados de renovação do certificado para, na sequência, iniciar o processo de geração de uma nova chave privada. A nova chave será gerada internamente no MSC do equipamento e nele ficará armazenada. O sistema retornará, por meio da interface com o usuário administrador, a requisição de geração (em base64) para ser gerado o certificado na AC. Caso ainda exista uma chave privada em uso pelo SCT, essa chave não será substituída pela nova chave privada gerada, que continuará armazenada até que sua chave pública correspondente seja cadastrada no sistema. Somente após

o cadastramento da nova chave pública, correspondente a nova chave privada, é que a chave em uso será descontinuada e substituída pela nova chave privada.

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

5.7 Comprometimento e Recuperação de Desastre

5.7.1 Disposições Gerais

5.7.1.1 A ACT Defesa possui um Plano de Continuidade de Negócios , estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], testado anualmente para garantir a continuidade de seus serviços críticos. Nos itens a seguir estão relacionados os procedimentos de notificação e de recuperação de desastres previstos nesse plano.

5.7.1.2 A ACT Defesa assegura, no caso de comprometimento de sua operação, por qualquer um dos motivos relacionados nos itens abaixo, que as informações relevantes sejam dispostas aos subscritores e às terceiras partes. A ACT Defesa disponibilizará 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 (ex: comprometimento da chave privada do SCT), suspeita de comprometimento ou perda de calibração, o SCT não emitirá carimbo do tempo até que sejam tomadas medidas para recuperação do comprometimento.

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

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, a ACT Defesa executará uma rigorosa inspeção para verificar a veracidade do fato e o nível de comprometimento dos recursos envolvidos. O procedimento será realizado por um grupo pré-determinado devidamente treinado para essa situação.

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado do SCT é revogado

5.7.3.1.1 Em caso de revogação do certificado do SCT, todos os carimbos do tempo subsequentes estarão automaticamente inválidos. O SCT será desabilitado pelo Administrador. Será necessária a geração de um novo par de chaves.

5.7.3.2 Chave privada do SCT é comprometida

5.7.3.2.1 Em caso de suspeita de comprometimento de chave do SCT, após a identificação da crise, serão notificados os gestores de segurança da ACT Defesa para que acionem as equipes envolvidas, de forma a indispor temporariamente os serviços da autoridade certificadora. Será necessária a revogação do certificado do SCT. Nesse caso o SCT será desabilitado pelo Administrador. Caso não exista outro SCT habilitado, para garantir a continuidade no serviço de carimbo do tempo, será necessária a geração de um novo par de chaves. 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; e

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

5.7.3.3 Calibração e sincronismo do SCT são perdidos

5.7.3.3.1 Na hipótese de perda de calibração e de sincronismo do SCT, o fato é imediatamente comunicado aos gestores da EAT, que deverão entrar em contato na interface de auditoria do SAS e executar o procedimento de calibração e sincronismo do SCT que apresentou problema.

5.7.4 Capacidade de continuidade de negócio após desastre

5.7.4.1 A ACT Defesa possui um Plano de Recuperação de Desastres (PRD) que é parte integrante do PCN. Nesse plano são especificadas as ações a serem tomadas no caso de desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro.

O propósito do PRD é restabelecer as principais operações da ACT Defesa quando a operação de sistemas é significativamente e adversamente abalada por fogo, inundação, greves, etc.

5.8 Extinção dos serviços de ACT ou PSS

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

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

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

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

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

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

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

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

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

g) a ACT notificará todas as entidades afetadas.

5.8.4 A ACT Defesa providenciará os meios para o cumprimento dos requisitos mínimos acima estabelecidos.

6 CONTROLES TÉCNICOS DE SEGURANÇA

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

6.1 Ciclo de Vida de Chave Privada do SCT

O SCT permite um controle completo do ciclo de vida de sua chave privada, com os seguintes controles;

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); e

f) proteção de chaves privadas.

6.1.1 Geração do par de chaves

6.1.1.1 Neste item, a DPCT Defesa descreve os requisitos e procedimentos referentes ao processo de geração do par de chaves criptográficas da ACT Defesa. O par de chaves criptográficas dos SCTs da ACT Defesa são gerados pela própria ACT Defesa, 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 Defesa assegura que quaisquer chaves criptográficas são geradas em circunstâncias controladas. Em particular:

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

b) que a geração da chave de assinatura do SCT é realizada dentro do Módulo de Segurança Criptográfico (MSC) que cumpre os requisitos dispostos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [11]; e

c) que o algoritmo de geração de chave do SCT, o comprimento da chave assinante resultante e o algoritmo de assinatura usado para assinar o carimbo do tempo são aqueles constantes no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [11].

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

6.1.2 Geração de Requisição de Certificado Digital.

6.1.2.1 O SCT da ACT Defesa possui mecanismo para geração de requisição de certificado digital correspondente à chave privada gerada no módulo criptográfico associado ao SCT, que atende ao formato definido pela ICP-Brasil. A requisição é retornada 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.

6.1.3 Exclusão de Requisição de Certificado Digital

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

6.1.4 Instalação de Certificado Digital

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

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

b) verificar se o certificado possui as extensões obrigatórias;

c) validar o caminho de certificação.

6.1.5 Renovação de Certificado Digital

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

6.1.6 Disponibilização de chave pública da ACT para usuários

6.1.6.1 A ACT Defesa disponibiliza o certificado dos seus SCT e todos os certificados da cadeia de certificação para usuários da ICP-Brasil, por meio do endereço de internet *https://www.acdefesa.mil.br/carimbodotempo*

6.1.7 Tamanhos de chave

6.1.7.1 A ACT Defesa define o tamanho das chaves criptográficas dos SCTs que opera, com base nos requisitos aplicáveis estabelecidos pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP- BRASIL [11]. O tamanho das chaves criptogáficas dos SCT está declarada na PCT.

6.1.8 Geração de parâmetros de chaves assimétricas

6.1.8.1 A geração dos parâmetros de chaves assimétricas é feita em módulo de segurança criptográfico de acordo com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

6.1.9 Verificação da qualidade dos parâmetros

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

6.1.10 Geração de chave por hardware ou software

6.1.10.1 O processo de geração da chave privada é feito por *hardware*.

6.1.11 Propósitos de uso de chave

6.1.11.1 As chaves privadas dos SCT operadas pela ACT Defesa somente são utilizadas para assinatura dos carimbos do tempo por ela emitidos.

6.2 Proteção da Chave Privada

Nos itens seguintes, a DPCT estabelece os procedimentos de segurança que adota para a proteção da chave privada de seus SCTs.

6.2.1 Padrões para módulo criptográfico

6.2.1.1 Para o controle do ciclo de vida e armazenamento da chave privada do SCT, o módulo criptográfico de geração e guarda de chaves assimétricas da ACT Defesa adota o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP- BRASIL [11].

6.2.2 Controle "n"de "m"para chave privada

Não se aplica

6.2.3 Custódia (*escrow*) de chave privada

6.2.3.1 Não é 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 dos SCTs. As mesmas ficam armazenadas no módulo de segurança criptográfica.

6.2.4 Cópia de segurança de chave privada

6.2.4.1 Não é permitido, no âmbito da ICP-Brasil, a geração de cópia de segurança (*backup*) de chaves privadas de assinatura digital de SCT.

6.2.5 Arquivamento de chave privada

6.2.5.1 A ACT Defesa não arquiva chaves privadas com validade vencida ou de uso descontinuado de seus SCTs, entendendo-se como arquivamento o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6 Inserção de chave privada em módulo criptográfico

Não se aplica

6.2.7 Método de ativação de chave privada

6.2.7.1 A ativação da chave privada da ACT Defesa em *hardware* criptográfico é implementada após a autenticação de dois (2) operadores responsáveis utilizando cartões criptográficos, protegidos por senha. As senhas utilizadas obedecem à política de senhas estabelecida pela ACT Defesa.

6.2.7.2 Após a autenticação dos operadores, a chave privada é ativada automaticamente pelo sistema.

6.2.8 Método de desativação de chave privada

6.2.8.1 A desativação da chave privada da ACT Defesa em *hardware* criptográfico é implementada após a autenticação de dois (2) operadores responsáveis utilizando cartões criptográficos, protegidos por senha. A desativação da chave é realizada automaticamente pelo sistema com o desligamento dos SCTs.

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 critptográfico e necessita a autenticação de no mínimo dois (2) operadores do sistema. A destruição é feita somente após a criação de uma nova chave privada.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

6.3.1.1 As chaves públicas dos SCTs da ACT Defesa, após a expiração dos certificados correspondentes, são guardadas pela AC que emitiu os certificados, permanentemente, para verificação de assinaturas geradas durante seu período de validade. Adicionalmente, as chaves públicas também continuam armazenadas nos SCTs, mesmo após a destruição de sua chave privada correspondente do HSM.

6.3.2 Períodos de uso para as chaves pública e privada

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

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

6.4 Dados de Ativação da Chave do SCT.

Não se aplica.

6.4.1 Geração e instalação dos dados de ativação

Não se aplica

6.4.2 Proteção dos dados de ativação

Não se aplica.

6.4.3 Outros aspectos dos dados de ativação

Não se aplica.

6.5 Controles de Segurança Computacional

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

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

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

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

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

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

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

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

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

6.5.1.4 Qualquer equipamento incorporado à ACT Defesa é preparado e configurado como previsto na Política de Segurança (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 Defesa segue as recomendações *Common Criteria.*

6.5.3 Características do SCT

6.5.3.1 O Sistema de Carimbo do tempo é um sistema de *hardware e software* que executa a geração de carimbos do tempo, atendendo às especificações descritas nesta seção. A responsabilidade pelo atendimento é do fabricante do SCT.

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

6.5.3.3 Qualquer 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 é instalado e operado 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 Neste item da DPCT, estão definidas as características dos SCTs utilizados pela ACT Defesa. O SCT possui como características mínimas:

a) a emissão de carimbos do tempo na mesma ordem em que são recebidas as requisições;

b) o gerenciamento e proteção de chaves privadas;

c) utiliza certificado digital válido emitido por AC credenciada pelo Comitê Gestor da ICP-Brasil;

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

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

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

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

h) possui certificado de especificações emitido pelo fabricante;

i) somente emite 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 HSM nos SCTs são realizadas sempre com a presença no mínimo de duas pessoas formalmente designadas para a tarefa em ambiente seguro e controlado. Para a geração de chaves é necessária a autenticação por meio de cartões criptográficos, protegidos com senha, para cessar a interface administrativa.

6.5.5 Auditoria e Sincronização de Relógio de SCT

6.5.5.1 A ACT Defesa certifica-se que seus SCTs estejam sincronizados com a FCT dentro da precisão declarada na PCT Defesa respectiva 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 Defesa;

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 Defesa 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 da DPCT Defesa são descritos, quando aplicáveis, os controles implementados pela ACT Defesa e seu PSS no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1 Controles de desenvolvimento de sistema

6.6.1.1 O desenvolvimento de sistemas é orientado pela metodologia RUP, uma abordagem iterativa baseada em disciplinas para atribuir tarefas e responsabilidades dentro de uma organização de desenvolvimento. O processo de desenvolvimento utilizado 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. Esse plano contém informações sobre o projeto, estimativas de esforço, tamanho e custos do projeto, riscos associados, cronogramas e dados a serem gerenciados;

b) Para cada iteração, são realizadas três etapas; análise, desenvolvimento e fiscalização. Esta é uma fase dinâmica, após a finalização da iteração, volta-se para a análise. Na fase de análise são estimados os esforços 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 elaborado o manual de instruções de uso referente ao programa desenvolvido.

6.6.1.2 Os processos de projeto e desenvolvimento conduzidos pela ACT Defesa e pelo seu fornecedor da solução de carimbo de tempo proveem documentação suficiente para suportar avaliações externas de segurança dos componentes da ACT.

6.6.2 Controles de gerenciamento de segurança

6.6.2.1 A ACT Defesa 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 do níveis configurados de segurança e averiguação do fato gerador do problema para evitar sua recorrência.

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

6.6.3 Classificações de segurança de ciclo de vida

6.6.3.1 A maturidade do ciclo de vida do Servidor de Aplicativo (SA) e a do Sistema de Carimbo de 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 Defesa, são descritos os controles relativos à segurança da rede da ACT Defesa, incluindo *firewall* e recursos similares, observado o disposto no item "redes das entidades da ICP-Brasil" da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.7.1.2 Todos os servidores e elementos de infraestrutura e proteção de rede, tais como: roteadores, *hubs, switches, firewalls* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda os SCT, estão localizados e operam em ambiente de, no mínimo, 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 Os acessos lógicos aos elementos de infraestrutura e proteção de rede são restritos, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

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

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

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

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

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

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

6.7.2 Firewall

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

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

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

6.7.3 Sistema de detecção de intrusão (IDS)

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

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

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

6.7.4 Registro de acessos não autorizados à rede

6.7.4.1 As tentativas de acesso não autorizado - em roteadores, *firewalls* ou IDS - são registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro é, no mínimo, semanal e todas as ações tomadas em decorrência desse exame são documentadas.

6.7.5 Outros controles de segurança de rede

6.7.5.1 A ACT Defesa implementa serviço de *proxy*, restringindo o acesso, a partir de todas suas estações de trabalho, a serviço que possam comprometer a segurança do ambiente da ACT Defesa.

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

6.7.5.3 Os relógios dos SCTs 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 é detectada e registrada e detectada.

6.8 Controles de Engenharia do Módulo Criptográfico

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

7 PERFIS DOS CARIMBOS DO TEMPO

7.1 Diretrizes Gerais

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

7.2 Perfil do Carimbo do Tempo

Todos os carimbos do tempo emitidos pela ACT Defesa 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: de acordo com o documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

7.2.1.2 Perfil do formato de 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: de acordo com o documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

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

7.2.2 Requisitos para um servidor TSP

7.2.2.1 Perfil para o formato do pedido:

a) Parâmetros a serem suportados:

i. não necessita suportar nenhuma extensão;

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

b) Algoritmos a serem usados: de acordo com o documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

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

b) Algoritmos a serem suportados: de acordo com o documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [11].

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

7.2.3 Perfil do Certificado do SCT

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

7.2.3.2 O certificado correspondente contém apenas uma instância do campo de extensão, conforme definido na RFC 3280, com o subcampo *KeyPurposeID* contendo o valor *id-kptimeStamping.* Essa extensão deve ser crítica

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

7.2.4 Formatos de Nome

7.2.4.1 O certificado digital emitido para o SCT da ACT Defesa 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 de Defesa>
CN = <nome do Servidor de Carimbo do tempo>

7.3 Protocolos de Transporte

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

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 Frequência e circunstâncias das avaliações

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

8.2 Identificação/Qualificação do avaliador

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

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

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

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

8.3 Relação do avaliador com a entidade avaliada

8.3.1 Em acordo com o documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA 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 Defesa recebeu auditoria prévia da EAT para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.4.3 A ACT Defesa recebeu auditoria prévia da EAT quanto aos aspectos de autenticação e sincronismo, sendo regularmente auditada, para fins de continuidade de operação, com base no disposto no documento PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3].

8.4.4 a ACT Defesa não possui entidade da ICP-Brasil a ela diretamente vinculadas.

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

A ACT Defesa não comercializa os serviços de emissão de carimbo do tempo por ela emitidos.

9.1.1 Tarifas de emissão de carimbo do tempo

A ACT DEFESA não cobra tarifas referente ao serviço de emissão do carimbo de tempo.

9.1.2 Tarifas de acesso ao de carimbo do tempo

Não há cobrança de tarifas sobre este serviço.

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

Não se aplica.

9.1.5 Política de reembolso

Não se aplica.

9.2 Responsabilidade Financeira

A responsabilidade da ACT DEFESA 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 Considerar-se-á como informação sigilosa pela ACT Defesa, responsável por esta DPCT, todas àquelas informações coletadas, geradas, transmitidas e mantidas pela ACT Defesa que não foram especificadas no tópico 9.3.2 desta DPCT.

9.3.1.2 O princípio geral, estabelecido por esta DPCT, é o de que nenhum documento, informação ou registro fornecido pelo subscritor à ACT Defesa 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 As informações e documentos considerados não sigilosos pela ACT Defesa, responsável por esta DPCT e pelos PSSs a ela vinculadas, são os seguintes:

a) os certificados dos SCTs;

b) as PCTs implemantadas pela ACT;

c) a DPCT da ACT Defesa;

d) versões públicas de PS;

e) a conclusão dos relatórios de auditoria; e

f) todo o conteúdo de livre acesso disponibilizado na página *web* da ACT Defesa.

9.3.3 Responsabilidade em proteger a informação confidencial

9.3.3.1 Os participantes que recebem ou tem acesso a informações confidenciais possuem 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, foi gerada pela própria ACT Defesa, sendo também por ela mantida, sendo responsável pelo seu sigilo.

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

A ACT Defesa 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 Defesa 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

As tratadas do item 9.3.2. nesse documento

9.4.4 Responsabilidade para proteger a informação privadas

9.4.4.1 A ACT Defesa 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 Defesa poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável. O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.
Autorizações formais podem ser apresentadas de duas formas:

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

b) por meio de pedido escrito com firma reconhecida.

9.4.6 Divulgação em processo judicial ou administrativo

9.4.6.1 Como diretriz geral, nenhum documento, informação ou registro sob a guarda da ACT Defesa 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 Defesa poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7 Outras circunstâncias de divulgação de informação

9.4.7.1 Não se aplica.

9.4.8 Informações a terceiros

9.4.8.1 Nenhum documento, informação ou registro sob a guarda da ACT Defesa, responsável pela DPCT, será fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver corretamente identificada e autorizada para fazê-lo.

9.5 Direitos de Propriedade Intelectual

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 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 esteja 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 responsável e do subscritor.

9.7 Isenção de Garantias

Não se aplica

9.8 Limitações de responsabilidades

9.8.1 A ACT DEFESA 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 DEFESA 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

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

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 As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPCT serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por ofício da autoridade competente ou publicação no Diário Oficial da União.

9.12 Alterações

9.12.1 Procedimento para emendas

Qualquer alteração nesta DPCT será submetida à aprovação da AC Raiz.

9.12.2 Mecanismo de notificação e períodos

Mudanças nesta DPCT serão publicadas no site da ACT Defesa.

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

9.13.3 Os casos omissos serão encaminhados para apreciação da EAT.

9.14 Lei aplicável

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

9.15 Conformidade com a Lei aplicável

9.15.1 A ACT Defesa 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 Defesa. 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

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

Ref.	Nome do documento	Código
[1]	VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-11
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-13
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[4]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[5]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[6]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[8]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS 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
[12]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[13]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

11 REFERÊNCIAS BIBLIOGRÁFICAS

RFC 3161 - IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001, disponível em https://tools.ietf.org/

RFC 3628 - IETF - Policy Requirements for Time Stamping Authorities, November 2003, disponível em https://tools.ietf.org/

RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003, disponível em https://tools.ietf.org/

ETSI TS 101.861 - v 1.2.1 - Technical Specification / Time Stamping Profile, março de 2002, disponível em https://www.etsi.org/