DIGITALSIGN CERTIFICAÇÃO DIGITAL LTDA.
(AC DIGITALSIGN RFB)

POLÍTICA DE CERTIFICADO DE ASSINATURA DIGITAL
== TIPO A3 ==

VERSÃO 6.0 – 11/01/2022

HISTÓRICO DE VERSÕES

Data	*Versão*	*Observações*
25/07/2012	0.0	Redação Inicial
30/01/2013	1.0	Revisão
25/06/2013	1.1	Revisão
22/10/2014	2.0	Revisão
14/07/2015	2.1	Revisão
19/10/2018	2.2	Revisão
25/02/2019	2.3	Revisão
10/04/2019	2.4	Revisão
07/04/2020	3.0	Adequações às Resoluções nº 151, 154 e 155
29/06/2020	4.0	Adequações às Resoluções nº 156 e 169
30/10/2020	5.0	Adequações à Resolução nº 179
11/01/2022	6.0	Adequações às Resoluções nº 196 e 197

AVISO LEGAL

Copyright © DigitalSign Certificação Digital LTDA. Todos os direitos reservados.
DigitalSign é uma marca registrada da DigitalSign Certificação Digital LTDA. Todas as restantes marcas, trademarks e service marks são propriedade dos seus respectivos detentores.

É expressamente proibida a reprodução, total ou parcial, do conteúdo deste documento, sem prévia autorização escrita emitida pela DigitalSign.

Qualquer dúvida ou pedido de informação relativamente ao conteúdo deste documento deverá ser dirigido a suporte@digitalsigncertificadora.com.br.

CONTEÚDO

1. Introdução 11
1.1. Visão Geral 11
1.2. Nome do documento e identificação 11
1.3. Participantes da ICP-Brasil 11
1.3.1. Autoridades Certificadoras 11
1.3.2. Autoridades de Registro 12
1.3.3. Titulares de Certificado 12
1.3.4. Partes Confiáveis 12
1.3.5. Outros Participantes 12
1.4. Usabilidade do Certificado 12
1.4.1. Uso apropriado do certificado 12
1.4.2. Uso proibitivo do certificado 13
1.5. Política de Administração 13
1.5.1. Organização administrativa do documento 13
1.5.2. Contatos 13
1.5.3. Pessoa que determina a adequabilidade da DPC com a PC 13
1.5.4. Procedimentos de aprovação da PC 13
1.6. Definições e Acrônimos 14
2. Responsabilidades de Publicação e Repositório 16
2.1. Repositórios 16
2.2. Publicação de informações dos certificados 16
2.3. Tempo e Frequência de publicação 16
2.4. Controle de acesso aos repositórios 16
3. Identificação e Autenticação 17
3.1. Nomeação 17
3.1.1. Tipos de nomes 17
3.1.2. Necessidade dos nomes serem significativos 17
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado 17
3.1.4. Regras para interpretação de vários tipos de nomes 17
3.1.5. Unicidade de nomes 17
3.1.6. Procedimento para resolver disputa de nomes 17
3.1.7. Reconhecimento, autenticação e papel de marcas registradas 17
3.2. Validação inicial de identidade 17
3.2.1. Método para comprovar a posse de chave privada 17
3.2.2. Autenticação da identificação da organização 17
3.2.3. Autenticação da identidade de equipamento ou aplicação 17
3.2.4. Autenticação da identidade de um indivíduo 17

3.2.5. Informações não verificadas do titular do certificado 17
3.2.6. Validação das autoridades 17
3.2.7. Critérios para interoperação 17
3.3. Identificação e autenticação para pedidos de novas chaves 17
3.3.1. Identificação e autenticação para rotina de novas chaves 17
3.3.2. Identificação e autenticação para novas chaves após a revogação 17
3.4. Identificação e Autenticação para solicitação de revogação 17
4. Requisitos Operacionais do Ciclo de Vida do Certificado 18
4.1. Solicitação de Certificado 18
4.1.1. Quem pode submeter uma solicitação de certificado 18
4.1.2. Processo de registro e responsabilidades 18
4.2. Processamento de Solicitação de Certificado 18
4.2.1. Execução das funções de identificação e autenticação 18
4.2.2. Aprovação ou rejeição de pedidos de certificado 18
4.2.3. Tempo para processar a solicitação de certificado 18
4.3. Emissão de Certificado 18
4.3.1. Ações da AC durante a emissão de um certificado 18
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado 18
4.4. Aceitação de Certificado 18
4.4.1. Conduta sobre a aceitação do certificado 18
4.4.2. Publicação do certificado pela AC 18
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades 18
4.5. Usabilidade do par de chaves e do certificado 18
4.5.1. Usabilidade da Chave privada e do certificado do titular 18
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis 18
4.6. Renovação de Certificados 19
4.6.1. Circunstâncias para renovação de certificados 19
4.6.2. Quem pode solicitar a renovação 19
4.6.3. Processamento de requisição para renovação de certificados 19
4.6.4. Notificação para nova emissão de certificado para o titular 19
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado ... 19
4.6.6. Publicação de uma renovação de um certificado pela AC 19
4.6.7. Notificação de emissão de certificado pela AC para outras entidades 19
4.7. Nova chave de certificado 19
4.7.1. Circunstâncias para nova chave de certificado 19
4.7.2. Quem pode requisitar a certificação de uma nova chave pública 19
4.7.3. Processamento de requisição de novas chaves de certificado 19

4.7.4. Notificação de emissão de novo certificado para o titular 19
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada 19
4.7.6. Publicação de uma nova chave certificada pela AC 19
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades 19
4.8. Modificação de certificado 19
4.8.1. Circunstâncias para modificação de certificado 19
4.8.2. Quem pode requisitar a modificação de certificado 19
4.8.3. Processamento de requisição de modificação de certificado 19
4.8.4. Notificação de emissão de novo certificado para o titular 19
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado 19
4.8.6. Publicação de uma modificação de certificado pela AC 19
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades 19
4.9. Suspensão e Revogação de Certificado 20
4.9.1. Circunstâncias para revogação 20
4.9.2. Quem pode solicitar revogação 20
4.9.3. Procedimento para solicitação de revogação 20
4.9.4. Prazo para solicitação de revogação 20
4.9.5. Tempo em que a AC deve processar o pedido de revogação 20
4.9.6. Requisitos de verificação de revogação para as partes confiáveis 20
4.9.7. Frequência de emissão de LCR 20
4.9.8. Latência máxima para a LCR 20
4.9.9. Disponibilidade para revogação/verificação de status on-line 20
4.9.10. Requisitos para verificação de revogação on-line 20
4.9.11. Outras formas disponíveis para divulgação de revogação 20
4.9.12. Requisitos especiais para o caso de comprometimento de chave 20
4.9.13. Circunstâncias para suspensão 20
4.9.14. Quem pode solicitar suspensão 20
4.9.15. Procedimento para solicitação de suspensão 20
4.9.16. Limites no período de suspensão 20
4.10. Serviços de status de certificado 20
4.10.1. Características operacionais 20
4.10.2. Disponibilidade dos serviços 20
4.10.3. Funcionalidades operacionais 20
4.11. Encerramento de atividades 20
4.12. Custódia e recuperação de chave 20
4.12.1. Política e práticas de custódia e recuperação de chave 20
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão 20

5. Controles operacionais, gerenciamento e de instalações 21
5.1. Controles Físicos 21
5.1.1. Construção e localização das instalações 21
5.1.2. Acesso físico 21
5.1.3. Energia e ar condicionado 21
5.1.4. Exposição à água 21
5.1.5. Prevenção e proteção contra incêndio 21
5.1.6. Armazenamento de mídia 21
5.1.7. Destruição de lixo 21
5.1.8. Instalações de segurança (backup) externas (off-site) para AC 21
5.2. Controles Procedimentais 21
5.2.1. Perfis qualificados 21
5.2.2. Número de pessoas necessário por tarefa 21
5.2.3. Identificação e autenticação para cada perfil 21
5.2.4. Funções que requerem separação de deveres 21
5.3. Controles de Pessoal 21
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade 21
5.3.2. Procedimentos de verificação de antecedentes 21
5.3.3. Requisitos de treinamento 21
5.3.4. Frequência e requisitos para reciclagem técnica 21
5.3.5. Frequência e sequência de rodízio de cargos 21
5.3.6. Sanções para ações não autorizadas 21
5.3.7. Requisitos para contratação de pessoal 21
5.3.8. Documentação fornecida ao pessoal 21
5.4. Procedimentos de Log de Auditoria 22
5.4.1. Tipos de eventos registrados 22
5.4.2. Frequência de auditoria de registros 22
5.4.3. Período de retenção para registros de auditoria 22
5.4.4. Proteção de registros de auditoria 22
5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria 22
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo) 22
5.4.7. Notificação de agentes causadores de eventos 22
5.4.8. Avaliações de vulnerabilidade 22
5.5. Arquivamento de Registros 22
5.5.1. Tipos de registros arquivados 22
5.5.2. Período de retenção para arquivo 22
5.5.3. Proteção de arquivo 22
5.5.4. Procedimentos de cópia de arquivo 22

5.5.5. Requisitos para datação de registros 22
5.5.6. Sistema de coleta de dados de arquivo (interno e externo) 22
5.5.7. Procedimentos para obter e verificar informação de arquivo 22
5.6. Troca de chave 22
5.7. Comprometimento e Recuperação de Desastre 22
5.7.1. Procedimentos de gerenciamento de incidente e comprometimento 22
5.7.2. Recursos computacionais, software, e/ou dados corrompidos 22
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade 22
5.7.4. Capacidade de continuidade de negócio após desastre 22
5.8. Extinção da AC 22
6. Controles Técnicos de Segurança 23
6.1. Geração e Instalação do Par de Chaves 23
6.1.1. Geração do par de chaves 23
6.1.2. Entrega da chave privada à entidade titular do certificado 24
6.1.3. Entrega da chave pública para emissor de certificado 24
6.1.4. Disponibilização de chave pública da AC para usuários 24
6.1.5. Tamanhos de chave 24
6.1.6. Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros 25
6.1.7. Propósitos de uso de chave (conforme o campo "key usage" na X.509v3) 25
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico . 25
6.2.1. Padrões e controle para módulo criptográfico 25
6.2.2. Controle "n de m" para chave privada 25
6.2.3. Custódia (escrow) de chave privada 25
6.2.4. Cópia de segurança de chave privada 25
6.2.5. Arquivamento de chave privada 26
6.2.6. Inserção de chave privada em módulo criptográfico 26
6.2.7. Armazenamento de chave privada em módulo criptográfico 26
6.2.8. Método de ativação de chave privada 26
6.2.9. Método de desativação de chave privada 26
6.2.10. Método de destruição de chave privada 26
6.3. Outros Aspectos do Gerenciamento do Par de Chaves 26
6.3.1. Arquivamento de chave pública 26
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada 26
6.4. Dados de Ativação 27
6.4.1. Geração e instalação dos dados de ativação 27
6.4.2. Proteção dos dados de ativação 27

6.4.3. Outros aspectos dos dados de ativação 27
6.5. Controles de Segurança Computacional 27
6.5.1. Requisitos técnicos específicos de segurança computacional 27
6.5.2. Classificação da segurança computacional 28
6.6. Controles Técnicos do Ciclo de Vida 28
6.6.1. Controles de desenvolvimento de sistema 28
6.6.2. Controles de gerenciamento de segurança 28
6.6.3. Controles de segurança de ciclo de vida 28
6.6.4. Controles na Geração de LCR 28
6.7. Controles de Segurança de Rede 28
6.8. Carimbo de Tempo 28
7. Perfis de Certificado, LCR e OCSP 29
7.1. Perfil do Certificado 29
7.1.1. Número de versão 29
7.1.2. Extensões de certificado 29
7.1.3. Identificadores de algoritmo 33
7.1.4. Formatos de nome 33
7.1.5. Restrições de nome 35
7.1.6. OID (Object Identifier) de Política de Certificado 35
7.1.7. Uso da extensão "Policy Constraints" 36
7.1.8. Sintaxe e semântica dos qualificadores de política 36
7.1.9. Semântica de processamento para extensões críticas de PC 36
7.2. Perfil de LCR 36
7.2.1. Número(s) de versão 36
7.2.2. Extensões de LCR e de suas entradas 36
7.3. Perfil de OCSP 37
7.3.1. Número(s) de versão 37
7.3.2. Extensões de OCSP 37
8. Auditoria de Conformidade e Outras Avaliações 38
8.1. Frequência e circunstâncias das avaliações 38
8.2. Identificação/Qualificação do avaliador 38
8.3. Relação do avaliador com a entidade avaliada 38
8.4. Tópicos cobertos pela avaliação 38
8.5. Ações tomadas como resultado de uma deficiência 38
8.6. Comunicação dos resultados 38
9. Outros negócios e assuntos jurídicos 39
9.1. Tarifas 39
9.1.1. Tarifas de emissão e renovação de certificados 39

9.1.2. Tarifas de acesso ao certificado 39
9.1.3. Tarifas de revogação ou de acesso à informação de status 39
9.1.4. Tarifas para outros serviços 39
9.1.5. Política de reembolso 39
9.2. Responsabilidade Financeira 39
9.2.1. Cobertura do seguro 39
9.2.2. Outros ativos 39
9.2.3. Cobertura de seguros ou garantia para entidades finais 39
9.3. Confidencialidade da informação do negócio 39
9.3.1. Escopo de informações confidenciais 39
9.3.2. Informações fora do escopo de informações confidenciais 39
9.3.3. Responsabilidade em proteger a informação confidencial 39
9.4. Privacidade da informação pessoal 39
9.4.1. Plano de privacidade 39
9.4.2. Tratamento de informação como privadas 39
9.4.3. Informações não consideradas privadas 39
9.4.4. Responsabilidade para proteger a informação privadas 39
9.4.5. Aviso e consentimento para usar informações privadas 39
9.4.6. Divulgação em processo judicial ou administrativo 39
9.4.7. Outras circunstâncias de divulgação de informação 39
9.5. Direitos de Propriedade Intelectual 39
9.6. Declarações e Garantias 40
9.6.1. Declarações e Garantias da AC 40
9.6.2. Declarações e Garantias da AR 40
9.6.3. Declarações e garantias do titular 40
9.6.4. Declarações e garantias das terceiras partes 40
9.6.5. Representações e garantias de outros participantes 40
9.7. Isenção de garantias 40
9.8. Limitações de responsabilidades 40
9.9. Indenizações 40
9.10. Prazo e Rescisão 40
9.10.1. Prazo 40
9.10.2. Término 40
9.10.3. Efeito da rescisão e sobrevivência 40
9.11. Avisos individuais e comunicações com os participantes 40
9.12. Alterações 40
9.12.1. Procedimento para emendas 40
9.12.2. Mecanismo de notificação e períodos 40

9.12.3. Circunstâncias na qual o OID deve ser alterado. 40
9.13. Solução de conflitos 40
9.14. Lei aplicável 41
9.15. Conformidade com a Lei aplicável 41
9.16. Disposições Diversas 41
9.16.1. Acordo completo 41
9.16.2. Cessão 41
9.16.3. Independência de disposições 41
9.16.4. Execução (honorários dos advogados e renúncia de direitos) 41
9.17. Outras provisões 41
10. Documentos Referenciados 42

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Esta "Política de Certificado" (PC) descreve as políticas de certificação de certificados de Assinatura Digital de Tipo A3 da Autoridade Certificadora DigitalSign RFB na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1.2. A estrutura desta PC está baseada no DOC-ICP-04 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil.

1.1.3. A estrutura desta PC está baseada na RFC 3647.

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

1.1.5. O tipo de certificado emitido sob esta PC é o Tipo A3.

1.1.6. Não se aplica.

1.1.7. Esta PC refere-se exclusivamente a certificados de Pessoa Física, Pessoa Jurídica, de Equipamento e Aplicação do Tipo A3 da Autoridade Certificadora DigitalSign RFB.

1.1.8. Não se aplica.

1.1.9. Não se aplica.

1.1.10. Não se aplica.

1.1.11. Não se aplica.

1.1.12. Não se aplica.

1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Esta PC é designada de "Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora DigitalSign RFB" e referida como "PC A3 da AC DigitalSign RFB". Esta PC descreve os procedimentos e práticas da AC DigitalSign RFB e os usos relacionados ao certificado de Assinatura Digital do tipo A3. O OID (object identifier) desta PC é 2.16.76.1.2.3.42

1.2.2. Não se aplica.

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1. AUTORIDADES CERTIFICADORAS

1.3.1.1. Esta PC refere-se exclusivamente à AC DigitalSign RFB no âmbito da ICP-Brasil.

1.3.1.2. As práticas e procedimentos de certificação da AC DigitalSign RFB estão descritos na Declaração de Práticas de Certificação da AC DigitalSign RFB (DPC).

1.3.2. AUTORIDADES DE REGISTRO

1.3.2.1. Os dados seguintes, referentes às Autoridades de Registro – AR utilizadas pela AC DigitalSign RFB para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC DigitalSign RFB (http://repositorio.digitalsigncertificadora.com.br/rfb):

a) relação de todas as AR credenciadas.
b) relação de AR que tenham se descredenciado da cadeia da AC DigitalSign RFB, com respectiva data do descredenciamento.

1.3.2.2. A AC DigitalSign RFB mantém as informações acima sempre atualizadas.

1.3.3. TITULARES DE CERTIFICADO

Os titulares de certificado de assinatura do Tipo A1 podem ser pessoas físicas ou jurídicas, equipamentos ou aplicações.

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. São também publicados em serviço de diretório e/ou em página web da AC DigitalSign RFB (http://repositorio.digitalsigncertificadora.com.br/rfb):

a) relação de todos os Prestadores de Serviços de Suporte – PSS.
b) relação de todos os Prestadores de Serviços Biométricos – PSBios.
c) relação de todos os Prestadores de Serviço de Confiança – PSC.

1.4. USABILIDADE DO CERTIFICADO

1.4.1. USO APROPRIADO DO CERTIFICADO

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

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

1.4.1.3. A AC DigitalSign RFB 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.

1.4.1.4. Os certificados emitidos sob esta PC são apropriados ao uso em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações

1.4.1.5. Não se aplica.

1.4.1.6. Não se aplica.

1.4.1.7. Não se aplica.

1.4.1.8. Não se aplica.

1.4.2. USO PROIBITIVO DO CERTIFICADO

Os certificados emitidos sob esta PC devem apenas ser usados na medida em que seja consistente com a lei aplicável.

1.5. POLÍTICA DE ADMINISTRAÇÃO

1.5.1. ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome: DigitalSign Certificação Digital LTDA

1.5.2. CONTATOS

Endereço: Rua General Bertoldo Klinger, 111 – Paulicéia – São Bernardo do Campo/SP

Telefone: (55 11) 2666 7280

Página Web: www.digitalsigncertificadora.com.br

Email: suporte@digitalsigncertificadora.com.br

1.5.3. PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Guilherme Salgueiro de Almeida

Telefone: (55 11) 2666 7280

Email: suporte@digitalsigncertificadora.com.br

1.5.4. PROCEDIMENTOS DE 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. DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
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
PIS	Programa de Integração Social
PSS	Prestadores de Serviço de Suporte

RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SSL	Secure Socket Layer
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC DigitalSign RFB.

2.1. REPOSITÓRIOS

2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.3. TEMPO E FREQUÊNCIA DE PUBLICAÇÃO

2.4. CONTROLE DE ACESSO AOS REPOSITÓRIOS

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC DigitalSign RFB.

3.1. NOMEAÇÃO

3.1.1. TIPOS DE NOMES

3.1.2. NECESSIDADE DOS NOMES SEREM SIGNIFICATIVOS

3.1.3. ANONIMATO OU PSEUDÔNIMO DOS TITULARES DO CERTIFICADO

3.1.4. REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES

3.1.5. UNICIDADE DE NOMES

3.1.6. PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES

3.1.7. RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS

3.2. VALIDAÇÃO INICIAL DE IDENTIDADE

3.2.1. MÉTODO PARA COMPROVAR A POSSE DE CHAVE PRIVADA

3.2.2. 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 DPC da AC DigitalSign RFB.

4.1. SOLICITAÇÃO DE CERTIFICADO

4.1.1. QUEM PODE SUBMETER UMA SOLICITAÇÃO DE CERTIFICADO

4.1.2. PROCESSO DE REGISTRO E RESPONSABILIDADES

4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1. EXECUÇÃO DAS FUNÇÕES DE IDENTIFICAÇÃO E AUTENTICAÇÃO

4.2.2. APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO

4.2.3. TEMPO PARA PROCESSAR A SOLICITAÇÃO DE CERTIFICADO

4.3. EMISSÃO DE CERTIFICADO

4.3.1. AÇÕES DA AC DURANTE A EMISSÃO DE UM CERTIFICADO

4.3.2. NOTIFICAÇÕES PARA O TITULAR DO CERTIFICADO PELA AC NA EMISSÃO DO CERTIFICADO

4.4. ACEITAÇÃO DE CERTIFICADO

4.4.1. CONDUTA SOBRE A ACEITAÇÃO DO CERTIFICADO

4.4.2. PUBLICAÇÃO DO CERTIFICADO PELA AC

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

4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

4.5.1. USABILIDADE DA CHAVE PRIVADA E DO CERTIFICADO DO TITULAR

4.5.2. USABILIDADE DA CHAVE PÚBLICA E DO CERTIFICADO DAS PARTES CONFIÁVEIS

4.6. RENOVAÇÃO DE CERTIFICADOS

4.6.1. CIRCUNSTÂNCIAS PARA RENOVAÇÃO DE CERTIFICADOS

4.6.2. QUEM PODE SOLICITAR A RENOVAÇÃO

4.6.3. PROCESSAMENTO DE REQUISIÇÃO PARA RENOVAÇÃO DE CERTIFICADOS

4.6.4. NOTIFICAÇÃO PARA NOVA EMISSÃO DE CERTIFICADO PARA O TITULAR

4.6.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO

4.6.6. PUBLICAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO PELA AC

4.6.7. NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES

4.7. NOVA CHAVE DE CERTIFICADO

4.7.1. CIRCUNSTÂNCIAS PARA NOVA CHAVE DE CERTIFICADO

4.7.2. QUEM PODE REQUISITAR A CERTIFICAÇÃO DE UMA NOVA CHAVE PÚBLICA

4.7.3. PROCESSAMENTO DE REQUISIÇÃO DE NOVAS CHAVES DE CERTIFICADO

4.7.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR

4.7.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA NOVA CHAVE CERTIFICADA

4.7.6. PUBLICAÇÃO DE UMA NOVA CHAVE CERTIFICADA PELA AC

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

4.8. MODIFICAÇÃO DE CERTIFICADO

4.8.1. CIRCUNSTÂNCIAS PARA MODIFICAÇÃO DE CERTIFICADO

4.8.2. QUEM PODE REQUISITAR A MODIFICAÇÃO DE CERTIFICADO

4.8.3. PROCESSAMENTO DE REQUISIÇÃO DE MODIFICAÇÃO DE CERTIFICADO

4.8.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR

4.8.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO

4.8.6. PUBLICAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO PELA AC

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

4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.9.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO
4.9.2. QUEM PODE SOLICITAR REVOGAÇÃO
4.9.3. PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO
4.9.4. PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO
4.9.5. TEMPO EM QUE A AC DEVE PROCESSAR O PEDIDO DE REVOGAÇÃO
4.9.6. REQUISITOS DE VERIFICAÇÃO DE REVOGAÇÃO PARA AS PARTES CONFIÁVEIS
4.9.7. FREQUÊNCIA DE EMISSÃO DE LCR
4.9.8. LATÊNCIA MÁXIMA PARA A LCR
4.9.9. DISPONIBILIDADE PARA REVOGAÇÃO/VERIFICAÇÃO DE STATUS ON-LINE
4.9.10. REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO ON-LINE
4.9.11. OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO
4.9.12. REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE
4.9.13. CIRCUNSTÂNCIAS PARA SUSPENSÃO
4.9.14. QUEM PODE SOLICITAR SUSPENSÃO
4.9.15. PROCEDIMENTO PARA SOLICITAÇÃO DE SUSPENSÃO
4.9.16. LIMITES NO PERÍODO DE SUSPENSÃO

4.10. SERVIÇOS DE STATUS DE CERTIFICADO

4.10.1. CARACTERÍSTICAS OPERACIONAIS
4.10.2. DISPONIBILIDADE DOS SERVIÇOS
4.10.3. FUNCIONALIDADES OPERACIONAIS

4.11. ENCERRAMENTO DE ATIVIDADES

4.12. CUSTÓDIA E RECUPERAÇÃO DE CHAVE

4.12.1. POLÍTICA E PRÁTICAS DE CUSTÓDIA E RECUPERAÇÃO DE CHAVE
4.12.2. POLÍTICA E PRÁTICAS DE ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVE DE SESSÃO

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens seguintes são referidos os itens correspondentes da DPC da AC DigitalSign RFB.

5.1. CONTROLES FÍSICOS

5.1.1. CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES

5.1.2. ACESSO FÍSICO

5.1.3. ENERGIA E AR CONDICIONADO

5.1.4. EXPOSIÇÃO À ÁGUA

5.1.5. PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO

5.1.6. ARMAZENAMENTO DE MÍDIA

5.1.7. DESTRUIÇÃO DE LIXO

5.1.8. INSTALAÇÕES DE SEGURANÇA (BACKUP) EXTERNAS (OFF-SITE) PARA AC

5.2. CONTROLES PROCEDIMENTAIS

5.2.1. PERFIS QUALIFICADOS

5.2.2. NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA

5.2.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

5.2.4. FUNÇÕES QUE REQUEREM SEPARAÇÃO DE DEVERES

5.3. CONTROLES DE PESSOAL

5.3.1. ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE

5.3.2. PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES

5.3.3. REQUISITOS DE TREINAMENTO

5.3.4. FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA

5.3.5. FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

5.3.6. SANÇÕES PARA AÇÕES NÃO AUTORIZADAS

5.3.7. REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL

5.4. PROCEDIMENTOS DE LOG DE AUDITORIA

5.4.1. TIPOS DE EVENTOS REGISTRADOS

5.4.2. FREQUÊNCIA DE AUDITORIA DE REGISTROS

5.4.3. PERÍODO DE RETENÇÃO PARA REGISTROS DE AUDITORIA

5.4.4. PROTEÇÃO DE REGISTROS DE AUDITORIA

5.4.5. PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTROS DE AUDITORIA

5.4.6. SISTEMA DE COLETA DE DADOS DE AUDITORIA (INTERNO OU EXTERNO)

5.4.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

5.4.8. AVALIAÇÕES DE VULNERABILIDADE

5.5. ARQUIVAMENTO DE REGISTROS

5.5.1. TIPOS DE REGISTROS ARQUIVADOS

5.5.2. PERÍODO DE RETENÇÃO PARA ARQUIVO

5.5.3. PROTEÇÃO DE ARQUIVO

5.5.4. PROCEDIMENTOS DE CÓPIA DE ARQUIVO

5.5.5. REQUISITOS PARA DATAÇÃO DE REGISTROS

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

5.5.7. PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO

5.6. TROCA DE CHAVE

5.7. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

5.7.1. PROCEDIMENTOS DE GERENCIAMENTO DE INCIDENTE E COMPROMETIMENTO

5.7.2. RECURSOS COMPUTACIONAIS, SOFTWARE, E/OU DADOS CORROMPIDOS

5.7.3. PROCEDIMENTOS NO CASO DE COMPROMETIMENTO DE CHAVE PRIVADA DE ENTIDADE

5.7.4. CAPACIDADE DE CONTINUIDADE DE NEGÓCIO APÓS DESASTRE

5.8. EXTINÇÃO DA AC

6. CONTROLES TÉCNICOS DE SEGURANÇA

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 criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração do par 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. O processo de geração de chaves do tipo A3, contemplada nesta PC, exige:

a) a instalação de hardware e software relacionados à mídia armazenadora do certificado selecionada pelo cliente;
b) geração do par de chaves criptográficas ocorre utilizando hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO;
c) o responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado deve executar pessoalmente a geração dos pares de chaves criptográficas.

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

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil. As chaves privadas correspondentes aos certificados poderão ser armazenadas em hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO, conforme definido para o tipo de certificado A3.

6.1.1.5. O usuário deve assegurar que 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. O meio 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;

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. O meio de armazenamento não deve modificar os dados a serem assinados, nem impedir que estes dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8. O tipo de certificado emitido pela AC DigitalSign RFB descrito nesta PC é o A3.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

6.1.2. ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR DO CERTIFICADO

Item não aplicável.

6.1.3. ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

A entrega da chave pública do solicitante do certificado é feita por meio eletrônico, em formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.4. DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC PARA USUÁRIOS

A AC DigitalSign RFB disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, de entre outras, em formato PKCS#7 através de endereço Web:

- Para certificados emitidos pela AC DigitalSign RFB (**G1**):
  - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFB.p7b
- Para certificados emitidos pela AC DigitalSign RFB **G2**:
  - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFBG2.p7b
- Para certificados emitidos pela AC DigitalSign RFB **G3**:
  - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFBG3.p7b

6.1.5. TAMANHOS DE CHAVE

6.1.5.1. O tamanho mínimo das chaves criptográficas associadas aos certificados emitidos pela AC DigitalSign RFB é de 2048 bits.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A3 da ICP-Brasil está definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

Os parâmetros de geração de chaves assimétricas da AC DigitalSign RFB seguem o padrão de Homologação da ICP-Brasil ou Certificação INMETRO, em conformidade ao estabelecido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

Os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

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

6.2.1. PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO

Não se aplica

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 de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura sem o consentimento do titular do certificado.

6.2.4. CÓPIA DE SEGURANÇA DE CHAVE PRIVADA

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

6.2.4.2. A AC DigitalSign RFB não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital.

6.2.4.3. Em qualquer caso, a cópia de segurança deverá ser armazenada, cifrada, por algoritmo simétrico 3-DES, IDEA, SAFER+ ou outros aprovados em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia deve ser efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

6.2.5. ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1. A AC DigitalSign RFB não arquiva cópias de chaves privadas de assinatura digital de titulares de certificados.

6.2.5.2. Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6. INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

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

De acordo com o art. 5° da Instrução Normativa RFB N° 222, de 11 de Outubro de 2002, o titular de certificado de e-CPF ou e-CNPJ deve obrigatoriamente utilizar senha para a proteção de sua chave privada.

6.2.9. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

Não se aplica.

6.2.10. MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

Cada titular de certificado deve definir procedimentos necessários para a destruição de sua chave privada.

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. ARQUIVAMENTO DE CHAVE PÚBLICA

As chaves públicas dos titulares de certificados de assinatura digital emitidos pela AC DigitalSign RFB permanecem armazenadas após a expiração dos certificados correspondentes, pelo período legalmente estabelecido, 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 de assinatura dos respectivos titulares de certificados são utilizadas apenas durante período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo

determinado pela legislação aplicável, para verificação das assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. O período máximo de validade admitido para certificados de Assinatura Digital Tipo A3 é de 5 (cinco) anos.

6.3.2.4. Não se aplica.

6.3.2.5. Não se aplica.

6.4. 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

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

a) Controle de acesso lógico ao sistema operacional;
b) Exigência de uso de senhas fortes;
c) Diretivas de senha e de bloqueio de conta;
d) Antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;
e) Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
f) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
g) Proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2. CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL

Item não aplicável.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

Não se aplica.

6.6.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA

Não se aplica.

6.6.2. CONTROLES DE GERENCIAMENTO DE SEGURANÇA

Não se aplica.

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 LCR geradas pela AC são verificadas 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, LCR E OCSP

7.1. PERFIL DO CERTIFICADO

Todos os certificados emitidos pela AC DigitalSign RFB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1. NÚMERO DE VERSÃO

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

7.1.2. EXTENSÕES DE CERTIFICADO

7.1.2.1. Neste item, a PC descreve todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2. Extensões Obrigatórias:

a) "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC DigitalSign RFB;

b) "*Key Usage*", crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;

c) "*Certificate Policies*", não crítica contém:

- O campo policyIdentifier contém o OID desta PC: 2.16.76.1.2.3.42;
- O campo policyQualifiers contém o endereço Web da DPC da AC que emite o certificado: http://www.digitalsigncertificadora.com.br/repositorio/rfb

d) "*CRL Distribution Points*", não crítica: contém os endereços Web onde se obtém a LCR correspondente:

- Para certificados emitidos pela AC DigitalSign RFB (**G1**):
  - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFB.crl
  - http://www.digitaltrust.com.br/repositorio/rfb/ACDIGITALSIGNRFB.crl
  - http://repositorio.icpbrasil.gov.br/lcr/DigitalSign/ACDIGITALSIGNRFB.crl
- Para certificados emitidos pela AC DigitalSign RFB **G2**:
  - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFBG2.crl
  - http://www.digitaltrust.com.br/repositorio/rfb/ACDIGITALSIGNRFBG2.crl
- Para certificados emitidos pela AC DigitalSign RFB **G3**:
  - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFBG3.crl
  - http://www.digitaltrust.com.br/repositorio/rfb/ACDIGITALSIGNRFBG3.crl

e) "*Authority Information Access*", não crítica, contém:

- o endereço web onde se poderá obter a cadeia de certificação:
  - Para certificados emitidos pela AC DigitalSign RFB (**G1**):
    - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFB.p7b
  - Para certificados emitidos pela AC DigitalSign RFB **G2**:
    - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFBG2.p7b
  - Para certificados emitidos pela AC DigitalSign RFB **G3**:
    - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFBG2.p7b
- o endereço web onde se pode aceder ao serviço OCSP, através do link:
  - Para certificados emitidos pela AC DigitalSign RFB **G3**:
    - http://ocsp.digitalsigncertificadora.com.br

7.1.2.3. Os certificados emitidos pela AC DigitalSign RFB possuem a extensão "Subject Alternative Name", não crítica e com os seguintes formatos:

a) Para certificado de pessoa física (e-CPF):

a.1) 3 (três) campos otherName, obrigatórios, contendo:

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

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

iii. OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

a.2) 1 (um) campo otherName, obrigatório para certificados digitais cujas titularidades foram validadas pela AR dos conselhos de classes profissionais regulamentados por lei específica, contendo:

i. OID = 2.16.76.1.4.2.n e conteúdo = de tamanho variável correspondente ao número de identificação profissional emitido por conselho de classe profissional e outras informações, se necessário.

a.3) Não aplicável.

a.4) Não aplicável.

a.5) campo otherName, não obrigatório, contendo:

i. rfc822Name, contém o endereço de correio eletrónico do titular do certificado;

ii. OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo = Nome Principal que contém o domínio de login em estações de trabalho (UPN).

b) Para certificado de pessoa Jurídica (e-CNPJ):

b.1) 4 (quatro) campos otherName, contendo,:

i. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI) do responsável; nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

ii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pela Pessoa Jurídica.

iii. OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

iv. OID = 2.16.76.1.3.7 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.

b.2) Campos otherName, não obrigatórios, contendo:

i. rfc822Name, contém o endereço de correio eletrónico do titular do certificado;

c) Para certificado de equipamento ou aplicação:

c.1) Não se aplica.

c.2) Para os demais tipos de certificado de equipamento ou aplicação, 4 (quatro) campos otherName, obrigatórios, contendo:

i. OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica.

ii. OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica.

iii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado.

iv. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI) do responsável; nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

c.3) Quando os certificados de equipamento forem emitidos para servidores de Domain Controller, adicionalmente, irão conter um campo otherName com OID = 1.3.6.1.4.1.311.25.1 e conteúdo = identificador (Globally Unique Identifier – GUID) do Domain Controller;

c.4) Campo DNS Name, opcional, contendo o nome do domínio.

d) Não aplicável.

e) Não aplicável.

7.1.2.4. Os campos otherName, definidos como obrigatórios, estão de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo otherName é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING, ou PRINTABLE STRING, com exceção do campo UPN que possui uma cadeia de caracteres do tipo ASN.1 UTF8 STRING.

b) Quando os números de NIS (PIS, PASEP ou CI), RG, CEI ou Título de Eleitor não estiverem disponíveis, os campos correspondentes são integralmente preenchidos com caracteres "zero".

c) Se o número do RG não estiver disponível, não é preenchido o campo de órgão emissor e UF. O mesmo ocorre para o campo do município e UF se não houver número de inscrição do Título de Eleitor.

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, tal como RG, são preenchidos com caracteres "zero" à 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, sendo utilizados apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre municípios e UF do Título de Eleitor.

g) Para os campos OtherName, com exceção do UPN, apenas caracteres de A a Z e 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 aplicável.

7.1.2.5. Campos otherName adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidos pela AC DigitalSign RFB, podem ser utilizados com OID atribuídos ou aprovados pela AC-Raiz.

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

7.1.2.7. As extensões "Key Usage" e "Extended Key Usage" para os referidos tipos de certificado são obrigatórias e devem obedecer os propósitos de uso e a criticalidade conforme descrição abaixo:

a) Para certificados de Assinatura de Resposta OCSP:
   - "Key Usage", crítica: deve conter o bit digitalSignature ativado, podendo conter o bit nonRepudiation ativado;
   - "Extended Key Usage", não crítica: somente o propósito OCSPSigning OID =1.3.6.1.5.5.7.3.9 deve estar presente;

b) Para os demais certificados de Assinatura e/ou Proteção de e-Mail:

- "Key Usage", crítica: deve conter o bit digitalSignature ativado, podendo conter os bits keyEncipherment e nonRepudiation ativados;
- "Extended Key Usage", não crítica, contém no mínimo um dos propósitos "client authentication" (OID 1.3.6.1.5.5.7.3.2) e/ou "E-mail protection" (OID 1.3.6.1.5.5.7.3.4), e podendo conter o valor "Smart Card Logon" (OID 1.3.6.1.4.1.311.20.2.2), quando for utilizado o campo "UPN" na extensão "Subject Alternative Name".

7.1.3. IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC DigitalSign RFB são assinados utilizando o algoritmo RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11) conforme o padrão PKCS#1.

7.1.4. FORMATOS DE NOME

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

a) e-CPF:

C = BR
O = ICP-Brasil
OU = Secretaria da Receita Federal do Brasil - RFB
OU = RFB e-CPF A3
OU = <Empresa ou órgão fornecedor do certificado>
OU = <CNPJ da AR que realizou a identificação>
OU = <Tipo de identificação utilizada (presencial, videoconferencia ou certificado digital)>
CN = <Nome da Pessoa Física>:<número de inscrição no CPF>

Onde:
O Common Name (CN) é composto do nome da pessoa física, obtido do Cadastro de Pessoas Físicas (CPF) da RFB, com cumprimento máximo de 52 (cinquenta e dois) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da pessoa física do titular neste cadastro composto por 11 (onze) caracteres.
São 5 (cinco) os campos *Organizational Unit* (OU) definidos no certificado, assim constituídos:

a) Um "OU" informando o tipo de identificação utilizada (presencial, videoconferencia ou certificado digital).

b) Um "OU" informando CNPJ da AR que realizou a identificação.

c) Um "OU" com conteúdo variável, informando a identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for seu empregado, funcionário ou servidor. Caso esse OU não seja utilizado, o mesmo deverá ser grafado com o texto "(EM BRANCO)".

d) Um "OU" com conteúdo fixo "RFB e-CPF A3".

e) Um "OU" com conteúdo fixo "Secretaria da Receita Federal do Brasil - RFB".

b) e-CNPJ:

C = BR
O = ICP-Brasil
S = <Sigla da Unidade da Federação>

L = <Cidade>
OU = Secretaria da Receita Federal do Brasil - RFB
OU = RFB e-CNPJ A3
OU = <CNPJ da AR que realizou a identificação>
OU = <Tipo de identificação utilizada (presencial, videoconferencia ou certificado digital)>
CN = <Nome Empresarial>:<número de inscrição no CNPJ>

Onde:
O Common Name (CN) é composto do nome empresarial da pessoa jurídica, obtido do Cadastro Nacional da Pessoa Jurídica (CNPJ) da RFB, com cumprimento máximo de 49 (quarenta e nove) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da empresa titular do certificado neste cadastro composto por 14 (quatorze) caracteres.
São 4 (quatro) os campos *Organizational Unit* (OU) definidos no certificado, assim constituídos:

a) Um "OU" informando o tipo de identificação utilizada (presencial, videoconferencia ou certificado digital).
b) Um "OU" informando CNPJ da AR que realizou a identificação.
c) Um "OU" com conteúdo fixo "RFB e-CNPJ A3".
d) Um "OU" com conteúdo fixo "Secretaria da Receita Federal do Brasil - RFB".

O campo Locality (L) com conteúdo correspondente ao nome da cidade onde a empresa está localizada. O campo deve ser preenchido sem acentos nem abreviaturas.
O campo State or Province Name (S) com conteúdo correspondente a sigla do estado onde a empresa está localizada.

c) e-Aplicação:

C = BR
O = ICP-Brasil
OU = Secretaria da Receita Federal do Brasil - RFB
OU = RFB e-Aplicacao A3
OU = <CNPJ da AR que realizou a identificação>
OU = <Tipo de identificação utilizada (presencial, videoconferencia ou certificado digital)>
CN = <Nome da Aplicação>:<número de inscrição no CNPJ>

Onde:
O "Common Name" (CN) é composto do nome da aplicação, com cumprimento máximo de 49 (quarenta e nove) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição no Cadastro de Pessoas Jurídica (CNPJ), composto por 14 (quatorze) caracteres
São 4 (quatro) os campos *Organizational Unit* (OU) definidos no certificado, assim constituídos:

a) Um "OU" informando o tipo de identificação utilizada (presencial, videoconferencia ou certificado digital).
b) Um "OU" informando CNPJ da AR que realizou a identificação.
c) Um "OU" com conteúdo fixo "RFB e-Aplicacao A3".
d) Um "OU" com conteúdo fixo "Secretaria da Receita Federal do Brasil - RFB".

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. Não se aplica.

7.1.5. RESTRIÇÕES DE NOME

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

7.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC DigitalSign RFB são as seguintes:

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Além dos caracteres alfanuméricos, podem 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 desta PC é: 2.16.76.1.2.3.42

7.1.7. USO DA EXTENSÃO "POLICY CONSTRAINTS"

Não se aplica.

7.1.8. SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Os campos policyQualifiers da extensão "Certificate Policies" contém o endereço web da DPC da AC DigitalSign RFB. (http://www.digitalsigncertificadora.com.br/repositorio/rfb)

7.1.9. SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS DE PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. PERFIL DE LCR

7.2.1. NÚMERO(S) DE VERSÃO

As LCR geradas pela AC DigitalSign RFB 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. Neste item são descritas todas as extensões de LCR utilizadas pela AC DigitalSign RFB e sua criticalidade.

7.2.2.2. As LCR da AC DigitalSign RFB obedecem a ICP-Brasil que define como obrigatórias as seguintes extensões:

a) "Authority Key Identifier": não crítica: contém o hash SHA-1 da chave pública da AC que assina a LCR;
b) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC que assina a LCR.

A AC DigitalSign RFB define como obrigatória a seguinte extensão para suas LCRs:

a) "Authority Information Access", não crítica: contém o endereço web onde se poderá obter a cadeia de certificação:
   - Para certificados emitidos pela AC DigitalSign RFB (**G1**):
     - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFB.p7b
   - Para certificados emitidos pela AC DigitalSign RFB **G2**:
     - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFBG2.p7b
   - Para certificados emitidos pela AC DigitalSign RFB **G3**:
     - http://www.digitalsigncertificadora.com.br/repositorio/rfb/ACDIGITALSIGNRFBG3.p7b

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

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 DigitalSign RFB.

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 DigitalSign RFB.

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

Qualquer alteração nesta PC é submetida à aprovação da AC Raiz.

9.12.2. MECANISMO DE NOTIFICAÇÃO E PERÍODOS

Mudança nesta PC será publicado no site da AC DigitalSign RFB.

9.12.3. CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO.

9.13. SOLUÇÃO DE CONFLITOS

9.14. LEI APLICÁVEL

9.15. CONFORMIDADE COM A LEI APLICÁVEL

9.16. DISPOSIÇÕES DIVERSAS

9.16.1. ACORDO COMPLETO

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

9.16.2. CESSÃO

9.16.3. INDEPENDÊNCIA DE DISPOSIÇÕES

9.16.4. EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)

9.17. OUTRAS PROVISÕES

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC DigitalSign RFB, 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, foi verificada a compatibilidade entre a PC e a DPC da AC DigitalSign RFB.

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
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[6]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

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