



PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Secretaria-Executiva da Casa Civil
Secretaria de Administração
Diretoria de Tecnologia
Autoridade Certificadora

Declaração de Práticas de Certificação
da
Autoridade Certificadora
da
Presidência da República

Assinatura Geral e Proteção de E-mail (S/MIME)

(DPC ACPR Versão 15)

ÍNDICE

CONTROLE DE ALTERAÇÕES	7
1. INTRODUÇÃO	9
1.1. VISÃO GERAL	9
1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO	9
1.3. PARTICIPANTES DA ICP-BRASIL	9
1.3.1 AUTORIDADES CERTIFICADORAS	9
1.3.2 AUTORIDADES DE REGISTRO	9
1.3.3. TITULARES DE CERTIFICADO	9
1.3.4. PARTES CONFIÁVEIS	9
1.3.5. OUTROS PARTICIPANTES	9
1.4. USABILIDADE DO CERTIFICADO	10
1.4.1. USO APROPRIADO DO CERTIFICADO	10
1.4.2. USO PROIBITIVO DO CERTIFICADO	10
1.5. POLÍTICA DE ADMINISTRAÇÃO	10
1.5.1. ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO	10
1.5.2. CONTATOS	10
1.5.3. PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC	10
1.5.4. PROCEDIMENTOS DE APROVAÇÃO DA DPC	10
1.6. DEFINIÇÕES E ACRÔNIMOS	10
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	12
2.1. REPOSITÓRIOS	12
2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS	12
2.3. TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO	13
2.4. CONTROLE DE ACESSO AOS REPOSITÓRIOS	13
3. IDENTIFICAÇÃO E AUTENTICAÇÃO	13
3.1. ATRIBUIÇÃO DE NOMES	13
3.1.1. TIPOS DE NOMES	13
3.1.2. NECESSIDADE DOS NOMES SEREM SIGNIFICATIVOS	13
3.1.3. ANONIMATO OU PSEUDÔNIMO DOS TITULARES DO CERTIFICADO	13
3.1.4. REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES	13
3.1.5. UNICIDADE DE NOMES	13
3.1.6. PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES	14
3.1.7. RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS	14
3.2. VALIDAÇÃO INICIAL DE IDENTIDADE	14
3.2.1. MÉTODO PARA COMPROVAR O CONTROLE DE CHAVE PRIVADA	14
3.2.2. AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO	14
3.2.3. AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO	16
3.2.4. INFORMAÇÕES NÃO VERIFICADAS DO TITULAR DO CERTIFICADO	17
3.2.5. VALIDAÇÃO DAS AUTORIDADES	18
3.2.6. CRITÉRIOS PARA INTEROPERAÇÃO	18
3.2.7. AUTENTICAÇÃO DA IDENTIDADE DE UM EQUIPAMENTO OU APLICAÇÃO	18
3.2.8. PROCEDIMENTOS COMPLEMENTARES	18
3.2.9. PROCEDIMENTOS ESPECÍFICOS	19
3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES	19
3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO	20
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	20
4.1. SOLICITAÇÃO DO CERTIFICADO	20
4.1.1. QUEM PODE SUBMETER UMA SOLICITAÇÃO DE CERTIFICADO	20
4.1.2. PROCESSO DE REGISTRO E RESPONSABILIDADES	20
4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO	22
4.2.1. EXECUÇÃO DAS FUNÇÕES DE IDENTIFICAÇÃO E AUTENTICAÇÃO	22
4.2.2. APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO	22
4.2.3. TEMPO PARA PROCESSAR A SOLICITAÇÃO DE CERTIFICADO	22
4.3. EMISSÃO DE CERTIFICADO	22
4.3.1. AÇÕES DA AC DURANTE A EMISSÃO DE UM CERTIFICADO	22
4.3.2. NOTIFICAÇÕES PARA O TITULAR DO CERTIFICADO PELA AC NA EMISSÃO DO CERTIFICADO	22
4.4. ACEITAÇÃO DE CERTIFICADO	22
4.4.1. CONDUTA SOBRE A ACEITAÇÃO DO CERTIFICADO	22

4.4.2. PUBLICAÇÃO DO CERTIFICADO PELA AC	23
4.4.3. NOTIFICAÇÃO DE EMISSÃO DO CERTIFICADO PELA AC RAIZ PARA OUTRAS ENTIDADES	23
4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO	23
4.5.1. USABILIDADE DA CHAVE PRIVADA E DO CERTIFICADO DO TITULAR	23
4.5.2. USABILIDADE DA CHAVE PÚBLICA E DO CERTIFICADO DAS PARTES CONFIÁVEIS	23
4.6. RENOVAÇÃO DE CERTIFICADOS	23
4.6.1. CIRCUNSTÂNCIAS PARA RENOVAÇÃO DE CERTIFICADOS	23
4.6.2. QUEM PODE SOLICITAR A RENOVAÇÃO	23
4.6.3. PROCESSAMENTO DE REQUISIÇÃO PARA RENOVAÇÃO DE CERTIFICADOS	24
4.6.4. NOTIFICAÇÃO PARA NOVA EMISSÃO DE CERTIFICADO PARA O TITULAR	24
4.6.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO	24
4.6.6. PUBLICAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO PELA AC	24
4.6.7. NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES	24
4.7. NOVA CHAVE DE CERTIFICADO (RE-KEY)	24
4.7.1. CIRCUNSTÂNCIAS PARA NOVA CHAVE DE CERTIFICADO	24
4.7.2. QUEM PODE REQUISITAR A CERTIFICAÇÃO DE UMA NOVA CHAVE PÚBLICA	24
4.7.3. PROCESSAMENTO DE REQUISIÇÃO DE NOVAS CHAVES DE CERTIFICADO	24
4.7.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR	24
4.7.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA NOVA CHAVE CERTIFICA	24
4.7.6. PUBLICAÇÃO DE UMA NOVA CHAVE CERTIFICADA PELA AC	24
4.7.7. NOTIFICAÇÃO DE UMA EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES	24
4.8. MODIFICAÇÃO DE CERTIFICADO	24
4.8.1. CIRCUNSTÂNCIAS PARA MODIFICAÇÃO DE CERTIFICADO	24
4.8.2. QUEM PODE REQUISITAR A MODIFICAÇÃO DE CERTIFICADO	24
4.8.3. PROCESSAMENTO DE REQUISIÇÃO DE MODIFICAÇÃO DE CERTIFICADO	24
4.8.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR	24
4.8.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO	24
4.8.6. PUBLICAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO PELA AC	25
4.8.7. NOTIFICAÇÃO DE UMA EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES	25
4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	25
4.9.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO	25
4.9.2. QUEM PODE SOLICITAR REVOGAÇÃO	25
4.9.3. PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO	26
4.9.4. PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO	26
4.9.5. TEMPO EM QUE A AC DEVE PROCESSAR O PEDIDO DE REVOGAÇÃO	26
4.9.6. REQUISITOS DE VERIFICAÇÃO DE REVOGAÇÃO PARA AS PARTES CONFIÁVEIS	26
4.9.7. FREQUÊNCIA DE EMISSÃO DE LCR	26
4.9.8. LATÊNCIA MÁXIMA PARA A LCR	26
4.9.9. DISPONIBILIDADE PARA REVOGAÇÃO/VERIFICAÇÃO DE STATUS ON-LINE	27
4.9.10. REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO ON-LINE	27
4.9.11. OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO	27
4.9.12. REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE	27
4.9.13. CIRCUNSTÂNCIAS PARA SUSPENSÃO	27
4.9.14. QUEM PODE SOLICITAR SUSPENSÃO	27
4.9.15. PROCEDIMENTO PARA SOLICITAÇÃO DE SUSPENSÃO	27
4.9.16. LIMITES NO PERÍODO DE SUSPENSÃO	27
4.10. SERVIÇOS DE STATUS DE CERTIFICADO	27
4.10.1. CARACTERÍSTICAS OPERACIONAIS	27
4.10.2. DISPONIBILIDADE DOS SERVIÇOS	27
4.10.3. FUNCIONALIDADES OPERACIONAIS	27
4.11. ENCERRAMENTO DE ATIVIDADES	27
4.12. CUSTÓDIA E RECUPERAÇÃO DE CHAVE	27
4.12.1. POLÍTICA E PRÁTICAS DE CUSTÓDIA E RECUPERAÇÃO DE CHAVE	28
4.12.2. POLÍTICA E PRÁTICAS DE ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVE DE SESSÃO	28
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES	28
5.1 CONTROLES FÍSICOS	28
5.1.1 CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES DE AC	28
5.1.2 ACESSO FÍSICO	28
5.1.3 ENERGIA E AR-CONDICIONADO	30
5.1.4 EXPOSIÇÃO À ÁGUA	30

5.1.5	PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO NAS INSTALAÇÕES DA AC	30
5.1.6	ARMAZENAMENTO DE MÍDIA	31
5.1.7	DESTRUIÇÃO DE LIXO	31
5.1.8	INSTALAÇÕES DE SEGURANÇA (BACKUP) EXTERNAS (OFF-SITE) PARA AC	31
5.2	CONTROLES PROCEDIMENTAIS	31
5.2.1	PERFIS QUALIFICADOS	31
5.2.2	NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA	31
5.2.3	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL	31
5.2.4	FUNÇÕES QUE REQUEREM SEPARAÇÃO DE DEVERES	32
5.3	CONTROLES DE PESSOAL	32
5.3.1	ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE	32
5.3.2	PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES	32
5.3.3	REQUISITOS DE TREINAMENTO	32
5.3.4	FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA	33
5.3.5	FREQUÊNCIA E SEQUÊNCIA DE RODÍZIOS DE CARGOS	33
5.3.6	SANÇÕES PARA AÇÕES NÃO AUTORIZADAS	33
5.3.7	REQUISITOS PARA CONTRATAÇÃO DE PESSOAL	33
5.3.8	DOCUMENTAÇÃO FORNECIDA AO PESSOAL	33
5.4	PROCEDIMENTOS DE LOG DE AUDITORIA	33
5.4.1	TIPOS DE EVENTO REGISTRADOS	33
5.4.2	FREQUÊNCIA DE AUDITORIA DE REGISTROS	34
5.4.3	PERÍODO DE RETENÇÃO PARA REGISTROS DE AUDITORIA	35
5.4.4	PROTEÇÃO DE REGISTRO DE AUDITORIA	35
5.4.5	PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTROS DE AUDITORIA	35
5.4.6	SISTEMA DE COLETA DE DADOS DE AUDITORIA (INTERNO OU EXTERNO)	35
5.4.7	NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS	36
5.4.8	AVALIAÇÕES DE VULNERABILIDADE	36
5.5	ARQUIVAMENTO DE REGISTROS	36
5.5.1	TIPOS DE REGISTROS ARQUIVADOS	36
5.5.2	PERÍODO DE RETENÇÃO PARA ARQUIVO	36
5.5.3	PROTEÇÃO DE ARQUIVOS	36
5.5.4	PROCEDIMENTOS PARA CÓPIA DE ARQUIVOS	36
5.5.5	REQUISITOS PARA DATAÇÃO DE REGISTROS	37
5.5.6	SISTEMA DE COLETA DE DADOS DE ARQUIVO (INTERNO E EXTERNO)	37
5.5.7	PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO	37
5.6	TROCA DE CHAVE	37
5.7	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE	37
5.7.1	PROCEDIMENTOS GERENCIAMENTO DE INCIDENTE E COMPROMETIMENTO	37
5.7.2	RECURSOS COMPUTACIONAIS, SOFTWARE, E/OU DADOS CORROMPIDOS	38
5.7.3	PROCEDIMENTOS NO CASO DE COMPROMETIMENTO DE CHAVE PRIVADA DE ENTIDADE	38
5.7.4	CAPACIDADE DE CONTINUIDADE DE NEGÓCIO APÓS DESASTRE	38
5.8	EXTINÇÃO DA AC	38
6	CONTROLES TÉCNICOS DE SEGURANÇA	38
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	39
6.1.1	GERAÇÃO DO PAR DE CHAVES	39
6.1.2	ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR	39
6.1.3	ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO	39
6.1.4	ENTREGA DE CHAVE PÚBLICA DA AC ÀS TERCEIRAS PARTES	39
6.1.5	TAMANHOS DE CHAVE	39
6.1.6	GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS E VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS	39
6.1.7	PROPÓSITOS DE USO DE CHAVE (CONFORME CAMPO “KEY USAGE” NA X.509 v3)	40
6.2	PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO	40
6.2.1	PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO	40
6.2.2	CONTROLE “N DE M’ PARA CHAVE PRIVADA	40
6.2.3	CUSTÓDIA (ESCROW) DE CHAVE PRIVADA	40
6.2.4	CÓPIA DE SEGURANÇA (BACKUP) DE CHAVE PRIVADA	40
6.2.5	ARQUIVAMENTO DE CHAVE PRIVADA	40
6.2.6	INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO	40
6.2.7	ARMAZENAMENTO DA CHAVE PRIVADA EM MÓDULOS CRIPTOGRÁFICOS	40

6.2.8. MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA	41
6.2.9. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA	41
6.2.10. MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA	41
6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	41
6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA	41
6.3.2 PERÍODOS DE OPERAÇÃO DO CERTIFICADO E PERÍODOS DE USO PARA AS CHAVES PÚBLICA E PRIVADA	41
6.4 DADOS DE ATIVAÇÃO	41
6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO	41
6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO	41
6.4.3 OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO	42
6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL	42
6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL	42
6.5.2. CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL	42
6.5.3. CONTROLES DE SEGURANÇA PARA AS AUTORIDADES DE REGISTRO	42
6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA	42
6.6.1 CONTROLES DE DESENVOLVIMENTO DE SISTEMA	43
6.6.2. CONTROLES DE GERENCIAMENTO DE SEGURANÇA	43
6.6.3 CONTROLES DE SEGURANÇA DE CICLO DE VIDA	43
6.6.4 CONTROLES NA GERAÇÃO DE LCR	43
6.7 CONTROLES DE SEGURANÇA DE REDE	43
6.7.1 DIRETRIZES GERAIS	43
6.7.2 FIREWALL	44
6.7.3 SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS)	44
6.7.4 REGISTRO DE ACESSOS NÃO AUTORIZADOS À REDE	44
6.8. CARIMBO DE TEMPO	44
7. PERFIS DE CERTIFICADO, LCR E OCSP	44
7.1. PERFIL DO CERTIFICADO	45
7.1.1. NÚMERO DE VERSÃO	45
7.1.2. EXTENSÕES DE CERTIFICADO	45
7.1.3. IDENTIFICADORES DE ALGORITMO	45
7.1.4. FORMATOS DE NOME	45
7.1.5. RESTRIÇÕES DE NOME	45
7.1.6. OID (OBJECT IDENTIFIER) DA DPC	45
7.1.7. USO DA EXTENSÃO “POLICY CONSTRAINTS”	45
7.1.8. SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA	45
7.1.9. SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS	45
7.2. PERFIL DE LCR	45
7.2.1. NÚMERO(S) DE VERSÃO	45
7.2.2. EXTENSÕES DE LCR E DE SUAS ENTRADAS	45
7.3. PERFIL DE OCSP	46
7.3.1. NÚMERO(S) DE VERSÃO	46
7.3.2. EXTENSÕES DE OCSP	46
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	46
8.1. FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES	46
8.2. IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR	46
8.3. RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA	46
8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO	46
8.5. AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA	46
8.6. COMUNICAÇÃO DOS RESULTADOS	47
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS	47
9.1. TARIFAS	47
9.1.1. TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS	47
9.1.2. TARIFAS DE ACESSO AO CERTIFICADO	47
9.1.3. TARIFAS DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS	47
9.1.4. TARIFAS PARA OUTROS SERVIÇOS	47
9.1.5. POLÍTICA DE REEMBOLSO	47
9.2. RESPONSABILIDADE FINANCEIRA	47
9.2.1. COBERTURA DO SEGURO	47
9.2.2. OUTROS ATIVOS	47

9.2.3. COBERTURA DE SEGUROS OU GARANTIA PARA ENTIDADES FINAIS	47
9.3. CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO	47
9.3.1. ESCOPO DE INFORMAÇÕES CONFIDENCIAIS	47
9.3.2. INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS	47
9.3.3. RESPONSABILIDADE EM PROTEGER A INFORMAÇÃO CONFIDENCIAL	48
9.4. PRIVACIDADE DA INFORMAÇÃO PESSOAL	48
9.4.1. PLANO DE PRIVACIDADE	48
9.4.2. TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS	48
9.4.3. INFORMAÇÕES NÃO CONSIDERADAS PRIVADAS	48
9.4.4. RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADAS	48
9.4.5. AVISO E CONSENTIMENTO PARA USAR INFORMAÇÕES PRIVADAS	48
9.4.6. DIVULGAÇÃO EM PROCESSO JUDICIAL OU ADMINISTRATIVO	49
9.4.7. OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO	49
9.4.8. INFORMAÇÕES A TERCEIROS	49
9.5. DIREITOS DE PROPRIEDADE INTELECTUAL	49
9.6. DECLARAÇÕES E GARANTIAS	49
9.6.1. DECLARAÇÕES E GARANTIAS DA AC	49
9.6.2. DECLARAÇÕES E GARANTIAS DA AR	50
9.6.3. DECLARAÇÕES E GARANTIAS DO TITULAR	50
9.6.4. DECLARAÇÕES E GARANTIAS DAS TERCEIRAS PARTES	50
9.6.5. REPRESENTAÇÕES E GARANTIAS DE OUTROS PARTICIPANTES	50
9.7. ISENÇÃO DE GARANTIAS	50
9.8. LIMITAÇÕES DE RESPONSABILIDADES	50
9.9. INDENIZAÇÕES	50
9.10. PRAZO E RESCISÃO	50
9.10.1. PRAZO	50
9.10.2. TÉRMINO	51
9.10.3. EFEITO DA RESCISÃO E SOBREVIVÊNCIA	51
9.11. AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES	51
9.12. ALTERAÇÕES	51
9.12.1. PROCEDIMENTO PARA EMENDAS	51
9.12.2. MECANISMO DE NOTIFICAÇÃO E PERÍODOS	51
9.12.3. CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO.	51
9.13. SOLUÇÃO DE CONFLITOS	51
9.14. LEI APLICÁVEL	51
9.15. CONFORMIDADE COM A LEI APLICÁVEL	51
9.16. DISPOSIÇÕES DIVERSAS	51
9.16.1. ACORDO COMPLETO	51
9.16.2. CESSÃO	51
9.16.3. INDEPENDÊNCIA DE DISPOSIÇÕES	51
9.16.4. EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)	52
9.17. OUTRAS PROVISÕES	52
10. DOCUMENTOS REFERENCIADOS	52
11. REFERÊNCIAS BIBLIOGRÁFICAS	53

Controle de Alterações

Versão	Data	Responsável	Descrição
15.0	19/11/2024	Sthefano Benathar	Inclusão da nova versão da AC PR = V6, abaixo da AC RAIZ V12. Nessa DPC foram declaradas a emissão para Pessoa Física, v5 e v6 e para Pessoa Jurídica na v5, apenas.
14.1	05/09/2024	Sthefano Benathar	Alteração das informações do responsável pela AC.
14.0	26/09/2022	Gustavo Freire	Adequação à Resolução CG ICP-Brasil nº 204, de 15.09.2022, onde altera o item 4.5.1.2 do DOC-ICP-O5, aprovado pela Resolução nº 177, de 20 de outubro de 2020.
13.0	19/04/2022	Gustavo Freire	Adequação à Resolução CG ICP-Brasil nº 197, de 16.11.2021, onde regulamenta os procedimentos e requisitos técnicos para a operacionalização de Autoridade de Registro Eletrônica na ICP-Brasil.
12.0	22/01/2021	Gustavo Freire	Adequação à Resolução CG ICP-Brasil nº 181, de 22.01.2021 Versão 6.1, onde: inclui a previsão de batimento biométrico e biográfico, realizado em base oficial nacional, no processo de identificação de requerente de certificado digital ICP-Brasil.
11.0	20/10/2020	Gustavo Freire	Adequação à Resolução 177, de 20/10/2020, versão 6.0 (Revisão e consolidação do DOC-ICP-05, conforme Decreto nº 10.139, de 28/11/2019 e regulamenta a emissão de certificado digital de pessoa física de forma conjunta com Carteira de Identidade (RG) e Carteira Nacional de Habilitação (CNH) e a emissão de certificado digital de pessoa jurídica pelas juntas comerciais. Ainda, ajustes para emissão por meio de videoconferência.)
10.0	30/04/2020	Gustavo Freire	Adequação às Resoluções 164, 167 e 170: alteração do tempo de armazenamento do vídeo resultante da gravação 24x7; alteração dos prazos máximos previstos para a emissão de LCR e conclusão do processo de revogação de certificado; novos procedimentos a serem observados na emissão de um certificado digital por videoconferência.
9.0	07/10/2019	Gustavo Freire	Adequação à Resolução 151, de 30/05/2019: requisitos para conformidade ao Programa WebTrust para as entidades da ICP-Brasil e simplificação de processos da ICP-Brasil. Adequação à Resolução 154, de 01/10/2019

			(alteração da alínea “b”, do item 3.2.3.1.3; alteração do item 6.1.1.4)
8.1	19/04/2018	Gustavo Freire	Acertos de links de Repositórios e verificação de LCRs, correção de textos e formatação do documento.
8.0	05/02/2018	Gustavo Freire	Adequação às Resoluções 119 e 121, de 06/07/2017. Adequação à Resolução 130, de 19/09/2017. Adequação à Resolução 131, de 10/11/2017

1. INTRODUÇÃO

1.1. Visão geral

1.1.1. Esta Declaração de Práticas de Certificação - DPC descreve as práticas e os procedimentos empregados pela Autoridade Certificadora da Presidência da República (AC PR), Autoridade Certificadora (AC) integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, na execução de seus serviços.

1.1.2. Esta DPC adota obrigatoriamente a mesma estrutura recomendada pelo documento DOC-ICP-05.

1.1.3 A estrutura desta DPC está baseada na RFC 3647.

1.1.4 AAC responsável deverá manter todas as informações da sua DPC sempre atualizadas.

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

1.2. Nome do documento e identificação

1.2.1. Esta DPC é chamada “Declaração de Práticas de Certificação da Autoridade Certificadora da Presidência da República”, integrante da ICP-Brasil, e comumente referida como “DPC ACPR”. O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil é **2.16.76.1.1.1**.

1.2.2 As ACs emissoras de certificados para usuários finais devem ser exclusivas e separadas de acordo com os seguintes propósitos de uso de chaves:

- a) não se aplica;
- b) assinatura de documento e proteção de e-mail (S/MIME) e garantia de origem e integridade;
- c) não se aplica.

1.3. Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

Esta DPC se refere unicamente à AC PR, integrante da ICP-Brasil.

1.3.2 Autoridades de Registro

1.3.2.1. O endereço da página *Web* (URL) da AC PR é <https://certificados.serpro.gov.br/acpr> onde estão publicados os dados abaixo referentes à Autoridade de Registro (AR) a ela vinculada, responsável pelos processos de recebimento, identificação 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; e
- b) relação de ARs que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

1.3.3. Titulares de certificado

Os Titulares de Certificados, segundo esta DPC, são pessoas físicas ou jurídicas da Presidência da República e, supletivamente, da Vice-Presidência da República, assim como, servidores de outros órgãos da administração pública federal, que utilizam sistemas de interesse da Presidência da República.

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. AAC PR utiliza o Serviço Federal de Processamento de Dados (SERPRO) como Prestador de Serviço de Suporte – PSS, Prestador de Serviço de Biométrico – PSBio e Prestador de Serviço de Confiança - PSC, conforme disponibilizado na página web <https://certificados.serpro.gov.br/acpr>.

1.4. Usabilidade do certificado

1.4.1. Uso apropriado do certificado

Política de Certificado (PC) implementada pela AC PR: **PC ACPR A3**, OID: **2.16.76.1.2.3.1**

1.4.2. Uso proibitivo do certificado

As aplicações para as quais são adequados os certificados emitidos pela AC PR e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso destes certificados, estão relacionadas na PC correspondente.

1.5. Política de administração

Esta DPC é administrada pela Diretoria de Tecnologia da Secretaria de Administração da Secretaria-Executiva da Casa Civil da Presidência da República (DITEC/SA/SE/CC/PR).

1.5.1. Organização administrativa do documento

Autoridade Certificadora da Presidência da República (AC PR).

1.5.2. Contatos

Administrativo:

Autoridade Certificadora da DITEC – ACPR/DITEC
Endereço: Anexo IV do Palácio do Planalto, Brasília, Distrito Federal, CEP: 70.150-900.
Página web: <https://www.planalto.gov.br/acpr>
E-mail: acpr@presidencia.gov.br
Telefone: (61) 3411-2668

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

Nome: Sthefano Giovanni Lobato Benathar
Telefone: (61) 3411-3398
E-mail: acpr@presidencia.gov.br

1.5.4. Procedimentos de aprovação da DPC

Esta DPC é aprovada pela AC PR e pelo ITI.

Os procedimentos de aprovação da DPC da AC PR 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
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
DETRAN	Departamento Nacional de Trânsito
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	<i>Intrusion Detection System</i>
IEC	<i>International Electrotechnical Commission</i>
IETF PKIX	<i>Internet Engineering Task Force - Public-Key Infrastructured (X.509)</i>
ISO	<i>International Organization for Standardization</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	<i>Online Certificate Status Protocol</i>

OID	<i>Object Identifier</i>
OM-BR	Objetos Metrológicos ICP-Brasil
OU	<i>Organization Unit</i>
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade do 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	<i>Request For Comments</i>
RG	Registro Geral
SNMP	<i>Simple Network Management Protocol</i>
UF	Unidade de Federação
URL	<i>Uniform Resource Locator</i>

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios

2.1.1. Obrigações:

- a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC PR e a sua LCR;
- b) disponibilizar para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
- c) implementar os recursos necessários para garantir a segurança dos dados nele armazenados.

2.1.2. Os requisitos aplicáveis aos repositórios da AC PR estão abaixo descritos:

- a) localização física:

Endereço: Presidência da República, Anexo IV do Palácio do Planalto, Brasília, Distrito Federal, CEP: 70.150-900.

Para os certificados emitidos pela AC PR, tem-se os repositórios nos seguintes endereços:

Versão	Repositório
V6	http://repositorio.serpro.gov.br/lcr/acprv6.crl , http://certificados2.serpro.gov.br/lcr/acprv6.crl

V5

<http://repositorio.serpro.gov.br/lcr/acprv5.crl>,
<http://certificados2.serpro.gov.br/lcr/acprv5.crl>

- b) a disponibilidade está referida no item 2.2.1;
- c) protocolos de acesso: HTTP e HTTPS; e
- d) requisitos de segurança: obedece aos requisitos definidos no item 5.

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

2.1.4. A AC PR disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR: <http://repositorio.serpro.gov.br/lcr/acprv6.crl> e <http://repositorio.serpro.gov.br/lcr/acprv5.crl>.

2.2. Publicação de informações dos certificados

2.2.1. AAC PR publica e mantém disponível em sua página web as informações descritas no item 2.2.2. no endereço <https://certificados.serpro.gov.br/acpr>. A disponibilidade da página é de no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2. As seguintes informações são publicadas na página *web*;

- a) seu próprio certificado;
- b) suas LCRs;
- c) sua DPC;
- d) a PC que implementa;
- e) uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços; e
- f) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3. Tempo ou frequência de publicação

Deve ser informada a frequência de publicação das informações de que trata o item anterior, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

2.3.1. Os certificados e a LCR são publicados imediatamente após sua emissão pela AC PR. As demais informações mencionadas no item 2.2.2. serão publicadas sempre que sofrerem alterações.

2.4. Controle de acesso aos repositórios

2.4.1. Não existe nenhuma restrição ao acesso para consulta a esta DPC, à sua PC, aos certificados emitidos e à LCR da AC PR. Acessos para escrita nos locais de armazenamento e publicação são permitidos apenas às pessoas responsáveis, designadas especificamente para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

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

3.1. Atribuição de nomes

3.1.1. Tipos de nomes

3.1.1.1. Os tipos de nomes admitidos para os titulares de certificados da AC PR são:

- a) Certificados de pessoa física, para a AC PR v5 e AC PR v6, o campo "Common name" (CN) é composto do nome do Titular do Certificado;

b) Certificados de pessoa jurídica, para a AC PR v5, o campo "Common name" (CN) é composto do nome empresarial da pessoa jurídica.

3.1.1.2. Não se aplica.

3.1.2. Necessidade dos nomes serem significativos

Para identificação dos titulares dos certificados emitidos, a AC PR faz uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem.

3.1.3. Anonimato ou pseudônimo dos titulares do certificado

Não se aplica.

3.1.4. Regras para interpretação de vários tipos de nomes

3.1.4.1 Os requisitos e procedimentos específicos, quando aplicáveis, estão detalhados na PC implementada.

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

3.1.5. Unicidade de nomes

No âmbito da AC PR, os identificadores do tipo "Distinguished name" (DN) é único para cada titular de certificado. Números ou letras adicionais são incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6. Procedimento para resolver disputa de nomes

AAC PR reserva-se o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes. Durante o processo de confirmação de identidade, cabe ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.2. Validação inicial de identidade

Os procedimentos e os requisitos para a primeira identificação e cadastramento junto à ICP-Brasil de pessoas físicas titulares ou responsáveis por certificados digitais, compreende os seguintes processos:

- a) identificação e cadastro iniciais do titular do certificado – identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2 e 3.2.3, observado o quanto segue:
 - i. para certificados de pessoa física: comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação e biometrias apresentadas, vedada qualquer espécie de procuração para tal fim.
 - ii. para certificados de pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado, e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação.

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

3.2.1. Método para comprovar o controle de chave privada

A confirmação de que a entidade solicitante controla a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo as referências contidas na RFC 4210 e 6712.

3.2.2. Autenticação da identidade de uma organização

3.2.2.1. Disposições Gerais

3.2.2.1.1 Os procedimentos empregados pela AR vinculada para a confirmação da identidade de uma pessoa jurídica é feita mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

3.2.2.1.2 Sendo titular do certificado pessoa jurídica, será designado pessoa física, como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

3.2.2.1.3 É feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

- a) apresentação do rol de documentos elencados no item 3.2.2.2;
- b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;
- c) coleta e verificação biométrica da pessoa física responsável pelo certificado, conforme regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, que definam os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado ICP-Brasil, bem com os procedimentos para identificação biométrica na ICP-Brasil; e
- d) assinatura do termo de titularidade de que trata o item 4.1 pelo responsável pelo certificado.

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

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

3.2.2.1.5 O disposto no item 3.2.2.1.3 é realizado:

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

3.2.2.2. Documentos para efeitos de identificação de uma organização

A confirmação da identidade de uma pessoa jurídica é feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos a sua habilitação jurídica:

- i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do CNPJ;
- ii. se entidade privada:
 1. certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e
 2. documentos da eleição de seus representantes legais, quando aplicável;

b) Relativos a sua habilitação fiscal:

- i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ; ou
- ii. prova de inscrição no Cadastro Nacional de Obras – CNO.

Nota 1: As confirmações de que trata o item 3.2.2.2 podem ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório que essas validações constem no dossiê eletrônico do titular do certificado.

3.2.2.3 Responsabilidade decorrente do uso do certificado de uma organização

Os atos praticados com o certificado digital de titularidade de uma organização estão sujeitos ao regime de responsabilidade definido em lei.

3.2.2.4. Informações contidas no certificado emitido para uma organização

3.2.2.4.1. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

- a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;
- b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
- c) Nome completo do responsável pelo certificado, sem abreviações; e
- d) Data de nascimento do responsável pelo certificado.

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

3.2.3. Autenticação da identidade de um indivíduo

Procedimento empregado pela AR vinculada à AC PR para a identificação e cadastramento iniciais de um indivíduo na ICP-Brasil. A confirmação é realizada mediante a presença física do interessado ou por um dos procedimentos listados nas alíneas abaixo, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico:

- a) não se aplica;
- b) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz; ou
- c) não se aplica.

3.2.3.1. Procedimento para identificação de um indivíduo

A identificação da pessoa física requerente do certificado é realizada como segue:

- a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:

- i. Registro de Identidade, se brasileiro; ou
- ii. Título de Eleitor, com foto; ou
- iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
- iv. Passaporte, se estrangeiro não domiciliado no Brasil.

b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual define os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

Nota 1: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

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

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

3.2.3.1.3. Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, são verificados:

- a) por AGR distinto do que realizou a etapa de identificação;
- b) pela AR ou AR própria da AC PR ou ainda AR própria do PSS da AC PR; e
- c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

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

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.1.7. Para a identificação de indivíduo na emissão de certificado digital em conjunto à Carteira de Identidade (RG) ou à Carteira Nacional de Habilitação (CNH), por Órgão de Identificação ou Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, deverá ser observado o disposto no item 3.2.9.8.

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

3.2.3.1.8.1. Não se aplica.

3.2.3.2. Informações contidas no certificado emitido para um indivíduo

3.2.3.2.1. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:

- a) nome completo, sem abreviações;
- b) data de nascimento; e
- c) Cadastro de Pessoa Física (CPF).

3.2.3.2.1.1. Não se aplica.

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

- a) número de Identificação Social - NIS (PIS, PASEP ou CI);

- b) número do Registro Geral - RG do titular e órgão expedidor;
- c) número do Cadastro Específico do INSS (CEI) ou CAEPF;
- d) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor; e
- e) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

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

3.2.3.2.3.1. Não se aplica.

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

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

3.2.4. Informações não verificadas do titular do certificado

Não se aplica.

3.2.5. Validação das autoridades

Não se aplica.

3.2.6. Critérios para interoperação

Não se aplica.

3.2.7. Autenticação da identidade de um equipamento ou aplicação

3.2.7.1. Disposições Gerais

Não se aplica.

3.2.7.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação

Não se aplica.

3.2.7.3. Informações contidas no certificado emitido para um equipamento ou aplicação

Não se aplica.

3.2.7.4. Autenticação de identificação de equipamento para certificado CF-e-SAT

Não se aplica.

3.2.7.5. Procedimentos para efeitos de identificação de um equipamento SAT

Não se aplica.

3.2.7.6. Informações contidas no certificado emitido para um equipamento SAT

Não se aplica.

3.2.7.7. Autenticação de identificação de equipamentos para certificado OM-BR

Não se aplica.

3.2.7.8. Procedimentos para efeitos de identificação de um equipamento metrológico

Não se aplica.

3.2.7.9. Informações contidas no certificado emitido para um equipamento metrológico

Não se aplica.

3.2.8. Procedimentos complementares

3.2.8.1. AAC PR mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC PR é membro, bem como os Princípios e Critérios *WebTrust*.

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

3.2.8.2.1. Não se aplica.

3.2.8.3. É mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias são mantidas em papel ou em forma digitalizada, observadas as condições definidas em regulamento editado por Instrução Normativa da AC Raiz que defina as CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs da ICP-Brasil [1].

3.2.8.3.1. Não se aplica.

3.2.8.3.2. No caso de certificados emitidos em conjunto à Carteira de Identidade (RG) ou à Carteira Nacional de Habilitação (CNH), por Órgão de Identificação ou Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, deverá ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade do indivíduo, incluindo, a Carteira de Identidade ou CNH emitida em conjunto ao certificado. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas em regulamento editado por Instrução Normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.3.3. Não se aplica.

3.2.8.4. A AC PR disponibiliza para a AR vinculada, a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6] e em regulamento editado por instrução normativa da AC Raiz que defina os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil.

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

3.2.8.4.2. Não se aplica.

3.2.9. Procedimentos específicos

3.2.9.1. Nos casos de certificado digital emitido para Servidores do Serviço Exterior Brasileiro, em missão permanente no exterior, assim caracterizados conforme a Lei no 11.440, de 29 de dezembro de 2006, se houver impedimentos para a identificação conforme o disposto no item 3.2, é facultada a remessa da documentação pela mala diplomática e a realização da identificação por outros meios seguros, a serem definidos e aprovados pela AC-Raiz da ICP-Brasil.

3.2.9.2. Não se aplica.

3.2.9.3. Não se aplica.

3.2.9.4. Não se aplica.

3.2.9.5. Não se aplica.

3.2.9.6. Não se aplica.

3.2.9.7. Não se aplica.

3.2.9.8. Não se aplica.

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. Esta DPC estabelece os processos de identificação e confirmação do cadastro do solicitante, utilizados pela AC PR responsável para a geração de novo par de chaves e de seu correspondente novo certificado.

3.3.2. Esse processo é conduzido segundo uma das seguintes possibilidades:

- a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3;
- b) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, cujo certificado requisitado seja do mesmo nível de segurança ou inferior; ou
- c) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico;

3.3.2.1. Não se aplica.

3.3.3. Não existem procedimentos específicos na PC implementada.

3.3.4. Não se aplica.

3.4. Identificação e autenticação para solicitação de revogação

O solicitante da revogação de certificado é identificado.

O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.9.3. As solicitações de revogação de certificado são registradas no sistema da AC PR.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. Solicitação do certificado

Os requisitos e procedimentos operacionais estabelecidos pela AC PR e sua AR vinculada para as solicitações de emissão de certificado compreendem, em detalhes, todas as ações necessárias tanto do indivíduo solicitante quanto da AC e AR no processo de solicitação de certificado digital. Contempla ainda:

- a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
- b) mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do AGR responsável pelas solicitações de emissão e de revogação de certificados;
- c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico, e, ainda, quando emissão para servidor público da ativa e militar da União, Estados e Distrito Federal pela autoridade designada formalmente pelos órgãos competentes;

d) não se aplica.

4.1.1. Quem pode submeter uma solicitação de certificado

A submissão da solicitação é sempre por intermédio da AR vinculada à AC PR.

4.1.1.1. Não se aplica.

4.1.1.2. Não se aplica.

4.1.1.3. Não se aplica.

4.1.1.4. Não se aplica.

4.1.2. Processo de registro e responsabilidades

Nos itens a seguir são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1. Responsabilidades da AC PR

4.1.2.1.1. AAC PR responde pelos danos a que der causa.

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

4.1.2.1.3. Não se aplica.

4.1.2.2. Obrigações da AC PR

- a) operar de acordo com a sua DPC e com a PC que implementa;
- b) gerar e gerenciar os seus pares de chaves criptográficas;
- c) assegurar a proteção de suas chaves privadas;
- d) não se aplica;
- e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- f) distribuir o seu próprio certificado;
- g) emitir, expedir e distribuir os certificados da AR a ela vinculada e de usuários finais;
- h) informar a emissão do certificado ao respectivo solicitante;
- i) revogar os certificados por ela emitidos;
- j) emitir, gerenciar e publicar suas LCRs;
- k) publicar na página web a sua DPC e PC aprovadas que implementa;
- l) publicar, na página web, as informações definidas no item 2.2.2 deste documento;
- m) publicar, na página web, informações sobre o descredenciamento de AR;
- n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
- o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementa, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
- t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;
- u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
- v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;

- w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
- x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de sua AR, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada às ACs que utilizam de seus serviços; e
- y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por AGR e estações de trabalho autorizados.

4.1.2.3. Responsabilidades da AR

A AR é responsável pelos danos a que der causa.

4.1.2.4. Obrigações da AR

As obrigações da AR vinculada à AC PR responsável por esta DPC são as abaixo relacionadas:

- a) receber solicitações de emissão ou de revogação de certificados;
- b) confirmar a identidade do solicitante e a validade da solicitação;
- c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC PR utilizando protocolo de comunicação seguro, conforme padrão definido em regulamento editado por Instrução Normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil;
- d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC PR vinculada e pela ICP-Brasil, em especial com o contido em regulamento editado por Instrução Normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil, bem como Princípios e Critérios WebTrust para AR [5];
- f) manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;
- g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2 e 3.2.3; e
- h) divulgar suas práticas, relativas a cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios WebTrust para AR [5].

4.2. Processamento de solicitação de certificado

4.2.1. Execução das funções de identificação e autenticação

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

4.2.2. Aprovação ou rejeição de pedidos de certificado

4.2.2.1. Não se aplica.

4.2.2.2. A AC PR e AR vinculada aceitam ou rejeitam, com a devida justificativa formal, pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC.

4.2.3. Tempo para processar a solicitação de certificado

A AC deve cumprir os procedimentos determinados na ICP-Brasil. Não haverá tempo máximo para processar as solicitações na ICP-Brasil.

4.3. Emissão de certificado

4.3.1. Ações da AC durante a emissão de um certificado

4.3.1.1. Os certificados são emitidos pela AC PR de acordo com os seguintes passos:

- a) O AGR da AR vinculada verifica o completo e correto preenchimento da solicitação do certificado, bem como a documentação do solicitante;
- b) O AGR da AR aprova a solicitação, disponibilizando o certificado para a instalação por seu solicitante;
- c) O software de AC emite automaticamente um e-mail informando ao solicitante que o certificado está disponível para instalação.

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

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

O software de AC emite automaticamente um e-mail informando ao solicitante que o certificado está disponível para instalação.

4.4 Aceitação de certificado

4.4.1. Conduta sobre a aceitação do certificado

4.4.1.1. O recebimento de um certificado pelo Titular de Certificado e o uso subsequente das chaves e certificado, constitui aceitação do certificado por parte do Titular de Certificado. Aceitando um certificado, o Titular de Certificado:

- a) concorda estar de acordo com as responsabilidades contínuas, obrigações e deveres impostos a ele pelo Termo de Titularidade e PC implementada pela AC PR e esta DPC;
- b) garante que por seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado; e
- c) afirma que as informações de certificado fornecidas durante o processo de solicitação são verdadeiras e foram publicadas dentro do certificado com precisão.

4.4.1.2. A aceitação de todo certificado emitido para pessoa física é garantida pela assinatura do Termo de Titularidade pelo respectivo titular. No caso de certificado emitido para pessoa jurídica, a aceitação é feita pela pessoa física responsável pelo certificado.

4.4.1.3. Não se aplica.

4.4.2. Publicação do certificado pela AC

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

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

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

4.5 Usabilidade do par de chaves e do certificado

O titular do certificado para usuário final deve operar de acordo com a DPC e PC que a AC PR implementa, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

4.5.1. Usabilidade da chave privada e do certificado do titular

4.5.1.1. AAC PR utiliza sua chave privada e garante a proteção dessa chave conforme o previsto nesta DPC.

4.5.1.2. Obrigações do Titular do Certificado

As obrigações do titular de certificado emitido de acordo com esta DPC e constantes dos termos de titularidade de que trata o item 4.1, são as abaixo relacionadas:

- a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- b) garantir a proteção e o sigilo de suas chaves privadas, código de ativação (PIN) e dispositivos criptográficos;
- c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
- d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;
- e) informar à AC PR qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente; e
- f) garantir a proteção do PUK, sendo permitido o gerenciamento por entidade autorizada pelo titular do certificado, mediante identificação presencial ou outro método com nível de segurança equivalente.

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

4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Em acordo com item 3.3 desta DPC.

4.6.1. Circunstâncias para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.2. Quem pode solicitar a renovação

Em acordo com item 3.3 desta DPC.

4.6.3. Processamento de requisição para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.4. Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com item 3.3 desta DPC.

4.6.6. Publicação de uma renovação de um certificado pela AC

Não se aplica.

4.6.7. Notificação de emissão de certificado pela AC para outras entidades

Em acordo com item 4.3 desta DPC.

4.7. Nova chave de certificado (Re-key)

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica.

4.7.2. Quem pode requisitar a certificação de uma nova chave pública

Não se aplica.

4.7.3. Processamento de requisição de novas chaves de certificado

Não se aplica.

4.7.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.7.5. Conduta constituindo a aceitação de uma nova chave certifica

Não se aplica.

4.7.6. Publicação de uma nova chave certificada pela AC

Não se aplica.

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

Não se aplica.

4.8. Modificação de certificado

Não se aplica.

4.8.1. Circunstâncias para modificação de certificado

Não se aplica.

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3. Processamento de requisição de modificação de certificado

Não se aplica.

4.8.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica.

4.8.6. Publicação de uma modificação de certificado pela AC

Não se aplica.

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

Não se aplica.

4.9. Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

4.9.1.1. A AC PR pode revogar um certificado por ela emitido pelos seguintes motivos:

- a) Solicitação de revogação corretamente preenchida pelo Titular do Certificado;
- b) Solicitação de revogação enviada à AC por um terceiro autorizado, por exemplo, uma determinação judicial;
- c) Solicitação de revogação feita por uma pessoa com procuração do Titular do Certificado;
- d) Titular de Certificado deixa a comunidade de interesses sob a qual seu certificado foi emitido, por exemplo:

- Titular de Certificado organizacional deixa o emprego;

- Ocorre o falecimento do Titular de Certificado.

4.9.1.2. Um certificado é revogado obrigatoriamente pelos seguintes motivos.

- a) quando constatada emissão imprópria ou defeituosa;
- b) quando for necessária a alteração de qualquer informação constante no mesmo;
- c) no caso de dissolução da AC PR; ou
- d) no caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3. Em relação à revogação, deve ainda ser observado que:

- a) A AC Raiz, deverá revogar, no prazo definido no item 4.9.3.3, o certificado da entidade que deixa de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil; e
- b) O CG da ICP-Brasil ou a AC Raiz determina a revogação do certificado da AC que deixa de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

4.9.1.4. Todo certificado deverá ter a sua validade verificada, na respectiva LCR ou OCSP, antes de ser utilizado.

4.9.1.5. A autenticidade da LCR deverá também ser confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR.

4.9.2. Quem pode solicitar revogação

A solicitação para a revogação de um certificado somente é feita:

- a) Por solicitação do titular do certificado;
- b) Por solicitação do responsável pelo certificado, no caso de certificado pessoa jurídica;
- c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- d) Pela AC emitente;
- e) Por uma AR vinculada;
- f) Por determinação do CG da ICP-Brasil ou da AC Raiz;
- g) Não se aplica.
- h) Não se aplica.
- i) Não se aplica.
- j) Não se aplica.

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. O procedimento para a solicitação de uma revogação varia dependendo de quem a origina. A solicitação de revogação de certificado pode ser realizada de duas formas:

- a) Através da página web <https://certificados.serpro.gov.br/arpr> de solicitação do certificado na opção "Revogar"; ou
- b) Emissão do Termo de Revogação disponível na opção "Outras Funções". Só serão aceitos pedidos de revogação do Titular do Certificado.

4.9.3.2. Como diretrizes gerais, esta DPC estabelece que:

- a) O solicitante da revogação de um certificado será identificado;
- b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas;

- c) As justificativas para a revogação de um certificado são documentadas; e
- d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

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

4.9.3.4. Não se aplica.

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

4.9.3.6. Não existem procedimentos específicos na PC implementada.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação é imediata quando configuradas as circunstâncias definidas no item 4.9.1.

4.9.4.2. A AC PR estabelece o prazo de 5 (cinco) dias úteis para a aceitação do certificado solicitado por seu titular, dentro dos quais a revogação do certificado poderá ser solicitada sem cobrança de tarifa pela AC PR.

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

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC PR processa a revogação imediatamente após a análise do pedido.

4.9.6. Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7. Frequência de emissão de LCR

4.9.7.1. A frequência de emissão de LCR referente a certificados de usuários finais é a cada 30 (trinta) minutos.

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

4.9.7.3. Não se aplica.

4.9.7.4. Não se aplica.

4.9.7.5. Não se aplica.

4.9.8. Latência máxima para a LCR

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

4.9.9. Disponibilidade para revogação/verificação de status on-line

Não se aplica.

4.9.10. Requisitos para verificação de revogação on-line

Não se aplica.

4.9.11. Outras formas disponíveis para divulgação de revogação

4.9.11.1. A AC PR não suporta outras formas para divulgação da revogação que não através da publicação de LCR.

4.9.11.2. Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. Quando há comprometimento ou suspeita de comprometimento da chave privada, o Titular do Certificado deve comunicar imediatamente à AC PR.

4.9.12.2. A comunicação à AC PR é por e-mail ou contato telefônico, conforme dados informados no item 1.5.2. desta DPC.

4.9.13. Circunstâncias para suspensão

Não se aplica.

4.9.14. Quem pode solicitar suspensão

Não se aplica.

4.9.15. Procedimento para solicitação de suspensão

Não se aplica.

4.9.16. Limites no período de suspensão

Não se aplica.

4.10. Serviços de status de certificado

4.10.1. Características operacionais

AAC PR fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR.

4.10.2. Disponibilidade dos serviços

Ver item 4.9.

4.10.3. Funcionalidades operacionais

Ver item 4.9.

4.11. Encerramento de atividades

4.11.1. O descredenciamento da AC PR poderá ocorrer em algumas hipóteses:

- a) quando da expiração do prazo de validade do certificado da AC PR, sem que haja a emissão de novo certificado para substituí-lo;
- b) quando descredenciamento da AC de nível imediatamente superior;
- c) a pedido da própria AC PR, mediante requerimento, em relação às suas atividades; ou
- d) por determinação da AC Raiz, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.11.2. Não se aplica.

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

Não se aplica.

4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão

Não se aplica.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO e DE INSTALAÇÕES

A seguir, estão descritos os controles de segurança implementados pela AC PR e pela AR a ela vinculada para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 Controles Físicos

5.1.1 Construção e localização das instalações de AC PR

5.1.1.1. A localização e o sistema de certificação utilizado para a operação da AC PR não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Todos os aspectos de construção das instalações da AC PR, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos abaixo:

- a) instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, retificadores e estabilizadores e similares;
- b) instalações para sistemas de telecomunicações;
- c) sistemas de aterramento e de proteção contra descargas atmosféricas ; e
- d) iluminação de emergência.

5.1.2. Acesso físico

O acesso físico às dependências da AC PR é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.1.2.1 Níveis de Acesso

5.1.2.1.1. São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da AC, e mais 2 (dois) níveis relativos à proteção da chave privada de AC.

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro nível e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico, e o uso de crachá.

5.1.2.1.5. O terceiro nível – ou nível 3 – é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

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

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

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

5.1.2.1.9. No quarto nível, as paredes, piso e o teto são inteiriços e revestidos de aço e concreto, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física

das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem a chamada sala cofre - possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10. A sala cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.

5.1.2.1.11. São três os ambientes de quarto nível abrigados pela sala cofre:

- a) Sala de equipamentos de produção *on-line* e cofre de armazenamento;
- b) Sala de equipamentos de produção *off-line* e cofre de armazenamento; e
- c) Equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

5.1.2.1.12. O quinto nível – ou nível 5 – é interno aos ambientes de nível 4, e compreende cofres e gabinetes reforçados trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre ou o gabinete obedecem às seguintes especificações mínimas:

- a) Ser feito em aço ou material de resistência equivalente; e
- b) Possuir tranca com chave.

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

5.1.2.2 Sistemas físicos de detecção

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

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

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes.

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

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

5.1.2.2.6. Os sistemas de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmaras de vídeo cujo posicionamento permite o acompanhamento das ações.

5.1.2.3 Sistema de Controle de Acesso

O sistema de controle de acesso está baseado em um ambiente de nível 4.

5.1.2.4 Mecanismos de emergência

5.1.2.4.1. Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

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

5.1.3 Energia e ar-condicionado

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

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

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

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

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

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

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

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

5.1.3.9. O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC PR é garantida por meio de:

- a) Geradores de porte compatível;
- b) Geradores de reserva;
- c) Sistemas de *no-breaks* redundantes;
- d) Sistemas redundantes de ar-condicionado.

5.1.4. Exposição à água

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

5.1.5. Prevenção e proteção contra incêndio nas instalações da AC

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

5.1.5.2. Nas instalações da AC PR não é permitido fumar ou portar objetos que produzam fogo ou fumaça.

5.1.5.3. A sala cofre possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala cofre são eclusas, uma porta só se abre quando a anterior está fechada.

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

5.1.6. Armazenamento de mídia

A AC PR atende a norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7. Destruição de lixo

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo.

5.1.7.2. Todos os dispositivos eletrônicos não mais utilizáveis, e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, são fisicamente destruídos.

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

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

5.2. Controles Procedimentais

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

5.2.1.1. A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com o seu perfil.

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

5.2.1.3. Todos os operadores do sistema de certificação da AC PR recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4. Quando um empregado se desliga da AC PR, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da AC PR, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC PR no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC, conforme o descrito em 6.2.2.

5.2.2.3. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC PR necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da AC PR. As demais tarefas da AC PR podem ser executadas por um único operador.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Pessoas que ocupam os perfis designados pela AC PR passam por um processo rigoroso de seleção. Todo funcionário da AC PR tem sua identidade e perfil verificados antes de:

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

5.2.3.2. Os certificados, contas e senhas utilizados para identificação e autenticação dos funcionários:

- a) São diretamente atribuídos a um único operador (funcionário da AC devidamente qualificado);
- b) Não são compartilhados;
- c) São restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC PR implementa um padrão de utilização de "senhas fortes", definido em sua Política de Segurança (PS) e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], junto a procedimentos de validação dessas senhas.

5.2.4. Funções que requerem separação de deveres

Na AC PR existe a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3. Controles de Pessoal

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC PR, pela AR e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. A DPC garante que todos os empregados da AC PR e da AR e PSS vinculados, encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

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

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC PR e AR vinculada, envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3.2. Procedimentos de Verificação de Antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC PR e da AR vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é submetido aos seguintes processos, antes do começo das atividades de:

- a) Verificação de antecedentes criminais;
- b) Verificação de situação de crédito;
- c) Verificação de histórico de empregos anteriores; e
- d) Comprovação de escolaridade e de residência.

5.3.2.2. AAC PR poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

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

- a) Princípios e mecanismos de segurança da AC PR e da AR vinculada;
- b) Sistema de certificação em uso na AC PR;
- c) Procedimentos de recuperação de desastres e de continuidade do negócio;
- d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.2.2 e 3.2.3; e
- e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC PR e da AR vinculada, envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC ou da AR.

5.3.5 Frequência e sequência de rodízios de cargos

AAC não implementa rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. A AC PR, na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC ou de uma AR vinculada, suspenderá de imediato o acesso dessa pessoa ao seu sistema de certificação e instaurará processo administrativo para apurar os fatos e, se for o caso, adotará as medidas legais cabíveis.

5.3.6.2. O processo administrativo referido acima conterá, no mínimo, os seguintes itens:

- a) Relato da ocorrência com “modus operandis”;
- b) Identificação dos envolvidos;
- c) Eventuais prejuízos causados;

- d) Punições aplicadas, se for o caso; e
- e) Conclusões.

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

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

- a) Advertência;
- b) Suspensão por prazo determinado; ou
- c) Impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC PR e da AR vinculada, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC PR poderá definir requisitos adicionais para a contratação.

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC PR disponibiliza para todo o seu pessoal e para o pessoal da AR vinculada, no mínimo:

- a) Esta DPC;
- b) A PC que implementa;
- c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];
- d) Documentação operacional relativa às suas atividades; e
- e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela AC PR.

5.4. Procedimentos de Log de auditoria

Nos itens seguintes, esta DPC descreve os aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC PR com o objetivo de manter um ambiente seguro.

5.4.1. Tipos de Evento Registrados

5.4.1.1. Todas as ações executadas pelo pessoal da AC PR, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou. A AC PR registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

- a) Iniciação e desligamento do sistema de certificação;
- b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC;
- c) Mudanças na configuração da AC ou nas suas chaves;
- d) Mudanças nas políticas de criação de certificados;
- e) Tentativas de acesso (login) e de saída do sistema (logout);
- f) Tentativas não-autorizadas de acesso aos arquivos de sistema;
- g) Geração de chaves próprias da AC ou de chaves de usuários finais;
- h) Emissão e revogação de certificados;
- i) Geração de LCR;
- j) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
- k) Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
- l) Operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1. Não se aplica.

5.4.1.2. A AC PR registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, quais sejam:

- a) Registros de acessos físicos;
- b) Manutenção e mudanças na configuração de seus sistemas;
- c) Mudanças de pessoal e de perfis qualificados;
- d) Relatórios de discrepância e comprometimento; e
- e) Registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

5.4.1.3. Os registros de auditoria mínimos a serem mantidos pela AC incluem além dos acima:

- a) Registros de solicitação, inclusive registros relativos a solicitações rejeitadas;
- b) Pedidos de geração de certificado, mesmo que a geração não tenha êxito;
- c) Registros de solicitação de emissão de LCR.

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

5.4.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC PR é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.1.6. A AR vinculada à AC PR responsável pela DPC deverá registrar eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

- a) Os AGRs que realizaram as operações;
- b) Data e hora das operações;
- c) A associação entre os agentes que realizaram a validação e aprovação e o certificado gerado; e
- d) A assinatura digital do executante.

5.4.1.6.1. Não se aplica.

5.4.1.7. A AC PR armazena digitalmente as cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados e dos termos de titularidade.

5.4.2. Frequência de auditoria de registros

A periodicidade de auditoria de registros não é superior a uma semana, sendo que os registros de auditoria são analisados pelo pessoal operacional da AC PR. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando-se que não foram alterados. Em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3. Período de Retenção para registros de auditoria

A AC PR mantém localmente, nas instalações do SERPRO, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 5.5.

5.4.4. Proteção de registro de auditoria

5.4.4.1. Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação.

5.4.4.2. As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação.

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

5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria

AAC PR executa procedimentos de backup, de todo o sistema de certificação (sistemas operacionais, aplicação e banco de dados) de duas formas:

- a) Diariamente: cópia de segurança; e
- b) Semanalmente: cópia armazenada para processos de auditoria.

5.4.6. Sistema de coleta de dados de auditoria(interno ou externo)

O sistema de coleta de dados de auditoria da AC PR é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação da AC PR, pelo sistema de controle de acesso e pelo pessoal operacional. A localização dos recursos se encontra na tabela abaixo:

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de log-in e log-out	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional
Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados	Automático	Software de AC ou AR
Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado	Automático	Software de AR
Logs de Backup e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de software e hardware	Manual	Pessoal de operações
Manutenção de sistema	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	Software de controle de acesso e pessoal de operações

5.4.7. Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da AC PR não são notificados à pessoa, organização, dispositivo ou aplicação que causou o evento.

5.4.8. Avaliações de vulnerabilidade

Eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC PR, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

5.5. Arquivamento de Registros

Nos itens seguintes é descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC PR e pela AR vinculada.

5.5.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC PR:

- a) Solicitações de certificados;
- b) Solicitações de revogação de certificados;
- c) Notificações de comprometimento de chaves privadas;
- d) Emissões e revogações de certificados;
- e) Emissões de LCR;
- f) Trocas de chaves criptográficas da AC PR; e
- g) Informações de auditoria previstas no item 5.4.1.

5.5.2. Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são os seguintes:

- a) As LCRs referentes a certificados de assinatura digital são retidas permanentemente, para fins de consulta histórica;
- b) Os dossiês dos titulares são retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e
- c) As demais informações, inclusive os arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

5.5.3. Proteção de arquivos

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.5.4. Procedimentos para cópia de arquivos

5.5.4.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo à AC PR e recebem o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

5.5.4.3. É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para datação de registros

Os servidores da AC PR são sincronizados com a hora fornecida pela AC Raiz por meio de sua Fonte Confiável do Tempo – FCT conforme DOC-ICP 07 [13]. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.

No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

5.5.6. Sistema de coleta de dados de arquivo (interno e externo)

O sistema de coleta de dados de arquivos da AC PR é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC PR e pelo pessoal operacional.

Tipo de evento	Sistema de coleção	Registrado por
----------------	--------------------	----------------

Solicitações de certificados	Automático e manual	Software de AC/AR e pessoal de operações
Solicitações de revogação de certificados	Automático e manual	Software de AC/AR e pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados	Automático	Software de AC/AR
Emissões de LCR	Automático	Software de AC/AR
Correspondências formais	Manual	Pessoal de operações

5.5.7. Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da AC PR e da AR vinculada é verificada na ocasião em que o arquivo é preparado ou diariamente com a execução automática de script.

5.6. Troca de chave

5.6.1. A AC PR comunica os Titulares de Certificado, por e-mail, a necessidade de renovação do certificado, com antecedência de 30 dias, com instruções para a renovação do certificado.

5.6.2. Detalhes dos procedimentos estão descritos nas PC implementadas.

5.7. Comprometimento e Recuperação de Desastre

A AC PR declara que os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres estão descritos no PCN da AC, conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], para garantir a continuidade dos seus serviços críticos.

5.7.1. Procedimentos gerenciamento de incidente e comprometimento

5.7.1.1. AAC PR possui ainda um Plano de Continuidade de Negócio (PCN), de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade de serviços críticos. Possui ainda o Plano de Respostas a Incidentes (PRI) e Plano de Recuperação de Desastres (PRD).

5.7.1.2. Os procedimentos no PCN da AR para recuperação, total ou parcial das atividades da AR vinculada à AC PR são os seguintes:

- a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;
- b) Identificação e concordância de todas as responsabilidades e procedimentos de emergência;
- c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários.
- d) Documentação dos processos e procedimentos acordados;
- e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e
- f) Teste e atualização dos planos.

5.7.2. Recursos computacionais, software, e/ou dados corrompidos

A AC PR possui o um PCN, que contém ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos e que podem ser resumidas no seguinte:

- a) É feita a identificação de todos os elementos corrompidos;
- b) O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
- c) É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um backup de segurança até a revogação do certificado da AC PR.

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

5.7.3.1. Certificado de entidade é revogado

A AC PR possui um PCN que especifica as ações a serem tomadas no caso em que o certificado da AC PR é revogado, e que podem ser resumidas da seguinte forma:

- a) AAC, a AC Raiz e os Titulares de Certificados serão notificadas por comunicação segura;
- b) AAC revoga os certificados por ela emitidos;
- c) AAC solicita um novo certificado;
- d) Iniciam-se os procedimentos para emissão dos novos certificados de usuários.

5.7.3.2. Chave de entidade é comprometida

A AC PR possui um PCN que especifica as ações a serem tomadas no caso de comprometimento de sua chave privada. Após a identificação da crise são notificados os gestores do processo de certificação digital que acionam as equipes envolvidas, para ativar o site de contingência.

5.7.4. Capacidade de continuidade de negócio após desastre

A AC PR possui um PRD que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da AC PR quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.

O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC PR faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a AC PR para tornar acessível os registros lógicos mantidos dentro do software. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo uma ordem de prioridade.

5.8. Extinção da AC

Conforme CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes são definidas as medidas de segurança implantadas pela AC PR para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. Também são definidos outros controles técnicos de segurança utilizados pela AC PR e pela AR vinculada 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. Após o deferimento do pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil, o par de chaves criptográficas da AC PR responsável por esta DPC é gerada pela própria AC.

6.1.1.2. Pares de chaves são gerados somente pelo titular do certificado correspondente. Os procedimentos específicos estão descritos na PC implementada.

6.1.1.3. A PC implementada pela AC PR define o meio utilizado para armazenamento das respectivas chaves privadas, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

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

6.1.1.6. A chave privada da AC PR é gerada, armazenada e utilizada apenas em hardware criptográfico específico. O módulo criptográfico da AC PR segue padrões de referência definidos em regulamento

editado por Instrução Normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.2. Entrega da chave privada à entidade titular

Não se aplica. É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Não se aplica.

6.1.3.2. As chaves públicas dos solicitantes de certificados são entregues por meio de uma troca on-line utilizando funções automáticas do software de certificação da AC PR.

6.1.4. Entrega de chave pública da AC PR às terceiras partes

As formas para a disponibilização do certificado da AC PR, e de todos os certificados da cadeia de certificação, para os usuários e terceiras partes, compreendem:

- a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato definido em regulamento editado por Instrução Normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil;
- b) Diretório;
- c) Página *web* da AC; e
- d) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC PR está definido no mesmo item da PC da AC PR, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.5.2. Não se aplica.

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

6.1.6.1. Os parâmetros de geração de chaves assimétricas da AC PR seguem o padrão definido em regulamento editado por Instrução Normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido 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 campo “Key usage” na X.509 v3)

6.1.7.1. Os certificados emitidos pela AC PR têm no campo “Key usage” (2.5.29.15) ativado os bits digitalSignature, nonRepudiation e keyEncipherment. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC PR, bem como as possíveis restrições cabíveis em conformidade com as aplicações definidas para os certificados correspondentes, estão especificados na PC que implementa.

6.1.7.2. A chave privada da AC PR é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCRs.

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

A chave privada da AC PR é gerada, armazenada e utilizada apenas em hardware criptográfico homologado e com padrão de segurança definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], não havendo, portanto, tráfego da mesma em nenhum momento.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC PR adota o padrão definido em regulamento editado por Instrução Normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.1.2. Os módulos de geração de chaves criptográficas dos titulares de certificados são aqueles definidos em regulamento editado por Instrução Normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.2. Controle “n de m’ para chave privada

6.2.2.1. A AC PR implementa o controle múltiplo para a ativação e desativação da sua chave privada através de controles de acesso físico e do software de certificação.

6.2.2.2. É exigido a presença no mínimo de 2 (dois) detentores da chave de ativação (“n”) de um grupo de 15 (quinze) (“m”) para a ativação da chave da AC PR.

6.2.3. Custódia (escrow) de chave privada

Não se aplica.

6.2.4. Cópia de segurança (backup) de chave privada

6.2.4.1. Como diretriz geral, qualquer entidade titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. AAC PR, responsável por esta DPC, mantém cópia de segurança de sua própria chave privada.

6.2.4.3. A AC PR não mantém cópia de segurança das chaves privadas de titulares de certificados de assinatura digital por ela emitido.

6.2.4.4. A cópia de segurança é armazenada cifrada por algoritmo simétrico definido 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.

6.2.5. Arquivamento de chave privada

6.2.5.1. AAC PR não existe arquivamento de chaves privadas de assinatura digital.

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

6.2.6. Inserção de chave privada em módulo criptográfico

A chave privada da AC PR é inserida no módulo criptográfico de acordo com os procedimentos especificados pelo fornecedor do módulo.

6.2.7. Armazenamento da chave privada em módulos criptográficos

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A ativação da chave privada da AC PR é implementada por meio de cartões criptográficos, protegidos com senha e após a identificação de 2 (dois) dos detentores da chave, será feita a ativação da chave criptográfica da AC. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC. As senhas utilizadas obedecem à política de senhas estabelecida pela AC PR.

6.2.9. Método de desativação de chave privada

A desativação da chave privada da AC PR é implementada por meio de cartões criptográficos, protegidos com senha e após a identificação de 2 (dois) dos detentores da chave, será feita a desativação da chave criptográfica da AC. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC. As senhas utilizadas obedecem à política de senhas estabelecida pela AC PR.

6.2.10. Método de destruição de chave privada

Quando a chave privada da AC PR for desativada, em decorrência de expiração ou revogação, esta deve ser destruída da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estiver armazenada, deve ser sobrescrito; todas as cópias de segurança da chave privada da AC e os cartões criptográficos dos custodiantes serão destruídos. Os agentes autorizados para realizar estas operações são os administradores e os custodiantes das chaves de ativação da AC.

6.3. Outros aspectos do gerenciamento do par de chaves

6.3.1. Arquivamento de chave pública

A AC PR armazena as chaves públicas da própria AC PR e dos titulares de certificados, bem como as LCRs emitidas, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas da AC PR e dos titulares de certificados de assinatura digital por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas são utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Os certificados emitidos na AC PR estão definidos na PCA3 da seguinte forma:
Certificados do tipo A3, com validade de até 5 (cinco) anos.

6.3.2.3. A validade admitida para certificados da AC PR é limitada à validade do certificado da AC RAIZ, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior (AC RAIZ).

6.4. Dados de ativação

Nos itens seguintes, estão descritos os requisitos gerais de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Cada PC implementada deve descrever os requisitos específicos aplicáveis.

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação da chave privada da AC PR são únicos e aleatórios.

6.4.1.2. Não se aplica.

6.4.2. Proteção dos dados de ativação

6.4.2.1. Os dados de ativação da AC PR são protegidos contra o uso não autorizado, por meio de mecanismos de criptografia e de controle de acesso físico.

6.4.2.2. Cada PC implementada garante que 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

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

6.5.1.2. Os requisitos gerais de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC PR estão descritos na PC implementada.

6.5.1.3. Os computadores servidores, utilizados pela AC PR, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

- a) Controle de acesso aos serviços e perfis da AC;
- b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC;
- c) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- d) Geração e armazenamento de registros de auditoria da AC;
- e) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- f) Mecanismos para cópias de segurança (*backup*).

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

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde residem os equipamentos utilizados para operação da AC, o equipamento que passou por manutenção é inspecionado. Todo equipamento que deixar de ser utilizado em caráter permanente, serão destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC PR. Todos esses eventos são registrados para fins de auditoria.

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

6.5.2. Classificação da segurança computacional

Não disponível.

6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. As estações de trabalho da AR, vinculada à AC PR, incluindo equipamentos portáteis, recebem as configurações de segurança especificadas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

6.5.3.2. Além dos itens descritos no item 6.5.3.1, são incluídos, pelo menos, os requisitos especificados em regulamento editado por Instrução Normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

6.5.3.3. Não se aplica.

6.6. Controles técnicos do ciclo de vida

Nos itens seguintes são descritos os controles implementados pela AC PR e pela AR a ela vinculada no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1 Controles de desenvolvimento de sistema

6.6.1.1. A AC PR adota o Sistema de Certificação Digital do SERPRO (Serviço Federal de Processamento de Dados), seu PSS. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e depois de concluído os testes é colocado em um ambiente de homologação. Finalizado o processo de homologação das customizações, o Gerente do Prestador de Serviço de Suporte avalia e decide quando será a implementação no ambiente de produção.

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

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. As ferramentas e os procedimentos empregados pela AC PR para garantir que os seus sistemas implementem os níveis configurados de segurança são os seguintes:

- a) A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1;
- b) A AC PR possui ferramenta automatizada para verificar integridade de arquivos e configurações.

6.6.2.2. O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC PR, envolve o teste de mudanças planejadas no Ambiente de Desenvolvimento e Homologação, isolados, antes de sua implantação no ambiente de Produção, incluindo as seguintes atividades:

- a) Instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;
- b) Implantação ou modificação de Autoridades Certificadoras com customizações em nível de certificados, páginas *web*, *scripts* etc;
- c) Implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos; e
- d) Instalação de novos serviços na plataforma de processamento.

6.6.3. Controles de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na geração de LCR

Todas as LCRs geradas pela AC PR são cheçadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7. Controles de segurança de rede

6.7.1. Diretrizes Gerais

6.7.1.1. Os controles implementados para garantir a confidencialidade, integridade e disponibilidade dos serviços da AC PR são os seguintes:

- a) Os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewalls* e sistemas de detecção de intrusão (IDS), que atendem o segmento de rede dos servidores *web* do sistema de certificação da AC PR, estão localizados e operam em ambiente protegido por perímetros de segurança controlados por vigilantes e controle de acesso biométrico;
- b) As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento e homologação;
- c) O acesso lógico aos elementos de infraestrutura e proteção de rede é restrito por meio de sistema de autenticação e autorização de acesso;
- d) Infraestrutura de conectividade, incluindo:
 - i. Alojamento seguro de equipamento de comunicação;
 - ii. Firewall seguro e serviços de roteador;
 - iii. Serviço de LAN seguro; e
 - iv. Serviço de internet seguro e redundante.

e) Prevenção incidente e avaliação, incluindo:

- i. Descoberta de intrusão;
- ii. Análise de vulnerabilidade;
- iii. Configuração segura de servidor; e
- iv. Auditorias técnicas.

f) Administração de infraestrutura, incluindo:

- i. Monitoramento de servidor;
- ii. Monitoramento de rede;
- iii. Monitoramento de URL; e
- iv. Relatórios de largura da banda.

6.7.1.2. Nos servidores e elementos de infraestrutura e proteção de rede utilizados pela AC, somente os serviços estritamente necessários são habilitados.

6.7.1.3. Os servidores e elementos de infraestrutura e proteção de rede tais como roteadores, hubs, switches, firewalls localizados no segmento de rede que hospeda o sistema de certificação da AC, estão localizados e operam em ambiente de nível 4.

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

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

6.7.2. Firewall

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

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

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1. O sistema de detecção de intrusão tem capacidade de reconhecer ataques em tempo real e respondê-los automaticamente com medidas tais como: enviar traps SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

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

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

6.7.4. Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – são registradas em arquivos para análise e são automatizadas. A frequência de exame dos arquivos de registro é diária ou quando ocorrer algum evento, e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. Carimbo de Tempo

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR E OCSP

Nos seguintes itens são descritos os aspectos dos certificados e LCR emitidos pela AC PR. A PC abaixo, implementada pela AC PR, especifica os formatos dos certificados gerados e das correspondentes LCRs. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

PC ACPR A3	2.16.76.1.2.3.1
------------	-----------------

7.1. Perfil do certificado

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

7.1.1. Número de versão

Todo certificado emitido pela AC PR implementa 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

Aquelas definidas pela AC PR no mesmo item da PC que implementa que são extensões obrigatórias para certificados de AC, conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I do DOC-ICP-04, aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC PR são assinados com o uso do algoritmo definido em regulamento editado por Instrução Normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

7.1.4. Formatos de nome

Os formatos de nome estão definidos pela AC no mesmo item da PC que implementa.

7.1.5. Restrições de nome

Restrições definidas pela AC PR estão definidas no mesmo item da PC que implementa.

7.1.6. OID (Object Identifier) da DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil após a conclusão do processo de credenciamento, é **2.16.76.1.1.1**.

7.1.7. Uso da extensão “Policy Constraints”

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos pela AC PR, o campo `policyQualifiers` da extensão “*Certificate Policies*” contém o endereço *web* (URL) da DPC da AC PR.

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas, no âmbito da AC PR, conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCRs geradas pela AC PR 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. AAC PR adota as seguintes extensões de LCR:

- a) “**Authority Information Access**”, **não crítica**: contém somente o método de acesso *id-ad-calssuer*, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação. Não deve ser utilizado nenhum outro método de acesso diferente de *id-ad-calssuer*.

7.2.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

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

7.3. Perfil de OCSP

7.3.1. Número (s) de versão

Não se aplica.

7.3.2. Extensões de OCSP

Não se aplica.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. Frequência e circunstâncias das avaliações

As entidades integrantes da ICP-Brasil sofrem auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento.

8.2. Identificação/Qualificação do avaliador

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

8.2.2. Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.3. Relação do avaliador com a entidade avaliada

Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, a auditoria da AC é realizada pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.4. Tópicos cobertos pela avaliação

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

8.4.2. AAC informa que recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e que é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.4.3. A AC informa que as entidades da ICP-Brasil a ela diretamente vinculadas, AR, PSS, também receberam auditoria prévia, para fins de credenciamento, e que AAC é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

8.5. Ações tomadas como resultado de uma deficiência

Em acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.6. Comunicação dos resultados

Em acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

As tarifas de emissão e de renovação de certificado pela AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [13].

9.1.2. Tarifas de acesso ao certificado

Não se aplica.

9.1.3. Tarifas de revogação ou de acesso à informação de status

Não se aplica.

9.1.4. Tarifas para outros serviços

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

9.1.5. Política de reembolso

Não se aplica.

9.2. Responsabilidade Financeira

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

9.2.1. Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2. Outros ativos

Conforme regramento desta DPC.

9.2.3. Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3. Confidencialidade da informação do negócio

9.3.1. Escopo de informações confidenciais

9.3.1.1. Todas as informações coletadas, geradas, transmitidas e mantidas pela AC PR são consideradas sigilosas, exceto aquelas informações citadas no item 9.3.2.

9.3.1.2. Como princípio geral, nenhum documento, informação ou registro fornecido à AC ou à AR vinculada é divulgado.

9.3.2. Informações fora do escopo de informações confidenciais

Os seguintes documentos da AC PR e AR vinculada, considerados não sigilosos, compreendem, entre outros:

- a) os certificados e as LCRs emitidas pela AC;
- b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
- c) a PC implementada pela AC;
- d) a DPC da AC;
- e) versões públicas de PS; e
- f) a conclusão dos relatórios de auditoria.

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

9.3.2.2. Os seguintes documentos da AC PR também são considerados documentos não confidenciais:

- a) a PC que implementa;
- b) a DPC que implementa;
- c) versões públicas de PS; e
- d) a conclusão dos relatórios da auditoria.

9.3.2.3. AAC PR também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados emitidos no âmbito da ICP-Brasil.

9.3.3. Responsabilidade em proteger a informação confidencial

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

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

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

9.3.3.4. Não se aplica.

9.4. Privacidade da informação pessoal

9.4.1. Plano de privacidade

AAC PR assegura a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2. Tratamento de informação como privadas

Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC PR será considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

9.4.3. Informações não consideradas privadas

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

9.4.4. Responsabilidade para proteger a informação privadas

AAC PR e AR vinculada são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5. Aviso e consentimento para usar informações privadas

As informações privadas obtidas pela AC PR poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável.

O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

Autorizações formais podem ser apresentadas de duas formas:

- a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou
- b) por meio de pedido escrito com firma reconhecida.

9.4.6. Divulgação em processo judicial ou administrativo

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

As informações privadas ou confidenciais sob a guarda da AC PR poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7. Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8. Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro, sob a guarda da AC PR ou AR vinculada, será fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

9.5. Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da AC

A AC PR declara e garante o quanto segue:

9.6.1.1. Autorização para certificado

A AC PR implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC. A AC PR, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos da AR a ela vinculada na forma de sua DPC, PC e normas complementares.

9.6.1.2. Precisão da informação

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

9.6.1.3. Identificação do requerente

A AC PR implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC PR, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos da AR a ela vinculada na forma de sua DPC, PC e normas complementares.

9.6.1.4. Consentimento dos titulares

AAC PR implementa termos de consentimento ou titularidade, contidas nos itens 3 e 4 desta DPC.

9.6.1.5. Serviço

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

9.6.1.6. Revogação

AAC PR revogará certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos Princípios e Critérios *WebTrust*

9.6.1.7. Existência Legal

Esta DPC está em conformidade legal com a MP 2.200-2, de 24 de agosto de 2001, com a Medida Provisória nº 951, de 15 de abril de 2020, e legislação aplicável.

9.6.2. Declarações e garantias da AR

Em acordo com item 4 desta DPC.

9.6.3. Declarações e garantias do titular

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

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

9.6.4. Declarações e garantias das terceiras partes

9.6.4.1. As terceiras partes:

- a) recusam a utilização do certificado para fins diversos dos previstos nesta DPC;
- b) verificam, a qualquer tempo, a validade do certificado.

9.6.4.2. O certificado da AC PR é considerado válido quando:

- i. tiver sido emitido pela AC;
- ii. não constar como revogado pela AC;
- iii. não estiver expirado; e
- iv. puder ser verificado com o uso do certificado válido da AC.

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

9.6.5. Representações e garantias de outros participantes

Não se aplica.

9.7. Isenção de garantias

Não se aplica.

9.8. Limitações de responsabilidades

AAC PR não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação vigente.

9.9. Indenizações

AAC PR responde pelos danos que der causa, e lhe sejam imputáveis, na forma da legislação vigente, assegurado o direito de regresso contra o agente ou entidade responsável.

Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

Não existe responsabilidade da terceira parte perante a AC PR ou AR, a ela vinculada, que requeira prática de indenização, exceto na hipótese de prática de ato ilícito.

9.10. Prazo e rescisão

9.10.1. Prazo

Esta DPC entra em vigor a partir da publicação que a aprovar, e permanecerá válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.2. Término

Esta DPC vigorará por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.3. Efeito da rescisão e sobrevivência

Os atos praticados na vigência desta DPC são válidos e eficazes para todos os fins de direito, produzindo efeitos mesmo após a sua revogação ou substituição.

9.11. Avisos individuais e comunicações com os participantes

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por ofício da autoridade competente ou publicação no Diário Oficial da União.

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC é submetida para AC Raiz.

9.12.2. Mecanismo de notificação e períodos

Mudança nesta DPC será publicado no site da AC PR.

9.12.3. Circunstâncias na qual o OID deve ser alterado.

Não se aplica.

9.13. Solução de conflitos

9.13.1. Os litígios decorrentes desta DPC serão solucionados de acordo com a legislação vigente.

9.13.2. Também está estabelecido que a DPC da AC não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.14. Lei aplicável

A DPC da AC PR obedece às leis da República Federativa do Brasil notadamente a Medida Provisória nº 2.200-2, de 24.08.2001, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas em vigor no Brasil.

9.15. Conformidade com a Lei aplicável

A AC PR está sujeita à legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em lei.

9.16. Disposições Diversas

9.16.1. Acordo completo

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

9.16.2. Cessão

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

9.16.3. Independência de disposições

A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPC não prejudicará as demais disposições, as quais permanecerão plenamente válidas e eficazes. Neste caso a disposição inválida, nula ou ineficaz será considerada como não escrita, de forma que esta DPC será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes.

9.16.4. Execução (honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17. Outras provisões

Não se aplica.

10. DOCUMENTOS REFERENCIADOS

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

Ref	Nome do documento	Código
------------	--------------------------	---------------

[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 25, de 24 de outubro de 2003	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 29 de agosto de 2003	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001.	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pelo Resolução nº 02, de 25 de setembro de 2001.	DOC-ICP-02
[1]	DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL Aprovado pela Resolução nº 10, de 14 de fevereiro de 2002	DOC-ICP-12

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

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

11. REFERÊNCIAS BIBLIOGRÁFICAS

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 11.515/NB 1334: Critérios de segurança física relativos ao armazenamento de dados. 2007.

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

RFC 4210, IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), september 2005.

RFC 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, september 2007.

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

RFC 6712, IETF - Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), september 2012.

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