V/ Cert

Política de Certificado SE-S da Autoridade Certificadora VALID BRASIL (PC SE-S da AC VALID BRASIL)

OID 2.16.76.1.2.201.9
Versão 1.0
Novembro 2024

Sumário

CONTROLE DE ALTERAÇÕES:

Versão	Data	Resolução que aprova a alteração	Item Alterado	Descrição da Alteração
1.0	19/11/2024	Resolução 211	Diversos	Criação da Política de Certificado Digital de Selo Eletrônico em Software - PC SE-S

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 Está "Política de Certificado" (PC) descreve as políticas de certificação de certificados de Assinatura Digital Tipo SE-S da Autoridade Certificadora VALID BRASIL na Infraestrutura de Chaves Públicas Brasileira.

1.1.2 A estrutura desta PC está baseada no DOC-ICP-04– REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-Brasil.

1.1.3 A estrutura desta PC está baseada na RFC 3647.

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

1.1.5. O tipo de certificado emitido sob esta PC é o Tipo SE-S.

1.1.6. Não se aplica.

1.1.7. Certificados do tipo SE-S são certificados de selo eletrônico, respectivamente em software, e devem ser emitidos apenas para pessoas jurídicas.

1.1.8. Não se aplica.
1.1.9. Não se aplica.
1.1.10. Não se aplica.
1.1.11. Não se aplica.

1.1.12. Outros tipos de certificado, além dos anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescidas aos tipos de certificados aceitos pela ICP-Brasil.

1.2. Nome do Documento e Identificação

1.2.1. Esta PC é chamada Política de Certificado de Assinatura Digital, Tipo A3, da Autoridade Certificadora da VALID BRASIL. O OID (*Object Identifier*) atribuído para esta PC, após processo de credenciamento da AC junto à ICP-Brasil, é: ***2.16.76.1.2.201.9.***

1.2.2. A PC possui o OID 2.16.76.1.2.201.9.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC é implementada pela Autoridade Certificadora AC VALID BRASIL, integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora AC VALID, que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira.

1.3.1.2. As práticas e procedimentos de certificação utilizados pela AC VALID BRASIL estão descritas em sua Declaração de Práticas de Certificação (DPC da AC VALID BRASIL) que se encontra publicada no seu repositório, no seguinte endereço: http://icp-brasil.validcertificadora.com.br/ac-validbrasil/dpc-ac-validbrasilv12.pdf

1.3.2. Autoridades de Registro

1.3.2.1. A AC VALID BRASIL mantém página web e/ou diretório com endereço: https://validcertificadora.com.br/pages/repositorio onde estão publicados os seguintes dados, referentes às Autoridades de Registro (ARs) que realizam os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

a) relação de todas as ARs credenciadas;
b) relação de AR que tenham se descredenciado da cadeia da AC VALID BRASIL, com respectiva data do descredenciamento.

1.3.2.2. A AC VALID BRASIL mantém as informações acima sempre atualizadas.

1.3.3 Titulares de Certificado

Os titulares dos certificados emitidos nesta PC são pessoas jurídicas de direito público ou privado, nacionais ou estrangeiras, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis, podem ser Titulares de Certificado. O titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada. Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.4. Partes Confiáveis

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

1.3.5. Outros Participantes

A relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC VALID BRASIL e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC VALID BRASIL https://validcertificadora.com.br/pages/repositorio.

1.4. Usabilidade do Certificado

1.4.1 Uso Apropriado do Certificado

1.4.1.1. Neste item são relacionadas as aplicações para as quais os certificados definidos nesta PC são adequados.

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

1.4.1.3. A AC VALID BRASIL leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

Os certificados emitidos pela AC VALID BRASIL no âmbito desta PC podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.4. Não se aplica.

1.4.1.5. Certificados do tipo SE-S são utilizados para garantir origem e integridade de um documento eletrônico, servindo de prova da emissão do documento por uma pessoa jurídica.

1.4.1.6. Não se aplica.
1.4.1.7. Não se aplica.
1.4.1.8. Não se aplica.
1.4.1.9. Não se aplica.

1.4.2. Uso Proibitivo do Certificado

1.4.2.1. É proibido o uso do certificado de aplicações específicas com a finalidade de autenticação de servidor (SSL/TLS) destinado ao reconhecimento confiável pelos navegadores de internet (browsers).
1.4.2.2. Não se aplica.
1.4.2.3. Não se aplica.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

Nome da AC: AC VALID BRASIL

1.5.2. Contatos

Endereço: Alameda Rio Claro, 241 - Bela Vista - São Paulo, SP -
CEP: 01332-010
Telefone: (011) 3004-6363
Página Web: http://www.validcertificadora.com.br
E-mail: pki.compliance@valid.com

1.5.3. Pessoa que determina a adequabilidade da DPC com a PC

Nome: Kamila Burunsizian Marciano
E-mail: pki.compliance@valid.com
Telefone: (011) 3004-6363

1.5.4 Procedimentos para aprovação da PC

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

1.6. Definição e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environmen
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
AGR	Agente de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas

CPF	Cadastro de Pessoas Físicas
CS	Code Signing
CSR	Certificate Signing Request
DETRAN	Departamento Nacional de Trânsito
DN	*Distinguished Name*
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	*International Electrotechnical Commission*
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITSEC	Information Technology Security Evaluation Criteria
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	*Online 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	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIN	Personal Identification Number
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
PUK	PIN Unbloking Key
RFC	*Request For Comments*
RG	Registro Geral
SAT	Sistema Autenticador e Transmisso
SIGEPE	Sistema de Gestão de Pessoal da Administração Pública Federal

SNMP	Simple Network Management Protocol
SSL	*Secure Socket Layer*
TCSEC	Trusted System Evaluation Criteria
TLS	Transport Layer Security
TSDM	Trusted Software Development Methodology
TSE	Tribunal Superior Eleitoral
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC VALID BRASIL.

2.1. Repositórios
2.2. Publicação de informações dos certificados
2.3. Tempo ou Frequência de Publicação
2.4. Controle de Acesso aos Repositórios

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC VALID BRASIL.

3.1. Nomeação
3.1.1. Tipos de nomes
3.1.2. Necessidade de nomes significativos
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado
3.1.4. Regras para interpretação de vários tipos de nomes
3.1.5. Unicidade de nomes
3.1.6. Procedimento para resolver disputa de nomes
3.1.7. Reconhecimento, autenticação e papel de marcas registradas
3.2. Validação Inicial de Identidade
3.2.1. Método para comprovar a posse de chave privada
3.2.2. Autenticação da identificação da organização
3.2.3. Autenticação da identidade de equipamento ou aplicação
3.2.4. Autenticação da identidade de um indivíduo
3.2.5. Informações não verificadas do titular do certificado
3.2.6. Validação das autoridades
3.2.7. Critérios para interoperação
3.3. Identificação e autenticação para pedidos de novas chaves
3.3.1. Identificação e autenticação para rotina de novas chaves
3.3.2. Identificação e autenticação para novas chaves após a revogação
3.4. Identificação e Autenticação para solicitação de revogação

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC VALID BRASIL.

4.1. Solicitação do certificado
4.1.1. Quem pode submeter uma solicitação de certificado
4.1.2. Processo de registro e responsabilidades
4.2. Processamento de Solicitação de Certificado
4.2.1. Execução das funções de identificação e autenticação
4.2.2. Aprovação ou rejeição de pedidos de certificado
4.2.3. Tempo para processar a solicitação de certificado
4.3. Emissão de Certificado
4.3.1. Ações da AC durante a emissão de um certificado
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado
4.4. Aceitação de Certificado
4.4.1. Conduta sobre a aceitação do certificado
4.4.2. Publicação do certificado pela AC
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades
4.5. Usabilidade do par de chaves e do certificado
4.5.1. Usabilidade da Chave privada e do certificado do titular
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis
4.6. Renovação de Certificados
4.6.1. Circunstâncias para renovação de certificados
4.6.2. Quem pode solicitar a renovação
4.6.3. Processamento de requisição para renovação de certificados
4.6.4. Notificação para nova emissão de certificado para o titular
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado
4.6.6. Publicação de uma renovação de um certificado pela AC
4.6.7. Notificação de emissão de certificado pela AC para outras entidades
4.7. Nova chave de certificado
4.7.1. Circunstâncias para nova chave de certificado
4.7.2. Quem pode requisitar a certificação de uma nova chave pública
4.7.3. Processamento de requisição de novas chaves de certificado
4.7.4. Notificação de emissão de novo certificado para o titular
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada
4.7.6. Publicação de uma nova chave certificada pela AC
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades
4.8. Modificação de certificado
4.8.1. Circunstâncias para modificação de certificado

5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade

5.7.4. Capacidade de continuidade de negócio após desastre

5.8. Extinção da AC

6. CONTROLES TÉCNICOS DE SEGURANÇA

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

6.1. Geração e Instalação do par de chaves

6.1.1. Geração do par de chaves

6.1.1.1. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1. Não se aplica.

6.1.1.1.2. Não se aplica

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) existente na estação do solicitante apresentado pelo browser e, quando da geração, a chave privada é armazenada no HD da estação.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados adota o padrão RSA conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado SE-S.

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

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

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

6.1.1.7. Esta mídia de armazenamento não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8. O tipo de certificado emitido pela AC VALID BRASIL e descrito nesta PC é o SE-S.

TIPO DE CERTIFICADO	MÍDIA ARMAZENADORA DE CHAVE CRIPTOGRÁFICA (Requisitos Mínimos)
SE-S	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima.

Nota: A responsabilidade pela segurança na garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do titular ou responsável pelo uso do certificado, conforme especificado no Termo de Titularidade.

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC VALID BRASIL por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC VALID BRASIL. A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital, realizada com a chave privada correspondente à chave pública contida na solicitação.

A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - *Secure Socket Layer*

6.1.4. Entrega de chave pública da AC às terceiras partes

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC VALID BRASIL, compreendem:

A AC VALID BRASIL disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço *Web* https://validcertificadora.com.br/pages/repositorio:

a) página *web* da AC VALID BRASIL;

b) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Os certificados emitidos de acordo com esta PC situam-se sob a cadeia da Autoridade Certificadora Raiz Brasileira (V12). O tamanho das chaves criptográficas associadas é de 2048 bits.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo SE-S da ICP-Brasil está em conformidade com o definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [1]

6.1.6 Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros

Os parâmetros de geração de chaves assimétricas da AC VALID BRASIL seguem o padrão de Homologação da ICP-Brasil ou Certificação INMETRO, em conformidade ao estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.7 Propósitos de uso de chave (conforme o campo "*key usage*" na X.509 v3)

Os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment. Os pares de chaves correspondentes aos certificados emitidos pela AC VALID BRASIL podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves.

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

Nos itens seguintes, a PC define os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos pela AC VALID BRASIL.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. Não se aplica

6.2.1.2. Os requisitos aplicáveis ao módulo criptográfico utilizado para geração de chaves criptográficas dos titulares de certificado seguem os definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.2. Controle “n de m” para chave privada

Não se aplica.

6.2.3. Custódia (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4. Cópia de segurança (*backup*) de chave privada

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

6.2.4.2. A AC VALID BRASIL responsável por esta PC não mantém cópia de segurança de chave privada de titular.

6.2.4.3. A cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1] e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. Não se aplica.

6.2.5 Arquivamento de chave privada

6.2.5.1. Não se aplica, uma vez que a ICP-Brasil não admite o arquivamento de 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
A chave privada é ativada mediante senha solicitada pelo software de proteção da chave privada.

6.2.9. Método de desativação de chave privada
Cada entidade titular de certificado pode definir os procedimentos necessários para a desativação da sua chave privada.

6.2.10. Método de destruição de chave privada
Cada entidade titular de certificado pode definir os procedimentos necessários para a destruição da sua chave privada.

6.3 Outros Aspectos do Gerenciamento do par de chaves
6.3.1 Arquivamento de chave pública
As chaves públicas da AC VALID BRASIL, de titulares dos certificados de assinatura digital e as *LCRs* emitidas pela AC VALID BRASIL são armazenadas permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada
6.3.2.1. As chaves privadas dos respectivos Titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. Certificados do tipo SE-S previstos nesta PC podem ter a validade de minutos, horas, dias e até 1 (um) ano.

6.3.2.4. Não se aplica.
6.3.2.5. Não se aplica.

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

6.4.1 Geração e instalação dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

6.4.2 Proteção dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são 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

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. O equipamento onde são gerados os pares de chaves criptográficas do titular do Certificado deve dispor de mecanismos mínimos que garantam a segurança computacional, com proteção antivírus e criptografia 3DES para a chave privada, armazenada no HD.

6.5.2 Classificação da segurança computacional

Não se aplica.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

Não se aplica.

6.6.1. Controles de desenvolvimento de sistema

A AC VALID BRASIL utiliza os modelos clássico espiral e SCRUM no desenvolvimento dos sistemas, de acordo com a melhor adequação destes modelos ao projeto em desenvolvimento. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC VALID BRASIL utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos.

Os processos de projeto e desenvolvimento conduzidos pela AC VALID BRASIL proveem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC VALID BRASIL.

6.6.2 Controles de gerenciamento de segurança

A AC VALID BRASIL verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as

configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

A AC VALID BRASIL utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3 Classificações de segurança de ciclo de vida
Não se aplica.

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

6.7. Controles de Segurança de Rede
Não se aplica.

6.8 Carimbo de Tempo
Não se aplica.

7. PERFIS DE CERTIFICADO E LCR E OCSP
Os itens seguintes especificam os formatos dos certificados e das LCR/ OCSP gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1 Perfil do Certificado
Todos os certificados emitidos pela AC VALID BRASIL estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 Número de versão
Todos os certificados emitidos pela AC VALID BRASIL, segundo esta PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado
7.1.2.1. A AC VALID BRASIL implementa todas as extensões de certificado utilizadas e sua criticalidade, conforme especificado na Tabela de Perfis de Certificado e LCR, anexo I deste documento.

7.1.2.2. Os campos otherName devem estar de acordo com as seguintes especificações:

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

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

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

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

7.1.3. Identificadores de algoritmo

Certificados emitidos pela AC VALID BRASIL são assinados com o uso do algoritmo RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11), conforme o padrão PKCS#1, observados os algoritmos admitidos no âmbito da ICP-Brasil, documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

7.1.4 Formatos de nome

7.1.4.1. O nome do titular do certificado, constante do campo “Subject”, deverá adotar o “Distinguished Name” (DN) do padrão ITU X.500/ISO 9594, conforme especificado na Tabela de Perfis de Certificado e LCR, anexo I deste documento.

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

7.1.5. Restrições de nome

7.1.5.1. Neste item da PC, são descritas as restrições aplicáveis para os nomes dos titulares de certificados.

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

a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e
b) além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

CARACTERE	CÓDIGO NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*****	2ª
+	2B
,	2C
-	2D
.	2E
/	2F

:	3ª
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6 OID (*Object Identifier*) de Política de Certificado

O OID atribuído a esta Política de Certificado é: ***2.16.76.1.2.201.9.***

7.1.7 Uso da extensão "*Policy Constraints*"

Não se aplica.

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo ***policyQualifiers*** da extensão "*Certificate Policies*" contém o endereço da página *Web* (URL) com a DPC da AC VALID BRASIL, sendo: http://icp-brasil.validcertificadora.com.br/ac-validbrasil/dpc-ac-validbrasilv12.pdf

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são ser interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número de versão

As LCRs geradas pela AC VALID BRASIL segundo a PC, implementam a versão 2 de LCR definida no 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. A AC VALID BRASIL implementa todas as extensões de LCR utilizadas e sua criticalidade, conforme especificado na Tabela de Perfis de Certificado e LCR, anexo I deste documento.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

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

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes da DPC da AC VALID BRASIL.

8.1. Frequência e circunstâncias das avaliações
8.2. Identificação/Qualificação do avaliador
8.3. Relação do avaliador com a entidade avaliada
8.4. Tópicos cobertos pela avaliação
8.5. Ações tomadas como resultado de uma deficiência
8.6. Comunicação dos resultados

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC VALID BRASIL.

9.1. Tarifas
9.1.1. Tarifas de emissão e renovação de certificados
9.1.2. Tarifas de acesso ao certificado
9.1.3. Tarifas de revogação ou de acesso à informação de status
9.1.4. Tarifas para outros serviços
9.1.5. Política de reembolso
9.2. Responsabilidade Financeira
9.2.1. Cobertura do seguro
9.2.2. Outros ativos
9.2.3. Cobertura de seguros ou garantia para entidades finais
9.3. Confidencialidade da informação do negócio
9.3.1. Escopo de informações confidenciais
9.3.2. Informações fora do escopo de informações confidenciais
9.3.3. Responsabilidade em proteger a informação confidencial
9.4. Privacidade da informação pessoal
9.4.1. Plano de privacidade
9.4.2. Tratamento de informação como privadas
9.4.3. Informações não consideradas privadas
9.4.4. Responsabilidade para proteger a informação privadas
9.4.5. Aviso e consentimento para usar informações privadas
9.4.6. Divulgação em processo judicial ou administrativo
9.4.7. Outras circunstâncias de divulgação de informação

9.5. Direitos de Propriedade Intelectual

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da AC

9.6.2. Declarações e Garantias da AR

9.6.3. Declarações e garantias do titular

9.6.4. Declarações e garantias das terceiras partes

9.6.5. Representações e garantias de outros participantes

9.7. Isenção de garantias

9.8. Limitações de responsabilidades

9.9. Indenizações

9.10. Prazo e Rescisão

9.10.1. Prazo

9.10.2. Término

9.10.3. Efeito da rescisão e sobrevivência

9.11. Avisos individuais e comunicações com os participantes

9.12. Alterações

9.12.1. Procedimento para emendas

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC VALID BRASIL. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Procedimento para emendas

A AC VALID BRASIL mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço *Web:* http://icp-brasil.validcertificadora.com.br/ac-validbrasil/pcSE-S-ac-validbrasil.pdf

9.12.3. Procedimento para emendas

9.13. Solução de conflitos

9.14. Lei aplicável

9.15. Conformidade com a Lei aplicável

9.16. Disposições Diversas

9.16.1. Acordo completo

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

9.17. Outras provisões

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC VALID BRASIL, conforme o estabelecido no documento CRITÉRIOS E

PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desse processo, além da conformidade com este documento, deverá ser verificada a compatibilidade entre a PC e a DPC da AC VALID BRASIL.

10. DOCUMENTOS REFERENCIADOS

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL Aprovado pela Resolução nº 132, de 10 de novembro de 2017	DOC-ICP-17
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	DOC-ICP-12
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

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]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01

11 REFERÊNCIAS BIBLIOGRÁFICAS

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

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

RFC 2818, IETF - HTTP Over TLS, may 2000.

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.

Anexo I

Tabela de Perfis de Certificado e LCR

Detalhamento dos campos e extensões dos Certificados de Selo Eletrônico para Pessoa Jurídica

Campo	Valor	Presença	Criticalidade	Comentário/Referência
1. Versão	3 (0x2)	O	-	
2. Número de série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos	O	-	
3. Algoritmo de assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
4. Emissor	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Emitente>	O	-	
5. Período de validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo Time, conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	**C** = BR **O** = ICP-Brasil **CN** = <Razão Social> **SerialNumber** = <número CNPJ>	O	-	Outros atributos poderão ser utilizados na forma e propósitos definidos conforme RFC5280.
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01

8. Extensões X.509v3		-	-	Outros campos de extensão poderão ser utilizados na forma e propósitos definidos conforme RFC5280.
8.1. Authority Key Identifier	Hash 160 bits SHA-1 da chave pública da AC VALID BRASIL que emite o certificado	O	não-critica	
8.2. Subject Key Identifier	Hash 160 bits SHA-1 da chave pública da AC titular do certificado	O	não-critica	
8.3. Key Usage	digitalSignature	O	critica	
	keyEncipherment	P		
	nonRepudiation	P		
8.4. Certificate Policies	PolicyIdentifier especificando o OID da PC correspondente ao certificado: Policyqualifiers OID 1.3.6.1.5.5.7.2.1 cPSuri: URI do endereço web da DPC da AC emitente: http://icp-brasil.validcertificadora.com.br/ac-validbrasil/dpc-ac-validbrasilv12.pdf	O	não-critica	
8.5. Subject Alternative Name	OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado	O*	não-critica	(*) A obrigatoriedade com restrição implica recomendação de manutenção desse otherName de forma provisória, até 31/12/2028, com o propósito de possibilitar que todas as aplicações possam ser ajustadas para obtenção dessa informação pelo atributo serialNumber (OID 2.5.4.5), do campo DN do titular. Após 31/12/2028, fica opcional o uso desse otherName.
8.6. Basic Constraints	cA = False	O	critica	
	Client authentication OID = 1.3.6.1.5.5.7.3.2	O		

8.7. Extended Key Usage	E-mail protection OID = 1.3.6.1.5.5.7.3.4	P	não-critica	
8.8. CRL Distribution Points	*DistributionPointName* do tipo URI contendo HTTP URL do serviço de LCR da AC VALID BRASIL emissora desse certificado: http://icp-brasil.validcertificadora.com.br/ac-validbrasil/lcr-ac-validbrasilv12.crl http://icp-brasil2.validcertificadora.com.br/ac-va/lidbrasil/lcr-ac-validbrasilv12.crl	O	não-critica	Deve conter mais de uma entrada para endereços onde se obtém a LCR.
	reasons	N		
	cRLIssuer	N		
8.9. Authority Information Access	id-ad-calssuer do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado: http://icp-brasil.validcertificadora.com.br/ac-validbrasil/ac-validbrasilv12.p7b	O	não-crítica	
	id-ad-ocsp do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado: http://ocspv12.validcertificadora.com.br	P		
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICPBrasil– DOC-ICP-01.01.	O	-	DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (bit string).	O	-	

Legenda: O = Obrigatório, P = Permitido e N = Não permitido