DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

DA

AC SAFEWEB TIMESTAMPING

DPC - AC SAFEWEB TIMESTAMPING

Versão 1.0

Junho 2020

AC SAFEWEB TIMESTAMPING
DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado
1.0	19/06/2020	N/A	Versão inicial

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Esta Declaração de Práticas de Certificação (DPC), constitui os requisitos mínimos, obrigatoriamente observados pela Autoridade Certificadora Safeweb Timestamping (AC Safeweb Timestamping), integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e descreve as práticas e os procedimentos utilizados pela AC Safeweb Timestamping na execução de seus serviços.

1.1.2 Esta DPC adota a mesma estrutura utilizada no DOC-ICP-05, que estabelece os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [5].

1.1.3 Não se aplica.

1.1.4 A estrutura desta DPC está baseada na RFC 3647.

1.1.5 A AC Safeweb Timestamping mantém todas as informações da sua DPC sempre atualizadas.

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Este documento é chamado “Declaração de Práticas de Certificação da AC Safeweb Timestamping”, referido a seguir simplesmente como "DPC - AC Safeweb Timestamping" e descreve as práticas e os procedimentos empregados pela AC Safeweb Timestamping no âmbito da ICP-Brasil. O OID da DPC - AC Safeweb Timestamping, atribuído pela AC Raiz na conclusão do seu processo de credenciamento, é **2.16.76.1.1.150.**

1.2.2 Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC Safeweb Timestamping, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes são: assinatura de carimbo do tempo (*Timestamping*).

1.3 PARTICIPANTES DA ICP-BRASIL

1.3.1 AUTORIDADE CERTIFICADORA - AC

Esta DPC se refere à AC Safeweb Timestamping e encontra-se publicada no endereço *web* http://repositorio.acsafeweb.com.br/ac-safewebts/dpc-acsafewebts.pdf.

AC Safeweb Timestamping está no nível imediatamente subsequente ao da Autoridade Certificadora Safeweb (AC Safeweb), que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira (AC Raiz). Com relação aos tipos específicos de certificados emitidos pela AC Safeweb Timestamping, devem ser observadas suas Políticas de Certificado (PC), que explicam como os certificados são gerados, administrados pela AC Safeweb Timestamping e utilizados pela comunidade.

1.3.2 AUTORIDADE DE REGISTRO - AR

1.3.2.1 Os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência das Autoridades de Registro (AR). As ARs vinculadas à AC Safeweb Timestamping estão relacionadas na página www.safeweb.com.br que contém as seguintes informações:

a) relação de todas as AR credenciadas;

b) relação de AR que tenha se descredenciado da cadeia da AC, com respectivas datas do descredenciamento.

1.3.3 TITULARES DE CERTIFICADO

1.3.3.1 Pessoas jurídicas de direito público ou privado, nacionais ou estrangeiras, podem ser titulares de certificado emitidos segundo esta DPC.

1.3.3.2 Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.4 PARTES CONFIÁVEIS

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas pela ICP-Brasil.

1.3.5 OUTROS PARTICIPANTES

Os Prestadores de Serviços de Suporte (PSS), Prestadores de Serviços Biométricos (PSBios) e os Prestadores de Serviço de Confiança (PSC), vinculados à AC Safeweb Timestamping, estão relacionados na página https://www.safeweb.com.br/repositorio.

1.4 USABILIDADE DO CERTIFICADO

1.4.1 USO APROPRIADO DO CERTIFICADO

A AC Safeweb Timestamping pratica as seguintes Políticas de Certificado Digital:

Política de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo T3 da AC Safeweb Timestamping	PC T3 - AC Safeweb Timestamping	2.16.76.1.2.303.9
Política de Certificado de Assinatura Digital tipo T4 da AC Safeweb Timestamping	PC T4 - AC Safeweb Timestamping	2.16.76.1.2.304.9

As PCs correspondentes relacionam as aplicações para as quais são adequados os certificados emitidos pela AC Safeweb Timestamping.

1.4.2 USO PROIBITIVO DO CERTIFICADO

Quando cabível, as aplicações para as quais existem restrições ou proibições para o uso desses certificados estão listadas nas PCs implementadas.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AC: AC Safeweb Timestamping

1.5.2 CONTATOS

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

1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Gisele Strey
Telefone: (51) 3018-0300
E-mail: compliance@safeweb.com.br
Outros: Setor de Compliance

1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA DPC

Esta DPC é aprovada AC Safeweb e pelo ITI. Os procedimentos de aprovação da DPC da AC Safeweb Timestamping são estabelecidos conforme critérios do CG da ICP-Brasil.

1.6 DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	*Automatic Certificate Management Environment*
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CMVP	*Cryptographic Module Validation Program*

CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	*Comitee of Sponsoring Organizations*
CPF	Cadastro de Pessoas Físicas
CS	*Code Signing*
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	*Extended Validation (WebTrust for Certification Authorities)*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IETF	*PKIX Internet Engineering Task Force - Public-Key Infrastructured (X.509)*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITSEC	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	*National Institute of Standards and Technology*
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
OM-BR	Objetos Metrológicos ICP-Brasil
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	*Proof of Possession*
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	*Simple Network Management Protocol*

SSL	*Secure Socket Layer*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 REPOSITÓRIOS

2.1.1 As obrigações da AC Safeweb Timestamping em relação ao seu repositório são:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC Safeweb Timestamping e a sua LCR;

b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e

c) implementar os recursos necessários para a garantia da segurança dos dados nele armazenados.

2.1.2 Os requisitos aplicáveis aos repositórios utilizados pela AC Safeweb Timestamping, são:

a) localização física e lógica: ambiente de nível 4 (quatro) e rede independente;

b) disponibilidade: 99,5% (noventa e nove e meio por cento), 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

c) protocolos de acesso: HTTP; e

d) requisitos de segurança: cada computador servidor da AC Safeweb Timestamping, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, inclusive o servidor de repositório, implementa os controles descritos no item 6.5 desta DPC.

2.1.3 O repositório da AC Safeweb Timestamping está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.4 A AC Safeweb Timestamping disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de suas LCR.

a) Rep.1: http://repositorio.acsafeweb.com.br/ac-safewebts/lcr-ac-safewebts.crl

b) Rep.2: http://repositorio2.acsafeweb.com.br/ac-safewebts/lcr-ac-safewebts.crl

2.2 PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.2.1 A AC Safeweb Timestamping publica e mantém disponível em seu site https://www.safeweb.com.br/repositório informações com disponibilidade mínima de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2 As seguintes informações, no mínimo, são publicadas pela AC Safeweb Timestamping em página web:

a) Seu próprio certificado;

b) Suas LCRs;

c) Sua DPC;

d) As Políticas de Certificado, que pratica;

e) Uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços;

f) Uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3 TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.3.1 Certificados da AC Safeweb Timestamping são publicados imediatamente após sua emissão.

2.3.2 A publicação da LCR se dá conforme determinado na PC correspondente.

2.3.3 As versões ou alterações desta DPC e das PCs, assim como os endereços das ARs vinculadas, são atualizados no site da AC Safeweb Timestamping após aprovação da AC Raiz da ICP-Brasil.

2.4 CONTROLE DE ACESSO AOS REPOSITÓRIOS

2.4.1 Não existe qualquer restrição de acesso para consulta aos endereços das AR vinculadas, a esta DPC, às PC implementadas e às LCRs emitidas pela AC Safeweb Timestamping.

2.4.2 São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado.

2.4.3 O servidor que armazena estas informações se encontra em nível 4 (quatro) e requer senha de acesso.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC Safeweb Timestamping verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os direitos de propriedade intelectual de terceiros. A AC Safeweb Timestamping reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1 ATRIBUIÇÃO DE NOMES

3.1.1 TIPOS DE NOMES

3.1.1.1 A AC Safeweb Timestamping emite certificados com nomes que possibilitam determinar a identidade da pessoa ou organização a que se referem. Para tanto utiliza o "D*istinguished Name*" do padrão ITU X.500. Informações específicas, estão descritas nas PC implementadas, no item 7.1.4.

3.1.1.2 Não se aplica.

3.1.2 NECESSIDADE DOS NOMES SEREM SIGNIFICATIVOS

3.1.2.1 Os certificados emitidos pela AC Safeweb Timestamping exigem o uso de nomes significativos que possibilitam determinar univocamente a identidade da pessoa ou da organização titular do certificado a que se referem, para a identificação dos titulares dos certificados emitidos pela AC Safeweb Timestamping.

3.1.3 ANONIMATO OU PSEUDÔNIMO DOS TITULARES DO CERTIFICADO

Não se aplica.

3.1.4 REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES

Não se aplica.

3.1.5 UNICIDADE DE NOMES

3.1.5.1 Os identificadores do tipo "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC Safeweb Timestamping.

3.1.5.1 Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6 PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES

3.1.6.1 A AC Safeweb Timestamping reserva-se no direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrente da igualdade de nomes entre os solicitantes diversos de certificados.

3.1.6.2 Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7 RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS

Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

3.2 VALIDAÇÃO INICIAL DE IDENTIDADE

A AC Safeweb Timestamping e as ARs vinculadas utilizam os seguintes requisitos e procedimentos para realização dos seguintes processos:

a) Identificação do titular do certificado: identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3 e 3.2.7 observado o quanto segue:

i. para certificados de pessoa física: Não se aplica

ii. para certificados de pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado, e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação.

b) emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC Safeweb Timestamping. A extensão *Subject Alternative Name* é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

3.2.1 MÉTODO PARA COMPROVAR A POSSE DE CHAVE PRIVADA

3.2.1.1 A AR verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. As RFC 4210 e 6712 são utilizadas como referência para essa finalidade.

3.2.1.2 No caso em que sejam requeridos procedimentos específicos para as PCs implementadas, eles são descritos nessas PCs, no item correspondente.

3.2.2 AUTENTICAÇÃO DA IDENTIFICAÇÃO DA ORGANIZAÇÃO

3.2.2.1 DISPOSIÇÕES GERAIS

3.2.2.1.1 Não se aplica.

3.2.2.1.1 Não se aplica.

3.2.2.1.2 Não se aplica.

3.2.2.1.3 Não se aplica.

3.2.2.1.4 Não se aplica.

3.2.2.2 DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO

A AC Safeweb Timestamping realiza a confirmação da identidade de uma pessoa jurídica mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos à sua habilitação jurídica:

I - Se pessoa jurídica criada ou autorizada por lei:

1) Cópia do CNPJ.

II - Se entidade privada:

1) Certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e

2) Documentos da eleição de seus administradores, quando aplicável.

b) Relativos à sua habilitação fiscal:

I - Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou

II - Prova de inscrição no Cadastro Específico do INSS – CEI.

c) Relativos à habilitação técnica:

I - Deferimento da ACT no Diário Oficial da União;

II - Serial da Protocoladora.

Nota: Essas confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

3.2.2.3 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UMA ORGANIZAÇÃO

3.2.2.3.1 Não se aplica.

3.2.2.3.2 Não se aplica.

3.2.2.4 RESPONSABILIDADE DECORRENTE DO USO DO CERTIFICADO DE UMA ORGANIZAÇÃO

Não se aplica.

3.2.3 AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO

3.2.3.1 DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO

3.2.3.1.1 Não se aplica.

3.2.3.1.2 Não se aplica.

3.2.3.1.3 Não se aplica.

3.2.3.1.4 Não se aplica.

3.2.3.1.5 Não se aplica.

3.2.3.1.6 Não se aplica.

3.2.3.2 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO

Não se aplica.

3.2.4 INFORMAÇÕES NÃO VERIFICADAS DO TITULAR DO CERTIFICADO

Não se aplica.

3.2.5 VALIDAÇÃO DAS AUTORIDADES

Na emissão de certificado de ACT é verificado se a pessoa física é o representante legal da empresa.

3.2.6 CRITÉRIOS PARA INTEROPERAÇÃO

Não se aplica.

3.2.7 AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO OU APLICAÇÃO

3.2.7.1 DISPOSIÇÕES GERAIS

3.2.7.1.1 Em se tratando de certificado emitido para equipamento ou aplicação, o titular será a pessoa jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

3.2.7.1.2 Não se aplica.

3.2.7.1.3 Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) Apresentação do rol de documentos elencados no item 3.2.2.2;

b) Apresentação de RG, CPF ou CNH do responsável pelo certificado;

c) Presença física do responsável pelo certificado; e

d) Assinatura do termo de titularidade de que trata o item 4.1 pelo responsável pelo certificado.

3.2.7.1.4 Não se aplica.

3.2.7.1.5 Não se aplica.

3.2.7.2 PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO OU APLICAÇÃO

3.2.7.2.1 Não se aplica.

3.2.7.2.2 Para emissão de certificados do tipo T3 ou T4, para equipamentos de ACT credenciadas na ICP-Brasil, a solicitação deve conter: o nome de servidor e o número de série do equipamento. Esses dados devem ser validados comparando-os com aqueles publicados pelo ITI no Diário Oficial da União, quando do deferimento do credenciamento da ACT.

3.2.7.3 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO OU APLICAÇÃO

3.2.7.3.1 É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nos documentos apresentados:

a) URL ou nome da aplicação[1];

b) nome completo do responsável pelo certificado, sem abreviações[2];

[1] No campo *Subject*, como parte do *Common Name*, que compõe o *Distinguished Name*
[2] No campo *Subject Alternative Name*, OID 2.16.76.1.3.2

c) data de nascimento do responsável pelo certificado[3];

d) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações[4], se o titular for pessoa jurídica;

e) Cadastro Nacional de Pessoa Jurídica (CNPJ)[5];

f) Número serial da protocoladora.

3.2.7.3.2 Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.2.3.2.

3.2.7.4 AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTO PARA CERTIFICADO CF-E-SAT

Não se aplica.

3.2.7.5 PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO SAT

Não se aplica.

3.2.7.6 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO SAT

Não se aplica.

3.2.7.7 AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTOS PARA CERTIFICADO OM-BR

Não se aplica.

3.2.7.8 PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO METROLÓGICO

Não se aplica.

3.2.7.9 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO METROLÓGICO

Não se aplica.

[3] No campo *Subject Alternative Name*, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.4
[4] No campo *Subject Alternative Name*, OID 2.16.76.1.3.8
[5] No campo *Subject Alternative Name*, OID 2.16.76.1.3.3

3.2.8 PROCEDIMENTOS COMPLEMENTARES

3.2.8.1 A AC Safeweb Timestamping mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos *Webtrust Principles and Criteria for Certification Authorities* [15], disponível no endereço *Webtrust CA*.

3.2.8.2 Todo o processo de identificação do titular do certificado deve ser registrado com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. O sistema biométrico da ICP-BRASIL deve solicitar aleatoriamente qual dedo o AGR deve apresentar para autenticação, o que exige a inclusão de todos os dedos dos AGR no cadastro do sistema biométrico. Tais registros devem ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.2.8.3 Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

3.2.8.3.1 Não se aplica.

3.2.8.4 A AC Safeweb Timestamping disponibiliza para todas as AR vinculadas na sua cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital, conforme estabelecido no DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

3.2.8.4.1 Na hipótese de identificação positiva no processo biométrico da ICP-Brasil, fica dispensada a apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação conforme item 3.2.3.1.

3.2.9 PROCEDIMENTOS ESPECÍFICOS

3.2.9.1 Não se aplica.

3.2.9.2 Não se aplica.

3.2.9.3 Não se aplica.

3.2.9.4 Não se aplica.

3.2.9.5 Não se aplica.

3.2.9.6 Não se aplica.

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

3.3.1 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA ROTINA DE NOVAS CHAVES ANTES DA EXPIRAÇÃO

3.3.1.1 Esta DPC estabelece os processos de identificação do solicitante utilizados pela AC Safeweb Timestamping para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

3.3.1.2 Esse processo é conduzido através da adoção dos mesmos requisitos e procedimentos exigidos no item 3.2.7.

3.3.1.2.1 Não se aplica.

3.3.1.3 Caso sejam requeridos procedimentos específicos para as PC implementadas, os mesmos devem ser descritos nessas PC, no item correspondente.

3.3.2 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA NOVAS CHAVES APÓS A REVOGAÇÃO

3.3.2.1 Após a revogação ou expiração do certificado, o solicitante pode solicitar um novo certificado, enviando à AR vinculada uma solicitação, na forma, condições e prazo estabelecidos para a solicitação inicial de um certificado.

3.3.2.2 Não se aplica.

3.3.2.3 Não se aplica.

3.3.2.4 Não se aplica.

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

3.4.1 A solicitação de revogação de certificado é realizada através de formulário específico ou página *web*, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita através da confrontação de dados fornecidos no momento da solicitação de revogação, com os dados previamente cadastrados na AR. O item 4.9.2 desta DPC descreve quem pode solicitar a revogação de um certificado.

3.4.2 Os procedimentos para solicitação de revogação de certificado estão descritos no item 4.9.3 desta DPC.

3.4.3 As solicitações de revogação de certificados são registradas.

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 SOLICITAÇÃO DE CERTIFICADO

A solicitação de emissão de um certificado digital é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR Safeweb. Toda referência a formulário deverá ser

entendida também como referência a outras formas que a AR Safeweb possa vir a adotar. Dentre os requisitos e procedimentos operacionais estabelecidos pela AC Safeweb Timestamping para as solicitações de emissão de certificado, estão:

a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.2;

b) O uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado do tipo A3;

c) Um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico.

Nota: na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados SSL, de equipamento, aplicação, *codesign*, carimbo de tempo e outros que façam uso de CSR) será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo uso do certificado, no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo será necessária a verificação da assinatura contra o documento de identificação.

4.1.1 QUEM PODE SUBMETER UMA SOLICITAÇÃO DE CERTIFICADO

A submissão da solicitação é por intermédio da AR.

4.1.1.1 Não se aplica.

4.1.1.2 A solicitação de certificado para equipamento de carimbo do tempo de Autoridade de Carimbo do Tempo (ACT) credenciada na ICP-Brasil somente será possível após a notificação do deferimento do credenciamento, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.1.3 Não se aplica.

4.1.1.4 Não se aplica.

4.1.2 PROCESSO DE REGISTRO E RESPONSABILIDADES

Nos itens a seguir são descritas as obrigações gerais das entidades envolvidas. As obrigações específicas, quando aplicáveis, estão descritas nas PCs implementadas.

4.1.2.1 Responsabilidades da AC

4.1.2.1.1 A AC Safeweb Timestamping responde pelos danos a que der causa.

4.1.2.1.2 A AC Safeweb Timestamping responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

4.1.2.1.3 Não se aplica.

4.1.2.2 Obrigações da AC

a) operar de acordo com a sua DPC e com as PCs que implementa;

b) gerar e gerenciar os seus pares de chaves criptográficas;

c) assegurar a proteção de suas chaves privadas;

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

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

f) distribuir o seu próprio certificado;

g) emitir, expedir e distribuir os certificados de ACT;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas LCRs;

k) publicar em sua página web sua DPC e as PCs aprovadas que implementa;

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

m) publicar, em página web, informações sobre o descredenciamento de AR;

n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;

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

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

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

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

s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;

t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;

u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;

v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;

w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;

x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada às ACs que utilizam de seus serviços; e

y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados.

4.1.2.3 Responsabilidades da Autoridade de Registro

A AR será responsável pelos danos a que der causa.

4.1.2.4 Obrigações das Autoridades de Registro

As ARs vinculadas à AC Safeweb Timestamping têm as seguintes obrigações:

a) receber solicitações de emissão ou de revogação de certificados;

b) confirmar a identidade do solicitante e a validade da solicitação;

c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC responsável, utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1];

d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;

e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em

especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1], bem como Princípios e Critérios *WebTrust* para AR [14];

f) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;

g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma do item 3.2.7; e

h) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios *WebTrust* para AR [14].

4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1 EXECUÇÃO DAS FUNÇÕES DE IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC e AR executam as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2 APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO

4.2.2.1 Não se aplica.

4.2.2.2 A AC Safeweb Timestamping e a AR a ela vinculada podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC.

4.2.3 TEMPO PARA PROCESSAR A SOLICITAÇÃO DE CERTIFICADO

A AC Safeweb Timestamping cumpre os procedimentos determinados na ICP-Brasil. Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3 EMISSÃO DE CERTIFICADO

4.3.1 AÇÕES DA AC SAFEWEB TIMESTAMPING DURANTE A EMISSÃO DE UM CERTIFICADO

4.3.1.1 Depois da validação da solicitação do certificado, de que trata o item 3.2, a AC Safeweb Timestamping procede à emissão do certificado. O certificado emitido é inserido na relação de certificados emitidos pela AC Safeweb Timestamping.

4.3.1.2 Certificados são considerados válidos a partir do momento de sua emissão.

4.3.2 NOTIFICAÇÕES PARA O TITULAR DO CERTIFICADO PELA AC SAFEWEB TIMESTAMPING NA EMISSÃO DO CERTIFICADO

A notificação de emissão é feita através da assinatura dos seguintes documentos:

a) Termo de Cerimônia de Geração de Chaves;
b) Formulário de Solicitação de Emissão de Certificado;
c) Termo de Titularidade de Certificado;
d) Termo de Cerimônia de Emissão de Certificado; e
e) Termo de Acordo (no qual a ACT titular atesta ter recebido o seu certificado).

4.4 ACEITAÇÃO DO CERTIFICADO

4.4.1 CONDUTA SOBRE A ACEITAÇÃO DO CERTIFICADO

4.4.1.1 O titular do certificado ou pessoa física responsável verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

a) concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;

b) garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4.1.2 A aceitação de todo certificado emitido é declarada pelo respectivo titular.

4.4.1.3 A aceitação do certificado de uma ACT titular é declarada por seu responsável através da assinatura do Termo de Acordo de ACT.

4.4.2 PUBLICAÇÃO DO CERTIFICADO PELA AC

O certificado da AC Safeweb Timestamping é publicado de acordo com item 2.2 desta DPC.

4.4.3 NOTIFICAÇÃO DE EMISSÃO DO CERTIFICADO PELA AC RAIZ PARA OUTRAS ENTIDADES

A notificação se dará de acordo com item 2.2 da DPC da AC Raiz.

4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

O titular do certificado deve operar de acordo com essa Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) implementadas, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

4.5.1 USABILIDADE DA CHAVE PRIVADA E DO CERTIFICADO DO TITULAR

4.5.1.1 A AC Safeweb Timestamping utiliza sua chave privada e garante a proteção dessa chave conforme o previsto nesta DPC.

4.5.1.2 Obrigações do Titular do Certificado:

As obrigações dos titulares de certificados emitidos pela AC Safeweb Timestamping, constantes dos termos de titularidade de que trata o item 4.1, são as seguintes:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;

b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;

d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e

e) informar à AC Safeweb Timestamping qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Nota: Em se tratando de certificado emitido para equipamento estas obrigações se aplicam ao responsável pelo uso do certificado.

4.5.2 USABILIDADE DA CHAVE PÚBLICA E DO CERTIFICADO DAS PARTES CONFIÁVEIS

Em acordo com o item 9.6.4 desta DPC.

4.6. RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPC.

4.6.1 CIRCUNSTÂNCIAS PARA RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPC.

4.6.2 QUEM PODE SOLICITAR A RENOVAÇÃO

Em acordo com item 3.3 desta DPC.

4.6.3 PROCESSAMENTO DE REQUISIÇÃO PARA RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPC.

4.6.4 NOTIFICAÇÃO PARA NOVA EMISSÃO DE CERTIFICADO PARA O TITULAR

Em acordo com item 3.3 desta DPC.

4.6.5 CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO

Em acordo com item 3.3 desta DPC.

4.6.6 PUBLICAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO PELA AC

Não se aplica.

4.6.7 NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO PELA AC SAFEWEB TIMESTAMPING PARA OUTRAS ENTIDADES

Em acordo com item 4.3 desta DPC.

4.7 NOVA CHAVE DE CERTIFICADO (RE-KEY)

4.7.1 CIRCUNSTÂNCIAS PARA NOVA CHAVE DE CERTIFICADO

Não se aplica.

4.7.2 QUEM PODE REQUISITAR A CERTIFICAÇÃO DE UMA NOVA CHAVE PÚBLICA

Não se aplica.

4.7.3 PROCESSAMENTO DE REQUISIÇÃO DE NOVAS CHAVES DE CERTIFICADO

Não se aplica.

4.7.4 NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR

Não se aplica.

4.7.5 CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA NOVA CHAVE CERTIFICADA

Não se aplica.

4.7.6 PUBLICAÇÃO DE UMA NOVA CHAVE CERTIFICADA PELA AC

Não se aplica.

4.7.7 NOTIFICAÇÃO DE UMA EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES

Não se aplica.

4.8 MODIFICAÇÃO DE CERTIFICADO

4.8.1 CIRCUNSTÂNCIAS PARA MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.2 QUEM PODE REQUISITAR A MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.3 PROCESSAMENTO DE REQUISIÇÃO DE MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.4 NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR

Não se aplica.

4.8.5 CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.6 PUBLICAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO PELA AC

Não se aplica.

4.8.7 NOTIFICAÇÃO DE UMA EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES

Não se aplica.

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.9.1 CIRCUNSTÂNCIAS PARA REVOGAÇÃO

4.9.1.1 Um certificado poderá ser revogado a qualquer tempo, independentemente de qualquer circunstância, desde que respeitadas as regras da ICP-Brasil.

4.9.1.2 Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;

b) Quando for necessária a alteração de qualquer informação constante no mesmo;

c) Não se aplica; ou

d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3 Deve-se observar ainda que:

a) A AC Safeweb Timestamping revogará, no prazo definido no item 4.9.3.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil;

b) O CG da ICP-Brasil ou AC Raiz determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.9.1.4 Todo certificado tem a sua validade verificada, na respectiva LCR, antes de ser utilizado.

4.9.1.4.1 Não se aplica.

4.9.1.4.2 Não se aplica.

4.9.1.5 A autenticidade da LCR é confirmada por meio das verificações da assinatura da AC Safeweb Timestamping e do período de validade da LCR.

4.9.2 QUEM PODE SOLICITAR A REVOGAÇÃO

A revogação de um certificado somente pode ser feita:

a) Por solicitação do titular do certificado;

b) Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos e pessoas jurídicas;

c) Não se aplica;

d) Pela AC Safeweb Timestamping;

e) Por uma AR vinculada;

f) Por determinação da AC Safeweb, do CG da ICP-Brasil ou da AC Raiz;

g) Não se aplica;

h) Não se aplica;

i) Não se aplica.

4.9.3 PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.9.3.1 A solicitação de revogação do certificado à AC Safeweb Timestamping deve ser efetivada pelo preenchimento do Formulário de Solicitação de Revogação de Certificado. Esse formulário deverá ser assinado por seu representante legal. Quando utilizada a versão eletrônica do formulário, ele deve ser assinado digitalmente e enviado à AC Safeweb Timestamping. O formulário pode também ser preenchido e assinado em papel e entregue pessoalmente pelo representante à AC Safeweb Timestamping.

4.9.3.2 Como diretrizes gerais:

a) O solicitante da revogação de um certificado é identificado;

b) As solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas pela AC Safeweb Timestamping;

c) As justificativas para a revogação de um certificado são documentadas;

d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado.

4.9.3.3 O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 24 (vinte e quatro) horas.

4.9.3.4 Não se aplica.

4.9.3.5 A AC Safeweb Timestamping responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

4.9.3.6 Não se aplica.

4.9.4 PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.9.4.1 A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.1 desta DPC. O prazo máximo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa pela AC Safeweb Timestamping é de 3 (três) dias.

4.9.4.2 Não se aplica.

4.9.5 TEMPO EM QUE A AC SAFEWEB TIMESTAMPING DEVE PROCESSAR O PEDIDO DE REVOGAÇÃO

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC Safeweb Timestamping deve processar a revogação imediatamente após a análise do pedido.

4.9.6 REQUISITOS DE VERIFICAÇÃO DE REVOGAÇÃO PARA AS PARTES CONFIÁVEIS

Antes de confiar em um certificado, a parte confiável deve confirmar a validade de cada certificado na cadeia de certificação de acordo com os padrões IETF PKIX, incluindo a verificação da validade do certificado, encadeamento do nome do emissor e titular, restrições de uso de chaves e de políticas de certificação e o status de revogação por meio de LCRs identificados em cada certificado na cadeia de certificação.

4.9.7 FREQUÊNCIA DE EMISSÃO DE LCR

4.9.7.1 A frequência de emissão da LCR da AC Safeweb Timestamping referente a certificados de usuários finais é de 1 (uma) hora.

4.9.7.2 A frequência máxima admitida para a emissão de LCR para os certificados de usuários finais é de 6 (seis) horas.

4.9.7.3 Não se aplica.

4.9.7.4 Não se aplica.

4.9.7.5 Não se aplica.

4.9.8 LATÊNCIA MÁXIMA PARA A LCR

A LCR é divulgada no repositório em no máximo 4 (quatro) horas após sua geração.

4.9.9 DISPONIBILIDADE PARA REVOGAÇÃO/VERIFICAÇÃO DE STATUS ON-LINE

O processo de revogação *on-line* está disponível ao titular do certificado, conforme descrito no item 4.9.3.

4.9.10 REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO ON-LINE

Não se aplica.

4.9.11 OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

Não se aplica.

4.9.12 REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE

4.9.12.1 Havendo roubo, perda, modificação, acesso indevido ou qualquer forma de comprometimento da chave privada ou de sua mídia, o titular do certificado deve comunicar imediatamente a AC Safeweb Timestamping, de maneira escrita, solicitando a revogação de seu certificado.

4.9.12.2 O comprometimento ou suspeita de comprometimento de chave deve ser comunicado à AC Safeweb Timestamping através do formulário específico para tal fim, devidamente assinado, cujo objetivo é manter os procedimentos para resguardar o sigilo da informação.

4.9.13 CIRCUNSTÂNCIAS PARA SUSPENSÃO

Não se aplica.

4.9.14 QUEM PODE SOLICITAR SUSPENSÃO

Não se aplica.

4.9.15 PROCEDIMENTO PARA SOLICITAÇÃO DE SUSPENSÃO

Não se aplica.

4.9.16 LIMITES NO PERÍODO DE SUSPENSÃO

Não se aplica.

4.10 SERVIÇOS DE STATUS DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONAIS

A AC Safeweb Timestamping fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados, conforme item 4.9.

4.10.2 DISPONIBILIDADE DOS SERVIÇOS

Ver item 4.9.

4.10.3 FUNCIONALIDADES OPERACIONAIS

Ver item 4.9.

4.11 ENCERRAMENTO DE ATIVIDADES

4.11.1 Em caso de extinção da AC Safeweb Timestamping, serão adotados os procedimentos previstos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.11.2 Quando for necessário encerrar as atividades da AC Safeweb Timestamping ou da AR vinculada, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes, inclusive:

a) Notificar a AC Raiz da ICP-Brasil;

b) Extinguir a emissão, revogação e publicação de LCR após a revogação de todos os certificados emitidos;

c) Providenciar a transferência de chaves públicas, dos certificados e respectiva documentação para serem armazenados por outra AC, após aprovação da AC Raiz;

d) Transferir progressivamente o serviço e os registros operacionais para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC Safeweb Timestamping e ARs vinculadas;

e) Preservar qualquer registro não transferido a um sucessor;

f) Transferir, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas;

g) Repassar à AC Raiz os documentos referentes aos certificados digitais e as respectivas chaves públicas, caso essas não sejam assumidas por outra AC; e

h) Comunicar os usuários sobre a extinção dos serviços através de publicação em jornal de grande circulação.

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE

4.12.1 POLÍTICA E PRÁTICAS DE CUSTÓDIA E RECUPERAÇÃO DE CHAVE

A AC Safeweb Timestamping não executa práticas de custódia e recuperação de chaves.

4.12.2 POLÍTICA E PRÁTICAS DE ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVE DE SESSÃO

Não se aplica.

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Os controles descritos a seguir são implementados pela AC Safeweb Timestamping para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 CONTROLES FÍSICOS

Nos itens seguintes estão descritos os controles físicos referentes às instalações que abrigam os sistemas da AC Safeweb Timestamping e instalações das ARs vinculadas.

5.1.1 CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES DE AC

5.1.1.1 A localização e o sistema de certificação AC Safeweb Timestamping não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não são admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2 Na construção das instalações da AC Safeweb Timestamping foram considerados, entre outros, os seguintes aspectos relevantes para os controles de segurança física:

a) As instalações para equipamentos de apoio, tais como máquinas de ar condicionado, *nobreaks*, baterias, subestações, retificadores, estabilizadores e similares ficam em ambiente seguro, com entrada e saída controlada através de câmeras de monitoramento;

b) As instalações para sistemas de telecomunicações, quadros de distribuição de energia e de telefonia ficam em ambiente de nível 3 (três);

c) Existem sistemas de aterramento e de proteção contra descargas atmosféricas;

d) Existe iluminação de emergência em todos os níveis e áreas cobertas por câmeras de monitoramento.

5.1.2 ACESSO FÍSICO

A AC Safeweb Timestamping inseriu um sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a Política de Segurança implementada e os requisitos que seguem:

5.1.2.1 NÍVEIS DE ACESSO

5.1.2.1.1 A AC Safeweb Timestamping definiu 4 (quatro) níveis de acesso físico aos seus diversos ambientes e 2 (dois) níveis relativos à proteção da chave privada da AC Safeweb Timestamping.

5.1.2.1.2 O primeiro nível - ou nível 1 (um) - situa-se após a primeira barreira de acesso às instalações da AC Safeweb Timestamping. Para entrar em uma área de nível 1 (um), cada indivíduo deve ser identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação da AC devem transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC é executado nesse nível.

5.1.2.1.3 Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC Safeweb Timestamping, a partir do nível 1 (um). A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4 O segundo nível (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 AC. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá.

5.1.2.1.5 O terceiro nível (nível 3) situa-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC Safeweb Timestamping. Qualquer atividade relativa ao ciclo de vida dos certificados digitais é executada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6 No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: identificação individual por meio de senha e identificação biométrica.

5.1.2.1.7 Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC Safeweb Timestamping, não são admitidos a partir do nível 3 (três).

5.1.2.1.8 No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC tais como emissão e revogação de certificados, e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível, inclusive o sistema de AR. O nível 4 (quatro) possui os mesmos controles de acesso do nível 3 (três) e, adicionalmente, exige, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência no mínimo de duas pessoas autorizadas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9 No quarto nível todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física da área de quarto nível. Adicionalmente, esse ambiente de nível 4 possui proteção contra

interferência eletromagnética externa.

5.1.2.1.10 As salas-cofre do site principal e de contingência, foram construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas foram sanadas por normas internacionais pertinentes.

5.1.2.1.11 Na AC Safeweb Timestamping há 1 (um) ambiente de quarto nível para abrigar:

a) Equipamentos de produção *on-line* e cofre de armazenamento;

b) Equipamentos de produção *off-line* e cofre de armazenamento;

c) Equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

5.1.2.1.12 O quinto nível (nível 5), interior ao ambiente de nível 4 (quatro), compreende um cofre que armazena:

a) *Backups* das chaves criptográficas da AC Safeweb Timestamping;

b) Dados de ativação destas chaves; e

c) Documentos necessários para a ativação da contingência do ambiente, caso necessário.

5.1.2.1.13 Para garantir a segurança do material armazenado, o cofre obedece às seguintes especificações mínimas:

a) É feito em aço;

b) Possui tranca com chave e segredo.

5.1.2.1.14 O sexto nível (nível 6), consiste em pequenas caixas de aço localizadas no interior do cofre de quinto nível. Cada uma dessas caixas dispõe de uma fechadura individual. Os dados de ativação da chave privada da AC Safeweb Timestamping são armazenados nessas caixas.

5.1.2.2 SISTEMAS FÍSICOS DE DETECÇÃO

5.1.2.2.1 Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmeras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2 Os arquivos de imagens resultantes da gravação 24x7 são armazenadas por, no mínimo, 7 (sete) anos. Essas gravações são testadas (verificação de trechos aleatórios) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, um arquivo referente a cada semana. Essas gravações são armazenadas em ambiente de quarto nível.

5.1.2.2.3 Todas as portas de passagem entre os níveis de acesso 3 (três) e 4 (quatro) do ambiente são monitoradas por sistema de notificação de alarmes. A partir do nível 2 (dois), vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados ininterruptamente.

5.1.2.2.4 Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não é satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais empregados, o critério mínimo de ocupação deixa de ser satisfeito, ocorre a reativação automática dos sensores de presença.

5.1.2.2.5 O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

5.1.2.2.6 O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, é permanentemente monitorado, e estão localizados em ambiente de nível 3 (três). As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações.

5.1.2.3 SISTEMA DE CONTROLE DE ACESSO

O sistema de controle de acesso está baseado no ambiente de nível 4 (quatro).

5.1.2.4 MECANISMO DE EMERGÊNCIA

5.1.2.4.1 Mecanismos específicos foram implantados pela AC Safeweb Timestamping 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.

5.1.2.4.2 Todos os procedimentos referentes aos mecanismos de emergência são documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

5.1.3 ENERGIA E AR CONDICIONADO

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

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

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

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

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

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

5.1.3.7 O sistema de climatização atende os requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. No ambiente de nível 4 (quatro), o sistema de climatização é independente e tolerante a falhas.

5.1.3.8 A temperatura do ambiente de nível 4 (quatro) atendido pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9 O sistema de ar condicionado é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.10 A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC Safeweb Timestamping é garantida, por meio de:

a) Geradores de porte compatível;

b) Geradores de reserva;

c) Sistemas de *nobreaks* redundantes;

d) Sistemas redundantes de ar condicionado.

5.1.4 EXPOSIÇÃO À ÁGUA

A estrutura inteiriça do ambiente de nível 4 (quatro), construído na forma de célula estanque, provê proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5 PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO

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

5.1.5.2 Nas instalações da AC Safeweb Timestamping não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3 A sala-cofre de nível 4 (quatro) possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre constituem eclusas, onde uma porta só se abre quando a anterior estiver fechada.

5.1.5.4 Em caso de incêndio nas instalações da AC Safeweb Timestamping, o aumento da temperatura interna da sala-cofre de nível 4 (quatro) não excede 50 (cinquenta) graus Celsius, e a sala suporta esta condição por, no mínimo, 1 (uma) hora.

5.1.6 ARMAZENAMENTO DE MÍDIA

São observados os critérios estabelecidos na norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7 DESTRUIÇÃO DE LIXO

5.1.7.1 Todos os documentos em papel que contém 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 INSTALAÇÕES DE SEGURANÇA *(BACKUP)* EXTERNAS *(OFF-SITE)* PARA AC

As instalações de *backup* atendem os requisitos mínimos estabelecidos por este documento. Sua localização é tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de *backup* não serão atingidas e tornar-se-ão totalmente operacionais em condições idênticas em, no máximo, 48 (quarenta e oito) horas.

5.2 CONTROLES PROCEDIMENTAIS

Nos itens seguintes da DPC estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC Safeweb Timestamping e nas ARs a ela vinculadas, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, foi estabelecido o número de pessoas requerido para sua execução.

5.2.1 PERFIS QUALIFICADOS

5.2.1.1 A AC Safeweb Timestamping efetua separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize o seu sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.2.1.2 A AC Safeweb Timestamping estabelece 21 (vinte e um) perfis distintos, agrupados em 6 (seis) equipes, para manter o princípio de segregação de tarefas na sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. As responsabilidades e níveis de acesso

estão descritas em documentação interna. As equipes e os perfis estabelecidos são:

a) GERÊNCIA

a.1) Gerente da AC

b) COMPLIANCE

b.1) Coordenador de compliance

b.2) Operador de compliance

c) SISTEMAS

c.1) Coordenador de sistemas

c.2) Administrador de sistemas

c.3) Desenvolvedor de sistemas

d) INFRAESTRUTURA

d.1) Coordenador de infraestrutura

d.2) Administrador de domínio

d.3) Administrador de infraestrutura

d.4) Administrador de rede

d.5) Administrador de banco de dados

d.6) Administrador de backup

d.7) Operador de infraestrutura

e) OPERACIONAL

e.1) Coordenador operacional

e.2) Detentor de chaves de HSM

e.3) Detentor de chaves do SCT – Carimbo do Tempo

e.4) Operador de recursos humanos

e.5) Operador de serviços

e.6) Vigilante

f) SEGURANÇA DA INFORMAÇÃO

f.1) Coordenador de segurança da informação

f.2) Auditor interno

5.2.1.3 Todos os operadores do sistema de certificação da AC Safeweb Timestamping 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.

5.2.1.3.1 Não se aplica.

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

5.2.2 NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA

5.2.2.1 A AC Safeweb Timestamping utiliza o requisito de controle multiusuário para a geração e a utilização da sua chave privada, na forma definida no item 6.2.2.

5.2.2.2 Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Safeweb Timestamping requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC Safeweb Timestamping podem ser executadas por um único empregado.

5.2.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

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

a) Ser incluído em uma lista de acesso às instalações da AC Safeweb Timestamping;

b) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC Safeweb Timestamping;

c) Receber um certificado para executar suas atividades operacionais na AC Safeweb Timestamping;

d) Receber uma conta no sistema de certificação da AC Safeweb Timestamping.

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

a) São diretamente atribuídos a um único empregado;

b) Não são compartilhados; e

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

5.2.3.3 AC Safeweb Timestamping implementa um padrão de utilização de "senhas fortes", definido na Política de Segurança implementada e em conformidade com a POLÍTICA DE

SEGURANÇA DA ICP-BRASIL [8], juntamente com procedimentos de validação dessas senhas.

5.2.4 FUNÇÕES QUE REQUEREM SEPARAÇÃO DE DEVERES

A AC Safeweb Timestamping impõe a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3 CONTROLES DE PESSOAL

Nos itens seguintes desta DPC são descritos os requisitos e procedimentos, implementados pela AC Safeweb Timestamping, pelas ARs e PSS vinculado em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Todos os empregados da AC Safeweb Timestamping e das ARs vinculadas e PSS vinculado, encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

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

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

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

5.3.1 ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE

Todo o pessoal da AC Safeweb Timestamping e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e na Política de Segurança (PS) implementada pela AC.

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 AC Safeweb Timestamping e da ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido a:

a) Verificação de antecedentes criminais;

b) Verificação de situação de crédito;

c) Verificação de histórico de empregos anteriores;

d) Comprovação de escolaridade e de residência.

5.3.2.2 A AC Safeweb Timestamping não define requisitos adicionais para a verificação de antecedentes.

5.3.3 REQUISITOS DE TREINAMENTO

Todo o pessoal da AC Safeweb Timestamping e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e mecanismos de segurança da AC Safeweb Timestamping e das ARs vinculadas;

b) Sistema de certificação em uso na AC Safeweb Timestamping;

c) Procedimentos de recuperação de desastres e de continuidade do negócio;

d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.2.7; e

e) Outros assuntos relativos às atividades sob sua responsabilidade.

5.3.4 FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA

Todo o pessoal da AC Safeweb Timestamping e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC Safeweb Timestamping e das ARs vinculadas.

5.3.5 FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

A AC Safeweb Timestamping e as ARs vinculadas possuem pessoal e efetivo de contingência, devidamente treinados, não fazendo uso de rodízio de pessoal.

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 AC Safeweb Timestamping e das ARs vinculadas, a AC ou a AR suspenderá o acesso dessa pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2 O processo administrativo referido acima contém 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 AC Safeweb Timestamping encaminha suas conclusões à AC Safeweb.

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

a) Advertência;

b) Suspensão por prazo determinado; ou

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

5.3.7 REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

Todo o pessoal da AC Safeweb Timestamping e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e na Política de Segurança (PS) implementada pela AC Safeweb Timestamping.

5.3.8 DOCUMENTAÇÃO FORNECIDA AO PESSOAL

5.3.8.1 A AC Safeweb Timestamping torna disponível para todo o seu pessoal e para o pessoal das ARs vinculadas:

a) A DPC da AC Safeweb Timestamping;

b) As PCs que implementa;

c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e a sua PS;

d) Documentação operacional relativa às suas atividades; e

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

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

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA

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

5.4.1 TIPOS DE EVENTOS REGISTRADOS

5.4.1.1 A AC Safeweb Timestamping registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente inclusos em arquivos de auditoria:

a) Iniciação e desligamento do sistema de certificação;

b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC;

c) Mudanças na configuração da AC ou nas suas chaves;

d) Mudanças nas políticas de criação de certificados;

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 da AC ou de chaves de seus usuários finais;

h) Emissão e revogação de certificados;

i) Geração de LCR;

j) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;

k) Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e

l) Operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1 Não se aplica.

5.4.1.2 A AC Safeweb Timestamping registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

a) Registros de acessos físicos;

b) Manutenção e mudanças na configuração de seus sistemas;

c) Mudanças de pessoal e de perfis qualificados;

d) Relatórios de discrepância e comprometimento; e

e) Registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

5.4.1.3 A AC Safeweb Timestamping não registra outras informações.

5.4.1.4 Os registros de auditoria, eletrônicos ou manuais, contém a data e a hora do evento registrado e a identidade do agente que o causou.

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

AC Safeweb Timestamping é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.1.6 A AC Safeweb Timestamping registra eletronicamente, em arquivos de auditoria, todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos estão obrigatoriamente inclusos em arquivos de auditoria:

a) Os agentes de registro que realizaram as operações;

b) Data e hora das operações;

c) A associação entre os agentes que realizaram a validação e aprovação e o certificado gerado; e

d) A assinatura digital do executante.

5.4.1.7 A AC Safeweb Timestamping define, em documento disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

5.4.2 FREQUÊNCIA DE AUDITORIA DE REGISTROS

AC Safeweb Timestamping examina os registros de auditoria uma vez por semana. Todos os eventos significativos são analisados e explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3 PERÍODO DE RETENÇÃO PARA REGISTROS DE AUDITORIA

A AC Safeweb Timestamping mantém localmente seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena os seus registros de auditoria 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 previamente autorizadas pelo administrador do sistema, de acordo com o perfil do usuário. Os acessos lógicos aos registros de eventos de auditoria são registrados em *logs* do próprio sistema operacional.

5.4.4.2 Informações manuais de auditoria também são protegidos contra a leitura não autorizada, modificação e remoção, através de controles de acesso aos ambientes físicos onde são

armazenados estes registros.

5.4.4.3 Os mecanismos de proteção obedecem ao item 9.2.3 da Política de Segurança implementada pela AC Safeweb Timestamping e a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.5 PROCEDIMENTO PARA CÓPIA DE SEGURANÇA *(BACKUP)* DE REGISTRO DE AUDITORIA

A AC Safeweb Timestamping gera a cada semana cópias de segurança *(backup)* de seus registros de auditoria, através de procedimentos utilizando conexão segura.

5.4.6 SISTEMA DE COLETA DE DADOS DE AUDITORIA

O sistema de coleta de dados de auditoria é interno à AC Safeweb Timestamping e é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

5.4.7 NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

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

5.4.8 AVALIAÇÕES DE VULNERABILIDADE

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

5.5 ARQUIVAMENTO DE REGISTROS

5.5.1 TIPOS DE EVENTOS REGISTRADOS

Os tipos de registros arquivados pela AC Safeweb Timestamping, são:

a) Solicitações de certificados;

b) Solicitações de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR;

f) Trocas de chaves criptográficas da AC Safeweb Timestamping; e

g) Informações de auditoria previstas no item 5.4.1.

5.5.2 PERÍODO DE RETENÇÃO PARA ARQUIVO

Os períodos de retenção para cada evento arquivado, são:

a) As LCRs e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;

b) Os dossiês dos titulares são retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e

c) As demais informações, inclusive os arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

5.5.3 PROTEÇÃO DE ARQUIVO

Os registros arquivados da AC Safeweb Timestamping são classificados e armazenados com requisitos de segurança compatíveis com essa classificação e com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.5.4 PROCEDIMENTOS DE CÓPIA DE ARQUIVO

5.5.4.1 A AC Safeweb Timestamping mantém uma cópia de todo o material arquivado no *site* Principal e uma segunda cópia deste material é armazenada no *site Backup*, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

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

5.5.5 REQUISITOS PARA DATAÇÃO DE REGISTROS

Os servidores estão sincronizados com a hora *Greenwich Mean Time* (GMT). Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT no formato DD/MM/AAAA HH:MM:SS, inclusive os certificados emitidos por esses equipamentos. No caso dos registros feitos manualmente e formulários de requisição de certificados, estes contêm a Hora Oficial do Brasil.

5.5.6 SISTEMA DE COLETA DE DADOS DE ARQUIVO (INTERNO E EXTERNO)

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Safeweb Timestamping em seus procedimentos operacionais são automatizados ou manuais e internos, e executados por seu pessoal operacional ou por seus sistemas.

5.5.7 PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO

A verificação de informação de arquivo deve ser solicitada formalmente à AC Safeweb Timestamping ou à AR vinculada, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado.

5.6 TROCA DE CHAVE

5.6.1 Trinta dias antes da data de expiração do certificado digital, a AR vinculada comunica ao seu titular, através do e-mail cadastrado no formulário de solicitação de certificado, a data de expiração do certificado, junto com link para a solicitação de novo certificado.

5.6.2 Não se aplica.

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

Nos itens seguintes da DPC são descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no PCN da AC Safeweb Timestamping, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], para garantir a continuidade dos seus serviços críticos.

5.7.1 PROCEDIMENTOS GERENCIAMENTO DE INCIDENTE E COMPROMETIMENTO

5.7.1.1 A AC Safeweb Timestamping possui um Plano de Continuidade do Negócio - PCN, de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. Possui ainda um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.

5.7.1.2 Os procedimentos descritos no Plano de Continuidade do Negócio (PCN) das ARs vinculadas contemplam a recuperação, total ou parcial das atividades das ARs, contendo, no mínimo as seguintes informações:

a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;

b) Identificação e concordância de todas as responsabilidades e procedimentos de emergência;

c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários;

d) Documentação dos processos e procedimentos acordados;

e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e

f) Teste e atualização dos planos.

5.7.2 RECURSOS COMPUTACIONAIS, SOFTWARE E/OU DADOS CORROMPIDOS

5.7.2.1 Os procedimentos de recuperação utilizados pela AC Safeweb Timestamping, quando recursos computacionais, softwares ou dados estiverem corrompidos ou houver suspeita de corrupção, incluem, mas não se limitam a somente estes:

I. A identificação da crise;

II. Acionamento dos principais gestores;

III. Ativação das equipes;

IV. Contenção da crise;

V. Estimativa do alargamento da crise;

VI. Declaração do início das atividades de ativação da situação de recuperação;

VII. Notificação da crise;

VIII. Registro da crise; e

IX. Crítica para melhoria.

5.7.2.2 Nas circunstâncias de crise relacionadas aos recursos computacionais, softwares e dados corrompidos ou quando houver suspeita de corrupção desses componentes, após a identificação da crise ou confirmação da suspeita de corrupção, são comunicados os gestores de certificação digital, que acionam as equipes, de forma a identificar o grau de corrupção.

5.7.2.3 Os métodos de recuperação dos recursos computacionais, softwares e dados corrompidos envolvem: identificação da necessidade de recurso computacional alternativo e, em caso de necessidade, disponibilização de outro recurso computacional equivalente, instalação dos softwares necessários e recuperação dos dados através do arquivo de *backup*, conforme detalhado em documentação interna.

5.7.3 PROCEDIMENTOS NO CASO DE COMPROMETIMENTO DE CHAVE PRIVADA DE ENTIDADE

5.7.3.1 Certificado de entidade é revogado

Em caso de revogação do certificado da AC Safeweb Timestamping, após a identificação do

imprevisto, são comunicados os gestores de certificação digital, que ativam as equipes envolvidas, de forma a indisponibilizar provisoriamente os serviços de autoridade certificadora. Na confirmação do imprevisto, são revogados os certificados dos usuários finais, é gerado um novo par de chaves, emitido pela AC Safeweb um novo certificado para a AC Safeweb Timestamping associado ao novo par de chaves gerado e emitidos novos certificados digitais para os usuários finais.

5.7.3.2 Chave de entidade é comprometida

Em caso de comprometimento da chave da AC Safeweb Timestamping, após a identificação da crise são notificados os gestores do processo de certificação digital, que ativam as equipes envolvidas, de forma a indisponibilizar provisoriamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da AC Safeweb Timestamping e dos usuários finais, é gerado um novo par de chaves, emitido pela AC Safeweb um novo certificado para a AC Safeweb Timestamping associado ao novo par de chaves gerado e emitidos novos certificados digitais para os usuários finais.

5.7.4 CAPACIDADE DE CONTINUIDADE DE NEGÓCIO APÓS DESASTRE

Em caso de desastre natural ou de outra natureza, depois da identificação da crise são comunicados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de exposição e comprometimento do ambiente. Na confirmação do desastre e constatada a impossibilidade de operação no site principal, as atividades são transferidas para o site de contingência.

5.8 EXTINÇÃO DA AC

Em caso de extinção da AC Safeweb Timestamping, serão adotados os procedimentos previstos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 GERAÇÃO DO PAR DE CHAVES

6.1.1.1 O par de chaves criptográficos da AC Safeweb Timestamping é gerado pela própria AC Safeweb Timestamping em módulo criptográfico de hardware, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil. A geração do par de chaves da AC Safeweb Timestamping é feita pelo seu representante legal ou

pessoa devidamente designada para este fim através de procuração. Este processo é realizado no ambiente de nível 4 na presença de múltiplas pessoas de confiança e treinados para esta função, seguindo procedimento formalizado e auditável. O par de chaves da AC Safeweb Timestamping é gerado em módulo criptográfico de hardware com certificação INMETRO no padrão obrigatório, conforme definido no DOC-ICP-01.01

6.1.1.2 Pares de chaves são gerados somente pelo titular do certificado correspondente. Os procedimentos específicos estão descritos em cada PC implementada pela AC Safeweb Timestamping.

6.1.1.3 Cada PC implementada pela AC Safeweb Timestamping define o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.1.4 O processo de geração do par de chaves da AC Safeweb Timestamping é feito por hardware.

6.1.1.5 Cada PC implementada pela AC Safeweb Timestamping caracteriza o processo utilizado para a geração de chaves criptográficas dos titulares de certificados, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.1.6 O módulo criptográfico utilizado para armazenamento da chave privada da AC Safeweb Timestamping possui certificação INMETRO, conforme indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR

A geração e guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3 ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

6.1.3.1 Para a entrega de sua chave pública à AC Safeweb, encarregada da emissão de seu certificado, a AC Safeweb Timestamping fará uso do padrão PKCS#10.

6.1.3.2 A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - *Secure Socket Layer*. Os procedimentos específicos aplicáveis são detalhados em cada PC implementada.

6.1.4 ENTREGA DE CHAVE PÚBLICA DA AC ÀS TERCEIRAS PARTES

A AC Safeweb Timestamping disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através dos endereços *web*:

a) Rep.1: http://repositorio.acsafeweb.com.br/ac-safewebts/ac-safewebts.p7b

b) Rep.2: http://repositorio2.acsafeweb.com.br/ac-safewebts/ac-safewebts.p7b

6.1.5 TAMANHOS DE CHAVE

6.1.5.1 Cada PC implementada pela AC Safeweb Timestamping define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.5.2 Não se aplica.

6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS E VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS

6.1.6.1 Os parâmetros de geração de chaves assimétricas da AC Safeweb Timestamping adotam o padrão obrigatório com certificação INMETRO - NSH-2, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.6.2 Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7 PROPÓSITO DE USO DE CHAVE (CONFORME O CAMPO "*KEY USAGE*" NA X.509 V3)

6.1.7.1 Os pares de chaves correspondentes aos certificados emitidos pela AC Safeweb Timestamping podem ser utilizados em aplicações mantidas por Autoridades de Carimbo do Tempo, credenciadas na ICP-Brasil, para assinatura de carimbos do tempo. Para isso, os certificados emitidos pela AC Safeweb Timestamping têm ativados os bits *digitalSignature, nonRepudiation* e *keyEncipherment*.

6.1.7.2 A chave privada da AC Safeweb Timestamping é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

6.2 PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

A AC Safeweb Timestamping implementa uma combinação de controles físicos (item 5.1.2), lógicos e procedimentais (item 5.2), de forma a garantir a segurança de suas chaves privadas. As chaves privadas da AC Safeweb Timestamping são armazenadas de forma cifrada nos mesmos componentes seguros de hardware utilizados para sua geração. O acesso a esses componentes é controlado por meio de chave criptográfica de ativação. Os titulares de certificados emitidos pela AC Safeweb Timestamping, são responsáveis pela guarda da chave privada e adotam as medidas

de prevenção de perda, divulgação, modificação ou uso desautorizado das suas chaves privadas.

6.2.1 PADRÕES PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1 O módulo criptográfico de geração de chaves assimétricas da AC Safeweb Timestamping adota o padrão obrigatório com certificação INMETRO - NSH-2, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2 O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas possui certificação INMETRO. Cada PC implementada especifica os requisitos aplicáveis à geração de chaves criptográficas dos titulares de certificado.

6.2.2 CONTROLE "N DE M" PARA CHAVE PRIVADA

6.2.2.1 Para a utilização das suas chaves privadas, a AC Safeweb Timestamping define a forma de controle múltiplo, do tipo “n” pessoas de um grupo de “m”.

6.2.2.2 A AC Safeweb Timestamping estabelece como exigência de controle múltiplo para a utilização das suas chaves privadas: 2 (dois) de um grupo de 5 (cinco) pessoas com perfis qualificados da AC Safeweb Timestamping, detentores de partição da chave de ativação do equipamento criptográfico para utilização das suas chaves privadas.

6.2.3 RECUPERAÇÃO *(ESCROW)* DE CHAVE PRIVADA

6.2.3.1 A AC Safeweb Timestamping não implementa a custódia e recuperação de chaves privadas.

6.2.4 CÓPIA DE SEGURANÇA *(BACKUP)* DE CHAVE PRIVADA

6.2.4.1 Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2 A AC Safeweb Timestamping mantém cópia de segurança de sua própria chave privada.

6.2.4.3 A AC Safeweb Timestamping não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.4 Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1 A AC Safeweb Timestamping não arquiva chaves privadas de titulares de certificados.

6.2.5.2 Define-se arquivamento como 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

A AC Safeweb Timestamping gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

6.2.7 ARMAZENAMENTO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Ver item 6.1.

6.2.8 MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

6.2.8.1 A ativação das chaves privadas das AC Safeweb Timestamping é coordenada pelo setor de Compliance, onde 2 (dois) de um grupo de 5 (cinco) pessoas com perfis qualificados da AC Safeweb Timestamping, detentores de partição da chave de ativação do equipamento criptográfico, utilizam tais componentes, juntamente com suas senhas em cerimônia específica. Essas pessoas são identificadas pelo crachá funcional emitido pela AC Safeweb Timestamping contendo fotografia, nome, e departamento do funcionário.

6.2.8.2 Cada PC implementada descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

6.2.9 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

6.2.9.1 A chave privada da AC Safeweb Timestamping, está instalada no ambiente de nível 4 (quatro), onde só é permitido o acesso em duplas devidamente autorizadas pelo sistema de controle de acesso da AC Safeweb Timestamping. Somente as pessoas qualificadas, após a sua devida identificação e autorização feita através de utilização de senhas, têm acesso ao sistema de certificação de produção, onde são executados os comandos de *logoff* no módudo criptográfico e desativando a chave privada da AC Safeweb Timestamping. Essas pessoas são identificadas pelo crachá funcional contendo fotografia, nome, e departamento do funcionário.

6.2.9.2 Cada PC implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.10 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

6.2.10.1 Para a destruição das chaves privadas da AC Safeweb Timestamping exige-se 2 (dois) de um grupo de 5 (cinco) pessoas com perfis qualificados. A confirmação da identidade dessas pessoas é feita através de crachás e senhas, só lhes sendo permitido o acesso ao ambiente em

duplas devidamente autorizadas. As mídias de armazenamento das chaves privadas originais e suas cópias de segurança são reinicializadas de forma a não restarem nelas informações sensíveis, conforme cerimônia específica realizada no ambiente de nível 4 (quatro).

6.2.10.2 Cada PC implementada descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA

As chaves públicas da AC Safeweb Timestamping e dos titulares dos certificados de assinatura digital por ela emitidos, bem como as LCR emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 PERÍODOS DE OPERAÇÃO DO CERTIFICADO E PERÍODOS DE USO PARA CHAVES PÚBLICA E PRIVADA

6.3.2.1 As chaves privadas da AC Safeweb Timestamping e dos titulares de certificados de assinatura digital por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas, bem como as LCRs emitidas pela AC Safeweb Timestamping são 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 Não se aplica.

6.3.2.3 Cada PC implementada pela AC Safeweb Timestamping define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.3.2.4 A validade admitida para certificados da AC Safeweb Timestamping é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4 DADOS DE ATIVAÇÃO

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

6.4.1.1 Os dados de ativação do equipamento de criptografia que armazena as chaves privadas da AC Safeweb Timestamping são únicos e aleatórios.

6.4.1.2 Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, são únicos e aleatórios.

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

6.4.2.1 A AC Safeweb Timestamping garante que os dados de ativação de sua chave privada são protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2 Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra o uso não autorizado.

6.4.3 OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO

Não se aplica.

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL

6.5.1.1 A geração do par de chaves da AC Safeweb Timestamping é realizada *off-line*, para impedir o acesso remoto não autorizado.

6.5.1.2 Nos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC Safeweb Timestamping, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, tais como:

a) Senha de BIOS ativada;

b) Controle de acesso lógico ao sistema operacional;

c) Exigência de uso de senhas fortes;

d) Diretivas de senha e de bloqueio de conta;

e) Antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;

f) Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;

g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc.);

h) Proteção de tela acionada no máximo após 02 (dois) minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.1.2.1 Os requisitos específicos aplicáveis devem ser descritos em cada PC implementada.

6.5.1.3 Cada computador servidor da AC Safeweb Timestamping, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

a) Controle de acesso aos serviços e perfis da AC Safeweb Timestamping;

b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC Safeweb Timestamping;

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 AC Safeweb Timestamping;

e) Mecanismos internos de segurança para garantir integridade de dados e processos críticos; e

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

6.5.1.4 Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.

6.5.1.5 Qualquer equipamento, ou parte deste, 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. Ao retornar às instalações da AC Safeweb Timestamping, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixa de ser utilizado em caráter permanente, serão destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC Safeweb Timestamping. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6 Qualquer equipamento incorporado à AC Safeweb Timestamping é preparado e configurado como previsto na Política de Segurança, ou em outro documento aplicável, implementada de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2 CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL

A segurança computacional da AC Safeweb Timestamping segue as recomendações *Common Criteria*.

6.5.3 CONTROLES DE SEGURANÇA PARA AS AUTORIDADES DE REGISTRO

6.5.3.1 A AC Safeweb Timestamping implementa requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pela AR Vinculada para os processos de validação e aprovação de certificados.

6.5.3.2 São incluídos os seguintes requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]:

6.5.3.2.1 A(s) partição(ões) dos discos rígidos das estações de trabalho da AR que contém componentes da aplicação da AC/AR ou que armazenem dados de solicitantes de certificados digitais são criptografadas.

6.5.3.2.2 As estações de trabalho da AR implementam aplicação que faz o controle de integridade das configurações da aplicação de AR, bem como dos arquivos de configuração ou informações críticas mantidas na estação de trabalho.

6.5.3.2.3 As estações de trabalho da AR contém apenas aplicações e serviços que são suficientes e necessários para as atividades corporativas.

6.5.3.2.4 As estações de trabalho da AR, incluindo equipamentos portáteis, estão protegidas contra ameaças e ações não-autorizadas, bem como contra o acesso, uso ou exposição indevidos e recebem as seguintes configurações de segurança:

a) Controle de acesso lógico ao sistema operacional;

b) Diretivas de senha e de bloqueio de conta;

c) Logs de auditoria do sistema operacional ativados, registrando:

i. Iniciação e desligamento do sistema;

ii. Tentativas de criar, remover, definir senhas ou mudar privilégios de usuários;

iii. Mudanças na configuração da estação;

iv. Tentativas de acesso (*login*) e de saída do sistema (*logoff*);

v. Tentativas não-autorizadas de acesso aos arquivos de sistema;

vi. Tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.

d) Antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;

e) *Firewall* pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por *firewall* corporativo, para equipamentos instalados em redes que possuam esse dispositivo;

f) Proteção de tela acionada no máximo após 02 (dois) minutos de inatividade;

g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc.);

h) Utilização apenas de *softwares* licenciados e necessários para a realização das atividades do Agente de Registro;

i) Impedimento de *login* remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;

j) Utilização de data e hora sincronizadas com o pool.ntp.br;

k) Equipamentos de coleta biométrica, em atendimento aos padrões da ICP-Brasil;

l) Equipamentos que exijam a identificação biométrica do agente de registro durante a identificação biométrica do requerente do certificado.

6.5.3.2.5 Os *logs* de auditoria do sistema operacional registram os acessos aos equipamentos e ficam armazenados localmente para avaliação pela auditoria operacional ou equipe de segurança.

6.5.3.2.6 A análise desses *logs* somente é realizada em caso de suspeitas quanto a acessos não autorizados ou para dirimir outros tipos de dúvidas que possam surgir sobre a utilização dos equipamentos.

6.5.3.2.7 O Agente de Registro não possui perfil de administrador ou senha de *root* dos equipamentos ou com privilégios especiais do sistema, ficando essa tarefa delegada a outros da própria organização, para permitir segregação de funções. O Agente de Registro recebe acesso somente aos serviços e aplicações que tenham sido especificamente autorizados a usar.

6.5.3.2.8 O aplicativo que faz interface entre a AR e o sistema de certificação da AC possui as seguintes características de segurança:

a) Acesso permitido somente mediante autenticação por meio do certificado do tipo A3 de Agente de Registro, formalmente autorizado por autoridade competente para ser cadastrado no sistema da AC;

b) Acesso permitido somente a partir de equipamentos autenticados no sistema utilizando uma solução que permite identificar de forma unívoca o equipamento;

c) *Timeout* de sessão de acordo com a análise de risco da AC;

d) Registro em *log* de auditoria dos eventos citados no item 5.4.1 desta DPC;

e) Histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas;

f) Mecanismo para revogação automática dos certificados digitais.

6.5.3.2.9 O aplicativo da Autoridade de Registro:

a) Foi desenvolvido com documentação formal;

b) Possui mecanismos para controle de versões;

c) Possui documentação dos testes realizados em cada versão;

d) Possui documentação comprovando a homologação de cada versão em ambiente com as mesmas características do que será usado em produção, sendo esses ambientes, porém, obrigatoriamente apartados entre si;

e) Possui aprovação documentada do gerente da AC, ou responsável designado, para colocar cada versão em ambiente de produção.

6.5.3.2.10 Os *logs* gerados por esse aplicativo são armazenados na AC pelo prazo de 7 (sete) anos.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

Nos itens seguintes são descritos os controles implementados pela AC Safeweb Timestamping e pelas ARs a ela vinculadas no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1 CONTROLES DE DESENVOLVIMENTO DE SISTEMA

6.6.1.1 A AC Safeweb Timestamping utiliza metodologias ágeis no desenvolvimento dos sistemas. São realizadas as fases de análise de requisitos, codificação, testes e homologação (pré-produção) para cada interação do sistema. Como suporte a esse modelo, a AC Safeweb Timestamping utiliza uma gerência de configuração, gerência de mudanças, testes formais e outros processos. As estações de trabalho e servidores utilizados pelos desenvolvedores dos sistemas da AC Safeweb Timestamping possuem controles de segurança implementados a fim de garantir um ambiente segregado, mantendo o controle e integridade do processo de desenvolvimento.

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

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.6.2.1 A AC Safeweb Timestamping e ARs vinculadas utilizam ferramentas específicas para verificação da configuração de segurança dos seus sistemas semanalmente. Os dados coletados durante a verificação periódica são comparados com as configurações aprovadas. Caso haja divergência, são tomadas medidas adequadas para a recuperação da situação, levando-se em consideração a natureza do problema e a análise do fato gerador, para evitar a sua recorrência.

6.6.2.2 A AC Safeweb Timestamping utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do seu sistema de certificação.

6.6.3 CONTROLES DE SEGURANÇA DE CICLO DE VIDA

Não se aplica.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

Antes de publicadas, todas as LCRs geradas pela AC Safeweb Timestamping são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 DIRETRIZES GERAIS

6.7.1.1 A AC Safeweb Timestamping implementa os seguintes controles de segurança de rede:

a) *Firewall* de:

a.1) rede;

a.2) *host*; e

a.3) aplicação.

b) Segregação de tráfego utilizando VLANs;

c) Sistema de detecção e prevenção de intrusão de:

b.1) rede; e

b.2) *host*.

d) Antivírus;

e) *Sandbox*;

f) Filtragem *web*; e

g) Monitoramento 24x7.

6.7.1.2 Nos servidores do sistema de certificação da AC Safeweb Timestamping, somente os serviços estritamente necessários são habilitados.

6.7.1.3 Todos os servidores e elementos de infraestrutura e proteção de rede, localizados no segmento de rede que hospeda o sistema de certificação da AC Safeweb Timestamping, estão localizados e operam em ambiente de nível 4 (quatro).

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

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

6.7.2 *FIREWALL*

6.7.2.1 A AC Safeweb Timestamping utiliza *firewalls* dedicados que promovem o isolamento dos servidores com acesso externo em uma DMZ, separando-os dos servidores que possuem acesso exclusivamente interno.

6.7.2.2 O *firewall* utilizado pela AC Safeweb Timestamping provê o registro dos eventos em *logs*,

além de implementar uma gerência de configuração.

6.7.3 SISTEMA DE DETECÇÃO/PREVENÇÃO DE INTRUSÃO – IDS/IPS

6.7.3.1 O sistema de detecção/prevenção 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 pelos administradores da rede, enviar e-mail aos administradores, enviar mensagens de alerta aos *firewalls*, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração dos *firewalls*.

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

6.7.3.3 O sistema de detecção/prevenção de intrusão provê o registro dos eventos em *logs*, além de implementar uma gerência de configuração.

6.7.4 REGISTRO DE ACESSOS NÃO AUTORIZADOS À REDE

As tentativas de acesso não autorizado são registradas para posterior análise. Esses registros são analisados diariamente e todas as ações tomadas em decorrência dessa análise são documentadas.

6.8 CARIMBO DO TEMPO

Em acordo com os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL [5].

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 PERFIL DO CERTIFICADO

Todos os certificados emitidos pela AC Safeweb Timestamping estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8, de acordo com o perfil estabelecido na RFC 5280.

7.1.1 NÚMERO (S) DE VERSÃO

Todos os certificados emitidos pela AC Safeweb Timestamping implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 EXTENSÕES DE CERTIFICADO

Não se aplica.

7.1.3 IDENTIFICADORES DE ALGORITMO

Não se aplica.

7.1.4 FORMATOS DE NOME

Não se aplica.

7.1.5 RESTRIÇÕES DE NOME

Não se aplica.

7.1.6 OID *(OBJECT IDENTIFIER)* DA DPC

O OID desta DPC AC Safeweb Timestamping é **2.16.76.1.1.150**.

7.1.7 USO DA EXTENSÃO *"POLICY CONSTRAINTS"*

Não se aplica.

7.1.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Não se aplica.

7.1.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 PERFIL DE LCR

7.2.1 NÚMERO(s) DE VERSÃO

As LCRs geradas pela AC Safeweb Timestamping implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 EXTENSÕES DE LCR E DE SUAS ENTRADAS

7.2.2.1 As extensões de LCR utilizadas pela AC Safeweb Timestamping são: *"Authority Key Identifier"* e *"CRL Number",* ambas consideradas não críticas, conforme descritas no item 7.2.2.2.

7.2.2.2 As LCRs da AC Safeweb Timestamping obedecem a ICP-Brasil que define como obrigatórias as seguintes extensões:

a) *"Authority Key Identifier"*, não crítica: contém o *hash* SHA-1 da chave pública da AC Safeweb Timestamping; e

b) *"CRL Number"*, não crítica: contém um número sequencial para cada LCR emitida pela AC Safeweb Timestamping.

7.3 PERFIL DE OCSP

7.3.1 NÚMERO(s) DE VERSÃO

Não se aplica.

7.3.2 EXTENSÕES DE OCSP

Não se aplica.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

A AC Safeweb Timestamping, bem como as demais entidades integrantes da ICP-Brasil sofre auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento.

8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

8.2.1 As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

8.2.2 Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores 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 [3].

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

As auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores 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 [3].

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO

8.4.1 As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPCs, PCs, PSs e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust*.

8.4.2 A AC Safeweb Timestamping recebeu auditoria prévia da AC Raiz 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 [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.4.3 A entidades da ICP-Brasil diretamente vinculadas a AC Safeweb Timestamping, também receberam auditoria prévia, para fins de credenciamento. A AC Safeweb Timestamping é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

8.5 AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

A AC Safeweb Timestamping cumpre, no prazo estipulado no relatório de auditoria, as recomendações para corrigir as deficiências apontadas indo ao encontro da legislação, políticas, normas, práticas e regras estabelecidas, de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.6 COMUNICAÇÃO DOS RESULTADOS

Os resultados das regularizações são comunicados formalmente à AC Safeweb, na data de vencimento do prazo concedido no relatório de auditoria de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 TARIFAS

9.1.1 TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS

Variável conforme definição interna comercial.

9.1.2 TARIFA DE ACESSO AO CERTIFICADO

Não são cobradas tarifas de acesso ao certificado digital emitido.

9.1.3 TARIFA DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS

Não há tarifa de revogação.

9.1.4 TARIFA PARA OUTROS SERVIÇOS

Não são cobradas tarifas de acesso à LCR, bem como tarifas de revogação e de acesso aos certificados emitidos.

9.1.5 POLÍTICA DE REEMBOLSO

Não se aplica.

9.2 RESPONSABILIDADE FINANCEIRA

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

9.2.1 COBERTURA DE SEGURO

A AC Safeweb Timestamping mantém contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades.

9.2.2 OUTROS ATIVOS

A AC Safeweb Timestamping mantém contrato de seguro para os ativos relacionados às atividades de certificação digital, com cobertura suficiente e compatível com o risco dessas atividades.

9.2.3 COBERTURA DE SEGUROS OU GARANTIA PARA ENTIDADES FINAIS

A AC Safeweb Timestamping implementa uma política que contém informações sobre a utilização correta da garantia oferecida sobre os seus certificados digitais, cartões inteligentes, tokens e as leitoras de cartão inteligente, e está de acordo com a legislação vigente, especialmente, o Código de Defesa do Consumidor (CDC). A Política de Garantia está disponível no site da AC, através do link: https://safeweb.com.br/politica-garantia.

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1 ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

9.3.1.1 Como princípio geral, todo documento, informação ou registro fornecido à AC Safeweb Timestamping ou às AR vinculadas é sigiloso.

9.3.1.2 Como princípio geral, nenhum documento, informação ou registro fornecido à AC Safeweb Timestamping ou às ARs vinculadas será divulgado.

9.3.2 INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

Os tipos de informações consideradas não sigilosas pela AC Safeweb Timestamping e pelas ARs a ela vinculadas, compreendem, entre outros:

a) os certificados e as LCRs emitidos pela AC Safeweb Timestamping;

b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;

c) as PCs implementadas pela AC Safeweb Timestamping;

d) a DPC da AC Safeweb Timestamping;

e) versões públicas de PS da AC Safeweb Timestamping; e

f) a conclusão dos relatórios de auditoria.

9.3.2.1 Certificados, LCR, e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não confidenciais.

9.3.2.2 Os seguintes documentos da AC Safeweb Timestamping também são considerados documentos não confidenciais:

a) qualquer PC aplicável;

b) qualquer DPC;

c) versões públicas de Política de Segurança – PS; e

d) a conclusão dos relatórios da auditoria.

9.3.2.3 A AC Safeweb Timestamping poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados ou carimbos de tempo emitidos no âmbito da ICP-Brasil.

9.3.3 RESPONSABILIDADE EM PROTEGER A INFORMAÇÃO CONFIDENCIAL

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

9.3.3.2 A chave privada de assinatura digital da AC Safeweb Timestamping é gerada e mantida pela própria AC, que será responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC Safeweb Timestamping é de sua inteira responsabilidade.

9.3.3.3 Os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

9.3.3.4 Não se aplica.

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1 PLANO DE PRIVACIDADE

A AC Safeweb Timestamping assegura a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2 TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS

Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC Safeweb Timestamping é 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

Informações sobre revogação de certificados de usuários finais são fornecidas na LCR da AC Safeweb Timestamping.

9.4.4 RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADA

A AC Safeweb Timestamping e AR vinculadas são responsáveis 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 AC Safeweb Timestamping poderão ser utilizadas ou divulgadas a terceiros, mediante expressa autorização do respectivo titular, conforme legislação aplicável.

9.4.5.2 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.

9.4.5.3 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 AC Safeweb Timestamping 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 AC Safeweb Timestamping 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

Não se aplica.

9.4.8 INFORMAÇÕES A TERCEIROS

Nenhum documento, informação ou registro sob a guarda das AR ou da AC Safeweb Timestamping é fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

9.5 DIREITO DE PROPRIEDADE INTELECTUAL

De acordo com a legislação vigente.

9.6 DECLARAÇÕES E GARANTIAS

9.6.1 DECLARAÇÕES E GARANTIAS DA AC

A AC Safeweb Timestamping declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

A AC Safeweb Timestamping implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC. A AC Safeweb Timestamping, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das AR na forma de suas DPCs, PCs e normas complementares.

9.6.1.2 Precisão da informação

A AC Safeweb Timestamping implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC Raiz, no âmbito da precisão da informação contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs subsequentes e AR na forma de suas DPCs, PCs e normas complementares.

9.6.1.3 Identificação do requerente

A AC Safeweb Timestamping implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das AR na forma de suas DPCs, PCs e normas complementares.

9.6.1.4 Consentimento dos titulares

A AC Safeweb Timestamping implementa termos de consentimento ou titularidade, contidas nos itens 3 e 4 desta DPC.

9.6.1.5 Serviço

A AC Safeweb Timestamping mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios e LCRs.

9.6.1.6 Revogação

A AC Safeweb Timestamping irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil.

9.6.1.7 Existência Legal

Esta DPC está em conformidade legal com a MP 2.200-2, de 24 de agosto de 2001, e legislação aplicável.

9.6.2 DECLARAÇÕES E GARANTIAS DA AR

Em acordo com item 4 desta DPC.

9.6.3 DECLARAÇÕES E GARANTIAS DO TITULAR

9.6.3.1 Toda informação necessária para a identificação do titular de certificado deve ser fornecida de forma completa e precisa. Ao aceitar o certificado emitido pela AC Safeweb Timestamping, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6.3.2 A AC Safeweb Timestamping informa à AC Raiz qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

9.6.4 DECLARAÇÕES E GARANTIAS DAS TERCEIRAS PARTES

9.6.4.1 As terceiras partes devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;

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

9.6.4.2 O certificado da AC Safeweb Timestamping é considerado válido quando:

a) tiver sido emitido pela AC Safeweb;

b) não constar como revogado pela AC Safeweb;

c) não estiver expirado; e

d) puder ser verificado com o uso do certificado válido da AC Safeweb.

9.6.4.3 A utilização ou aceitação de certificados sem a observância das providências descritas é de conta e risco da terceira parte que usar ou aceitar a utilização do respectivo certificado.

9.6.5 REPRESENTAÇÕES E GARANTIAS DE OUTROS PARTICIPANTES

Não se aplica.

9.7 ISENÇÃO DE GARANTIAS

Não se aplica.

9.8 LIMITAÇÕES DE RESPONSABILIDADES

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

9.9 INDENIZAÇÕES

A AC Safeweb Timestamping 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 DPC 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 DPC 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

Os atos praticados na vigência desta DPC 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

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC 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 DPC será submetida para AC Raiz.

9.12.2 MECANISMO DE NOTIFICAÇÃO E PERÍODOS

Mudança nesta DPC será publicado no site da AC Safeweb Timestamping.

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 DPC serão solucionados de acordo com a legislação vigente.

9.13.2 A DPC da AC Safeweb Timestamping não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.14 LEI APLICÁVEL

Esta DPC 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

A AC Safeweb Timestamping 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

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

9.16.2 CESSÃO

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

9.16.3 INDEPENDÊNCIA DE DISPOSIÇÕES

A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPC 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 DPC será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes.

9.16.4 EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)

De acordo com a legislação vigente.

9.17 OUTRAS PROVISÕES

Não se aplica.

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 https://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[12]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[13]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

10.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser

alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio https://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	DOC-ICP-05.02
[11]	REGULAMENTO DO USO DE BIOMETRIA NO ÂMBITO DA ICP-BRASIL – SISTEMA BIOMÉTRICO DA ICP-BRASIL	DOC-ICP-05.03

10.3 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio https://www.iti.gov.br.

Ref.	Nome do documento	Código
[4]	TERMOS DE TITULARIDADE	ADE-ICP-05. B

11 REFERÊNCIAS BIBLIOGRÁFICAS

[14] *WebTrust Principles and Criteria for Registration Authorities*, disponível em: https://www.webtrust.org/.

[15] *Webtrust Principles and Criteria for Certification Authorities,* disponível em: https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/webtrust-for-ca-22.pdf?la=en&hash=F377F94E2E3D87A83D07DDAC54171AC01AE798FA