

POLÍTICA DE CERTIFICADO DE ASSINATURA TIPO A4

PC A4 - AC SAFEWEB CD

OID 2.16.76.1.2.4.65

**Versão 1.0
Agosto 2025**

AC SAFEWEB CD

POLÍTICA DE CERTIFICADO DE ASSINATURA TIPO A4

SUMÁRIO

1	INTRODUÇÃO	5
1.1	VISÃO GERAL	5
1.2	NOME DO DOCUMENTO E IDENTIFICAÇÃO	5
1.3	PARTICIPANTES DA ICP-BRASIL.....	5
1.4	USABILIDADE DO CERTIFICADO	6
1.5	POLÍTICA DE ADMINISTRAÇÃO	7
1.6	DEFINIÇÕES E ACRÔNIMOS	8
2	RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	9
2.1	REPOSITÓRIOS	9
2.2	PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS.....	9
2.3	TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO	9
2.4	CONTROLE DE ACESSO AOS REPOSITÓRIOS	9
3	IDENTIFICAÇÃO E AUTENTICAÇÃO	9
3.1	NOMEAÇÃO	9
3.2	VALIDAÇÃO INICIAL DE IDENTIDADE	9
3.3	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES.....	9
3.4	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO	10
4	REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	10
4.1	SOLICITAÇÃO DE CERTIFICADO.....	10
4.2	PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO	10
4.3	EMISSÃO DE CERTIFICADO	10
4.4	ACEITAÇÃO DE CERTIFICADO.....	10
4.5	USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO.....	10
4.6	RENOVAÇÃO DE CERTIFICADOS.....	10
4.7	NOVA CHAVE DE CERTIFICADO.....	11
4.8	MODIFICAÇÃO DE CERTIFICADO.....	11
4.9	SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	11
4.10	SERVIÇOS DE STATUS DE CERTIFICADO	12
4.11	ENCERRAMENTO DE ATIVIDADES.....	12
4.12	CUSTÓDIA E RECUPERAÇÃO DE CHAVE.....	12
5	CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES	12
5.2	CONTROLES PROCEDIMENTAIS	12
5.3	CONTROLE DE PESSOAL.....	13
5.4	PROCEDIMENTOS DE LOG DE AUDITORIA.....	13
5.5	ARQUIVAMENTO DE REGISTROS	13
5.6	TROCA DE CHAVE	14
5.7	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE.....	14
5.8	EXTINÇÃO DA AC	14
6	CONTROLES TÉCNICOS DE SEGURANÇA	14
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	14

6.2	PROTEÇÃO DE CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO.....	16
6.3	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	18
6.4	DADOS DE ATIVAÇÃO	19
6.5	CONTROLES DE SEGURANÇA COMPUTACIONAL.....	19
6.6	CONTROLES TÉCNICOS DO CICLO DE VIDA.....	20
6.7	CONTROLES DE SEGURANÇA DE REDE	20
6.8	CARIMBO DO TEMPO	20
7	PERFIS DE CERTIFICADO E LCR	20
7.1	PERFIL DO CERTIFICADO	21
7.2	PERFIL DE LCR.....	24
7.3	PERFIL DE OCSP	25
8	AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	25
8.1	FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES	25
8.2	IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR.....	25
8.3	RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA.....	25
8.4	TÓPICOS COBERTOS PELA AVALIAÇÃO	25
8.5	AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA.....	25
8.6	COMUNICAÇÃO DOS RESULTADOS	25
9	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	25
9.1	TARIFAS.....	25
9.2	RESPONSABILIDADE FINANCEIRA.....	25
9.3	CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO	26
9.4	PRIVACIDADE DA INFORMAÇÃO PESSOAL	26
9.4.1	PLANO DE PRIVACIDADE.....	26
9.4.2	TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS.....	26
9.5	DIREITO DE PROPRIEDADE INTELECTUAL	26
9.6	DECLARAÇÕES E GARANTIAS.....	26
9.7	ISENÇÃO DE GARANTIAS	26
9.8	LIMITAÇÕES DE RESPONSABILIDADES	26
9.9	INDENIZAÇÕES.....	26
9.11	AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES.....	27
9.12	ALTERAÇÕES.....	27
9.14	LEI APLICÁVEL	27
9.15	CONFORMIDADE COM A LEI APLICÁVEL.....	27
9.16	DISPOSIÇÕES DIVERSAS	27
9.17	OUTRAS PROVISÕES	28
10	DOCUMENTOS REFERENCIADOS.....	28
11	REFERÊNCIAS BIBLIOGRÁFICAS	28

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado
1.0	21/08/2025	N/A	Versão inicial

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 O documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras (AC), integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na elaboração de suas Políticas de Certificado (PC).

1.1.2 Esta Política de Certificado de Assinatura Digital tipo A4 da AC Safeweb CD", adota a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1].

1.1.3 A estrutura desta PC está baseada na RFC 3647.

1.1.4 Este documento compõe o conjunto da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10.

1.1.5 O tipo de certificado de assinatura digital emitido sob essa PC é o Tipo A4.

1.1.6 Os certificados do tipo A4 são certificados de assinatura e devem ser emitidos exclusivamente para pessoas físicas.

1.1.7 Não se aplica.

1.1.8 Não se aplica.

1.1.9 Não se aplica.

1.1.10 Não se aplica.

1.1.11 Não se aplica.

1.1.12 Não se aplica.

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Esta Política de Certificado de Assinatura Digital é do tipo A4 da Autoridade Certificadora Safeweb CD. O *Object Identifier* - OID da PC A4 da AC Safeweb CD, atribuído para esta PC, na conclusão do processo de credenciamento da AC junto à ICP-Brasil, é **2.16.76.1.2.4.65**

1.2.2 Não se aplica.

1.3 PARTICIPANTES DA ICP-BRASIL

1.3.1 AUTORIDADES CERTIFICADORAS

1.3.1.1 Esta PC se refere à AC Safeweb CD, integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), sob a hierarquia da Autoridade Certificadora Safeweb (AC Safeweb), que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira (AC Raiz).

1.3.1.2 As práticas e procedimentos de certificação da AC Safeweb CD estão descritos na Declaração de Práticas de Certificação da AC Safeweb CD (DPC - AC Safeweb CD).

1.3.2 AUTORIDADES DE REGISTRO

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 CD estão relacionadas na página <https://www.safeweb.com.br/repositorio>

- a) Relação de todas as ARs credenciadas;
- b) Relação de ARs que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

1.3.3 TITULARES DE CERTIFICADO

Pessoas físicas, nacionais ou estrangeiras, podem ser titulares de certificado.

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

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

1.4 USABILIDADE DO CERTIFICADO

1.4.1 USO APROPRIADO DO CERTIFICADO

1.4.1.1 Os certificados definidos por esta Política de Certificado têm sua utilização vinculada à assinatura digital, não repúdio, garantia de integridade da informação e autenticação de seu titular.

1.4.1.2 As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.4.1.3 Na definição das aplicações para o certificado definido pela PC, a AC Safeweb CD leva em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é

caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados - LCR e extensão do período de validade do certificado.

1.4.1.4 Os certificados de tipo A4 emitidos pela AC Safeweb CD serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.5 Não se aplica.

1.4.1.6 Não se aplica.

1.4.1.7 Não se aplica.

1.4.1.8 Não se aplica.

1.4.1.9 Não se aplica.

1.4.2 USO PROIBITIVO DO CERTIFICADO

Não se aplica.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AC: AC Safeweb CD

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: +55 (51) 3018-0300

E-mail: compliance@safeweb.com.br

Outros: Setor de Compliance

1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA PC

Esta PC é aprovada pela AC Safeweb e pelo ITI. Os procedimentos de aprovação da PC da AC Safeweb CD são estabelecidos a critério do CG da ICP-Brasil.

1.6 DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
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 ICP-Brasil	Comitê Gestor da ICP-Brasil
CMM-SEI	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNPJ	Cadastro Nacional de Pessoa Jurídica
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	<i>Code Signing</i>
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
EV	<i>Extended Validation</i>
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	<i>International Organization for Standardization</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	<i>Online Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OM-BR	Objetos Metrológicos ICP-Brasil
OU	<i>Organization Unit</i>
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PIS	Programa de Integração Social
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SSL	<i>Secure Socket Layer</i>
TSDM	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	<i>Uniform Resource Locator</i>

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Os itens seguintes estão referidos em seus correspondentes na DPC da AC Safeweb CD.

2.1 REPOSITÓRIOS

2.2 PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.3 TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.4 CONTROLE DE ACESSO AOS REPOSITÓRIOS

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão referidos em seus correspondentes na DPC da AC Safeweb CD.

3.1 NOMEAÇÃO

3.1.1 Tipos de nomes

3.1.2 Necessidade de os nomes serem significativos

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

3.1.4 Regras para interpretação de vários tipos de nomes

3.1.5 Unicidade de nomes

3.1.6 Procedimento para resolver disputa de nomes

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

3.2 VALIDAÇÃO INICIAL DE IDENTIDADE

3.2.1 Método para comprovar a posse de chave privada

3.2.2 Não aplica

3.2.3 Não se aplica

3.2.4 Autenticação da identidade de um indivíduo

3.2.5 Informações não verificadas do titular do certificado

3.2.6 Validação das autoridades

3.2.7 Critérios para interoperação

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

3.3.1 Identificação e autenticação para rotina de novas chaves

3.3.2 Identificação e autenticação para novas chaves após a revogação

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Os itens seguintes estão referidos em seus correspondentes na DPC da AC Safeweb CD.

4.1 SOLICITAÇÃO DE CERTIFICADO

4.1.1 Quem pode submeter uma solicitação de certificado

4.1.2 Processo de registro e responsabilidades

4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1 Execução das funções de identificação e autenticação

4.2.2 Aprovação ou rejeição de pedidos de certificado

4.2.3 Tempo para processar a solicitação de certificado

4.3 EMISSÃO DE CERTIFICADO

4.3.1 Ações da AC durante a emissão de um certificado

4.3.2 Notificações para o titular do certificado pela AC na emissão do certificado

4.4 ACEITAÇÃO DE CERTIFICADO

4.4.1 Conduta sobre a aceitação do certificado

4.4.2 Publicação do certificado pela AC

4.4.3 Notificação de emissão do certificado pela AC Raiz para outras entidades

4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

4.5.1 Usabilidade da Chave privada e do certificado do titular

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

4.6 RENOVAÇÃO DE CERTIFICADOS

4.6.1 Circunstâncias para renovação de certificados

4.6.2 Quem pode solicitar a renovação

4.6.3 Processamento de requisição para renovação de certificados

4.6.4 Notificação para nova emissão de certificado para o titular

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

4.6.6 Publicação de uma renovação de um certificado pela AC

4.6.7 Notificação de emissão de certificado pela AC para outras entidades

4.7 NOVA CHAVE DE CERTIFICADO

4.7.1 Circunstâncias para nova chave de certificado

4.7.2 Quem pode requisitar a certificação de uma nova chave pública

4.7.3 Processamento de requisição de novas chaves de certificado

4.7.4 Notificação de emissão de novo certificado para o titular

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

4.7.6 Publicação de uma nova chave certificada pela AC

4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades

4.8 MODIFICAÇÃO DE CERTIFICADO

4.8.1 Circunstâncias para modificação de certificado

4.8.2 Quem pode requisitar a modificação de certificado

4.8.3 Processamento de requisição de modificação de certificado

4.8.4 Notificação de emissão de novo certificado para o titular

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

4.8.6 Publicação de uma modificação de certificado pela AC

4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.9.1 Circunstâncias para revogação

4.9.2 Quem pode solicitar revogação

4.9.3 Procedimento para solicitação de revogação

4.9.4 Prazo para solicitação de revogação

4.9.5 Tempo em que a AC deve processar o pedido de revogação

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

4.9.7 Frequência de emissão de LCR

4.9.8 Latência máxima para a LCR

4.9.9 Disponibilidade para revogação/verificação de status on-line

4.9.10 Requisitos para verificação de revogação on-line

4.9.11 Outras formas disponíveis para divulgação de revogação

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.13 Circunstâncias para suspensão

4.9.14 Quem pode solicitar suspensão

4.9.15 Procedimento para solicitação de suspensão

4.9.16 Limites no período de suspensão

4.10 SERVIÇOS DE STATUS DE CERTIFICADO

4.10.1 Características operacionais

4.10.2 Disponibilidade dos serviços

4.10.3 Funcionalidades operacionais

4.11 ENCERRAMENTO DE ATIVIDADES

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE

4.12.1 Política e práticas de custódia e recuperação de chave Política e práticas de encapsulamento e recuperação de chave de sessão

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC da AC Safeweb CD.

5.1 CONTROLES FÍSICOS

5.1.1 Construção e localização das instalações de AC

5.1.2 Acesso físico

5.1.3 Energia e ar-condicionado

5.1.4 Exposição à água

5.1.5 Prevenção e proteção contra incêndio

5.1.6 Armazenamento de mídia

5.1.7 Destruição de lixo

5.1.8 Instalações de segurança (backup) externas (off-site) para AC

5.2 CONTROLES PROCEDIMENTAIS

5.2.1 Perfis qualificados

5.2.2 Número de pessoas necessário por tarefa

- 5.2.3 Identificação e autenticação para cada perfil
- 5.2.4 Funções que requerem separação de deveres
- 5.3 CONTROLE DE PESSOAL**
 - 5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade
 - 5.3.2 Procedimentos de verificação de antecedentes
 - 5.3.3 Requisitos de treinamento
 - 5.3.4 Frequência e requisitos para reciclagem técnica
 - 5.3.5 Frequência e sequência de rodízio de cargos
 - 5.3.6 Sanções para ações não autorizadas
 - 5.3.7 Requisitos para contratação de pessoal
 - 5.3.8 Documentação fornecida ao pessoal
- 5.4 PROCEDIMENTOS DE LOG DE AUDITORIA**
 - 5.4.1 Tipos de eventos registrados
 - 5.4.2 Frequência de auditoria de registros
 - 5.4.3 Período de retenção para registros de auditoria
 - 5.4.4 Proteção de registros de auditoria
 - 5.4.5 Procedimentos para cópia de segurança (Backup) de registros de auditoria
 - 5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)
 - 5.4.7 Notificação de agentes causadores de eventos
 - 5.4.8 Avaliações de vulnerabilidade
- 5.5 ARQUIVAMENTO DE REGISTROS**
 - 5.5.1 Tipos de registros arquivados
 - 5.5.2 Período de retenção para arquivo
 - 5.5.3 Proteção de arquivo
 - 5.5.4 Procedimentos de cópia de arquivo
 - 5.5.5 Requisitos para datação de registros
 - 5.5.6 Sistema de coleta de dados de arquivo (interno e externo)
 - 5.5.7 Procedimentos para obter e verificar informação de arquivo

5.6 TROCA DE CHAVE

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

5.7.2 Recursos computacionais, software, e/ou dados corrompidos

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.4 Capacidade de continuidade de negócio após desastre

5.8 EXTINÇÃO DA AC

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC. São também definidos outros controles técnicos de segurança utilizados pela AC Safeweb CD e pelas ARs vinculadas na execução de suas funções operacionais.

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 GERAÇÃO DO PAR DE CHAVES

6.1.1.1 Quando o titular de certificado for uma pessoa física, esta é a responsável pela geração dos pares de chaves criptográficas.

6.1.1.1.1 Não se aplica.

6.1.1.1.2 Não se aplica

6.1.1.2 O processo de geração de chaves do tipo A4, contemplada nesta PC, exige:

a) A geração do par de chaves ocorre em cartão inteligente, token ou HSM com certificação do INMETRO, protegidos por senha;

b) O responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado deve executar pessoalmente a geração dos pares de chaves criptográficas.

6.1.1.3 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é o RSA, conforme definido em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.1.4 Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme a Tabela 2 a seguir.

6.1.1.5 A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

6.1.1.6 A mídia de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a) A chave privada é única e seu sigilo é suficientemente assegurado;
- b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
- c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7 A mídia de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8 O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC Safeweb CD, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

Tabela 2 – Mídias Armazenadoras de Chaves Criptográficas

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica
A4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR

Não se aplica.

6.1.3 ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

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*.

6.1.4 ENTREGA DE CHAVE PÚBLICA DA AC SAFEWEB CD ÀS TERCEIRAS PARTES

As formas para a disponibilização do certificado da AC Safeweb CD, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

- a) No momento da disponibilização de um certificado para seu titular, usando formato definido em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil;

- b) Diretório;
- c) Página *web*:
 - c.1) Rep. 1: <http://repositorio.acsafeweb.com.br/ac-safewebcd/ac-safewebcdv12.p7b>
 - c.2) Rep. 2: <http://repositorio2.acsafeweb.com.br/ac-safewebcd/ac-safewebcdv12.p7b>
- d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil.;

6.1.5 TAMANHOS DE CHAVE

6.1.5.1 O tamanho mínimo das chaves criptográficas associadas aos certificados da AC Safeweb CD é de RSA 4096 bits para a hierarquia V12.

6.1.5.2 Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A4 da ICP-Brasil estão definidos em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

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

Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificados atendem ao padrão estabelecido em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

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

Os pares de chaves correspondentes aos certificados emitidos pela AC Safeweb CD podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves. Para isso, os certificados emitidos segundo esta PC têm ativados os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment*.

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

O repositório de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a) A chave privada é única e seu sigilo é suficientemente assegurado;
- b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
- c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros, pois é gerada em cartão, token ou HSM com certificação INMETRO. Esses módulos criptográficos não permitem a exportação da chave privada e exigem senha para a sua utilização.

6.2.1 PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1 O módulo criptográfico utilizado na geração e utilização de chaves criptográficas possui certificação INMETRO.

6.2.1.2 Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado seguem os padrões definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.2 CONTROLE "N DE M" PARA CHAVE PRIVADA

Não se aplica.

6.2.3 CUSTÓDIA (ESCROW) DE CHAVE PRIVADA

6.2.3.1 O agente de custódia (escrow) dos certificados emitidos pela AC Safeweb CD, é o PSC Safeweb. As chaves privadas são armazenadas criptografadas em partições exclusivas em hardware criptográfico certificado pelo INMETRO. Estas chaves estão acessíveis apenas a seus titulares através de duplo fator de autenticação (senha e *push notification*).

6.2.3.2 A AC Safeweb CD não implementa a recuperação de chaves privadas.

6.2.4 CÓPIA DE SEGURANÇA DE CHAVE PRIVADA

6.2.4.1 Como diretriz geral, 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 CD, não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, no entanto em casos em que o CD é emitido utilizando o PSC Safeweb, a guarda da cópia da chave privada é realizada pelo próprio PSC.

6.2.4.3 Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4 Através das tecnologias atualmente disponíveis, a entidade titular de certificado deve realizar a geração de cópia de segurança de sua chave privada.

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1 As chaves privadas das entidades titulares de certificados emitidos por esta PC não são arquivadas.

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 CD gera os 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

A chave privada é ativada, mediante senha solicitada pelo software de proteção da chave privada. A senha deve ser criada e mantida apenas pelo titular do certificado, sendo para seu uso e conhecimento exclusivo.

6.2.9 MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

A desativação da chave privada ocorre em função da expiração do certificado correspondente ou em função de sua revogação.

6.2.10 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

Para destruição da chave privada de certificados emitidos conforme esta PC, é preciso que o usuário acesse o software de proteção da chave privada, localize o certificado e o remova do repositório. A destruição da chave privada é irreversível e definitiva, não sendo mais possível a sua recuperação.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA

As chaves públicas da AC Safeweb CD, dos titulares de certificados de assinatura digital e as LCRs por ela 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 AS CHAVES PÚBLICA E PRIVADA

6.3.2.1 As chaves privadas dos respectivos titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

6.3.2.3 O período máximo de uso das chaves correspondentes aos certificados emitidos pela PC A4 da AC Safeweb CD é de 6 (seis) anos.

6.4 DADOS DE ATIVAÇÃO

Nos itens seguintes desta PC estão descritos os requisitos de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

Os certificados emitidos conforme esta PC, se utilizam de hardwares criptográficos para manter a segurança de suas chaves privadas. Estes hardwares possuem certificação INMETRO e protegem as chaves privadas armazenando-as em partições exclusivas para este fim, com acesso restrito apenas através da utilização de senha criada pelo próprio titular, não necessitando de outros dados de ativação para sua operação. Em casos de emissão através de PSC, as chaves estão acessíveis apenas a seus titulares através de duplo fator de autenticação (senha e *push notification*).

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

Conforme descrito no item 6.4.1, os certificados emitidos conforme esta PC, não necessitam de outros dados de ativação para sua operação além da própria senha criada pelo titular e da posse do hardware criptográfico. Para uma maior proteção, os hardwares possuem a capacidade de bloquear o acesso à chave privada caso a quantidade de tentativas de utilização com a senha errada exceda o limite pré-definido. A AC Safeweb CD recomenda:

- a) Nunca fornecer senha a terceiros;
- b) Escolher senhas de 8 ou mais caracteres;
- c) Definir senhas com caracteres numéricos e alfanuméricos;
- d) Memorizar a senha; e
- e) Não a escrever.

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

Nos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC Safeweb CD, 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.

6.5.2 CLASSIFICAÇÃO DE SEGURANÇA COMPUTACIONAL

Não se aplica.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 CONTROLES DE DESENVOLVIMENTO DO SISTEMA

Como descrito no item correspondente da DPC AC Safeweb CD.

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

Como descrito no item correspondente da DPC AC Safeweb CD.

6.6.3 CLASSIFICAÇÃO DE SEGURANÇA DE CICLO DE VIDA

Como descrito no item correspondente da DPC AC Safeweb CD.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

Antes de publicadas, todas as LCR geradas pela AC Safeweb CD 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

Não se aplica.

6.8 CARIMBO DO TEMPO

Não se aplica.

7 PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das LCRs gerados segundo esta PC.

São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1 PERFIL DO CERTIFICADO

Os certificados emitidos pela AC Safeweb CD estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 NÚMERO DE VERSÃO

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

7.1.2 EXTENSÕES DE CERTIFICADO

7.1.2.1 Os certificados emitidos pela AC Safeweb CD obedecem a ICP-Brasil, que define as seguintes extensões:

a) Authority Key Identifier, obrigatória, não crítica: contém o *hash 160 bits* SHA-1 da chave pública da AC Safeweb CD;

b) Key Usage, crítica:

b.1) o *bit digitalSignature* obrigatoriamente está ativado;

b.2) o *bit keyEncipherment* pode estar ativado ou não;

b.3) o *bit nonRepudiation* pode estar ativado ou não;

c) Certificate Policies, obrigatória, não crítica: contém os seguintes valores:

c.1) o campo *policyIdentifier* contém o OID desta PC **2.16.76.1.2.4.65**;

c.2) o campo *policyQualifiers* contém o OID 1.3.6.1.5.5.7.2.1;

c.3) o campo *cPSuri* contém o endereço *web* da DPC da AC Safeweb CD (<http://repositorio.acsafeweb.com.br/ac-safewebcd/dpc-acsafewebcd.pdf>)

d) Subject Alternative Name, não crítica: contém os seguintes valores:

I) OID = 2.16.76.1.3.1 (obrigatório) e conteúdo: nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do titular; nas 10 (dez) posições subsequentes, as siglas do órgão emissor do RG e respectiva UF;

II) OID = 2.16.76.1.3.6 (permitido) e conteúdo: nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado;

III) OID = 2.16.76.1.4.3 (permitido) e conteúdo: nome social do titular do certificado.

- e) **BasicConstraints**, obrigatório, crítica: contém o campo *cA=False*;
- f) **Extended Key Usage**, não crítica: contém os seguintes valores:
 - f.1) o campo *Client authentication* é obrigatório e contém o OID = 1.3.6.1.5.5.7.3.2;
 - f.2) o campo *E-mail protection* é obrigatório e contém OID = 1.3.6.1.5.5.7.3.4;
- g) **CRL Distribution Points**, obrigatório, não crítica: *DistributionPointName* do tipo URI contendo o endereço *web* (HTTP URL) do serviço de LCR da AC Safeweb CD:
 - g.1) <http://repositorio.acsafeweb.com.br/ac-safewebcd/lcr-ac-safewebcdv12.crl>
 - g.2) <http://repositorio2.acsafeweb.com.br/ac-safewebcd/lcr-ac-safewebcdv12.crl>
- h) **Authority Information Access**, obrigatória, não crítica: contém o método de acesso *id-ad-calssuer*, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação nos seguintes endereços:
 - h.1) Rep. 1: <http://repositorio.acsafeweb.com.br/ac-safewebcd/ac-safewebcdv12.p7b>
 - h.2) Rep. 2: <http://repositorio2.acsafeweb.com.br/ac-safewebcd/ac-safewebcdv12.p7b>

7.1.2.2 Os campos **otherName** estão de acordo com as seguintes especificações:

- a) O conjunto de informações definido em cada campo *otherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 *OCTET STRING* ou *PRINTABLE STRING*;
- b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNO ou CAEPF não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";
- c) Se o número do RG não estiver disponível, não se deve preencher os campos de órgão emissor e UF;
- d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional;
- e) Todas as informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;
- f) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita;
- g) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;
- h) Não se aplica.

7.1.2.3 Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC Safeweb CD, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

7.1.2.4 Os outros campos que compõem a extensão "*Subject Alternative Name*" poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.5 Todas as informações utilizadas para preenchimento dos campos do certificado devem ser verificadas.

7.1.3 IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC Safeweb CD às entidades titulares de certificado são assinados com o uso do algoritmo RSA com SHA-256 como função de *hash* (OID = 1.2.840.113549.1.1.11), conforme o padrão PKCS#1.

7.1.4 FORMATOS DE NOME

7.1.4.1 O nome do titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

CN = <Nome Civil>

OU= <Nome Social>

serialNumber = <número CPF>

7.1.4.2 Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.5 RESTRIÇÕES DE NOME

7.1.5.1 Neste item estão descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2 A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

a) Não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

b) Além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

Tabela 3

Caractere	Código NBR9611 (hexadecimal)	Caractere	Código NBR9611 (hexadecimal)
Branco	20	+	2B
!	21	,	2C
“	22	-	2D
#	23	.	2E
\$	24	/	2F
%	25	:	3A
&	26	;	3B
'	27	=	3D
(28	?	3F
)	29	@	40
*	2A	\	5C

7.1.6 OID (OBJECT IDENTIFIER) DA PC

O OID (*Object Identifier*) desta PC é **2.16.76.1.2.4.65**. Todo certificado emitido segundo a PC A4 da AC Safeweb CD contém o valor desse OID presente na extensão “*Certificate Policies*”.

7.1.7 USO DA EXTENSÃO "POLICY CONSTRAINTS"

Não se aplica.

7.1.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Nos certificados emitidos segundo esta PC, o campo *policyQualifiers* da extensão “*Certificate Policies*” contém o endereço *web* da DPC da AC Safeweb CD: <http://repositorio.acsafeweb.com.br/ac-safewebcd/dpc-acsafewebcd.pdf>

7.1.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS DE PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 PERFIL DE LCR

7.2.1 NÚMERO(S) DE VERSÃO

As LCR geradas pela AC Safeweb CD 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 LCR da AC Safeweb CD obedecem os padrões da ICP-Brasil e utilizam as seguintes extensões:

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

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

7.3 PERFIL DE OCSP

7.3.1 NÚMERO DE VERSÃO

Não se aplica.

7.3.2 EXTENSÕES DE OCSP

Não se aplica.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC-AC Safeweb CD.

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Safeweb CD.

8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO

8.5 AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

8.6 COMUNICAÇÃO DOS RESULTADOS

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Os itens seguintes estão referidos em seus correspondentes na DPC-AC Safeweb CD.

9.1 TARIFAS

9.1.1 TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS

9.1.2 TARIFAS DE ACESSO AO CERTIFICADO

9.1.3 TARIFAS DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS

9.1.4 TARIFAS PARA OUTROS SERVIÇOS

9.1.5 POLÍTICA DE REEMBOLSO

9.2 RESPONSABILIDADE FINANCEIRA

- 9.2.1 COBERTURA DE SEGURO
- 9.2.2 OUTROS ATIVOS
- 9.2.3 COBERTURA DE SEGUROS OU GARANTIA PARA ENTIDADES FINAIS
- 9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO**
 - 9.3.1 ESCOPO DE INFORMAÇÕES CONFIDENCIAIS**
 - 9.3.2 INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS**
 - 9.3.3 RESPONSABILIDADE EM PROTEGER A INFORMAÇÃO CONFIDENCIAL**
- 9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL**
 - 9.4.1 PLANO DE PRIVACIDADE
 - 9.4.2 TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS
 - 9.4.3 INFORMAÇÕES NÃO CONSIDERADAS PRIVADAS
 - 9.4.4 RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADA
 - 9.4.5 AVISO E CONSENTIMENTO PARA USAR INFORMAÇÕES PRIVADAS
 - 9.4.6 DIVULGAÇÃO EM PROCESSO JUDICIAL OU ADMINISTRATIVO
 - 9.4.7 OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO
- 9.5 DIREITO DE PROPRIEDADE INTELECTUAL**
- 9.6 DECLARAÇÕES E GARANTIAS**
 - 9.6.1 DECLARAÇÕES E GARANTIAS DA AC
 - 9.6.2 DECLARAÇÕES E GARANTIAS DA AR
 - 9.6.3 DECLARAÇÕES E GARANTIAS DO TITULAR
 - 9.6.4 DECLARAÇÕES E GARANTIAS DAS TERCEIRAS PARTES
 - 9.6.5 REPRESENTAÇÕES E GARANTIAS DE OUTROS PARTICIPANTES
- 9.7 ISENÇÃO DE GARANTIAS**
- 9.8 LIMITAÇÕES DE RESPONSABILIDADES**
- 9.9 INDENIZAÇÕES**

9.10 PRAZO E RESCISÃO

9.10.1 PRAZO

9.10.2 TÉRMINO

9.10.3 EFEITO DA RESCISÃO E SOBREVIVÊNCIA

9.11 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES

9.12 ALTERAÇÕES

9.12.1 PROCEDIMENTO PARA EMENDAS

A AC Safeweb CD segue um processo periódico de atualização de suas PCs, que contempla a revisão em duas etapas. A primeira realizada pela equipe de Compliance/ Segurança da Informação e a segunda pela aprovação da Diretoria, visando a adequação dos documentos conforme as normas, procedimentos e regulamentos atuais da AC Safeweb e ICP-Brasil. Qualquer alteração nesta PC será submetida à aprovação da AC Raiz.

9.12.2 MECANISMO DE NOTIFICAÇÃO E PERÍODOS

A AC Safeweb CD mantém a versão corrente desta PC para consulta pública em seu repositório *web*, no endereço: <http://repositorio.acsafeweb.com.br/ac-safewebcd/pc-a4-acsafewebcd.pdf>

9.12.3 CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO

9.13 SOLUÇÃO DE CONFLITOS

9.14 LEI APLICÁVEL

9.15 CONFORMIDADE COM A LEI APLICÁVEL

9.16 DISPOSIÇÕES DIVERSAS

9.16.1 ACORDO COMPLETO

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

9.16.2 CESSÃO

9.16.3 INDEPENDÊNCIA DE DISPOSIÇÕES

9.16.4 EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)

9.17 OUTRAS PROVISÕES

Esta PC foi submetida à aprovação, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2]. Como parte desse processo, além da conformidade com este documento, é verificada a compatibilidade entre a PC e a DPC da AC Safeweb CD.

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.it.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[2]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[3]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17

11 REFERÊNCIAS BIBLIOGRÁFICAS

RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.

RFC 5280, IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, may 2008.