Declaração de Práticas de Certificação da Autoridade Certificadora Certisign

DPC da AC Certisign

Versão 7.1 – 26/09/2019

Sumário

1. INTRODUÇÃO 10

1.1. VISÃO GERAL 10
1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO 10
1.3. PARTICIPANTES DA ICP-BRASIL 10
1.3.1. Autoridades Certificadoras 10
1.3.2. Autoridades de Registro 10
1.3.3. Titulares do Certificado 11
1.3.4. Partes Confiáveis 11
1.3.5. Outros Participantes 11
1.4. USABILIDADE DO CERTIFICADO 11
1.4.1 Uso apropriado do certificado 11
1.4.2 Uso proibitivo do certificado 11
1.5 POLÍTICA DE ADMINISTRAÇÃO 11
1.5.1 Organização administrativa do documento 11
1.5.2 Contatos 11
1.5.3 Pessoa que determina a adequabilidade da DPC com a PC 11
1.5.4 Procedimentos de aprovação da DPC 12
1.6 DEFINIÇÕES E ACRÔNIMOS 12

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 13

2.1. REPOSITÓRIOS 13
2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS 13
2.3. TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO 13
2.4. CONTROLE DE ACESSO AOS REPOSITÓRIOS 14

3. IDENTIFICAÇÃO E AUTENTICAÇÃO 14

3.1. ATRIBUIÇÃO DE NOMES 14
3.1.1. Tipos de nomes 14
3.1.2. Necessidade dos nomes serem significativos 14
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado 14
3.1.4. Regras para interpretação de vários tipos de nomes 14
3.1.5. Unicidade de nomes 14
3.1.6. Procedimento para resolver disputa de nomes 14
3.1.7. Reconhecimento, autenticação e papel de marcas registradas 15
3.2. VALIDAÇÃO INICIAL DE IDENTIDADE 15
3.2.1. Método para comprovar a posse de chave privada 15
3.2.2. Autenticação da identificação da organização 15
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 17
3.2.6. Critérios para interoperação 17
3.2.7. Autenticação da identidade de equipamento ou aplicação 17
3.2.8 Procedimentos complementares 18
3.2.9 Procedimentos específicos 18
3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES 18
3.3.1. Identificação e autenticação para rotina de novas chaves antes da expiração 18
3.3.2. Identificação e autenticação para novas chaves após a revogação 18
3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO 18

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 19

4.1. SOLICITAÇÃO DO CERTIFICADO 19
4.1.1. Quem pode submeter uma solicitação de certificado 19
4.1.2. Processo de registro e responsabilidades 19
4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO 21
4.2.1. Execução das funções de identificação e autenticação 21
4.2.2. Aprovação ou rejeição de pedidos de certificado 21
4.2.3. Tempo para processar a solicitação de certificado 21
4.3. EMISSÃO DE CERTIFICADO 21
4.3.1. Ações da AC durante a emissão de um certificado 21
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado 21
4.4. ACEITAÇÃO DE CERTIFICADO 21
4.4.1. Conduta sobre a aceitação do certificado 21
4.4.2. Publicação do certificado pela AC 21
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades 21
4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO 22
4.5.1. Usabilidade da Chave privada e do certificado do titular 22
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis 22
4.6. RENOVAÇÃO DE CERTIFICADOS 22
4.6.1. Circunstâncias para renovação de certificados 22
4.6.2. Quem pode solicitar a renovação 22
4.6.3. Processamento de requisição para renovação de certificados 22
4.6.4. Notificação para nova emissão de certificado para o titular 22
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado 22
4.6.6. Publicação de uma renovação de um certificado pela AC 22
4.6.7. Notificação de emissão de certificado pela AC para outras entidades 22
4.7. NOVA CHAVE DE CERTIFICADO (RE-KEY) 23
4.7.1. Circunstâncias para nova chave de certificado 23
4.7.2. Quem pode requisitar a certificação de uma nova chave pública 23
4.7.3. Processamento de requisição de novas chaves de certificado 23
4.7.4. Notificação de emissão de novo certificado para o titular 23
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada 23
4.7.6. Publicação de uma nova chave certificada pela AC 23
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades 23
4.8. MODIFICAÇÃO DE CERTIFICADO 23
4.8.1. Circunstâncias para modificação de certificado 23
4.8.2. Quem pode requisitar a modificação de certificado 23
4.8.3. Processamento de requisição de modificação de certificado 23
4.8.4. Notificação de emissão de novo certificado para o titular 23
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado 23
4.8.6. Publicação de uma modificação de certificado pela AC 23
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades 23
4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO 23
4.9.1. Circunstâncias para revogação 23
4.9.2. Quem pode solicitar revogação 24
4.9.3. Procedimento para solicitação de revogação 24
4.9.4. Prazo para solicitação de revogação 25
4.9.5. Tempo em que a AC deve processar o pedido de revogação 25
4.9.6. Requisitos de verificação de revogação para as partes confiáveis 25
4.9.7. Frequência de emissão de LCR 25
4.9.8. Latência máxima para a LCR 25
4.9.9. Disponibilidade para revogação/verificação de status on-line 25
4.9.10. Requisitos para verificação de revogação on-line 25

4.9.11. Outras formas disponíveis para divulgação de revogação *26*
4.9.12. Requisitos especiais para o caso de comprometimento de chave *26*
4.9.13. Circunstâncias para suspensão *26*
4.9.14. Quem pode solicitar suspensão *26*
4.9.15. Procedimento para solicitação de suspensão *26*
4.9.16. Limites no período de suspensão *26*
4.10. SERVIÇOS DE STATUS DE CERTIFICADO 26
4.10.1. Características operacionais *26*
4.10.2. Disponibilidade dos serviços *26*
4.10.3. Funcionalidades operacionais *26*
4.11. ENCERRAMENTO DE ATIVIDADES 26
4.12. CUSTÓDIA E RECUPERAÇÃO DE CHAVE 27
4.12.1. Política e práticas de custódia e recuperação de chave *27*
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão *27*

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES 27

5.1. CONTROLES FÍSICOS 27
5.1.1. Construção e localização das instalações de AC *27*
5.1.2. Acesso físico *28*
5.1.3. Energia e ar condicionado *30*
5.1.4. Exposição à água *31*
5.1.5. Prevenção e proteção contra incêndio *31*
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 *32*
5.2. CONTROLES PROCEDIMENTAIS 32
5.2.1. Perfis qualificados *32*
5.2.2. Número de pessoas necessário por tarefa *33*
5.2.3. Identificação e autenticação para cada perfil *33*
5.2.4. Funções que requerem separação de deveres *34*
5.3. CONTROLES DE PESSOAL 34
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade *34*
5.3.2. Procedimentos de verificação de antecedentes *34*
5.3.3. Requisitos de treinamento *34*
5.3.4. Frequência e requisitos para reciclagem técnica *34*
5.3.5. Frequência e sequência de rodízio de cargos *35*
5.3.6. Sanções para ações não autorizadas *35*
5.3.7. Requisitos para contratação de pessoal *35*
5.3.8. Documentação fornecida ao pessoal *35*
5.4. PROCEDIMENTOS DE LOG DE AUDITORIA 35
5.4.1. Tipos de eventos registrados *36*
5.4.2. Frequência de auditoria de registros *36*
5.4.3. Período de retenção para registros de auditoria *37*
5.4.4. Proteção de registros de auditoria *37*
5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria *37*
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo) *37*
5.4.7. Notificação de agentes causadores de eventos *37*
5.4.8. Avaliações de vulnerabilidade *37*
5.5. ARQUIVAMENTO DE REGISTROS 37
5.5.1. Tipos de registros arquivados *38*
5.5.2. Período de retenção para arquivo *38*
5.5.3. Proteção de arquivo *38*

5.5.4. Procedimentos de cópia de arquivo *38*
5.5.5. Requisitos para datação de registros *38*
5.5.6. Sistema de coleta de dados de arquivo (interno e externo) *38*
5.5.7. Procedimentos para obter e verificar informação de arquivo *39*
5.6. Troca de chave 39
5.7. Comprometimento e Recuperação de Desastre 39
5.7.1. Procedimentos de gerenciamento de incidente e comprometimento *39*
5.7.2. Recursos computacionais, software, e/ou dados corrompidos *39*
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade *39*
5.7.4. Capacidade de continuidade de negócio após desastre *40*
5.8. Extinção da AC 40
6. CONTROLES TÉCNICOS DE SEGURANÇA 40
6.1. Geração e Instalação do Par de Chaves 40
6.1.1. Geração do par de chaves *40*
6.1.2. Entrega da chave privada à entidade *41*
6.1.3. Entrega da chave pública para emissor de certificado *41*
6.1.4. Entrega de chave pública da AC às terceiras partes *41*
6.1.5. Tamanhos de chave *41*
6.1.6. Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros *41*
6.1.7. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3) *41*
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico 42
6.2.1. Padrões e controle para módulo criptográfico *42*
6.2.2. Controle "n de m" para chave privada *42*
6.2.3. Custódia (escrow) de chave privada *42*
6.2.4. Cópia de segurança de chave privada *42*
6.2.5. Arquivamento de chave privada *42*
6.2.6. Inserção de chave privada em módulo criptográfico *43*
6.2.7 Armazenamento de chave privada em módulo criptográfico *43*
6.2.8. Método de ativação de chave privada *43*
6.2.9. Método de desativação de chave privada *43*
6.2.10. Método de destruição de chave privada *43*
6.3. Outros Aspectos do Gerenciamento do Par de Chaves 43
6.3.1. Arquivamento de chave pública *43*
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada. *43*
6.4. Dados de Ativação 44
6.4.1. Geração e instalação dos dados de ativação *44*
6.4.2. Proteção dos dados de ativação *44*
6.4.3. Outros aspectos dos dados de ativação *44*
6.5. Controles de Segurança Computacional 44
6.5.1. Requisitos técnicos específicos de segurança computacional *44*
6.5.2. Classificação da segurança computacional *45*
6.5.3. Controles de Segurança para as Autoridades de Registro *45*
6.6. Controles Técnicos do Ciclo de Vida 45
6.6.1. Controles de desenvolvimento de sistema *45*
6.6.2. Controles de gerenciamento de segurança *45*
6.6.3. Controles de segurança de ciclo de vida *46*
6.6.4 Controles na Geração de LCR *46*
6.7. Controles de Segurança de Rede 46
6.7.1 Diretrizes Gerais *46*
6.7.2. Firewall *46*
6.7.3. Sistema de detecção de intrusão (IDS) *46*

6.7.4. Registro de acessos não-autorizados à rede *47*
6.8. CARIMBO DE TEMPO 47
7. PERFIS DE CERTIFICADO, LCR E OCSP 47
7.1. PERFIL DO CERTIFICADO 47
7.1.1. Número de versão *47*
7.1.2. Extensões de certificado *47*
7.1.3. Identificadores de algoritmo *48*
7.1.4. Formatos de nome *48*
7.1.5. Restrições de nome *48*
7.1.6. OID (Object Identifier) da DPC *48*
7.1.7. Uso da extensão "Policy Constraints" *48*
7.1.8. Sintaxe e semântica dos qualificadores de política *48*
7.1.9. Semântica de processamento para as extensões críticas de PC *48*
7.2. PERFIL DE LCR 49
7.2.1. Número(s) de versão *49*
7.2.2. Extensões de LCR e de suas entradas *49*
7.3. PERFIL DE OCSP 49
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES 49
8.1. FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES 49
8.2. IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR 49
8.3. RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA 49
8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO 49
8.5. AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA 50
8.6. COMUNICAÇÃO DOS RESULTADOS 50
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS 50
9.1. TARIFAS 50
9.1.1. Tarifas de emissão e renovação de certificados *50*
9.1.2. Tarifas de acesso ao certificado *50*
9.1.3. Tarifas de revogação ou de acesso à informação de status *50*
9.1.4. Tarifas para outros serviços *50*
9.1.5. Política de reembolso *50*
9.2. RESPONSABILIDADE FINANCEIRA 50
9.2.1 Cobertura do seguro *50*
9.2.2 Outros ativos *50*
9.2.3 Cobertura de seguros ou garantia para entidades finais *51*
9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO 51
9.3.1 Escopo de informações confidenciais *51*
9.3.2 Informações fora do escopo de informações confidenciais *51*
9.3.3 Responsabilidade em proteger a informação confidencial *52*
9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL 52
9.4.1 Plano de privacidade *52*
9.4.2 Tratamento de informação como privadas *52*
9.4.3 Informações não consideradas privadas *52*
9.4.4 Responsabilidade para proteger a informação privadas *52*
9.4.5 Aviso e consentimento para usar informações privadas *52*
9.4.6 Divulgação em processo judicial ou administrativo *52*
9.4.7 Outras circunstâncias de divulgação de informação *53*
9.4.8 Informações a terceiros *53*
9.5 DIREITOS DE PROPRIEDADE INTELECTUAL 53

9.6 Declarações e Garantias 53
9.6.1 Declarações e Garantias da AC 53
9.6.2 Declarações e Garantias da AR 54
9.6.3 Declarações e garantias do titular 54
9.6.4 Declarações e garantias das terceiras partes 54
9.6.5 Representações e garantias de outros participantes 54
9.7 Isenção de garantias 54
9.8 Limitações de responsabilidades 54
9.9 Indenizações 54
9.10 Prazo e Rescisão 54
9.10.1 Prazo 54
9.10.2 Término 55
9.10.3 Efeito da rescisão e sobrevivência 55
9.11 Avisos individuais e comunicações com os participantes 55
9.12. Alterações 55
9.12.1. Procedimento para emendas 55
9.12.2. Mecanismo de notificação e períodos 55
9.12.3. Circunstâncias na qual o OID deve ser alterado 55
9.13. Solução de conflitos 55
9.14. Lei aplicável 55
9.15. Conformidade com a Lei aplicável 55
9.16. Disposições Diversas 55
9.16.1. Acordo completo 55
9.16.2. Cessão 55
9.16.3. Independência de disposições 56
9.16.4. Execução (honorários dos advogados e renúncia de direitos) 56
9.17. Outras provisões 56
10. DOCUMENTOS REFERENCIADOS 56
11. REFERÊNCIAS BIBLIOGRÁFICAS 57

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
6.4	03/12/2015	Resolução 107, de 25.08.2015 Resolução 113, de 30.09.2015 Resolução 114, de 30.09.2015 Resolução 115, de 11.11.2015	3.1.1.1,3.1.1.7,3.1.1.8,3.1.1.4.1.,3.1.9, 3.1.9.1,3.1.12, 4.4.2	Referência aos parágrafos referente à Política de Certificado A CF-e-SAT. Obrigatoriedade da coleta de dados biométricos do requerente do certificado digital. Limita o prazo de validade para até 90 dias nas procurações. Restringe a renovação automática não presencial apenas para pessoa física, limitando o prazo para pessoa jurídica até 31/12/2015.
6.5	11/03/2016	Resolução N°116, de 09 de dezembro de 2015 Resolução N°118, de 09 de dezembro de 2015	2.6.4.1,6.1.1.2, 6.1.5.2, 6.1.6, 6.1.8.1, 6.2.1.1, 6.8, 7.3.2.2	Referência à autoridade certificadora Raiz V5 e suas cadeias subsequentes. Aprova a retirada do campo AIA da LCR e define a obrigatoriedade de 1 ponto de obtenção da LCR em novas cadeias de certificação digital ICP-Brasil.
6.6	03/08/2016	Não se aplica Instrução Normativa N°07, de 15 de julho de 2016	4.6.2, 7.2.2.	Correção da URL da LCR da AC RAIZ BRASILEIRA. Ampliação do período de retenção.

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
6.7	13/11/2017	Resolução N°119 de 06 de julho de 2017, Resolução N°123 de 06 de julho de 2017 e Resolução N°130, de 19 de setembro de 2017 Não se aplica	2.7.1,3.1.1.2,3.1.1.2.1,3.1.1.2.2, 3.1.1.2.3, 3.1.1.2.4, 3.1.1.2.5.,3.1.9.14.4.10.1, 4.4.10.2.,6.1.1.2, 6.1.6, 6.1.8.1, 6.2.1.1, 6.5.3.2, 6.8 e 7.2.2	Obrigatoriedade de realização de auditorias WebTrust Procedimentos de validação fora do ambiente físico da AR. Atualiza mídias armazenadoras de chaves criptográficas Requisitos para verificação de LCR Correção dos CRL Distribution Points dos certificados emitidos na V5 Adequação do item k) a versão 2.1 do DOC-ICP-03.01 Validade da CNH.
7.0	14/06/2019	Resolução N°151 de 14 de junho de 2019	Vários	Adequação à resolução 151
7.1	26/09/2019	Não se aplica	1.5.2 3.2.3.1.2 4.1. Vários itens	Atualização dos dados de contato da AC Retirada da nota 2 Retirada da nota 3 Adequações a AC aos itens fora da Resolução 151, já propostos pelo DOC-ICP-05 – Como AC de 1º Nível

Declaração de Práticas de Certificação da Autoridade Certificadora Certisign

1. INTRODUÇÃO

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

1.1. Visão Geral

1.1.1. Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora Certisign (AC Certisign) integrante na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços de certificação digital.

1.1.2. A estrutura desta DPC está baseada no DOC-ICP-05– REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICA DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL[5].

As referências a formulários presentes nesta DPC deverão ser entendidas também como referências a outras formas que a AC Certisign ou entidades a ela vinculadas possa vir a adotar.

1.1.3 Para as ACs emissoras de certificados SSL e CS, devem ser observados e descritos os princípios e critérios WebTrust.

1.1.4 A estrutura desta DPC está baseada na RFC 3647.

1.1.5 A AC Certisign mantem todas as informações da sua DPC sempre atualizadas.

1.1.6. A AC Certisign está certificada em nível imediatamente subsequente ao da AC Raiz da ICP-Brasil. O certificado da AC Certisign contém a chave pública correspondente à sua chave privada, utilizada para assinar de AC de nível imediatamente subseqüente (AC Subseqüente) ao seu e para assinar a sua Lista de Certificados Revogados (LCR).

1.2. Nome do documento e identificação

1.2.1. Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora Certisign e referida como "DPC da AC Certisign", cujo OID (object identifier) é 2.16.76.1.1.5.

1.2.2. Não se aplica.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

Esta DPC refere-se exclusivamente à AC Certisign no âmbito da ICP-Brasil.

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pelas ACs subsequentes à AC Certisign para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web de cada AC subsequente à AC Certisign, contendo:

a) relação de todas as AR credenciadas;

b) relação de AR que tenham se descredenciado da cadeia da AC subsequente a AC Certisign, com respectiva data do descredenciamento.

1.3.3. Titulares do Certificado

Apenas pessoas jurídicas podem ser titulares de certificados de AC Subsequente emitidos pela AC Certisign.

1.3.4. Partes Confiáveis

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

1.3.5. Outros Participantes

1.3.5.1. A relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC Certisign é publicada em serviço de diretório e/ou em página web da AC Certisign (http://icp-brasil.certisign.com.br/repositorio/ac_certisign.html).

1.4. Usabilidade do Certificado

1.4.1 Uso apropriado do certificado

Os certificados emitidos pela AC Certisign tem sua utilização exclusiva para assinatura de certificados digitais de AC de nível imediatamente subsequente (AC Subsequente) ao seu e de sua Lista de Certificados Revogados (LCR).

1.4.2 Uso proibitivo do certificado

Não se aplica.

1.5 Política de Administração

Neste item estão incluídos nome, endereço e outras informações da AC Certisign, assim como são informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC: Certisign Certificadora Digital S.A.

1.5.2 Contatos

Endereço: Rua Bela Cintra, 904 – 11. Andar – São Paulo - 01415-000

Telefone: (11) 4501-2215

Página web: http://icp-brasil.certisign.com.br/repositorio/ac_certisign.html

E-mail: normas@certisign.com.br

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome: Bruna Spirandelli

Área: Normas e Compliance

Telefone: (11) 4501-2215

E-mail: normas@certisign.com.br

1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

Os procedimentos de aprovação desta DPC da AC Certisign são estabelecidos a critério do CG da ICP-Brasil.

1.6 Acronimos

SIGLA	DESCRIÇÃO
ACME	Automatic Certificate Management Environment
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology
NIS	Número de Identificação Social
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession

PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios

2.1.1 A AC Certisign mantem disponível repositório atendendo as seguintes obrigações:
a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC Certisign e sua LCR;
b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
c) implementar os recursos necessários para a segurança dos dados nele armazenados.

2.1.2. As publicações da AC Certisign podem ser consultadas através do protocolo http.
Somente a AC Certisign, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar atualizações nas informações por ela publicadas no seu repositório.

2.1.3. O repositório da AC Certisign está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e pode ser encontrado na página Web (http://icp-brasil.certisign.com.br/repositorio/ac_certisign.html).

2.1.4 A AC Certisign disponibiliza 1 (um) repositório para distribuição de LCR.

2.2. Publicação de informações dos certificados

2.2.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC Certisign (http://icp-brasil.certisign.com.br/repositorio/ac_certisign.html), obedecendo as regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC Certisign em serviço de diretório e/ou página web é de 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 em serviço de diretório e/ou em página web da AC Certisign (http://icp-brasil.certisign.com.br/repositorio/ac_certisign.html):

a) seus próprios certificado;
b) suas LCR;
c) esta DPC;
d) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3. Tempo ou Frequência de Publicação

2.3.1. De modo a assegurar a disponibilização sempre atualizada de seus conteúdos:
a) os certificados são publicados imediatamente após sua emissão;

b) a publicação da LCR se dá conforme o item 4.9.7 desta DPC;
c) as versões ou alterações desta DPC são atualizadas no web site da Certisign após aprovação da AC Raiz da ICP-Brasil; e

2.4. Controle de Acesso aos Repositórios

2.4.1. Não há qualquer restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos e a LCR da AC Certisign.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado. A máquina que armazena as informações acima se encontra em nível 4 de segurança física e requer uma senha de acesso.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC Certisign, verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital.
As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os diretos de propriedade intelectual de terceiros.
A AC 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. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o "distinguished name" do padrão ITU X.500, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular.

3.1.1.2. Um certificado emitido para uma AC subsequente não deverá incluir o nome da pessoa responsável.

3.1.2. Necessidade dos nomes serem significativos

3.1.2.1. Os certificados emitidos pela AC Certisign exigem o uso de nomes significativos que possibilitam determinar univocamente a identidade da pessoa ou da organização titular do certificado a que se referem, para a identificação dos titulares dos certificados emitidos pela AC responsável.

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.5. Unicidade de nomes

Esta DPC estabelece que identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado emitido pela AC Certisign.
Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo DN.

3.1.6. Procedimento para resolver disputa de nomes

A AC Certisign se reserva o direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrente da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas são executados de acordo com a legislação em vigor.

3.2. Validação inicial de identidade

Neste item e nos seguintes, esta DPC descreve os requisitos e os procedimentos gerais utilizados pela AC Certisign, responsável para a realização dos seguintes processos:

a) identificação do titular do certificado - compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.2.2 e 3.2.3:

i. Confirmação da identidade de um indivíduo: comprovação de que a pessoa física que se apresenta como titular pelo certificado da AC subsequente à AC Certisign é realmente aquela cujos dados constam na documentação apresentada, sendo esse o responsável legal da AC subsequente.

ii. Confirmação da identidade de uma pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado da AC subsequente à AC Certisign, e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação;

b) emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado da AC Subsequente no sistema da AC Certisign. 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 a posse de chave privada

A confirmação de que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 4210, relativos a POP (Proof of Possession).

3.2.2. Autenticação da identificação da organização

3.2.2.1. Disposições Gerais

3.2.2.1.1. A Confirmação da identidade da pessoa física responsável pela AC subsequente à AC Certisign é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.

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

3.2.2.1.3. Deverá ser feita a confirmação da identidade da organização e da pessoa física, 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) presença física do responsável pelo certificado; e

d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo responsável pelo certificado.

Nota 1: Não se aplica.

3.2.2.1.4 Não se aplica.

3.2.2.2. Documentos para efeitos de identificação de uma organização

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

a) Relativos a sua habilitação jurídica:

i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do CNPJ;

ii. se entidade privada:

1. certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e

2. documentos da eleição de seus representantes legais, quando aplicável;

b) Relativos a sua habilitação fiscal:

i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou

ii. prova de inscrição no Cadastro Específico do INSS – CEI.

Nota 01: Essas confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

3.2.2.3. Informações contidas no certificado emitido para uma organização

Não se aplica.

3.2.3. Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos e pelo processo biométrico da ICP-Brasil.

3.2.3.1. Documentos para efeitos de identificação de um indivíduo

Deverá ser apresentada a seguinte documentação, em sua versão original oficial, podendo ser física ou digital, por meio de barramento ou aplicação oficial, e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado:

a) Registro de Identidade ou Passaporte, se brasileiro; ou

b) Título de Eleitor, com foto; ou

c) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou

d) Passaporte, se estrangeiro não domiciliado no Brasil;

e) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[11]; e

f) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[11].

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. Não se aplica.

3.2.3.1.2. Não se aplica.

3.2.3.1.3. Não se aplica.

3.2.3.1.4. Não se aplica.

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.2. Informações contidas no certificado emitido para um indivíduo

Não se aplica.

3.2.4. Informações não verificadas do titular do certificado

Não se aplica.

3.2.5. Validação das autoridades

Na emissão de certificado de AC subsequente é verificado se a pessoa física é o representante legal da AC.

3.2.6. Critérios para interoperação

Não se aplica.

3.2.7. Autenticação da identidade de equipamento ou aplicação

Não se aplica.

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

3.2.8.2 O processo de identificação do titular do certificado é registrado e tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.2.8.3 Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

3.2.8.3.1. Não se aplica.

3.2.8.4. Não se aplica.

3.2.9 Procedimentos específicos

O processo de emissão de certificados de AC subordinadas à AC CERTISIGN é registrado e tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. Identificação e autenticação para rotina de novas chaves antes da expiração

3.3.1.1 No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC Certisign para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

3.3.1.2 Esse processo é conduzido através da adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado.

3.3.1.3 Não se aplica.

3.3.2. Identificação e autenticação para novas chaves após a revogação

3.3.2.1. Após a revogação ou expiração do certificado, os procedimentos utilizados para confirmação da identidade do solicitante de novo certificado são os mesmos exigidos na solicitação inicial do certificado, na forma e prazo descritos nesta DPC.

3.3.2.2. Para o caso específico de revogação de um certificado de AC de nível imediatamente subsequente ao da AC Certisign após a expiração ou revogação de seu certificado, aquela AC deverá executar os processos regulares de geração de seu novo par de chaves.

3.4. Identificação e Autenticação para solicitação de revogação

A solicitação de revogação de certificado de AC de nível subsequente ao da AC Certisign é efetivada através do Formulário de Solicitação de Revogação de Certificado de Autoridade Certificadora habilitada, preenchido pelo representante legal da AC e assinado no ato de entrega realizada pessoalmente à AC Certisign.

O motivo da revogação do certificado será descrito no formulário.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. Solicitação do certificado

Os requisitos e procedimentos mínimos necessários para a solicitação de emissão de certificado são:

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.2;

b) não se aplica.

c) não se aplica.

Nota 1: Não se aplica.

Nota 2: Não se aplica.

4.1.1. Quem pode submeter uma solicitação de certificado

4.1.1.1. A solicitação de certificado para AC de nível imediatamente subsequente ao da AC Certisign somente será possível após o processo de credenciamento e a autorização de funcionamento da AC em questão, conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

4.1.1.2. Não se aplica.

4.1.1.3 Nos casos previstos no item 4.1.1.1, a AC subsequente deverá encaminhar a solicitação de certificado à AC Certisign por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

4.1.1.4 A solicitação de um certificado de AC de nível imediatamente subsequente deve ser feita pelos seus representantes legais.

4.1.2. Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1 Responsabilidades da AC

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

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

4.1.2.1.3 Não se aplica.

4.1.2.2 Obrigações da AC

As obrigações da AC Certisign são as abaixo relacionadas:

a) operar de acordo com a sua DPC;

b) gerar e gerenciar os seus pares de chaves criptográficas;

c) assegurar a proteção de suas chaves privadas;

d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

f) distribuir o seu próprio certificado;

g) emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas LCRs e, quando aplicável, disponibilizar consulta on-line de situação do certificado (OCSP - On-line Certificate Status Protocol);

k) publicar em sua página web sua DPC;

l) publicar, em sua página web, as informações definidas no item 2.2.2 deste documento;

m) não se aplica;

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 e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;

t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, 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) não se aplica;

y) não se aplica.

4.1.2.3 Responsabilidades da AR

Não se aplica.

4.1.2.4 Obrigações das ARs

Não se aplica.

4.2. Processamento de Solicitação de Certificado

4.2.1. Execução das funções de identificação e autenticação

A AC Certisign executa 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 A AC Certisign pode aceitar ou rejeitar pedidos de certificados das AC imediatamente subsequente de acordo com os procedimentos descritos no item 4.1 desta DPC.

4.2.2.2 A Certisign pode com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC.

4.2.3. Tempo para processar a solicitação de certificado

A AC Certisign cumpre os procedimentos determinados na ICP-Brasil.

Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

4.3.1.1 A emissão de uma AC subsequente a AC Certisign, é realizada por meio de cerimônia formal, na presença dos representantes legais ou procurador da AC responsável. Devem ser apresentados os documentos da empresa e dos representantes Legais. Se for o caso, deverão ser apresentados os documentos do procurador, em conjunto com a procuração.

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

A AC de nível subsequente a AC Certisign, é notificada da emissão e do método de retirada do certificado, no momento da cerimônia formal de emissão da AC.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

4.4.1.1 Quando a AC Certisign emite um certificado para uma AC de nível subsequente ao seu, ela garante que as informações contidas nesse certificado foram verificadas e que estão de acordo com esta DPC.

No momento da entrega do certificado, durante a cerimônia de sua emissão pela AC Certisign, a AC atesta o seu recebimento por meio de assinatura do Script de cerimônia e do Atestado de Testemunha de Emissão de Certificado.

4.4.1.2 A aceitação de todo certificado emitido é declarada pelo respectivo titular.

4.4.1.3 A aceitação do certificado de uma AC Subsequente é declarada por seu responsável através da assinatura do Termo de Aceitação.

4.4.2. Publicação do certificado pela AC

O certificado da AC Certisign e os certificados das ACs de nível imediatamente subsequente ao seu são publicados de acordo com item 2.2 desta DPC.

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

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

4.5. Usabilidade do par de chaves e do certificado

A AC subsequente titular de certificado emitido pela AC Certisign, deve operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementa, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.1.1 A AC titular deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto nesta DPC.

4.5.1.2 Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos pela AC constantes dos termos de titularidade de que trata o item 4.1 são os abaixo relacionados:

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, senhas e dispositivos criptográficos;

c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto nesta DPC;

d) conhecer os seus direitos e obrigações, contemplados pela DPC e por outros documentos aplicáveis da ICP-Brasil; e

e) informar à AC qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

NOTA: Não se aplica.

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

Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Em acordo com item 3.3 desta DPC.

4.6.1. Circunstâncias para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.2. Quem pode solicitar a renovação

Em acordo com item 3.3 desta DPC.

4.6.3. Processamento de requisição para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.4. Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

4.6.6. Publicação de uma renovação de um certificado pela AC

Não se aplica.

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

Em acordo com item 4.3 desta DPC.

4.7. Nova chave de certificado (Re-key)

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica.

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

Não se aplica.

4.7.3. Processamento de requisição de novas chaves de certificado

Não se aplica.

4.7.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica.

4.7.6. Publicação de uma nova chave certificada pela AC

Não se aplica.

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

Não se aplica.

4.8. Modificação de certificado

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. O representante legal da AC subsequente à AC Certisign pode solicitar a revogação de seu certificado a qualquer tempo, independentemente de qualquer circunstância.

4.9.1.2. O certificado deve ser obrigatoriamente revogado:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;

b) Quando for necessária a alteração de qualquer informação constante no mesmo;

c) No caso de dissolução de AC titular do certificado; ou

d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3. A AC Certisign define ainda que:

a) A AC Certisign deve revogar, no prazo definido no item 4.9.3.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e

b) O CG da ICP-Brasil ou AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.9.1.4. Não se aplica.

4.9.1.4.1. Não se aplica.

4.9.1.4.2. Não se aplica.

4.9.1.5. A autenticidade da LCR é também 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 revogação do certificado de uma AC de nível imediatamente subsequente ao da AC Certisign somente pode ser feita:

a) por solicitação da AC Titular do Certificado;
b) por determinação da AC Certisign;
c) por solicitação da AR Certisign;
d) por determinação do CG da ICP-Brasil;
e) por determinação da AC Raiz;
f) por determinação judicial.

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. A solicitação de revogação de certificado de AC subsequente à AC Certisign, deve ser realizado através do "Formulário de Revogação de AC", preenchido e assinado pelo representante da AC, podendo ser esse documento preenchido e assinado digitalmente e/ou preenchido em papel, e entregue a AC Certisign.

4.9.3.2. Como diretrizes gerais:

a) O Solicitante da revogação de um certificado é identificado;

b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC Certisign;

c) As justificativas para a revogação de um certificado são registradas;

d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado e com a atualização do status do certificado na resposta OCSP à base de dados da AC Certisign, quando aplicável.

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 12 (doze) horas.

4.9.3.4. O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação, é de 12 (doze) horas.

4.9.3.5. A AC Certisign 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 LCR correspondente.

4.9.3.6. Não se aplica.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 4.9.1 desta DPC.

4.9.4.2. Não se aplica.

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

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC Certisign 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 deve confirmar a validade de cada certificado na cadeia de certificação de acordo com os padrões IETF PKIX, incluindo a verificação da validade do certificado, encadeamento do nome do emissor e titular, restrições de uso de chaves e de políticas de certificação e o status de revogação por meio de LCRs identificados em cada certificado na cadeia de certificação.

4.9.7. Frequência de emissão de LCR

4.9.7.1. Neste item é definida a frequência de emissão da LCR referente a certificados de AC de nível subsequente ao da AC Certisign.

4.9.7.2. Não se aplica.

4.9.7.3. A frequência máxima admitida para a emissão de LCR referente a certificados de AC é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC responsável deverá emitir nova LCR no prazo previsto no item 4.9.3.4 e notificar todas as ACs de nível imediatamente subsequente ao seu.

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

Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. Se houver comprometimento ou suspeita de comprometimento da chave privada, a AC Titular do Certificado deverá comunicar imediatamente a AC Certisign.

4.9.12.2. A AC titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente a AC Certisign, assinando formulário de solicitação de revogação, observado o item 4.4.3 desta DPC.

Todos os documentos e relatórios relativos são arquivados após a conclusão deste processo.

4.9.13. Circunstâncias para suspensão

Não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados de AC de nível subsequente à AC Certisign.

4.9.14. Quem pode solicitar suspensão

A AC Certisign pode solicitar suspensão quando aprovado pelo Comitê Gestor.

4.9.15. Procedimento para solicitação de suspensão

Os procedimentos de solicitação de suspensão serão definidos em documento interno da AC Certisign.

4.9.16. Limites no período de suspensão

Os períodos de suspensão serão estabelecidos em documento interno da AC Certisign.

4.10. Serviços de status de certificado

4.10.1. Características operacionais

A AC Certisign deve fornecer um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados, conforme item 4.9.

4.10.2. Disponibilidade dos serviços

Ver item 4.9

4.10.3. Funcionalidades operacionais

Ver item 4.9

4.11. Encerramento de atividades

4.11.1. Observado o disposto no item sobre descredenciamento do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6], este item da DPC descreve os requisitos e os procedimentos que serão adotados nos casos de extinção ou encerramento dos serviços da AC Certisign, PSS ou PSBios a ela vinculados.

4.11.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC Certisign segue os requisitos e procedimentos descritos no documento Plano de Encerramento. Esse plano tem abordagem multidisciplinar

envolvendo aspectos de várias áreas da companhia, como jurídico, comercial, técnicos/tecnológicos, entre outros. De acordo com esse plano a AC Certisign:

a) Comunicará publicamente a extinção dos serviços da AC Certisign, através de publicação em jornal de grande circulação.

b) Revogará todos os certificados gerados pela AC Certisign nos prazos estipulados nesta DPC implementadas após a publicação e comunicará às partes afetadas através de mensagem eletrônica.

c) Extinguirá os serviços de emissão de certificados.

d) Extinguirá os serviços de revogação, como emissão da LCR e/ou conservação dos serviços de status on-line após a revogação completa de todos os certificados.

e) Destruirá a chave privada da AC Certisign extinta seguindo o procedimento descrito na DPC Item 6.2.9.

f) Transferirá os dados e gravações da AC Certisign para a Autoridade Certificadora sucessora, aprovada pela AC Raiz.

g) Transferirá as chaves públicas dos certificados emitidos pela AC Certisign para serem armazenadas por outra AC aprovada pela AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC Certisign. Caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

h) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC Certisign.

i) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

No caso de encerramento das atividades como PSS vinculada a AC Certisign, a AC Certisign, deverá seguir os seguintes requisitos e procedimentos :

a) Publicará, em sua página web, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso;

b) Manterá a guarda de toda a documentação comprobatória em seu poder.

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

A AC Certisign não executa práticas de custódia e recuperação de chaves.

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

A AC Certisign não executa tais práticas.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1. Controles Físicos

5.1.1. Construção e localização das instalações de AC

5.1.1.1. A localização e o sistema de certificação da AC Certisign não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não existem ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. As instalações para equipamentos de apoio, tais como máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares ficam em ambiente seguro.

As instalações para sistemas de telecomunicações, subestações e retificadores ficam em ambiente seguro com entrada e saída controlada.

Existem sistemas de aterramento e de proteção contra descargas atmosféricas

Existe iluminação de emergência em todos os ambientes de nível 4, além das áreas cobertas por câmeras de monitoramento.

5.1.2. Acesso físico

A AC Certisign possui sistema de controle de acesso físico que garante a segurança de suas instalações conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e os requisitos que seguem.

5.1.2.1 Níveis de acesso

5.1.2.1.1. A AC Certisign possui 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 2 (dois) níveis de proteção da chave privada da AC Certisign;

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC Certisign. 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 Certisign transitam devidamente identificadas e acompanhadas.

Nenhum tipo de processo operacional ou administrativo da AC Certisign é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC Certisign em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente são utilizados mediante autorização formal e supervisão.

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

5.1.2.1.5. O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da AC Certisign.

Qualquer atividade relativa ao ciclo de vida dos certificados digitais é executada a partir desse nível.

Pessoas não envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

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

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

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC Certisign tais como emissão e revogação de certificados e emissão de LCR e a disponibilidade à resposta a consulta OCSP. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível, inclusive o sistema de AR. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, 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 sendo ocupado.

5.1.2.1.9. No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto, são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - possuem proteção contra interferência eletromagnética externa.

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

5.1.2.1.11. Na AC Certisign, existem ambientes de quarto nível para abrigar e segregar:

a) equipamentos de produção on-line, gabinete reforçado de armazenamento e equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores - (Data Center);

b) equipamentos de produção off-line e cofre de armazenamento (Sala de cerimônia).

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre interior à sala de cerimônia e um gabinete reforçado trancado no Data Center. 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 e o gabinete obedecem às seguintes especificações:

a) confeccionado em aço;

b) possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) constitui-se de pequenos depósitos localizados no interior do cofre da sala de cerimônia (Nível 5). Cada um desses depósitos dispõe de 2 fechaduras, sendo uma individual e a outra comum a todos os depósitos. Os dados de ativação da chave privada da AC Certisign são armazenados nesses depósitos.

5.1.2.2 Sistemas físicos de detecção

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmeras não 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 um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) trimestralmente, com a escolha de, no mínimo, 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. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados ininterruptamente.

5.1.2.2.4. Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que o critério mínimo de ocupação deixa de ser satisfeito, devido à saída de um ou mais empregados, 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. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes estão localizados em ambiente de nível 3 e são permanentemente monitorados. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações.

5.1.2.3 Sistema de controle de acesso

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

5.1.2.4 Mecanismos de emergência

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

5.1.2.4.2. Todos os procedimentos referentes aos mecanismos de emergência são documentados. 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 Certisign está 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 Certisign e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC Certisign.

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

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

5.1.3.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, 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 os 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 à 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 Certisign é garantida, por meio de:

a)gerador de porte compatível;

b) gerador de reserva;

c) sistemas de no-breaks redundantes;

d) sistemas redundantes de ar condicionado.

5.1.4. Exposição à água

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

5.1.5. Prevenção e proteção contra incêndio

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

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

5.1.5.3. A sala-cofre de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre constituem eclusas, onde uma porta só abre quando a anterior estiver fechada.

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

5.1.6. Armazenamento de mídia

A AC Certisign atende às normas NBR 11.515 e 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

5.2.1. Perfis qualificados

5.2.1.1. A AC Certisign pratica uma política de segregação de funções, controlando e registrando o acesso físico e lógico às funções críticas do ciclo de vida dos certificados digitais, de forma a garantir a segurança da atividade de certificação e evitar a manipulação desautorizada do sistema. As ações permitidas são limitadas de acordo com o perfil de cada cargo.

5.2.1.2. A AC Certisign estabelece 4 perfis distintos para sua operação, atribuídos às seguintes áreas:

- Gerência de Operações Data Center:
    - Supervisão Operacional:

– configuração e manutenção do hardware e do software da AC;
– gerenciamento e controle da tecnologia empregada nos serviços de certificação da AC;
– controle de acesso lógico dos funcionários à rede AC ;
– gerenciamento dos operadores da AC;
– controle de acesso ao sistema de certificação.

    - Supervisão de PKI:

– administração e controle dos componentes criptográficos da AC;
– verificação dos registros de acesso aos diferentes níveis de proteção das chaves privadas das AC (logs);
– elaboração das cerimônias de geração de chaves de AC;
– armazenamento dos registros de auditoria do sistema de certificação;
– utilização de criptografia para segurança de acesso ao aplicativo de certificação.

- Gerência de Segurança:

– implementação da Política de Segurança da AC ;
– verificação dos registros de auditoria;
– supervisão do cumprimento das práticas e procedimentos determinados na Política de Segurança da AC;
– acompanhamento das auditorias de segurança realizadas por terceiros;
– verificação do cumprimento desta DPC;
– autorização e concessão de acesso às instalações físicas e autorização de acessos lógicos ao sistema de certificação;

- utilização de criptografia para a segurança da base de dados de registro de auditoria do sistema de certificação.

- Gerência de Operação:
  - Gerenciamento e controle dos processos de validação, verificação, emissão e revogação de certificados.

5.2.1.3. Os operadores do sistema de certificação da AC Certisign recebem treinamento específico antes de obter qualquer tipo de acesso ao sistema. O tipo e o nível de acesso estão determinados, em documento formal (Política de Segurança da AC Certisign), com base nas necessidades de cada perfil.

5.2.1.3.1. A AC Certisign realiza um exame, para emissão de certificados em cadeia do tipo SSL e CS, nos operadores do sistema de certificação da AC Certisign, de acordo com os requisitos de princípios e critérios WebTrust Baseline.

5.2.1.4. A AC Certisign possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos empregados. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o empregado devolve à AC Certisign 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 Certisign, conforme o descrito em 6.2.2.

5.2.2.2. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Certisign requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC Certisign podem ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC Certisign tem sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso às instalações da AC Certisign;

b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC Certisign;

c) receber um certificado para executar suas atividades operacionais na AC Certisign; e

d) receber uma conta no sistema de certificação da AC Certisign.

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

a) são diretamente atribuídos a um único empregado;

b) não são compartilhados; e

c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC Certisign adota padrão de utilização de "senhas fortes", definido na sua Política de Segurança e em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

5.2.4. Funções que requerem separação de deveres

A AC Certisign implementa a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3. Controles de Pessoal

Todos os empregados da AC Certisign 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;

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 Certisign envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.3.2. Procedimentos de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC Certisign envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido, pelo menos, a:

a) verificação de antecedentes criminais;

b) verificação de situação de crédito;

c) verificação de histórico de empregos anteriores; e

d) comprovação de escolaridade e de residência.

5.3.2.2. A AC Certisign poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC Certisign envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebem treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e mecanismos de segurança da AC Certisign;

b) sistema de certificação em uso na AC Certisign;

c) procedimentos de recuperação de desastres e de continuidade do negócio;

d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma dos itens 3.2.2 e 3.2.3 e 3.2.7; e

e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

O pessoal da AC Certisign envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC Certisign.

5.3.5. Frequência e sequência de rodízio de cargos

Não estabelecido.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC Certisign, o acesso dessa pessoa ao sistema de certificação é suspenso, é instaurado processo administrativo para apurar os fatos e, se for o caso, são tomadas as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima contém, 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 Certisign encaminha suas conclusões à AC Raiz.

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

a) advertência;

b) suspensão por prazo determinado; ou

c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da AC Certisign envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC Certisign disponibiliza para todo o seu pessoal:

a) A DPC da AC Certisign;

b) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8];

c) documentação operacional relativa a suas atividades; e

d) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. A documentação fornecida é classificada segundo a política de classificação de informação definida pela AC Certisign e é mantida atualizada.

5.4. Procedimentos de Log de Auditoria

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC Certisign com o objetivo de manter um ambiente seguro.

5.4.1. Tipos de eventos registrados

5.4.1.1. A AC Certisign registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) iniciação e desligamento do sistema de certificação;

b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC Certisign;

c) mudanças na configuração dos sistemas AC Certisign ou nas suas chaves;

d) mudanças nas políticas de criação de certificados;

e) tentativas de acesso (login) e de saída do sistema (logoff);

f) tentativas não autorizadas de acesso aos arquivos do sistema;

g) geração de chaves próprias da AC Certisign ou de chaves das ACs subsequentes;

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 Certisign também registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

a) registros de acessos físicos;

b) manutenção e mudanças na configuração de seus sistemas;

c) mudanças de pessoal e perfis qualificados;

d) relatórios de discrepância e comprometimento; e

e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

5.4.1.3. As informações registradas pela AC Certisign são todas as descritas nos itens acima.

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

5.4.1.5. A documentação relacionada aos serviços da AC Certisign é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.4.1.6. Não se aplica.

5.4.1.7. Não se aplica.

5.4.2. Frequência de auditoria de registros

A periodicidade com que os registros de auditoria da AC Certisign são analisados pelo pessoal operacional é de uma semana.

Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3. Período de retenção para registros de auditoria

A AC Certisign mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses e, subsequentemente, armazena-os da maneira descrita no item 5.5.

5.4.4. Proteção de registros de auditoria

5.4.4.1. O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção através das funcionalidades nativas dos sistemas operacionais. As ferramentas disponíveis no sistema operacional liberam os acessos lógicos aos registros de auditoria somente a usuários ou aplicações autorizadas, através de permissões dadas pelo administrador do sistema de acordo com a função dos usuários ou aplicações e orientação do departamento de segurança.

O próprio sistema operacional também registra os acessos aos arquivos onde estão armazenados os registros de auditoria.

5.4.4.2. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção através de controles de acesso aos ambientes físicos onde são armazenados estes registros.

5.4.4.3. Os mecanismos de proteção descritos obedecem à Política de Segurança da AC Certisign, em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

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

Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela AC Certisign têm cópias de segurança semanais, feitas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas. Estas cópias são enviadas ao departamento de segurança.

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

O sistema de coleta de dados de auditoria interno à AC Certisign é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

5.4.7. Notificação de agentes causadores de eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC Certisign, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

5.4.8. Avaliações de vulnerabilidade

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

5.5. Arquivamento de Registros

Nos itens seguintes da DPC está descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC Certisign e pelas ACs de nível subsequente a ela vinculadas.

5.5.1. Tipos de registros arquivados

Os tipos de registros arquivados são:

a) Solicitações de certificados;

b) Solicitações de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR;

f) Trocas de chaves criptográficas da AC responsável; e

g) Informações de auditoria previstas no item 5.4.1.

5.5.2. Período de retenção para arquivo

Os períodos de retenção por tipo de registro arquivado são:

a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;

b) Os dossiês dos titulares devem ser 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, deverão ser retidas por, no mínimo, 7 (sete) anos.

5.5.3. Proteção de arquivo

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

5.5.4. Procedimentos de cópia de arquivo

5.5.4.1. A AC Certisign estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC Certisign, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

5.5.4.3. A AC Certisign verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para datação de registros

Informações de data e hora nos registros baseiam-se no horário Greenwich Mean Time (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos for zero.

Nos casos em que por algum motivo os documentos formalizem o uso de outro formato, ele será aceito.

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

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Certisign em seus procedimentos operacionais são automatizados e manuais e internos.

5.5.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC Certisign, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

5.6. Troca de chave

5.6.1. O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico.

A AC Certisign fornece novo certificado a AC Subsequente utilizando o mesmo procedimento utilizado para emissão do certificado inicial. A AC Certisign comunica o titular do certificado, 13 (treze) meses antes da expiração do certificado, junto com instruções para a solicitação de um novo certificado.

A comunicação de expiração e solicitação de renovação é realizada através de e-mail.

5.6.2. Não se aplica.

5.7. Comprometimento e Recuperação de Desastre

Nos itens seguintes da DPC estão descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no PCN da AC Certisign, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], para garantir a continuidade dos seus serviços críticos.

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento

5.7.1.1 A AC Certisign possui um Plano de Continuidade do Negócio – PCN, de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. Possui ainda um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.

5.7.1.2 Não se aplica.

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

Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança da AC Certisign, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação. Caso haja necessidade, o Gerente de Segurança decretará a contingência.

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

5.7.3.1 Certificado de entidade é revogado

Em caso de revogação do certificado da AC Certisign o Gerente de Segurança, juntamente com a Supervisão de PKI da AC Certisign, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados. A AC Certisign emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

5.7.3.2 Chave de entidade é comprometida

Em caso de suspeita de comprometimento de chave da AC Certisign, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com a Supervisão de PKI da AC Certisign, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

a) Todos os certificados afetados serão revogados e as partes serão notificadas.

b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a AC Certisign estiver encerrando suas atividades.

5.7.4. Capacidade de continuidade de negócio após desastre

Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, o Departamento de Infraestrutura, responsável pela contingência, notifica o Gerente de Segurança e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:

a) garantir a integridade física das pessoas que se encontram nas instalações da AC Certisign;

b) monitorar e controlar o foco da contingência;

c) minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

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, a DPC define as medidas de segurança implantadas pela AC Certisign para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. São também definidos outros controles técnicos de segurança utilizados pela AC Certisign e pelas ARs vinculadas na execução de suas funções operacionais.

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas da AC Certisign é gerado pela própria AC Certisign, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. A geração do par de chaves de AC Certisign é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC Certisign, treinados para a função.

A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves da AC Certisign é gerado em módulo criptográfico de hardware no padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

Somente os titulares dos certificados emitidos pela AC Certisign geram os seus respectivos pares de chaves.

6.1.1.3. Não se aplica.

6.1.1.4. A geração do par de chaves de AC Subsequente é realizada em processo verificável, obrigatoriamente na presença de funcionários de confiança da AC Subsequente treinados para a função. A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves das AC Subsequente é gerado e armazenado em módulo criptográfico de hardware com padrão de segurança IPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.1.5. Não se aplica.

6.1.1.6. Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC Certisign são os indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.2. Entrega da chave privada à entidade

A geração e a guarda de uma chave privada será de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Os procedimentos utilizados pela AC Certisign para a entrega de sua chave pública à AC de nível hierárquico superior encarregada da emissão de seu certificado é definido pela AC superior.

6.1.3.2. A chave pública de uma AC Subsequente é entregue pelo representante legal da AC Subsequente, em cerimônia específica, em data e hora previamente estabelecidas pela AC Certisign. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

6.1.4. Entrega de chave pública da AC às terceiras partes

A AC Certisign disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web: http://icp-brasil.certisign.com.br/repositorio/ac_certisign.html.

6.1.5. Tamanhos de chave

6.1.5.1. Não se aplica.

6.1.5.2. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC Certisign é de 4096 bits. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo da ICP-Brasil está em conformidade com o definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

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 dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

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

6.1.7.1 Os certificados de assinatura emitidos pela AC Certisign têm ativados os bits keyCertSign e CRLSign ativados .

6.1.7.2 A chave privada AC Certisign é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

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

A AC Certisign implementa uma combinação de controles físicos lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas.

A chave privada da AC Certisign é armazenada de forma cifrada no mesmo componente seguro de hardware utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

Os titulares de certificados emitidos pela AC Certisign, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado da suas chaves privadas.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC Certisign adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.2.1.2. O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão de homologação ICP-Brasil ou Certificação INMETRO.

6.2.2. Controle “n de m” para chave privada

6.2.2.1. A AC Certisign exige controle múltiplo para utilização da sua chave privada.

6.2.2.2. É necessária a presença de pelo menos 3 (três) de um grupo de 10 (dez) funcionários de confiança, com perfis qualificados para a utilização da chave privada da AC Certisign.

6.2.3. Custódia (escrow) de chave privada

A AC Certisign não implementa tal prática.

6.2.4. Cópia de segurança de chave privada

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

6.2.4.2. A AC Certisign mantém cópia de segurança de sua chave privada.

6.2.4.3. Não se aplica.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo 3DES – 112 bits ou AES – 128 ou 256 bits, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC Certisign não arquiva cópias de chaves privadas de titulares de certificados.

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

6.2.6. Inserção de chave privada em módulo criptográfico

A AC Certisign gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A ativação das chaves privadas das AC Certisign é coordenada pela Supervisão de PKI, onde 3 de um grupo de 10 funcionários com perfis qualificados da AC Certisign, detentores de partição da chave de ativação do equipamento criptográfico (PIN), apresentam tais componentes em cerimônia específica.

Esses funcionários são identificados pelo crachá funcional emitido pela AC Certisign contendo fotografia, nome, e departamento do funcionário.

6.2.9. Método de desativação de chave privada

A chave privativa da AC Certisign, instalada em ambiente de produção dos sistemas de certificação, localiza-se em nível de segurança 4, onde só é permitido o acesso ao ambiente em duplas devidamente autorizadas pelo sistema de controle de acesso da AC Certisign.

Dentro deste ambiente, somente funcionários qualificados do departamento de operações têm acesso ao sistema de certificação de produção, onde são executados os comandos de desativação do sistema, após a sua devida identificação e autorização feita através de mecanismos nativos do sistema operacional.

Esses funcionários são identificados pelo crachá funcional emitido pela AC Certisign contendo fotografia, nome, e departamento do funcionário.

6.2.10. Método de destruição de chave privada

A Supervisão de PKI da AC Certisign, de posse da chave privada original e suas cópias de segurança a serem destruídas, acompanhado do Gerente de Segurança e do representante legal da AC Certisign, titular do certificado, conduz cerimônia especifica, em ambiente de nível 4 de segurança, para reinicialização das mídias de armazenamento das chaves privadas, não deixando informações remanescente sensíveis nessas mídias.

O Gerente de Segurança e Supervisão de PKI são identificados pelo crachá funcional emitido pela AC Certisign contendo fotografia, nome, e departamento do funcionário. O representante legal da AC Certisign é identificado através de cédula de identidade ou passaporte, se estrangeiro.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da AC Certisign e dos titulares dos certificados de assinatura digital por ela emitidos, bem como as LCR emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

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

6.3.2.1. As chaves privadas dos titulares dos certificados de assinatura digital emitidos pela AC Certisign são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes

chaves públicas podem ser utilizadas durante todo período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. Não se aplica.

6.3.2.4. A validade admitida para certificados da AC Certisign é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4. Dados de Ativação

Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação do equipamento de criptografia que armazena as chaves privadas da AC Certisign são únicos e aleatórios.

6.4.1.2. Não se aplica.

6.4.2. Proteção dos dados de ativação

6.4.2.1. A AC Certisign garante que os dados de ativação de sua chave privada são protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Não se aplica.

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 Certisign é realizada em ambiente próprio para a condução de Cerimônia de Geração de Chaves. O ambiente computacional é mantido off-line de modo a impedir o acesso remoto não autorizado.

6.5.1.2. A geração dos pares de chaves das AC subsequentes é realizada em ambiente próprio, protegido de modo a minimizar os riscos potenciais inerentes desta operação. O ambiente computacional é mantido off-line para impedir o acesso remoto não autorizado.

6.5.1.3. O ambiente computacional da AC Certisign relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes funções:

a) controle de acesso aos serviços e perfis da AC Certisign;

b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC Certisign;

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 Certisign;

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 mecanismos de segurança física.

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção deverá ter apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC Certisign, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, deverão ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC Certisign. Todos esses eventos deverão ser registrados para fins de auditoria.

6.5.1.6. Equipamentos utilizados pela AC Certisign são preparados e configurados como previsto na Política de Segurança da AC Certisign ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A segurança computacional da AC Certisign segue as recomendações Common Criteria.

6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.

6.5.3.2. Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistema

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

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

6.6.2. Controles de gerenciamento de segurança

6.6.2.1 As Ferramentas e procedimentos empregados pela AC Certisign para garantir que os seus sistemas implementem os níveis configurados de segurança são:

a) A operação dos Sistemas Operacionais é controlada pelos privilégios nomeados e pelos papéis confiados, descritos no item 5.2.1;

b) A AC Certisign opera em equipamento off-line para geração, emissão de LCR e assinatura de certificados. Este ambiente não necessita de configuração de segurança de rede.

6.6.2.2 O gerenciamento de configuração para a instalação e a continua manutenção do sistema de certificação utilizado pela AC Certisign, envolve o teste de mudanças planejadas no ambiente de

desenvolvimento e homologação, antes da sua implantação em ambiente de produção de acordo com o documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

6.6.3. Controles de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na Geração de LCR

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

6.7. Controles de Segurança de Rede

6.7.1 Diretrizes Gerais

6.7.1.1. Neste item são descritos os controles relativos à segurança da rede da AC Certisign, incluindo firewalls e recursos similares.

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

6.7.1.3. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls, e sistemas de detecção de intrusos (IDS), localizados no segmento de rede que hospeda o sistema de certificação 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 ou homologação.

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

6.7.2. Firewall

6.7.2.1. Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. 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 Certisign.

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 está configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar traps SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta aos firewalls ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas ou ainda a reconfiguração dos firewalls.

6.7.3.2. O sistema de detecção de intrusão reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com atualização da sua base de reconhecimento.

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

6.7.4. Registro de acessos não-autorizados à rede

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

6.8. Carimbo de Tempo

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR E OCSP

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC Certisign 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

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

7.1.2. Extensões de certificado

A ICP-Brasil define como obrigatórias as seguintes extensões para certificados de AC:

a) “Authority Key Identifier”, não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Certisign;

b) “Subject Key Identifier”, não crítica: contém o hash SHA-1 da chave pública da AC Certisign;

c) “Key Usage”, crítica: somente os bits keyCertSign e cRLSign estão ativados;

d) “Certificate Policies”, não crítica:

d.1) o campo policyIdentifier contém o OID da DPC da AC Certisign;

d.2) o campo policyQualifiers contém o endereço Web DPC da AC Certisign: http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign/DPC_AC_Certisign.pdf;

e) “Basic Constraints”, crítica: contém o campo cA=True; e

f) “CRL Distribution Points”, não crítica: contém o endereço na Web onde se obtém a LCR correspondente ao certificado da AC Certisign:

Para certificados emitidos na G2:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignG6/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignG6/LatestCRL.crl

Para certificados emitidos na G7:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignG7/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignG7/LatestCRL.crl

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC Certisign são assinados com o uso do algoritmo RSA com SHA-256 como função de hash (OID 1.2.840.113549.1.1.11) ou algoritmo RSA com SHA-512 como função de hash (OID 1.2.840.113549.1.1.13) conforme o padrão PKCS#1.

7.1.4. Formatos de nome

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

C = BR

O = ICP-Brasil

OU = nome da AC emitente

CN = nome da AC titular

7.1.5. Restrições de nome

7.1.5.1. Neste item da DPC, devem ser descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC Certisign são as seguintes:

a) não são admitidos sinais de acentuação, trema ou cedilhas;
b) além dos caracteres alfanuméricos, são utilizados somente os seguintes caracteres especiais:

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

7.1.6. OID (Object Identifier) da DPC

O OID desta DPC é 2.16.76.1.1.5.

7.1.7. Uso da extensão "Policy Constraints"

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço web da DPC da AC Certisign: http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign/DPC_AC_Certisign.pdf.

7.1.9. Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC Certisign implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC Certisign e sua criticalidade.

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

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

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

7.3. Perfil 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

As auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

8.4. Tópicos cobertos pela avaliação

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

8.4.2. A AC Certisign recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e 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. As entidades da ICP-Brasil diretamente vinculadas à AC Certisign (AC, AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC Certisign 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

A AC Certisign age de 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

A AC Certisign age de 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

Variável conforme definição interna Comercial.

9.1.2. Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

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

Não são cobradas tarifas de revogação e de acesso à informação de status.

9.1.4. Tarifas para outros serviços

Não são cobradas tarifas de acesso à informação de status do certificado e à LCR, bem como tarifas de revogação e de acesso aos certificados emitidos.

9.1.5. Política de reembolso

Em caso de revogação do certificado por motivo de comprometimento da chave privada ou da mídia armazenadora da chave privada da AC Certisign, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC Certisign, será emitido gratuitamente outro certificado em substituição.

9.2. Responsabilidade Financeira

A responsabilidade da AC Certisign 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 Como princípio geral, todo documento, informação ou registro fornecido à AC Certisign é sigiloso.

9.3.1.2. Nenhum documento, informação ou registro fornecido pelos titulares de certificado à AC Certisign será divulgado.

9.3.2 Informações fora do escopo de informações confidenciais

As informações consideradas não sigilosas compreendem:

a) os certificados e a LCR emitidos pela AC Certisign;

b) informações corporativas ou pessoais que façam parte do certificados ou em diretórios públicos;

c) esta DPC;

d) versões públicas da Política de Segurança;

e) resultados finais de auditorias; e

f) Termo de Titularidade ou solicitação de emissão do certificado.

A AC Certisign e a AC subsequente a ela vinculada tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

a) estejam na posse legítima da AC Certisign ou da AC subsequente a ela vinculada antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;

b) posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro(s) com direitos legítimos para divulgação sua sem quaisquer restrições para tal;

c) sejam requisitados por determinação judicial ou governamental, desde que a AC Certisign ou a AC subsequente a ela vinculada comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pela AC Certisign e pela AC subsequente a ela vinculada, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

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 Certisign também são considerados documentos não confidenciais:

a) está DPC;

b) versões públicas de Política de Segurança – PS; e

c) a conclusão dos relatórios da auditoria.

9.3.2.3. A AC Certisign também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados ou carimbos de tempo emitidos no âmbito da ICP-Brasil.

9.3.3 Responsabilidade em proteger a informação confidencial

9.3.3.1. Os participantes que receberem ou tiverem acesso a informações confidenciais devem possuir 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 Certisign será gerada e mantida pela própria AC, que será 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. Não se aplica.

9.3.3.4. No caso de certificados de sigilo emitidos pela AC Certisign, a DPC deve delimitar as responsabilidades pela manutenção e pela garantia do sigilo das respectivas chaves privadas.

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

A AC Certisign assegurará 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 Certisign 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 e de AC de nível imediatamente subsequente ao da AC são fornecidas na LCR da AC Certisign.

9.4.4 Responsabilidade para proteger a informação privadas

A AC Certisign e a AC subsequente a ela 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 Certisign 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 Certisign será 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 Certisign 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, que nenhum documento, informação ou registro sob a guarda da Certisign deverá ser fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

9.5 Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6 Declarações e Garantias

9.6.1 Declarações e Garantias da AC

A AC Certisign declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

A AC Certisign implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC. A AC Certisign, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das ACs subsequentes na forma de suas DPCs e normas complementares.

9.6.1.2 Precisão da informação

A AC Certisign 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 na forma de suas DPCs e normas complementares.

9.6.1.3 Identificação do requerente

A AC Certisign implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC Certisign, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs subsequentes na forma de suas DPCs e normas complementares.

9.6.1.4 Consentimento dos titulares

A AC Certisign implementa termos de consentimento ou titularidade, contidas nos itens 3 e 4 desta DPC.

9.6.1.5 Serviço

A AC Certisign mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios, das ACs subsequentes e LCRs.

9.6.1.6 Revogação

A AC irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil.

9.6.1.7 Existência Legal

Esta DPC está em conformidade legal com a MP 2.200-2, de 24 de agosto de 2001, e legislação aplicável.

9.6.2 Declarações e Garantias da AR

Em acordo com item 4 desta DPC.

9.6.3 Declarações e garantias do titular

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

9.6.3.2 A AC Certisign deve informar 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 devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;

b) verificar, a qualquer tempo, a validade do certificado.

9.6.4.2 O certificado da AC Certisign ou um certificado de AC de nível imediatamente subsequente ao da AC Certisign é considerado válido quando:

i. tiver sido emitido pela AC Certisign;

ii. não constar como revogado pela AC Certisign;

iii. não estiver expirado; e

iv. puder ser verificado com o uso do certificado válido da AC Certisign.

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

9.6.5 Representações e garantias de outros participantes

Não se aplica.

9.7 Isenção de garantias

Não se aplica.

9.8 Limitações de responsabilidades

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

9.9 Indenizações

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

9.10 Prazo e Rescisão

9.10.1 Prazo

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

9.10.2 Término

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

9.10.3 Efeito da rescisão e sobrevivência

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

9.11 Avisos individuais e comunicações com os participantes

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

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

A AC Certisign mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign/DPC_AC_Certisign.pdf.

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. A DPC da AC Certisign não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.14. Lei aplicável

Esta DPC é regida pela legislação da República Federativa do Brasil, notadamente a Medida Provisória Nº 2.200-2, de 24.08.2001, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas em vigor no Brasil.

9.15. Conformidade com a Lei aplicável

A AC Certisign 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 Certisign e suas ACs subsequentes e outras entidades citadas. Havendo conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2. Cessão

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

9.16.3. Independência de disposições

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

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

De acordo com a legislação vigente.

9.17. Outras provisões

Não se aplica.

10. DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTODAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

10.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	DOC-ICP-05.02
[11]	REGULAMENTO DO USO DE BIOMETRIA NO ÂMBITO DA ICP BRASIL – SISTEMA BIOMÉTRICO DA ICPBRASIL	DOC-ICP-05.03
[12]	REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS	DOC-ICP-01.02
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICA DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05

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

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

11. REFERÊNCIAS BIBLIOGRÁFICAS

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