Declaração de Práticas de Certificação da Autoridade Certificadora Serasa AC

DPC AC SERASA AC

https://serasa.certificadodigital.com.br/

V 10.1

20 de março de 2024

Sumário

Controle de alterações

Versão da DPC	Data da Alteração	Descrição da Alteração
10.1	20/03/2024	Atualização do número de grupo de pessoas para utilização de chave privada, item 6.2.2.1.
10.0	06/01/2022	Adequação à Resolução N° 197 de 16/12/2021
9.0	29/03/2021	Adequação à Resolução nº 177, de 20.10.2020 e Resolução CG ICP-Brasil nº 181, de 22.01.2021 e correção de numeração e/ou redação, itens: 1.1.6, 1.5.2, 1.5.3, 1.6, 3.2.2.1.3, 3.2.2.1.5, 3.2.2, 3.2.3.1.7, 3.2.3.1.8, 3.3.1.1, 3.3.2, 3.3.2.1, 3.3.3, 3.3.4, 5.1.3.1, 5.1.3.9, 5.7.1.2, 6.1.7.1, 7.1.
8.0	05/05/2020	Adequação às resoluções 153 (17/09/2019), 154 (01/10/2019), 155 (03/12/2019), 156 (07/02/2020), 164 e 167 (17/04/2020).
7.0	30/08/2019	Adequação ao Resolução 151, de 30/05/2019.

1. INTRODUÇÃO

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP-Brasil.

1.1 Visão Geral

1.1.1 Este documento estabelece os requisitos mínimos, obrigatoriamente observados pela Autoridade Certificadora Serasa AC, referida a seguir como “AC Serasa AC”, integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação – DPC. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução de seus serviços.

1.1.2 Esta DPC, elaborada no âmbito da ICP-Brasil, obrigatoriamente adota a mesma estrutura empregada no documento 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 Serasa AC é responsável pela atualização das informações de sua DPC.

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

1.2 Nome do documento e identificação

1.2.1 Esta Declaração de Práticas de Certificação, referida a seguir simplesmente como "DPC-AC Serasa AC", descreve as práticas e os procedimentos empregados pela AC Serasa AC no âmbito da ICP-Brasil.
O OID da DPC-Serasa AC é 2.16.76.1.1.4.

1.2.2 A AC SERASA AC emissora de certificados para usuários finais é exclusiva e separada de acordo com os propósitos de uso de chaves de Assinatura de documento e proteção de e-mail (S/MIME).

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

Esta DPC-Serasa AC se refere à AC Serasa AC (SERASA S.A., com sede na Avenida das Nações Unidas, 14401, Torre C-1 – Condomínio Parque da Cidade – Conjuntos:191, 192, 201, 202, 211, 212, 221, 222, 231, 232, 241 e 242, São Paulo, SP, CEP 04794-000, CNPJ no 62.173.620/0001-80).

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 da Serasa Autoridade de Registro, a seguir referida simplesmente como “Serasa AR”, e está identificada como tal na página https://serasa.certificadodigital.com.br/repositorio/.
A página https://serasa.certificadodigital.com.br/repositorio/ contém:
a) Relação de todas as ARs credenciadas;
b) Relação de AR que tenham se descredenciado da cadeia da AC, com respectivas datas do descredenciamento;

1.3.3 Titulares do Certificado

Podem ser Titulares de Certificado Digital Serasa, pessoas jurídicas de direito público ou privado, nacionais ou internacionais, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis.
NOTA 1: O representante legal da pessoa jurídica é designado como responsável pelo certificado e detentor da chave privada.

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
1.3.5.1 A publicação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC Serasa AC estão relacionados na página https://serasa.certificadodigital.com.br/repositorio/.

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do certificado
A AC Serasa AC implementa as seguintes Políticas de Certificado Digital:

Política de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo A1 da Serasa AC	PC SPB	2.16.76.1.2.1.2

Nas PCs correspondentes estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC Serasa AC.

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 correspondentes.

1.5 Política de Administração
Dúvidas decorrentes da leitura desta DPC-Serasa AC e que não sejam respondidas mediante a leitura da página https://serasa.certificadodigital.com.br/repositorio/ podem ser esclarecidas contatando:

1.5.1 Organização administrativa do documento
Autoridade Certificadora Serasa Autoridade Certificadora (AC Serasa AC)

1.5.2 Contatos
Endereço: Avenida das Nações Unidas, 14401, Torre C-1 – Condomínio Parque da Cidade – Conjuntos:191, 192,201,202,211,212,221,222,231,232,241 e 242, São Paulo, SP, CEP 04794-000.
Telefone: Tel. +55 11 2847-5083
Fax: +55 11 2847-9755
Página web: https://serasa.certificadodigital.com.br
E-mail: arcompliance@br.experian.com
Outros: N/A

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC
Nome: Giseli Mioti
Telefone: +55 11 2847-5083
E-mail: arcompliance@br.experian.com
Outros: N/A

1.5.4 Procedimentos de aprovação da DPC
Esta DPC Serasa AC é aprovada pelo ITI.
Os procedimentos de aprovação da DPC da AC são estabelecidos a critério 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
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
CSR	*Certificate Signing Request*
DETRAN	Departamento Nacional de Trânsito
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IETF PKIX	*Internet Engineering Task Force - Public-Key Infrastructured (X.509)*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
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
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
SNMP	*Simple Network Management Protocol*
SSL	*Secure Socket Layer*
TCSEC	*Trusted System Evaluation Criteria*
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Repositórios

2.1.1 A AC Serasa AC disponibiliza um repositório acessado pela página https://serasa.certificadodigital.com.br/repositorio/, atendendo as obrigações desta DPC, entre elas:
a) disponibilização, logo após a sua emissão, dos certificados emitidos pela AC e a sua LCR/OCSP;
b) disponibilidade para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
c) implementação dos recursos necessários para a segurança dos dados nele armazenados.

2.1.2 O repositório da AC Serasa AC possui os seguintes requisitos atendidos:
a) localização física e lógica; (localização lógica: https://serasa.certificadodigital.com.br/repositorio/)
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; e
d) requisitos de segurança.

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

2.1.4 A AC Serasa AC disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR/OCSP.
a) http://www.certificadodigital.com.br/repositorio/lcr/serasaacv5.crl; e
b) http://lcr.certificados.com.br/repositorio/lcr/serasaacv5.crl.

2.2 Publicação de informações dos certificados

2.2.1 A AC Serasa AC pública e mantém disponível em seu site (https://serasa.certificadodigital.com.br/repositorio/), em no mínimo 99,5% (noventa e nove e meio por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, as seguintes informações:

2.2.2 As seguintes informações são publicadas pela AC Serasa AC em página web:
a) Seu próprio certificado;

b) Suas LCRs / OCSP;
c) Sua DPC;
d) Não se aplica;
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 A AC Serasa AC manterá as informações de que trata o item anterior sempre atualizadas.

2.4 Controle de Acesso aos Repositórios
2.4.1. Não há qualquer restrição de acesso para consulta ao Repositório. São utilizados apenas controles de restrição para modificação de informações.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC Serasa AC 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 diretos de propriedade intelectual de terceiros. A AC Serasa AC 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 Serasa AC emite certificados com nomes que permitam a identificação unívoca. Para isso utiliza o "distinguished name" do padrão ITU X.500, endereços de correio eletrônico ou endereços de página Web (URL).

3.1.1.2 Não se aplica.

3.1.2 Necessidade dos nomes serem significativos
A AC Serasa AC faz uso de nomes significativos que possibilitam determinar a identidade da organização a que se referem, para a identificação dos titulares dos certificados emitidos pela AC Serasa AC.
Para certificados de pessoa física (e-CPF), o campo Common Name é composto do nome do Titular do Certificado, conforme consta no Cadastro de Pessoa Física.
Para os certificados de pessoa jurídica(e-CNPJ) o campo Common Name é composto do nome empresarial da pessoa jurídica, conforme consta no Cadastro Nacional de Pessoa Jurídica.

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado
Não se aplica.

3.1.4 Regras para interpretação de vários tipos de nomes

3.1.4.1 Não se aplica

3.1.4.2 É vedado o uso de nomes nos certificados que violem os direitos de propriedade intelectual de terceiros.

3.1.5 Unicidade de nomes
Os identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC Serasa AC. 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
A AC Serasa AC se reserva o direito de tomar todas as decisões referentes a disputas de nomes das entidades solicitantes de certificados. 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
De acordo com a legislação em vigor.

3.2 Validação inicial de identidade
A DPC da AC Serasa AC descreve em detalhes os requisitos e procedimentos utilizados pelas ARs vinculadas para realização dos seguintes processos:
a) Identificação do titular do certificado – identificação da pessoa jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3, observado o quanto segue:

i. 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 Serasa AC. 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.

Nota: Nos casos de falecimento dos responsáveis legais por quaisquer empresas de um modo geral, desde que haja decisão judicial com nomeação de inventariante e termo de compromisso de inventariante assinado, e nomeação expressa deste como administrador será admitida a pessoa nomeada na qualidade de responsável legal do Certificado Digital para todos os fins legais e administrativos, de acordo com a legislação vigente.

3.2.1 Método para comprovar o controle de chave privada
A confirmação de que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 4210 e 6712.

3.2.2 Autenticação da identificação da organização

3.2.2.1 Disposições Gerais
3.2.2.1.1 Neste item são definidos os procedimentos empregados pelas ARs vinculadas para a confirmação da identidade de uma pessoa jurídica.

3.2.2.1.2 Será designado como responsável pelo certificado o representante legal da pessoa jurídica requerente do certificado, ou o procurador constituído na forma do item 3.2, alínea ‘a’, inciso (ii) acima, o qual será o detentor da chave privada.

3.2.2.1.3 A confirmação da identidade da organização e das pessoas físicas é feita nos seguintes termos:
a) apresentação do rol de documentos elencados no item 3.2.2.2;
b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;
c) coleta e verificação biométrica da pessoa física responsável pelo certificado, conforme regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, que definam os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil, bem como os procedimentos para identificação biométrica na ICP-Brasil; e
d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo titular ou responsável pelo uso do certificado.

Nota 1: A AR pode solicitar uma assinatura manuscrita ao requerente ou responsável pelo uso do certificado em termo específico para a comparação com o documento de identidade ou contrato social. Nesse caso, o termo manuscrito digitalizado e assinado digitalmente pelo AGR será apensado ao dossiê eletrônico do certificado, podendo o original em papel ser descartado.

3.2.2.1.4 Fica dispensado o disposto no item 3.2.2.1.3, alíneas “b” e “c” caso o responsável pelo certificado possua certificado digital de pessoa física ICP-Brasil válido, do tipo A3 ou superior, com os dados biométricos devidamente coletados, e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

3.2.2.1.5 O disposto no item 3.2.2.1.3 poderá ser realizado:

a) mediante comparecimento presencial do responsável pelo certificado; ou
b) por videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

3.2.2.2 Documentos para efeitos de identificação de uma organização
A confirmação da identidade de uma pessoa jurídica é feita mediante a apresentação de, no mínimo, os seguintes documentos:
a) Relativos a sua habilitação jurídica:
   i. se pessoa jurídica criada ou autorizada a sua criação por lei, 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 representantes legais, quando aplicável;
b) Relativos a 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.

Nota 1: 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 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:
a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;[1]
b) Cadastro Nacional de Pessoa Jurídica (CNPJ); [2]
c) Nome completo do responsável pelo certificado, sem abreviações;[3] e
d) Data de nascimento do responsável pelo certificado.[4]

3.2.2.3.2 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 com suas informações pessoais, conforme item 3.2.3.2.

3.2.2.4 Responsabilidade decorrente do uso do certificado de uma organização
Os atos praticados com o certificado digital de titularidade de uma organização estão sujeitos ao regime de responsabilidade definido em lei quanto aos poderes de representação conferidos ao responsável de uso indicado no certificado.

3.2.3 Autenticação da identidade de um indivíduo
Neste item são definidos os procedimentos empregados pelas AR vinculadas a AC Serasa AC para a identificação e cadastramento de um indivíduo na ICP-Brasil. Essa confirmação é realizada mediante a presença física do interessado ou por um dos procedimentos listados nas alíneas abaixo, que deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico:

a) Não se aplica.
b) Por meio de videoconferência conforme procedimentos e requisitos técnicos definidos em instrução normativa da AC Raiz; ou
c) Não se aplica.

---

1 No campo Subject, como parte do Common Name, que compõe o Distinguished Name
2 No campo Subject Alternative Name, **OID 2.16.76.1.3.3**
3 No campo Subject Alternative Name, **OID 2.16.76.1.3.2**
4 No campo Subject Alternative Name, nas primeiras 8 (oito) posições do **OID 2.16.76.1.3.4**

3.2.3.1 Procedimento para identificação de um indivíduo
A identificação da pessoa física requerente do certificado deverá ser realizada como segue:
a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:
i. Registro de Identidade, se brasileiro; ou
ii. Título de Eleitor, com foto; ou
iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
iv. Passaporte, se estrangeiro não domiciliado no Brasil.
b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.
Nota 1: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

3.2.3.1.1 Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil fica dispensada a apresentação de qualquer dos documentos elencados no item 3.2.3.1 da etapa de verificação. As evidências desse processo farão parte do dossiê eletrônico do requerente.

3.2.3.1.2 Os documentos digitais são verificados por meio de barramentos ou aplicações oficiais dos entes federativos. Tal verificação faz parte do dossiê eletrônico do titular do certificado. Na hipótese da identificação positiva, fica dispensada a etapa de verificação conforme o item 3.2.3.1.3.

3.2.3.1.3 Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, são verificados:
a) por agente de registro distinto do que realizou a etapa de identificação;
b) pela AR ou AR própria da AC Serasa AC; e
c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.2.3.1.4 A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observa o disposto na lei vigente, e as normas editadas pelo Comitê Gestor da ICP-Brasil.

3.2.3.1.5 Não se aplica.

3.2.3.1.6 Não aplica.

3.2.3.1.7 Não se aplica.

3.2.3.1.8 A verificação biométrica do requerente poderá ser realizada por meio de batimento dos dados em base oficial nacional, conforme regulamentado em Instrução Normativa editada pela AC Raiz da ICP-Brasil, que deverá dispor acerca dos procedimentos e das bases oficiais admitidas para tal finalidade.

3.2.3.1.8.1 Não se aplica.

3.2.3.2 Informações contidas no certificado emitido para um indivíduo
3.2.3.2.1 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:
a) nome completo, sem abreviações;[5]
b) data de nascimento. [6]
c) cadastro de pessoas físicas (CPF)[3]

[3]No campo Subject Alternative Name, nas 11 (onze) posições subsequentes às 8 (oito) posições reservadas à data de nascimento, o Cadastro de Pessoa Física (CPF) – OID 2.16.76.1.3.1.

3.2.3.2.1.1 Não se aplica.

[5] No campo *Subject*, como parte do *Common Name,* que compõe o *Distinguished Name*
[6] No campo *Subject Alternative Name,* nas primeiras 8 (oito) posições do **OID 2.16.76.1.3.1**

3.2.3.2.2 Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, pode solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

a) número de Identificação Social - NIS (PIS, PASEP ou CI);
b) número do Registro Geral - RG do titular e órgão expedidor;
c) número do Cadastro Específico do INSS (CEI / CAEPF / CNO);
d) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor; e
e) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

3.2.3.2.3 Para tanto, o titular deve apresentar a documentação respectiva, caso a caso, em sua versão original.

3.2.3.2.3.1 Não se aplica.

Nota 1: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

Nota 2: O cartão CPF pode ser substituído por consulta à página da Receita Federal, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.2.4 Informações não verificadas do titular do certificado
Não se aplica.

3.2.5 Validação das autoridades
Não se aplica.

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 Não se aplica.

3.2.7.1.2 Não se aplica.

3.2.7.1.3 Não se aplica.

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 Não se aplica.

3.2.7.3 Informações contidas no certificado emitido para um equipamento ou aplicação
3.2.7.3.1 não se aplica.

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 e responsabilidade, 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

3.2.7.4.1 Disposições Gerais

3.2.7.4.2 Não se aplica.

3.2.7.4.3 Não se aplica.

3.2.7.4.4 Não se aplica.

3.2.7.5 Procedimentos para efeitos de identificação de um equipamento SAT
3.2.7.5.1 Não se aplica.

3.2.7.6 Informações contidas no certificado emitido para um equipamento SAT
3.2.7.6.1 Não se aplica.
a) Não se aplica.
b) Não se aplica.
c) Não se aplica.

3.2.7.6.2 Não se aplica.

3.2.7.7 Autenticação de identificação de equipamentos para certificado OM-BR
3.2.7.7.1 Disposições gerais

3.2.7.7.2 Não se aplica.

3.2.7.7.3 Não se aplica.

3.2.7.7.4 Não se aplica.

3.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico
3.2.7.8.1 Não se aplica.

3.2.7.9 Informações contidas no certificado emitido para um equipamento metrológico
3.2.7.9.1 Não se aplica.
a) Não se aplica.
b) Não se aplica.
c) Não se aplica.
d) Não se aplica.

3.2.7.9.2 Não se aplica.

3.2.8 Procedimentos complementares

3.2.8.1 A AC SERASA AC mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC SERASA AC é membro.

3.2.8.2 Não se aplica.

3.2.8.2.1 Não se aplica.

3.2.8.3 É mantido dossiê 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.

3.2.8.3.2 Não se aplica.

3.2.8.3.3 Não se aplica.

3.2.8.4 A AC Serasa AC disponibiliza, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, 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.

3.2.8.4.2 Não se aplica.

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.

3.2.9.3.1 Não se aplica.

Nota: Não se aplica.

3.2.9.3.2 Não se aplica.

3.2.9.3.3 Não se aplica.

3.2.9.4 Não se aplica.

3.2.9.4.1 Não se aplica.

Nota: Não se aplica.

3.2.9.5 Disposições para a Validação de Solicitação de Certificados do Tipo OM-BR:
Não se aplica.

3.2.9.6 Não se aplica.

3.2.9.7 Não se aplica.

3.2.9.8 Não se aplica.

3.3 Identificação e autenticação para pedidos de novas chaves
3.3.1 Este item estabelece os processos de identificação e confirmação de cadastro do solicitante utilizados pela AC Serasa AC para a geração de novo par de chaves e de seu correspondente novo certificado.

3.3.2 O processo de geração de novo par de chaves poderá ser realizado conforme uma das seguintes possibilidades:
a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2, 3.2.3.
b) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;
c) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido de uma organização, do tipo A3 ou superior, para o qual tenham sido coletados os dados biométricos do responsável pelo certificado, desde que, mantido nessa condição, apresente documento digital verificável por meio de barramento ou aplicação oficial dos entes federativos, que comprove poder de representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;
d) solicitação por meio eletrônico dada nas alíneas 'b' e 'c', acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação a ser editada pela AC-Raiz ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;
e) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico; ou
f) Não se aplica.

3.3.2.1 Não se aplica.

3.3.3 Não existem procedimentos específicos na PC implementada.

3.3.4 Não se aplica.

3.4 Identificação e Autenticação para solicitação de revogação
O solicitante da revogação de certificado deverá ser identificado. Somente os agentes descritos no item 4.9.2 podem solicitar a revogação do certificado da AC Serasa AC.
O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.9.3.
Solicitações de revogação de certificados devem ser registradas.

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 Solicitação do certificado

Neste item da DPC são descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC Serasa AC e suas ARs Vinculadas para as solicitações de emissão de certificado. Esses requisitos e procedimentos compreendem, em detalhes, todas as ações necessárias tanto do indivíduo solicitante quanto da AC Serasa AC e ARs no processo de solicitação de certificado digital. A descrição contempla ainda:
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 de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; e
c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico;
d) o uso de videoconferência, conforme regulamentado pelo DOC-ICP 05.05.

Nota 1: Não se aplica.

Nota 2: na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados SSL, de equipamento, aplicação, 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 deve ser sempre por intermédio da AR.

4.1.1.1 Não se aplica.

4.1.1.2 Não se aplica.

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.

4.1.2.1 Responsabilidades da AC

4.1.2.1.1 A AC Serasa AC responde pelos danos a que der causa.

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

4.1.2.1.3 Não se aplica

4.1.2.2 Obrigações da AC

As obrigações da AC Serasa AC são as abaixo relacionadas:
a) Operar de acordo com esta 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 Raiz, 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 AR a ela vinculadas e de usuários finais;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCRs e, quando aplicável, disponibilizar consulta on-line de situação do certificado (OCSP - On-line Certificate Status Protocol);
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 implementa, 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, e exigir sua manutenção, 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 AR

A AR será responsável pelos danos a que der causa.

4.1.2.4 Obrigações das ARs

As obrigações das ARs vinculadas à AC Serasa AC são as abaixo relacionadas
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 Serasa AC 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 Serasa AC 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 [5];
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 dos itens 3.2.2, 3.2.3 e 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 [5].

4.2 Processamento de Solicitação de Certificado

4.2.1 Execução das funções de identificação e autenticação
A AC Serasa AC e ARs Vinculadas 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 Serasa AC e ARs Vinculadas 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 Serasa AC deve cumprir 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 durante a emissão de um certificado

4.3.1.1 A AC Serasa AC realiza a emissão dos certificados digitais, tomando as precauções do item 3.2 e notifica os requerentes por e-mail logo após a conclusão do processo.

4.3.1.2 O certificado será considerado válido a partir do momento de sua emissão.

4.3.2 Notificações para o titular do certificado pela AC na emissão do certificado
Após a emissão do certificado, a AC Serasa AC envia um e-mail com a confirmação da conclusão do processo de emissão ao titular do certificado.

4.4 Aceitação de Certificado

4.4.1 Conduta sobre a aceitação do certificado
4.4.1.1 A emissão do Certificado Digital pelo seu titular caracteriza sua aceitação. A aceitação implica que o responsável pelo certificado reconhece a veracidade dos dados contidos nele. (No caso do certificado ser emitido para pessoas jurídicas a declaração é feita pela pessoa física responsável pelo certificado).

4.4.1.2 Ao aceitar um SPB ou um Certificado de Pessoa Jurídica, o Titular e o Responsável pelo uso do certificado:
a) Estão de acordo com as responsabilidades continuas, obrigações e deveres impostos a eles pelo Termo de Titularidade e Responsabilidade, pela PC correspondente e por esta DPC;
b) Garantem que por seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;
c) Afirmam que as informações contidas no certificado, fornecidas durante o processo de solicitação, são verdadeiras e foram publicadas dentro do certificado com precisão.

4.4.1.3 Não se aplica.

4.4.2 Publicação do certificado pela AC
O certificado da AC Serasa AC 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 para usuário final opera de acordo com esta Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) implementadas, estabelecidos em conformidade 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 Serasa AC utiliza sua chave privada e garante a proteção dessa chave conforme o previsto desta DPC.

4.5.1.2 Obrigações do Titular do Certificado
Constituem-se obrigações do titular de certificado emitido pela AC Serasa AC, constantes dos termos de titularidade de que trata o item 4.1:
a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação e assumir a responsabilidade pelo custo do processo de emissão do certificado;
b) Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos e utilizar obrigatoriamente senha para proteção da chave privativa do certificado e-CPF e e-CNPJ.
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-Serasa AC, pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e responsabilizar-se por todos os atos praticados perante a AC Serasa AC utilizando o referido certificado e sua correspondente chave privada.
e) informar à AC Serasa AC qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Nota: Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, 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 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
Não se aplica

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 Neste item da DPC, são descritas as circunstâncias nas quais um certificado poderá ser revogado.

4.9.1.2 O certificado deverá obrigatoriamente ser revogado:
a) Quando constatada emissão imprópria ou defeituosa do mesmo;
b) Quando for necessária a alteração de qualquer informação constante no mesmo;
c) No caso de dissolução da AC Serasa AC; ou
d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3 A DPC deve observar ainda que:
a) A AC Serasa AC deverá revogar, no prazo definido no item 4.9.3.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e
b) O CG da ICP-Brasil ou a AC Raiz deverá determinar a revogação do certificado da AC Serasa 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 terá sua validade verificada, na respectiva LCR ou OCSP, 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/OCSP também será confirmada por meio das verificações da assinatura da AC Serasa AC e do período de validade da LCR/OCSP.

4.9.2 Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:
a) Por solicitação do titular do certificado;
b) Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
d) Pela AC Serasa AC;
e) Por uma AR vinculada;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz; ou
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 de certificado deve ser feita através de formulário específico, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita com base na confrontação de dados entre a solicitação de revogação e a solicitação de emissão. Os agentes habilitados, conforme o item 4.9.2, podem facilmente e a qualquer tempo solicitar a revogação de certificados.

4.9.3.2 Como diretrizes gerais, esta DPC estabelece que:
a) O solicitante da revogação de um certificado será identificado;
b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas;
c) As justificativas para a revogação de um certificado serão documentadas; e
d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC Serasa AC.

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 Serasa AC 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 para revogação do Certificado, feita por seu titular, poderá ser realizada a qualquer momento, desde que identificada as circunstâncias definidas pelo item 4.9.1. As definições do procedimento de revogação, reemissão e restituição de valores estão divulgadas nas políticas de desistência e garantia em nosso site: https://serasa.certificadodigital.com.br/.

4.9.4.2 Não se aplica.

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

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC Serasa AC procederá com 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 ou respostas OCSP 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 referente a certificados de usuários finais da AC Serasa AC é de no máximo 6 (seis) horas.

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
A AC Serasa AC dispõe de recursos para verificação on-line de status de certificados. A verificação da situação de um certificado poderá ser feita diretamente na AC Serasa AC, por meio do protocolo OCSP (On-line Certificate Status Protocol).

4.9.10 Requisitos para verificação de revogação on-line
Não há requisitos específicos para a verificação on-line de informações de revogação de certificados por parte das terceiras partes (relying parties).

4.9.11 Outras formas disponíveis para divulgação de revogação
4.9.11.1 Não se aplica.

4.9.11.2 Não se aplica.

4.9.12 Requisitos especiais para o caso de comprometimento de chave
4.9.12.1 Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deverá notificar imediatamente a AC Serasa AC ou a AR vinculada, solicitando a revogação de seu certificado, através do formulário específico para tal fim.

4.9.12.2 O comprometimento ou suspeita de comprometimento de chave deve ser comunicado à AC Serasa AC através do formulário específico para tal fim.

4.9.13 Circunstâncias para suspensão
Não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados de usuários finais.

4.9.14 Quem pode solicitar suspensão
A AC Serasa AC, aprovados pelo Comitê Gestor.

4.9.15 Procedimento para solicitação de suspensão
Os procedimentos de solicitação de suspensão serão dados por norma específica das DPC e PCs associadas.

4.9.16 Limites no período de suspensão
Os períodos de suspensão serão estabelecidos por norma específica das DPC e PCs associadas.

4.10 Serviços de status de certificado

4.10.1 Características operacionais
A AC Serasa AC fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados ou OCSP, 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 Serasa AC, ARs vinculadas, PSS ou PSBios serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], que incluem a divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, transferência da guarda de bases de dados e registros de arquivo.

4.11.2 Os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivo, seguem conforme descritos na alínea 4.11.1 acima.

4.12 Custódia e recuperação de chave

4.12.1 Política e práticas de custódia e recuperação de chave
A AC Serasa AC não realiza práticas e políticas de custódia (escrow) e recuperação de chaves privadas.

4.12.2 Política e práticas de encapsulamento e recuperação de chave de sessão
Não se aplica.

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens seguintes são descritos os controles de segurança implementados pela AC Serasa AC em sua DPC e pelas ARs Vinculadas 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 da DPC são descritos os controles físicos referentes às instalações que abrigam os sistemas da AC Serasa AC 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 da AC Serasa AC 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 AC Serasa AC possui os seguintes controles de segurança física em suas instalações:
a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;
b) Instalações para sistemas de telecomunicações;
c) Sistemas de aterramento e de proteção contra descargas atmosféricas; e
d) Iluminação de emergência.

5.1.2 Acesso físico
A AC Serasa AC possui um sistema de controle de acesso físico, garantindo a segurança de suas instalações, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e os requisitos que seguem.

5.1.2.1 Níveis de acesso
5.1.2.1.1 A AC Serasa AC definiu 4 (quatro) níveis de acesso físico aos diversos ambientes, e 2 (dois) níveis relativos à proteção da chave privada da AC.

5.1.2.1.2 O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC. Para entrar em uma área de nível 1, cada indivíduo deve ser identificado e registrado por segurança armada. 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, a partir do nível 1. 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 – ou nível 2 – é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da 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 – ou nível 3 – situa-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não possuem 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: cartão eletrônico 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, não são admitidos a partir do nível 3.

5.1.2.1.8 No quarto nível – ou nível 4 -, interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC, tais como a emissão e revogação de certificados e a 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 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas 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 das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre – possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10 As salas-cofre são construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas são sanadas por normas internacionais pertinentes.

5.1.2.1.11 Na AC Serasa AC há 1 (um) ambiente de quarto nível para abrigar e segregar, respectivamente:
a) Equipamentos de produção on-line e cofre de armazenamento;
b) Equipamentos de produção off-line e cofre de armazenamento; e
c) Equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

5.1.2.1.12 O quinto nível – ou nível 5 -, interior aos ambientes de nível 4, compreende um cofre ou um gabinete reforçado trancado. Materiais criptográficos, tais como, chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13 Para garantir a segurança do material armazenado, o cofre ou o gabinete obedecem às seguintes especificações mínimas:
a) Ser feito em aço ou material de resistência equivalente; e
b) Possuir tranca com chave.

5.1.2.1.14 O sexto nível – ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da chave privada da AC são armazenados nesses depósitos.

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 devem permitir a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2 As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

5.1.2.2.3 Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente deverão ser monitoradas por sistema de notificação de alarmes. Onde houver, a partir do nível 2, vidros separando níveis de acesso, é implantado um mecanismo de alarme de quebra de vidros, que está ligado ininterruptamente.

5.1.2.2.4 Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais empregados, o critério mínimo de ocupação deixar de ser satisfeito, ocorrerá 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 está localizado em ambiente de nível 3. 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 em um ambiente de nível 4.

5.1.2.4 Mecanismos de emergência

5.1.2.4.1 Mecanismos específicos são implantados pela AC 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 através de relatório de inspeção. 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 é dimensionada com sistemas e dispositivos que garantam o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC e seus respectivos serviços. Um sistema de aterramento é implantado.

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

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

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

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

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

5.1.3.7 O sistema de climatização atende aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante a falhas.

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

5.1.3.9 O sistema de ar condicionando dos ambientes de nível 4 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 é garantida, por meio de:
a) Geradores de porte compatível;
b) Geradores de reserva;
c) Sistemas de no-breaks redundantes; e
d) Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água
A estrutura inteiriça do ambiente de nível 4, 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 é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3 A sala-cofre de nível 4 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 é aberta quando a anterior estiver fechada.

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

5.1.6 Armazenamento de mídia
A AC Serasa AC atende a 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 contenham informações classificadas como sensíveis deverão ser 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, deverão ser fisicamente destruídos.

5.1.8 Instalações de segurança (backup) externas (off-site) para AC
As instalações de *backup* da AC Serasa AC atendem aos requisitos mínimos estabelecidos por este documento. Em caso de sinistro, em que tornem inoperantes as instalações principais, as instalações de *backup* não são atingidas e ficam totalmente operacionais em condições idênticas em, no máximo, 48 (quarenta e oito) horas.

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

5.2.1 Perfis qualificados

5.2.1.1 A AC Serasa AC efetua a 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 Serasa AC estabelece 3 (três) perfis distintos para sua operação, distinguindo as operações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

5.2.1.3 Todos os operadores do sistema de certificação da AC Serasa AC 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, suas permissões de acesso são revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AC, suas permissões de acesso são revistas. Há uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deve devolver à AC Serasa AC no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1 A DPC estabelece o requisito de controle multiusuário para a geração e a utilização da chave privada da AC Serasa AC, 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 requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC poderão ser executadas por um único empregado.

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1 A DPC garante que todo empregado da AC Serasa AC verifica identidade e perfil antes de:

a) Ser incluído em uma lista de acesso às instalações da AC;
b) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC;
c) Receber um certificado para executar suas atividades operacionais na AC; e
d) Receber uma conta no sistema de certificação da AC.

5.2.3.2 Os certificados, contas e senhas utilizados 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 A AC Serasa AC implementa um padrão de utilização de "senhas fortes", definido em sua PS 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 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 da DPC são descritos requisitos e procedimentos, implementados pela AC Serasa AC, pelas ARs e PSSs vinculados 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. Esta DPC garante que todos os empregados da AC, das ARs e PSSs vinculados, encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

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

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo os funcionários da AC Serasa AC e das ARs vinculadas, envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, são admitidos conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

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 Serasa AC e das 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; e
d) Comprovação de escolaridade e de residência.

5.3.2.2 A AC Serasa AC define requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

Todo o pessoal da AC Serasa AC 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 Serasa AC e das ARs vinculadas;
b) Sistema de certificação em uso na AC Serasa AC;
c) Procedimentos de recuperação de desastres e de continuidade do negócio;
d) Reconhecimento de assinaturas e da validade dos documentos apresentados, na forma dos itens 3.2.2 e 3.2.3; e
e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC Serasa AC 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 ou das ARs.

5.3.5 Frequência e sequência de rodízio de cargos

A AC Serasa AC e as ARs vinculadas possuem pessoal e efetivo de contingência devidamente treinado, 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 Serasa AC e das ARs vinculadas, a AC suspenderá, de imediato, 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 operandis*";
b) Identificação dos envolvidos;
c) Eventuais prejuízos causados;
d) Punições aplicadas, se for o caso; e
e) Conclusões.

5.3.6.3 Concluído o processo administrativo, a AC Serasa AC encaminha suas conclusões à AC Raiz.

5.3.6.4 As punições passíveis de aplicação, em decorrência de processo administrativo, são:
a) Advertência;
b) Suspensão por prazo determinado; ou
c) Impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 Requisitos para contratação de pessoal

Todo o pessoal da AC Serasa AC 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 da Serasa AC.

5.3.8 Documentação fornecida ao pessoal

5.3.8.1. A AC Serasa AC torna disponível para todo o seu pessoal:
a) Sua DPC – Serasa AC;
b) As PCs que implementa;

c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];
d) Documentação operacional relativa a 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 Serasa AC e é mantida atualizada.

5.4 Procedimentos de Log de Auditoria
Nos itens seguintes da DPC são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC Serasa AC com o objetivo de manter um ambiente seguro.

5.4.1 Tipos de eventos registrados
5.4.1.1 A AC Serasa AC registra em arquivos de auditoria todos os eventos relacionados a segurança do seu sistema de certificação. Entre outros, os seguintes eventos são obrigatoriamente incluídos 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 Serasa AC registra também, 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 As informações registradas da AC Serasa AC estão descritas no item 5.4.1.2.

5.4.1.4 Todos os registros de auditoria, eletrônicos ou manuais, contêm 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 está armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.1.6 A AC Serasa AC 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 são obrigatoriamente incluídos 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.

5.4.1.6.1 Não se aplica.

5.4.1.7 A AC Serasa AC a que esteja vinculada a AR define, em documento a estar disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

5.4.2 Frequência de auditoria de registros
A periodicidade da análise dos registros de auditoria realizada pelo pessoal operacional da AC Serasa AC é de 1 (uma) semana. Todos os eventos significativos são 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 Serasa AC mantém localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena-os 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. Os acessos lógicos são liberados através da ferramenta nativa do sistema operacional de modo a assegurar o uso apenas a usuários ou processos autorizados.

5.4.4.2 Informações manuais de auditoria são protegidas contra a leitura não autorizada, modificação e remoção através de controles de acesso físico ao local de armazenamento dos registros.

5.4.4.3 Os mecanismos de proteção descritos obedecem à POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.5 Procedimentos para cópia de segurança (Backup) de registros de auditoria
A AC Serasa AC gera a cada semana cópia de backup de seus registros de auditoria, através de procedimentos utilizando conexão segura.

5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)
O sistema de coleta de dados de auditoria é interno à AC Serasa AC e utiliza processos automatizados e manuais.

5.4.7 Notificação de agentes causadores de eventos
Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC Serasa AC, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

5.4.8 Avaliações de vulnerabilidade
Esta DPC assegura que os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC Serasa AC, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC Serasa AC e registradas para fins de auditoria.

5.5 Arquivamento de Registros
Nos itens seguintes desta DPC é descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC Serasa AC e pelas ARs a ela vinculadas.

5.5.1 Tipos de registros arquivados
Os tipos de registros arquivados na AC Serasa AC 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 Serasa AC; e
g) Informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo
Neste item, esta DPC estabelece os períodos de retenção para cada registro arquivado:
a) As LCRs e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
b) Os dossiês dos titulares são retidos 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
Esta DPC estabelece que todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.5.4 Procedimentos de cópia de arquivo
5.5.4.1 Uma segunda cópia de todo o material arquivado será armazenada no site *disaster recovery*, 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 Serasa AC deverá verificar 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 Fonte Confiável de Tempo da AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário da Fonte Confiável de Tempo da AC Raiz, 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 Serasa AC em seus procedimentos operacionais são automatizados e manuais e internos.

5.5.7 Procedimentos para obter e verificar informação de arquivo
A verificação de informação de arquivo deve ser solicitada formalmente à AC Serasa AC 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 30 (trinta dias) antes da data de expiração do certificado digital, as ARs vinculadas comunicam ao seu titular, através do e-mail cadastrado no formulário de solicitação de certificado, a data de expiração do mesmo.

5.6.2 Não existem procedimentos específicos na PC implementada.

5.7 Comprometimento e Recuperação de Desastre
A AC Serasa AC possui um Plano de Continuidade de Negócio (PCN), estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. Esse Plano administra as situações de crise mediante: identificação do motivo da crise, acionamento dos principais responsáveis pelo processo de certificação digital, acionamento das equipes envolvidas na solução do incidente, ação para impedir a continuidade do problema, avaliação da extensão da crise, acionamento da situação de recuperação, ações de recuperação propriamente ditas, notificações à AC Raiz da evolução corretiva e solução, registro da crise e análise para melhoria.

5.7.1 Procedimentos gerenciamento de incidente e comprometimento
5.7.1.1 A AC Serasa AC 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 previstos no PCN das ARs vinculadas para recuperação, total ou parcial das atividades das ARs:
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

Os procedimentos descritos no Plano de Continuidade do Negócio da AC Serasa AC incluem a identificação da crise, acionamento dos principais gestores, acionamento das equipes, contenção da crise, avaliação da extensão da crise, declaração do início das atividades de acionamento da situação de recuperação, notificação da crise, registro da crise, análise para melhoria.

Nas situações de crise relacionadas aos recursos computacionais, software e dados corrompidos ou quando houver suspeita de corrupção dos mesmos, após a identificação da crise ou confirmação da suspeita de corrupção, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de corrupção.

Os procedimentos 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 back-up, conforme detalhado no Manual de Procedimentos de Acionamento de Situação de Recuperação dos Negócios de Certificação Digital.

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 Serasa AC, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, é gerado um novo par de chaves da AC Serasa AC e emitido certificado associado ao novo par de chaves gerado.

5.7.3.2 Chave de entidade é comprometida

Em caso de comprometimento da chave da AC Serasa AC, após a identificação da crise são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da AC Serasa AC e dos usuários finais, é gerado um novo par de chaves, emitido certificado 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, após a identificação da crise são notificados 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, as atividades são transferidas para o site de recuperação de desastre.

5.8 Extinção da AC

Em caso de extinção da AC Serasa AC serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], que incluem a divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, transferência da guarda de bases de dados e registros de arquivo.

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, esta DPC define as medidas de segurança implantadas pela AC Serasa AC para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. Definem também outros controles técnicos de segurança utilizados pela AC 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 O par de chaves criptográficos da AC Serasa AC é gerado pela própria AC, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

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 Serasa AC.

6.1.1.3 Cada PC implementada pela AC Serasa AC define o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos pelo documento 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 Serasa AC é feito por hardware.

6.1.1.5 Cada PC implementada pela AC Serasa AC deve caracterizar 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 Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC Serasa AC são os indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL DOC-ICP-01

6.1.2 Entrega da chave privada à entidade
A geração e a 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 Raiz, encarregada da emissão de seu certificado, a AC Serasa AC fará uso do padrão PKCS#10. Essa entrega é feita por seu representante legal, em cerimônia específica, em data e hora previamente estabelecida.

6.1.3.2 A Os usuários finais enviam suas chaves públicas à AC Serasa AC por meio eletrônico em formato PKCS#10, através de uma sessão segura fixada pelo Secure Socket Layer (SSL). Os procedimentos específicos aplicáveis estão detalhados em cada PC implementada.

6.1.4 Entrega de chave pública da AC às terceiras partes
A AC Serasa AC define as seguintes formas para a disponibilização do certificado, e de todos os certificados da cadeia de certificação, para os usuários e terceiras partes:
a) No momento da disponibilização de um certificado para seu titular; usando formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9];
b) Diretório;
c) Página *web* da AC; e
d) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave
6.1.5.1 A PC implementada pela AC Serasa AC define o tamanho da chave criptográfica associada 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 Serasa AC seguem os padrões definidos no documento DOC-ICP-01.01, NSH-2 homologação da ICP-Brasil ou Certificação INMETRO

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 Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)
6.1.7.1 Os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

6.1.7.2 A chave privada da AC Serasa AC 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
As chaves privadas da AC Serasa AC trafegam cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento.

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1 O módulo criptográfico de geração de chaves assimétricas da AC Serasa AC adota o padrão 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 segue o padrão definido no documento DOC-ICP-01.01, homologação da ICP-Brasil ou Certificação INMETRO.

6.2.2 Controle "n de m" para chave privada

6.2.2.1 A AC Serasa AC estabelece como exigência de controle múltiplo para a utilização das suas chaves privadas:

➢ Número mínimo de 4 ("n") (quatro) pessoas de um grupo de 8 ("m") (oito) pessoas para utilização das suas chaves privadas criadas nas cadeias V0, V1, V2 e V5;

6.2.2.2 As informações desse item estão descritas no item acima.

6.2.3 Custódia (escrow) de chave privada

Não se aplica.

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 Serasa AC mantém cópia de segurança de sua própria chave privada.

6.2.4.3 A AC Serasa AC 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 e mantida pelo prazo de validade do certificado correspondente.

6.2.5 Arquivamento de chave privada

6.2.5.1 Não são arquivadas chaves privadas de assinatura digital.

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

Não se aplica.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8 Método de ativação de chave privada

Para a ativação das chaves privadas exige-se um número mínimo de pessoas. A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. Esse número mínimo é:

a) 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco) pessoas para utilização das suas chaves privadas criadas nas cadeias V0, V1 e V2;

b) 3 ("n") (três) pessoas de um grupo de 6 ("m") (seis) pessoas para utilização das suas chaves privadas criadas na cadeia V5.

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 desativação de chave privada

A chave privada da AC Serasa AC está instalada em ambiente físico com nível de segurança 4, onde só é permitido o acesso por pelo menos 2 funcionários autorizados. Sua desativação é feita por meio de comandos

executados por funcionários de confiança, identificados e autorizados através de mecanismos nativos do sistema operacional.

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
Para a destruição das chaves privadas da AC Serasa AC exige-se um número mínimo de pessoas. A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. Esse número mínimo é:
a) 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco) pessoas para utilização das suas chaves privadas criadas nas cadeias V0, V1 e V2;
b) 3 (“n”) (três) pessoas de um grupo de 6 (“m”) (seis) pessoas para utilização das suas chaves privadas criadas na cadeia V5.
As mídias de armazenamento das chaves privadas são reinicializadas de forma a não restarem nelas informações sensíveis.

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 Serasa AC e dos titulares de certificados de assinatura digital por ela emitidos permanecem armazenadas 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 da AC Serasa AC responsável pela DPC e dos titulares de certificados de assinatura digital por ela emitidos define que serão utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

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

6.3.2.4 A validade admitida para certificados de AC 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
Nos itens seguintes da DPC, são descritos os requisitos gerais 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. Cada PC implementada deve descrever os requisitos específicos aplicáveis.

6.4.1 Geração e instalação dos dados de ativação
6.4.1.1 Os dados de ativação da chave privada da AC Serasa AC são únicos e aleatórios.

6.4.1.2 Cada PC implementada deve garantir que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão únicos e aleatórios.

6.4.2 Proteção dos dados de ativação
6.4.2.1 Os dados de ativação da chave privada da AC Serasa AC são protegidos contra uso não autorizado, por meio de mecanismos de criptografia e de controle de acesso físico.

6.4.2.2 Cada PC implementada deve garantir que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão protegidos contra 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 Serasa AC é realizada *off-line,* para impedir o acesso remoto não autorizado.

6.5.1.2 Os requisitos de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC Serasa AC são descritos em cada PC implementada.

6.5.1.3 Cada computador servidor da AC Serasa AC, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes características:
a) Controle de acesso aos serviços e perfis da AC;
b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC;
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;
e) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) Mecanismos para cópias de segurança (*backup*).

6.5.1.4 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 Serasa AC, 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 Serasa AC. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6 Qualquer equipamento incorporado à AC Serasa AC é preparado e configurado como previsto na Política de Segurança 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 Serasa AC segue as recomendações do Trusted System Evaluation Criteria (TCSEC).

6.5.3 Controles de Segurança para as Autoridades de Registro

6.5.3.1 A AC Serasa AC 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, pelo menos, os requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

6.5.3.3 Não se aplica.

6.6 Controles Técnicos do Ciclo de Vida

Nos itens seguintes da DPC são descritos, quando aplicáveis, os controles implementados pela AC Serasa AC 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 Serasa AC adota tecnologias de certificação digital e efetua as devidas customizações para adequar as necessidades do ambiente da AC, os quais são desenvolvidos por Analistas de Suporte, todos empregados de confiança. Estas customizações são realizadas inicialmente em um ambiente de

desenvolvimento e após concluído é colocado em um ambiente de homologação. Finalizado o processo de homologação é encaminhado um pedido para a "Gerência de Mudança" que é coordenada pelo Gestor do Processo de Certificação Digital e é composto de outras áreas da Serasa, como por exemplo Segurança de Sistemas de Informação, Produção, etc., que avaliam e decidem quanto a sua implementação.

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

6.6.2 Controles de gerenciamento de segurança
6.6.2.1 A AC Serasa AC utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação da AC.

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

6.6.3 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 Serasa AC 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 Neste item da DPC são descritos os controles relativos à segurança da rede da AC Serasa AC, incluindo *firewalls* e recursos similares.

6.7.1.2 Nos servidores do sistema de certificação da AC, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.

6.7.1.3 Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewalls* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC, estão localizados e operam em ambiente de nível, no mínimo, 4.

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

6.7.1.5 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 Mecanismos de *firewall* são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Um *firewall* promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC.

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

6.7.3 Sistema de detecção de intrusão (IDS)
6.7.3.1 O sistema de detecção de intrusão possui capacidade de ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar *traps SNMP*,executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall*

ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

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

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

6.7.4 Registro de acessos não autorizados à rede
As tentativas de acesso não autorizado – em roteadores, firewalls ou IDS – são registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro deverá ser, no mínimo, diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 Carimbo de Tempo

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 Perfil do Certificado
Todos os certificados emitidos pela AC Serasa AC estão em conformidade com o formato definido pelo padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.1 Número de versão
Todos os certificados emitidos pela AC Serasa AC implementam a versão 3.

7.1.2 Extensões de certificado
Não se aplica.

7.1.3 Identificadores de algoritmo
Não se aplica.

7.1.4 Formatos de nome
7.1.4.1 Não se aplica.

7.1.5 Restrições de nome
Não se aplica.

7.1.6 OID (Object Identifier) da DPC
O OID da DPC- AC Serasa AC é 2.16.76.1.1.4

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 as extensões críticas de PC
Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número(s) de versão
As LCRs geradas pela AC Serasa AC 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 LCRs utilizadas pela AC Serasa AC e sua criticalidade são as mesmas do item 7.2.2.2.

7.2.2.2 A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:
a) "***Authority Key Identifier***": deve conter o *hash* SHA-1 da chave pública da AC que assina a LCR; e
b) "***CRL Number***", **não crítica**: deve conter um número seqüencial para cada LCR emitida pela AC.

7.3 Perfil de OCSP

7.3.1 Número(s) de versão

Serviços de respostas OCSP implementam a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2 Extensões de OCSP

Os serviços de respostas OCSP da AC Serasa AC estão em conformidade com a RFC 6960.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 Frequência e circunstâncias das avaliações

As entidades integrantes da ICP-Brasil sofrem 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 Serasa AC recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil, sendo 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 AC Serasa AC informa que suas entidades vinculadas da ICP-Brasil (AC, AR e PSS), também receberam auditoria prévia para fins de credenciamento, sendo 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
Em 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
Em 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
As tarifas de emissão e de renovação de certificado pela AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [13].

9.1.2 Tarifas de acesso ao certificado
Não se aplica.

9.1.3 Tarifas de revogação ou de acesso à informação de status
Não há tarifa de revogação ou de acesso à informação de status de certificado.

9.1.4 Tarifas para outros serviços
Tarifas para outros serviços da AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [13].

9.1.5 Política de reembolso
Não se aplica.

9.2 Responsabilidade Financeira
A responsabilidade da AC será verificada conforme previsto na legislação brasileira.

9.2.1 Cobertura do seguro
Conforme item 4 desta DPC.

9.2.2 Outros ativos
Conforme regramento desta DPC.

9.2.3 Cobertura de seguros ou garantia para entidades finais
Conforme item 4 desta DPC.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais
9.3.1.1 Neste item são identificados os tipos de informações consideradas sigilosas pela AC Serasa AC e pelas ARs a ela vinculadas, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.3.1.2 Como princípio geral, nenhum documento, informação ou registro fornecido à AC Serasa AC ou às ARs vinculadas deve ser divulgado.

9.3.2 Informações fora do escopo de informações confidenciais
Não são considerados como informações sigilosas pela AC Serasa AC e pelas ARs vinculadas:
a) os certificados e as LCRs/OCSP emitidos pela AC Serasa AC;
b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
c) as PCs implementadas pela AC Serasa AC;
d) esta DPC-Serasa AC;
e) versões públicas de PS; e

f) a conclusão dos relatórios de auditoria.

9.3.2.1 Certificados, LCR/OCSP, 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 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 Serasa AC também 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 A AC Serasa AC e todas as entidades da ICP Brasil a ela vinculadas possui mecanismos para assegurar a proteção e a confidencialidade de todos os participantes que possuem ou tiveram acesso a informações confidenciais, 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 Serasa AC foi gerada e mantida pela própria AC, sendo responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura é de responsabilidade da AC Serasa AC.

9.3.3.3 A AC Serasa AC informa que as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas são de responsabilidade dos titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações. Além disso, são responsáveis também 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 Serasa AC 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 AC Serasa AC 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 da AC Serasa AC são fornecidas na LCR/OCSP da AC.

9.4.4 Responsabilidade para proteger a informação privadas
A AC e AR são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5 Aviso e consentimento para usar informações privadas
As informações privadas obtidas pela AC podem ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável.
O titular de certificado e seu representante legal possuem amplo acesso a quaisquer dos seus próprios dados e identificações, e podem autorizar a divulgação de seus registros a outras pessoas. Autorizações formais podem ser apresentadas de duas formas:
a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou
b) por meio de pedido escrito com firma reconhecida.

9.4.6 Divulgação em processo judicial ou administrativo
Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC é fornecido a qualquer pessoa, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.

As informações privadas ou confidenciais sob a guarda da AC podem 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
Este item da DPC estabelece como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AR ou da AC Serasa AC 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 Direitos de Propriedade Intelectual
De acordo com a legislação vigente.

9.6 Declarações e Garantias

9.6.1 Declarações e Garantias da AC

A AC Serasa AC declara e garante o quanto segue:

9.6.1.1 Autorização para certificado
A AC Serasa AC implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC. A AC, 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 Serasa AC 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 Serasa AC 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 ARs Vinculadas na forma de suas DPCs, PCs e normas complementares.

9.6.1.4 Consentimento dos titulares
A AC Serasa AC implementa termos de consentimento ou titularidade, contidas nos itens 3 e 4 desta DPC.

9.6.1.5 Serviço
A AC Serasa AC mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios, das ACs subsequentes e LCRs/OCSP.

9.6.1.6 Revogação
A AC Serasa AC 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 Serasa AC, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6.3.2 A AC Serasa AC irá informar a 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 Serasa AC é considerado válido quando:
i. tiver sido emitido pela AC;
ii. não constar como revogado pela AC;
iii. não estiver expirado; e
iv. puder ser verificado com o uso do certificado válido da AC.

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 Serasa AC 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 Serasa AC 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.

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 Deve também ser estabelecido que a DPC da AC Serasa AC 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 Serasa AC 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 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 http://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 PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[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
[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 http://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 ARs DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL	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]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA 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 http://www.iti.gov.br .

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

11 REFERÊNCIAS BIBLIOGRÁFICAS

[5] WebTrust Principles and Criteria for Registration Authorities, disponível em http://www.webtrust.org.