soluti

LIBERDADE DIGITAL

Declaração de Práticas de Certificação

da Autoridade Certificadora

SOLUTI

(DPC AC SOLUTI)

OID 2.16.76.1.1.46

Versão 2.0 de 1 de julho de 2020

Classificação: Ostensivo

www.acsoluti.com.br

Sumário

Controle de Versão 7

1 INTRODUÇÃO 8

1.1 Visão Geral 8
1.2 Nome do documento e identificação 8
1.3 Participantes da ICP-Brasil 8
1.3.1 Autoridades Certificadoras 8
1.3.2 Autoridades de Registro 8
1.3.3 Titulares do Certificado 8
1.3.4 Partes Confiáveis 8
1.3.5 Outros Participantes 9
1.4 Usabilidade do Certificado 9
1.4.1 Uso apropriado do certificado 9
1.4.2 Uso proibitivo do certificado 9
1.5 Política de Administração 9
1.5.1 Organização administrativa do documento 9
1.5.2 Contatos 9
1.5.3 Pessoa que determina a adequabilidade da DPC com a PC 9
1.5.4 Procedimentos de aprovação da DPC 9
1.6 Definições e Acrônimos 10

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 12

2.1 Repositórios 12
2.2 Publicação de informações dos certificados 12
2.3 Tempo ou Frequência de Publicação 12
2.4 Controle de Acesso aos Repositórios 12

3 IDENTIFICAÇÃO E AUTENTICAÇÃO 12

3.1 Atribuição de Nomes 13
3.1.1 Tipos de nomes 13
3.1.2 Necessidade dos nomes serem significativos 13
3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado 13
3.1.4 Regras para interpretação de vários tipos de nomes 13
3.1.5 Unicidade de nomes 13
3.1.6 Procedimento para resolver disputa de nomes 13
3.1.7 Reconhecimento, autenticação e papel de marcas registradas 13
3.2 Validação inicial de identidade 13
3.2.1 Método para comprovar a posse de chave privada 14
3.2.2 Autenticação da identificação da organização 14
3.2.3 Autenticação da identidade de um indivíduo 15
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 19
3.3 Identificação e autenticação para pedidos de novas chaves 19
3.3.1 Identificação e autenticação para rotina de novas chaves antes da expiração 19
3.3.2 Identificação e autenticação para novas chaves após a revogação ou expiração do certificado 20
3.4 Identificação e Autenticação para solicitação de revogação 20

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 20

4.1 Solicitação do certificado 20
4.1.1 Quem pode submeter uma solicitação de certificado 21
4.1.2 Processo de registro e responsabilidades 21

4.2 Processamento de Solicitação de Certificado....23
4.2.1 Execução das funções de identificação e autenticação....23
4.2.2 Aprovação ou rejeição de pedidos de certificado....23
4.2.3 Tempo para processar a solicitação de certificado....23
4.3 Emissão de Certificado....23
4.3.1 Ações da AC durante a emissão de um certificado....23
4.3.2 Notificações para o titular do certificado pela AC na emissão do certificado....23
4.4 Aceitação de Certificado....23
4.4.1 Conduta sobre a aceitação do certificado....23
4.4.2 Publicação do certificado pela AC....24
4.4.3 Notificação de emissão do certificado pela AC Raiz para outras entidades....24
4.5 Usabilidade do par de chaves e do certificado....24
4.5.1 Usabilidade da Chave privada e do certificado do titular....24
4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis....24
4.6 Renovação de Certificados....24
4.6.1 Circunstâncias para renovação de certificados....24
4.6.2 Quem pode solicitar a renovação....24
4.6.3 Processamento de requisição para renovação de certificados....24
4.6.4 Notificação para nova emissão de certificado para o titular....25
4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado....25
4.6.6 Publicação de uma renovação de um certificado pela AC....25
4.6.7 Notificação de emissão de certificado pela AC para outras entidades....25
4.7 Nova chave de certificado (Re-key)....25
4.7.1 Circunstâncias para nova chave de certificado....25
4.7.2 Quem pode requisitar a certificação de uma nova chave pública....25
4.7.3 Processamento de requisição de novas chaves de certificado....25
4.7.4 Notificação de emissão de novo certificado para o titular....25
4.7.5 Conduta constituindo a aceitação de uma nova chave certificada....25
4.7.6 Publicação de uma nova chave certificada pela AC....25
4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades....25
4.8 Modificação de certificado....25
4.8.1 Circunstâncias para modificação de certificado....25
4.8.2 Quem pode requisitar a modificação de certificado....25
4.8.3 Processamento de requisição de modificação de certificado....25
4.8.4 Notificação de emissão de novo certificado para o titular....25
4.8.5 Conduta constituindo a aceitação de uma modificação de certificado....25
4.8.6 Publicação de uma modificação de certificado pela AC....25
4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades....25
4.9 Suspensão e Revogação de Certificado....25
4.9.1 Circunstâncias para revogação....25
4.9.2 Quem pode solicitar revogação....26
4.9.3 Procedimento para solicitação de revogação....26
4.9.4 Prazo para solicitação de revogação....27
4.9.5 Tempo em que a AC deve processar o pedido de revogação....27
4.9.6 Requisitos de verificação de revogação para as partes confiáveis....27
4.9.7 Frequência de emissão de LCR....27
4.9.8 Latência máxima para a LCR....28
4.9.9 Disponibilidade para revogação/verificação de status on-line....28
4.9.10 Requisitos para verificação de revogação on-line....28
4.9.11 Outras formas disponíveis para divulgação de revogação....28
4.9.12 Requisitos especiais para o caso de comprometimento de chave....28
4.9.13 Circunstâncias para suspensão....28
4.9.14 Quem pode solicitar suspensão....28
4.9.15 Procedimento para solicitação de suspensão....28
4.9.16 Limites no período de suspensão....28
4.10 Serviços de status de certificado....28
4.10.1 Características operacionais....28
4.10.2 Disponibilidade dos serviços....28
4.10.3 Funcionalidades operacionais....28
4.11 Encerramento de atividades....29

4.12 Custódia e recuperação de chave....29
4.12.1 Política e práticas de custódia e recuperação de chave....29
4.12.2 Política e práticas de encapsulamento e recuperação de chave de sessão....29
5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES....29
5.1 Controles Físicos....29
5.1.1 Construção e localização das instalações de AC....29
5.1.2 Acesso físico....30
5.1.3 Energia e ar-condicionado....32
5.1.4 Exposição à água....33
5.1.5 Prevenção e proteção contra incêndio....33
5.1.6 Armazenamento de mídia....33
5.1.7 Destruição de lixo....33
5.1.8 Instalações de segurança (backup) externas (off-site) para AC SOLUTI....33
5.2 Controles Procedimentais....33
5.2.1 Perfis qualificados....33
5.2.2 Número de pessoas necessário por tarefa....34
5.2.3 Identificação e autenticação para cada perfil....34
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....35
5.3.2 Procedimentos de verificação de antecedentes....35
5.3.3 Requisitos de treinamento....35
5.3.4 Frequência e requisitos para reciclagem técnica....35
5.3.5 Frequência e sequência de rodízios de cargos....35
5.3.6 Sanções para ações não autorizadas....35
5.3.7 Requisitos para contratação de pessoal....36
5.3.8 Documentação fornecida ao pessoal....36
5.4 Procedimentos de Log de Auditoria....36
5.4.1 Tipos de eventos registrados....36
5.4.2 Frequência de auditoria de registros....37
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....38
5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)....38
5.4.7 Notificação de agentes causadores de eventos....38
5.4.8 Avaliações de vulnerabilidade....38
5.5 Arquivamento de Registros....38
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....39
5.5.6 Sistema de coleta de dados de arquivo (interno e externo)....39
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 gerenciamento de incidente e comprometimento....39
5.7.2 Recursos computacionais, software, e/ou dados corrompidos....40
5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade....40
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 42

6.1.7 Propósitos de uso de chave (conforme o campo “Key usage” na X.509 v3)....42
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....43
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....44
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....46
6.6.3 Controles de segurança de ciclo de vida....46
6.6.4 Controles na Geração da 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)....47
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....47
7.1.4 Formatos de nome....47
7.1.5 Restrições de nome....47
7.1.6 OID (Object Identifier) da DPC....47
7.1.7 Uso da extensão “Policy Constraints”....47
7.1.8 Sintaxe e semântica dos qualificadores de política....47
7.1.9 Semântica de processamento para as extensões criticas de PC....48
7.2 Perfil de LCR....48
7.2.1 Número(s) de versão....48
7.2.2 Extensões de LCR e de suas entradas....48
7.3 Perfil de OCSP....48
7.3.1 Número(s) de versão....48
7.3.2 Extensões de OCSP....48
8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES....48
8.1 Frequência e circunstâncias das avaliações....48
8.2 Identificação/Qualificação do avaliador....48
8.3 Relação do avaliador com a entidade avaliada....48
8.4 Tópicos cobertos pela avaliação....48
8.5 Ações tomadas como resultado de uma deficiência....49

8.6 Comunicação dos resultados 49
9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS 49
9.1 Tarifas 49
9.1.1 Tarifas de emissão e renovação de certificados 49
9.1.2 Tarifas de acesso ao certificado 49
9.1.3 Tarifas de revogação ou de acesso à informação de status 49
9.1.4 Tarifas para outros serviços 49
9.1.5 Política de reembolso 49
9.2 Responsabilidade Financeira 49
9.2.1 Cobertura do seguro 49
9.2.2 Outros ativos 49
9.2.3 Cobertura de seguros ou garantia para entidades finais 49
9.3 Confidencialidade da informação do negócio 50
9.3.1 Escopo de informações confidenciais 50
9.3.2 Informações fora do escopo de informações confidenciais 50
9.3.3 Responsabilidade em proteger a informação confidencial 50
9.4 Privacidade da informação pessoal 51
9.4.1 Plano de privacidade 51
9.4.2 Tratamento de informação como privadas 51
9.4.3 Informações não consideradas privadas 51
9.4.4 Responsabilidade para proteger a informação privada 51
9.4.5 Aviso e consentimento para usar informações privadas 51
9.4.6 Divulgação em processo judicial ou administrativo 51
9.4.7 Outras circunstâncias de divulgação de informação 51
9.4.8 Informações a terceiros 51
9.5 Direitos de Propriedade Intelectual 51
9.6 Declarações e Garantias 51
9.6.1 Declarações e Garantias da AC 51
9.6.2 Declarações e Garantias da AR 52
9.6.3 Declarações e garantias do titular 52
9.6.4 Declarações e garantias das terceiras partes 52
9.6.5 Representações e garantias de outros participantes 52
9.7 Isenção de garantias 53
9.8 Limitações de responsabilidades 53
9.9 Indenizações 53
9.10 Prazo e Rescisão 53
9.10.1 Prazo 53
9.10.2 Término 53
9.10.3 Efeitos de rescisão e sobrevivência 53
9.11 Avisos individuais e comunicações com os participantes 53
9.12 Alterações 53
9.12.1 Procedimento para emendas 53
9.12.2 Mecanismo de notificação e períodos 53
9.12.3 Circunstâncias na qual o OID deve ser alterado 53
9.13 Solução de conflitos 53
9.14 Lei aplicável 53
9.15 Conformidade com a Lei aplicável 53
9.16 Disposições Diversas 54
9.16.1 Acordo completo 54
9.16.2 Cessão 54
9.16.3 Independência de disposições 54
9.16.4 Execução (honorários dos advogados e renúncia de direitos) 54
9.17 Outras provisões 54
10 DOCUMENTOS REFERENCIADOS 54
11 REFERÊNCIAS BIBLIOGRÁFICAS 55

Controle de Versão

Versão	Data	Descrição
2.0	01/07/2020	Adequação à versão 5.5 do DOC-ICP-05.
1.1r2	22/05/2018	Alteração dos itens 2.7.1, 4.4.10, 4.4.10.1 e 4.4.10.2, referente à resolução no. 119 de 06 de julho de 2017. Alteração dos itens 3.1.1.2 e 3.1.1.2.1 a 3.1.1.2.5, referente à resolução de 19 de setembro de 2017.
1.1r1	07/11/2016	Adequação da DPC à versão 4.1 do DOC-ICP-05 versão 4.1. Itens alterados: 2.6.4, 3.1.1.1, 3.1.1.7, 3.1.1.8, 3.1.2, 3.1.9, 3.1.9.1, 4.4.2. Revisão dos procedimentos de revogação (item 4.4.3.1). Alteração no período de retenção (item 4.6.2) para atender ao DOC-ICP-01.02 Atualização dos dados de contato (item 1.4) Nova Fonte Confiável de Tempo estabelecida pela IN 7/2015 (item 4.6.5).
1.1	11/12/2012	Alterado item 7.2.4 (página 43) para incluir no DN do certificado o campo “OU = Autoridade Certificadora Raiz Brasileira v2”, atendendo ao disposto no DOC-ICP-01 versão 4.2 item 7.2.4.
1.0	01/11/2012	Versão inicial, a partir do DOC-ICP-05 versão 3.6.

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 DPC descreve as práticas e os procedimentos empregados pela Autoridade Certificadora SOLUTI, AC integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, na execução dos seus serviços de certificação digital.

1.1.2

Esta DPC foi elaborada adotando a mesma estrutura empregada no documento DOC-ICP-05 do Comitê Gestor da ICP-Brasil.

1.1.3

A AC SOLUTI não emite certificados SSL ou CS.

1.1.4

A estrutura desta DPC está baseada na RFC 3647.

1.1.5

A AC SOLUTI mantém todas as informações desta DPC atualizadas.

1.2 Nome do documento e identificação

1.2.1

Esta DPC é chamada “Declaração de Práticas de Certificação da Autoridade Certificadora SOLUTI, integrante da ICP-Brasil”, e comumente referida como “DPC AC SOLUTI”. O Identificador de Objeto (OID) desta DPC, atribuído pela AC Raiz, é 2.16.76.1.1.46.

1.2.2

Esta AC não emite certificados para usuários finais.

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

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

1.3.2 Autoridades de Registro

A atividade de identificação e cadastramento das ACs de nível imediatamente subsequente será realizada junto com o processo de credenciamento, não havendo participação de Autoridades de Registro – AR.

1.3.3 Titulares do Certificado

Os certificados emitidos pela AC SOLUTI tem como titulares as ACs de nível imediatamente subsequente ao seu.

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 AC SOLUTI publica em sua página web, http://ccd.acsoluti.com.br/, a relação de todos os

Prestadores de Suporte – PSS, Prestadores de Serviços Biométricos – PSBio e Prestadores de Serviço de Confiança – PSC, vinculados a AC responsável por esta DPC.

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do certificado

Esses certificados se destinam exclusivamente a identificação de ACs de nível imediatamente subsequente e à divulgação de chaves públicas de forma segura.

1.4.2 Uso proibitivo do certificado

Os certificados emitidos por esta AC não podem identificar ou verificar qualquer entidade ou assinatura além dos descritos nesta DPC.

1.5 Política de Administração

1.5.1 Organização administrativa do documento

Autoridade Certificadora SOLUTI

1.5.2 Contatos

AC SOLUTI
Endereço: Avenida 136, nº 797, Edifício New York Square, Sala 1901-B, Setor Sul
74.093-250 – Goiânia – Goiás
Telefones: (62) 3412-0200 / 3999-6000
E-mail: acsoluti@acsoluti.com.br

Website: www.acsoluti.com.br
A/C: Vinicius Vieira de Sousa

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Alexandre Henrique de Souza de Torres

Telefones: 62 3412-0200

E-mail: auditoria@soluti.com.br

1.5.4 Procedimentos de aprovação da DPC

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

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AGR	Agente de Registro
AR	Autoridade 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 Pessoa Jurídica
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
IEC	International Eletrotechnical Commission
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IDS	Instrusion Detection System
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria

SIGLA	DESCRIÇÃO
ITU	International Telecummunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	National Institutute of Satandards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifer
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Pessession
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RIC	Registro de Identificação Civil
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	Simpe Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade da Federação
URL	Uniform Resource Locator

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Repositórios

2.1.1

As obrigações gerais do uso do repositório da AC SOLUTI são:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC SOLUTI e a 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: são implementados scripts de verificação de emissão de LCRs como a verificação dos hash's dos documentos e certificados disponibilizados em seu repositório.

2.1.2

Os requisitos aplicáveis aos repositórios utilizados pela AC SOLUTI, são:

a) Localização física e lógica – A localização e o sistema de certificação utilizado para a operação da AC não são publicamente identificados, nem há identificação pública externa das instalações. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos;

b) Disponibilidade – aquela definida no item 2.1;

c) Protocolos de acesso – HTTP e HTTPS; e

d) Requisitos de Segurança – obedece aos requisitos definidos no item 2.1.

2.1.3

O repositório da AC SOLUTI encontra-se disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.4

A AC SOLUTI disponibiliza 2 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR:

a) http://ccd.acsoluti.com.br/

b) http://ccd2.acsoluti.com.br/

2.2 Publicação de informações dos certificados

2.2.1

A AC SOLUTI publica e mantém disponível em sua página web as informações descritas no item 2.2.2 no endereço http://ccd.acsoluti.com.br/. A disponibilidade da página é de no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2

As seguintes informações são publicadas na página web http://ccd.acsoluti.com.br/:

a) seu próprio certificado;

b) suas LCR;

c) sua DPC;

d) não se aplica;

e) uma relação, regularmente atualizada, contendo as ARs vinculadas as ACs subsequentes e seus respectivos endereços; e

f) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3 Tempo ou Frequência de Publicação

2.3.1

As informações mencionadas no item 2.2.2 serão publicadas sempre que sofrerem alterações.

As LCRs são publicadas imediatamente após sua emissão pela AC SOLUTI.

2.4 Controle de Acesso aos Repositórios

2.4.1

Não há nenhuma restrição ao acesso para consulta a esta DPC, aos certificados emitidos e à LCR da AC SOLUTI.

Acessos para escrita nos locais de armazenamento e publicação são permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC SOLUTI verifica a autenticidade da identidade e/ou atributos das ACs subsequentes antes da inclusão desses atributos em um certificado digital. As ACs subsequentes estão proibidas de usar nomes em seus certificados que violem os direitos de propriedade intelectual de terceiros. A AC SOLUTI reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1 Atribuição de Nomes

3.1.1 Tipos de nomes

3.1.1.1

Os tipos de nomes admitidos para os titulares de certificados da AC SOLUTI, segundo esta DPC é o "*distinguished name*", no padrão ITU X.500.

3.1.1.2

Certificados emitidos para ACs subsequentes ao da AC SOLUTI não incluirão o nome da pessoa responsável.

3.1.2 Necessidade dos nomes serem significativos

Os certificados emitidos pela AC SOLUTI devem incluir um identificador único que represente a AC de nível imediatamente subsequente para a qual o certificado foi emitido, conforme item 7.1.4.

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4 Regras para interpretação de vários tipos de nomes

Nomes distintos em certificados são interpretados usando os padrões ITU-T X.501 e a sintaxe ASN.1.

3.1.5 Unicidade de nomes

No campo "Distinguished Name" (DN) devem ser únicos e não ambíguos, para cada titular de certificado, no âmbito da AC emitente. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6 Procedimento para resolver disputa de nomes

A AC SOLUTI reserva-se o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes dos solicitantes de certificados. Durante o processo de

confirmação de identidade, o solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas serão executados por meio de consulta, verificação e análise junto ao sítio do Instituto Nacional de Propriedade Intelectual – INPI (www.inpi.gov.br), devendo seu titular fornecer o número do processo, protocolo ou número do registro na marca.

3.2 Validação inicial de identidade

A AC SOLUTI realiza a identificação do solicitante por meio da comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado.

3.2.1 Método para comprovar a posse de chave privada

A AC SOLUTI verifica se a AC credenciada possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. A RFC 4210, atualizada pela RFC 6712, é utilizada para essa finalidade.

3.2.2 Autenticação da identificação da organização

3.2.2.1 Disposições Gerais

3.2.2.1.1

A identificação de uma AC pela AC SOLUTI é executada por meio dos procedimentos descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES

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 do certificado.

3.2.2.1.4

Fica dispensado o disposto no item 3.2.2.1.3, alíneas “b” e “c” caso o responsável pelo certificado possua certificado digital de pessoa física ICP-Brasil válido, do tipo A3 ou superior, com os dados biométricos devidamente coletados, e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial DA ICP-BRASIL [6].

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 à sua habilitação fiscal:

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

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

NOTA 1: Essas confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

3.2.2.3 Informações contidas no certificado emitido para uma organização

3.2.2.3.1

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

a) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações;[1]

b) Cadastro Nacional de Pessoa Jurídica (CNPJ);[2]

c) nome completo do responsável pelo certificado, sem abreviações;[3] e

d) data de nascimento do responsável pelo certificado.[4]

3.2.2.3.2

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

3.2.2.4 Responsabilidade decorrente do uso do certificado

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

3.2.3 Autenticação da identidade de um indivíduo

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.

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

3.2.7 Autenticação da identidade de equipamento ou aplicação

Não se aplica.

3.2.8 Procedimentos complementares

Não se aplica.

3.2.9 Procedimentos específicos

Não se aplica.

3.3 Identificação e autenticação para pedidos de novas chaves

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

O processo de geração, pela AC SOLUTI, de um novo certificado para uma AC de nível imediatamente subsequente ao seu pode ser feito de forma simplificada, antes da expiração da validade do certificado vigente da AC. Para isso, um representante legal da AC deve fazer a solicitação formal assinada digitalmente. Após o recebimento da solicitação, desde que a documentação esteja regularmente atualizada, a AC SOLUTI iniciará o processo de emissão do novo certificado.

3.3.1.1

Um novo certificado poderá ser requerido pelo solicitante antes da expiração de seu certificado vigente, no qual deverá enviar à AC SOLUTI uma solicitação, por meio eletrônico, assinada digitalmente com o uso de um certificado de assinatura digital de mesmo nível de segurança do certificado a ser renovado.

A AC SOLUTI comunica o Titular de Certificado, por E-mail, da necessidade de renovação do certificado, com antecedência de 30 dias.

3.3.1.2

Esse processo será conduzido segundo uma das seguintes possibilidades:

a) Adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3;

b) Não se aplica.

c) Não se aplica.

d) Não se aplica.

e) Não se aplica.

3.3.1.2.1

Não se aplica.

3.3.1.3

Não se aplica.

3.3.2 Identificação e autenticação para novas chaves após a revogação ou expiração do certificado

O processo de geração, pela AC SOLUTI, de um novo certificado para uma AC de nível imediatamente subsequente ao seu pode ser feito de forma simplificada, antes da expiração da validade do certificado vigente da AC. Para isso, um representante legal da AC deve fazer a solicitação formal assinada digitalmente. Após o recebimento da solicitação, desde que a documentação esteja regularmente atualizada, a AC SOLUTI iniciará o processo de emissão do novo certificado.

3.3.2.1

O processo de identificação do solicitante quando da geração de novo par de chaves e emissão pela AC SOLUTI de novo certificado após expiração do anterior, será o mesmo da primeira emissão.

3.3.2.2

Não se aplica.

3.3.2.3

No caso de pessoa física titular de certificado expirado, previamente identificada e cadastrada presencialmente, e cujos dados biométricos tenham sido devidamente coletados, a geração de novo par de chaves poderá ser realizada mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação editada pela AC-Raiz.

3.3.2.4

No caso de uma organização titular de certificado expirado, cujo responsável pelo certificado seja o mesmo ora solicitando novo certificado, que foi previamente identificado e cadastrado presencialmente, e cujos dados biométricos tenham sido devidamente coletados, a geração de novo par de chaves poderá ser realizada mediante confirmação do respectivo cadastro, da organização e do responsável pelo certificado, por meio de videoconferência, conforme regulamentação editada pela AC-Raiz.

3.4 Identificação e Autenticação para solicitação de revogação

A solicitação de revogação de certificado de AC Subsequente é realizada através de solicitação formal assinada pelos representantes legais da entidade.

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 Solicitação do certificado

A solicitação de certificado será feita pelos indivíduos identificados conforme item 3.2 e após o processo de credenciamento junto ao ITI.

4.1.1 Quem pode submeter uma solicitação de certificado

4.1.1.1

A solicitação de certificado para AC Subsequente à AC SOLUTI somente será possível após o processo de credenciamento e a autorização de funcionamento da AC em questão, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

4.1.1.2

Não se aplica.

4.1.1.3

A AC subsequente deverá encaminhar a solicitação de certificado à AC SOLUTI 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

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

4.1.2.1 Responsabilidades da AC

4.1.2.1.1

A AC SOLUTI responde pelos danos a que der causa.

4.1.2.1.2

Não se aplica.

4.1.2.1.3

Não se aplica.

4.1.2.2 Obrigações da AC

São obrigações da AC SOLUTI:

a) operar de acordo com DPC da AC SOLUTI;

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

c) assegurar a proteção de suas chaves privadas;

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

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

f) distribuir o seu próprio certificado;

g) emitir, expedir e distribuir os certificados de ACs 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;

k) publicar na página web (http://ccd.acsoluti.com.br/) a DPC;

l) publicar, na página web (http://ccd.acsoluti.com.br/), 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) implementadas, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

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

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

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

t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;

u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;

v) informar à AC Raiz, a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;

w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;

x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais através de auditoria independente, por empresa credenciadas pela AC Raiz. ; e

y) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

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

A solicitação de certificado para uma AC de nível imediatamente subsequente ao da AC SOLUTI só é possível após o deferimento de seu pedido de credenciamento e a consequente autorização de funcionamento da AC em questão por parte do ITI, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

A AC de nível subsequente deve encaminhar a solicitação de seu certificado à AC SOLUTI por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

A AC SOLUTI não recebe solicitações de certificados para usuários finais. Portanto, não existe, para a AC SOLUTI, o cenário de restrições ou autorizações ao processamento de registros de DNS para autorização da autoridade de certificação.

4.2.1 Execução das funções de identificação e autenticação

A AC SOLUTI executa as funções de identificação e autenticação conforme item 3.2 desta DPC.

4.2.2 Aprovação ou rejeição de pedidos de certificado

4.2.2.1

A AC SOLUTI pode aceitar ou rejeitar pedidos de certificados das AC imediatamente subsequente de acordo com os procedimentos descritos no item 3.2 desta DPC. .

4.2.2.2

A AC SOLUTI 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 SOLUTI garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 30 (trinta) dias úteis após a autorização de funcionamento da AC em questão.

4.3 Emissão de Certificado

4.3.1 Ações da AC durante a emissão de um certificado

A emissão de um certificado pela AC SOLUTI é feita em cerimônia específica, com a presença de representante da AC SOLUTI, da AC credenciada e de convidados, na qual são registrados todos os procedimentos executados.

A emissão dos certificados das ACs de nível imediatamente subsequente é feita em equipamentos da AC SOLUTI que operam off-line.

A emissão de certificados pela AC SOLUTI para as ACs de nível imediatamente subsequente estará condicionada ao credenciamento por parte do ITI, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA

ICP-BRASIL [6].

4.3.1.1

O certificado é considerado válido a partir do momento em que é emitido.

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

Após a emissão do certificado, a AC SOLUTI encaminha mensagem eletrônica de confirmação.
.

4.4 Aceitação de Certificado

4.4.1 Conduta sobre a aceitação do certificado

4.4.1.1

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

A verificação dos dados do certificado deve ser realizada pela AC titular no prazo de 2 (dois) dias úteis, contados a partir do seu recebimento, após o qual o certificado será considerado aceito.

Ao aceitar o certificado, a AC titular:

a) concorda com as responsabilidades, obrigações e deveres a ela impostas pelo Termo de Acordo e esta DPC;

b) garante que com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado; e

c) afirma que todas as informações de certificado fornecidas durante o processo de credenciamento são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

A não aceitação de um certificado no prazo previsto implica a realização de nova cerimônia, onde é feita a revogação do certificado não aceito e a emissão de novo certificado.

4.4.1.2

A aceitação do certificado se dá no momento em que os dados constantes do mesmo são verificados pela AC ou na primeira utilização da chave privada correspondente.

4.4.1.3

No momento da entrega do certificado, durante a cerimônia de sua emissão pela AC Raiz, a AC atesta o seu recebimento por meio de assinatura de Termo de Cerimônia de Emissão de Certificado, Termo de Cerimônia de Entrega de Chave Pública e Termo de Acordo por seu representante legal.

4.4.2 Publicação do certificado pela AC

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

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

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

4.5 Usabilidade do par de chaves e do certificado

A AC subsequente titular de certificado emitido pela AC SOLUTI opera de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementam, 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 utiliza a sua chave privada e garante proteção da sua chave conforme o previsto na sua própria DPC.

4.5.1.2 Obrigações do Titular do Certificado

As obrigações do titular de certificado emitido de acordo com esta DPC AC SOLUTI são as abaixo relacionadas:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;

b) garantir a proteção e o sigilo de suas chaves privadas, 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 AC SOLUTI e por outros documentos aplicáveis da ICP-Brasil; e

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

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 o item 3.3 desta DPC.

4.6.1 Circunstâncias para renovação de certificados

Em acordo com o item 3.3 desta DPC.

4.6.2 Quem pode solicitar a renovação

Em acordo com o item 3.3 desta DPC.

4.6.3 Processamento de requisição para renovação de certificados

Em acordo com o item 3.3 desta DPC.

4.6.4 Notificação para nova emissão de certificado para o titular

Em acordo com o item 3.3 desta DPC.

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com o 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 o item 4.3 desta DPC.

4.7 Nova chave de certificado (Re-key)

4.7.1 Circunstâncias para nova chave de certificado

Não se aplica.

4.7.2 Quem pode requisitar a certificação de uma nova chave pública

Não se aplica.

4.7.3 Processamento de requisição de novas chaves de certificado

Não se aplica.

4.7.4 Notificação de emissão de novo certificado para o titular

Não se aplica.

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica.

4.7.6 Publicação de uma nova chave certificada pela AC

Não se aplica.

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

Não se aplica.

4.8 Modificação de certificado

Não se aplica.

4.8.1 Circunstâncias para modificação de certificado

Não se aplica.

4.8.2 Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3 Processamento de requisição de modificação de certificado

Não se aplica.

4.8.4 Notificação de emissão de novo certificado para o titular

Não se aplica.

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica.

4.8.6 Publicação de uma modificação de certificado pela AC

Não se aplica.

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

Não se aplica.

4.9 Suspensão e Revogação de Certificado

4.9.1 Circunstâncias para revogação

4.9.1.1

Um certificado de AC de nível imediatamente subsequente ao da AC SOLUTI pode ser revogado a qualquer instante, por solicitação da própria AC titular do certificado ou por decisão motivada da AC SOLUTI, resguardados os princípios do contraditório e da ampla defesa.

4.9.1.2

Um certificado é revogado obrigatoriamente pelos seguintes motivos:

a) quando constatada emissão imprópria ou defeituosa do mesmo;

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

c) no caso de dissolução da AC titular do certificado; ou

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

4.9.1.3

Em relação à revogação, deve ainda ser observado que:

a) A AC SOLUTI revogará, no prazo definido no item 4.9.3.3, o certificado da AC subsequente que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil; e

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

4.9.1.4

A AC SOLUTI garante que verifica a validade do certificado, na respectiva LCR, antes de ser utilizado.

4.9.1.4.1

Não se aplica.

4.9.1.4.2

Não se aplica.

4.9.1.5

A autenticidade da LCR, é confirmada por meios das verificações da assinatura da AC SOLUTI e do período de validade da LCR.

4.9.2 Quem pode solicitar revogação

A solicitação para a revogação de um certificado somente poderá ser feita:

a) por determinação da AC SOLUTI nos casos previstos no item 4.9.1.1;

b) por solicitação da AC titular do certificado;

c) por determinação judicial; ou

d) por determinação do CG da ICP-Brasil ou da AC Raiz.

4.9.3 Procedimento para solicitação de revogação

4.9.3.1

A solicitação de revogação do certificado à AC SOLUTI deve ser realizada por meio de documento formal assinado digitalmente por seu representante legal.

4.9.3.2

Fica estabelecido como diretrizes gerais que:

a) o solicitante da revogação de um certificado deve ser identificado;

b) as solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;

c) as justificativas para a revogação de um certificado são documentadas; e

d) o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.9.3.3

O processo de revogação de um certificado de AC é precedido, quando for o caso, do recebimento pela AC SOLUTI da solicitação de revogação e termina quando uma nova LCR, contendo o certificado revogado, é emitida e publicada pela AC SOLUTI. Concluído esse processo, a AC SOLUTI informa à AC afetada a revogação do certificado.

4.9.3.4

O prazo para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação, é de 24 (vinte e quatro) horas.

4.9.3.5

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

4.9.3.6

Não se aplica.

4.9.4 Prazo para solicitação de revogação

4.9.4.1

A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.1.

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 SOLUTI processa a revogação de forma imediata após a análise do pedido.

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

Antes de confiar em um certificado, a parte confiável confirma a validade de cada certificado na cadeia de certificação de acordo com os padrões IETF PKIX, incluindo a verificação da validade do certificado, encadeamento do nome do emissor e titular, restrições de uso de chaves e de politicas 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

A LCR da AC SOLUTI é atualizada a cada 30 (trinta) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC SOLUTI emite nova LCR no prazo previsto no item 4.9.3 e notifica todas as ACs de nível imediatamente subsequente ao seu.

4.9.7.2

Não se aplica.

4.9.7.3

A LCR da AC SOLUTI é atualizada, no máximo, a cada 90 (noventa) dias.

4.9.7.4

Não se aplica.

4.9.7.5

Não se aplica.

4.9.8 Latência máxima para a LCR

A AC SOLUTI publica sua LCR em seu repositório é dentro de um dia útil após sua geração.

4.9.9 Disponibilidade para revogação/verificação de status on-line

Não serão aceitos pedidos de revogação on-line ao sistema de certificação da AC SOLUTI. A única forma de consulta on-line de status de certificado é a realizada por meio da LCR.

4.9.10 Requisitos para verificação de revogação on-line

Não se aplica.

4.9.11 Outras formas disponíveis para divulgação de revogação

4.9.11.1.1

Não se aplica.

4.9.11.1.2

Não se aplica.

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.12.1

Quando houver comprometimento ou suspeita de comprometimento da chave privada, a AC subsequente deverá comunicar imediatamente a AC SOLUTI.

4.9.12.2

A comunicação a AC SOLUTI deverá ser através dos dados de contato informados no item 1.5.2.

4.9.13 Circunstâncias para suspensão

Não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados de AC Subsequente.

4.9.14 Quem pode solicitar suspensão

A AC, aprovados pelo Comitê Gestor.

4.9.15 Procedimento para solicitação de suspensão

A solicitação de suspensão deverá ser realizada formalmente por entidades competentes definidos no item 4.9.14 através dos dados de contato informados no item 1.5.2.

4.9.16 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC SOLUTI.

4.10 Serviços de status de certificado

4.10.1 Características operacionais

A AC SOLUTI fornece 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

Caso seja necessária a extinção dos serviços, a AC SOLUTI executará os procedimentos aplicáveis descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

4.11.2

Os procedimentos para notificação das ACs subsequentes e para a transferência da guarda de dados e registros de arquivos incluem:

a) notificação para o e-mail da AC Subsequente;

b) transferência progressiva do serviço e dos registros operacionais para um sucessor que tenha os mesmos requisitos de segurança da entidade extinta;

c) preservação de quaisquer registros não transferidos a um sucessor;

d) as chaves públicas dos certificados emitidos pela AC dissolvida serão armazenadas por outra AC após aprovação da AC Raiz;

e) quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC SOLUTI;

f) a AC SOLUTI, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda

das respectivas chaves públicas;

g) caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

4.12 Custódia e recuperação de chave

4.12.1 Política e práticas de custódia e recuperação de chave

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

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

A AC SOLUTI não realiza encapsulamento e recuperação de chave de sessão na AC.

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

O processo de gerenciamento de certificados da AC SOLUTI inclui os seguintes controles:

a) Segurança física e controles ambientais;

b) Controles de integridade dos sistemas, incluindo gerenciamento de configuração, manutenção de integridade de código confiável e detecção e prevenção de incidentes;

c) Segurança de rede e gerenciamento de firewalls, incluindo restrições de porta e filtragem de endereços IP;

d) Gerenciamento de usuários, segregação de funções, capacitação, conscientização e treinamento; e

e) Controles de acesso lógico, com registro de atividades e de inatividade, a fim de fornecer responsabilidades individuais.

5.1 Controles Físicos

A AC SOLUTI mantém políticas de segurança para os ativos e sistemas usados nos processos de gerenciamento de certificados. Essas políticas cobrem controles de acesso físico, proteção contra desastres naturais, segurança contra incêndios, falhas de suporte (como energia, telecomunicações, links de dados, entre outros), colapso de estrutura, inundação, proteção contra roubo, acessos indevidos e recuperação de desastres. Estes controles devem ser implementados para evitar perda, danos ou comprometimento de ativos, interrupção das atividades do negócio relacionadas aos processos de gerenciamento de certificados, roubo de informações e comprometimento das instalações de processamento de informações.

5.1.1 Construção e localização das instalações de AC

5.1.1.1

A localização e o sistema de certificação utilizado para a operação da AC SOLUTI não são publicamente identificados, nem há identificação pública externa das instalações. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2

A AC SOLUTI implementa os seguintes controles de segurança física relevantes para sua operação**:**

a) máquinas de ar-condicionado redundantes;

b) grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, retificadores e estabilizadores;

c) sistemas de telecomunicações redundantes;

d) sistema de aterramento e de proteção contra descargas atmosféricas;

e) sistema de detecção e prevenção a incêndio;

f) sistema de detecção e prevenção de umidade;

g) controle de acesso predial; e

h) iluminação de emergência.

5.1.2 Acesso físico

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

5.1.2.1 Níveis de Acesso

5.1.2.1.1

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

5.1.2.1.2 Nível 1

O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC SOLUTI. 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 SOLUTI transitam apenas devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC SOLUTI é executado nesse nível.

5.1.2.1.3

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

5.1.2.1.4 Nível 2

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

5.1.2.1.5 Nível 3

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

5.1.2.1.6

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

5.1.2.1.7

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

5.1.2.1.8 Nível 4

O quarto nível – ou nível 4 – é interno ao terceiro nível, é aquele no qual ocorrem atividades

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

5.1.2.1.9

No quarto nível todas as paredes, o piso e o teto são revestidos de aço e concreto. 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 da área de quarto nível. Adicionalmente, esse ambiente de nível 4 – que constituem a chamada sala cofre – possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10

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

5.1.2.1.11

A AC SOLUTI possui um único ambiente de nível 4 por instalação principal e de contingência.

5.1.2.1.12 Nível 5

O quinto nível – ou nível 5 – é interno aos ambientes de nível 4 e compreende o cofre. 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 obedece às seguintes especificações mínimas:

a) é feito em aço ou material de resistência equivalente; e

b) possui tranca com chave.

5.1.2.1.14 Nível 6

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

5.1.2.2 Sistema físico 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 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 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 não há vidros separando os níveis de acesso.

5.1.2.2.4

No ambiente de quarto nível, um alarme de detecção de movimentos permanece ativo

enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar de ser satisfeito, ocorre a reativação automática dos sensores de presença.

5.1.2.2.5

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

5.1.2.2.6

O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por 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 foram implantados para garantir a segurança do pessoal e dos equipamentos da AC SOLUTI em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.2.4.2

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

5.1.3 Energia e ar-condicionado

5.1.3.1

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

5.1.3.2

Todos os cabos elétricos são protegidos por tubulações e dutos apropriados.

5.1.3.3

São utilizadas tubulações, dutos, calhas, quadros e caixas de passagem, de distribuição e de terminação, projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos para os cabos de energia separados dos dutos para cabos de telefonia e de 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 aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. No ambiente de nível 4, o sistema de climatização é independente e tolerante a falhas.

5.1.3.8

A temperatura do ambiente atendido pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9

O sistema de ar-condicionado do ambiente 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 SOLUTI é garantida por meio de:

a) geradores de porte compatível;

b) geradores de reserva;

c) sistemas de no-breaks redundantes;

d) sistemas redundantes de ar-condicionado.

5.1.4 Exposição à água

A estrutura 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 da área de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes 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 SOLUTI não é permitido fumar ou portar objetos que produzam fogo, ou faísca.

5.1.5.3

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

5.1.5.4

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

5.1.6 Armazenamento de mídia

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

5.1.7 Destruição de lixo

5.1.7.1

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

5.1.7.2

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

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

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

5.2 Controles Procedimentais

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

5.2.1 Perfis qualificados

5.2.1.1

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

5.2.1.2

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

5.2.1.3

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

5.2.1.3.1

Não se aplica.

5.2.1.4

Quando um empregado se desliga da AC SOLUTI, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da AC, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC 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 SOLUTI, 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 SOLUTI necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da AC SOLUTI. As demais tarefas da AC SOLUTI podem ser executadas por um único operador.

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1

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

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

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

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

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

5.2.3.2

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

a) diretamente atribuídos a um único operador, funcionário da AC SOLUTI devidamente qualificado;

b) não são compartilhados; e

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

5.2.3.3

A AC SOLUTI implementa um padrão de utilização de “senhas fortes”, definido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com procedimentos de validação dessas senhas.

5.2.4 Funções que requerem separação de deveres

A AC SOLUTI impõe 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 SOLUTI 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 AC SOLUTI;

c) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e

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

5.3.2 Procedimentos de verificação de antecedentes

5.3.2.1

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

a) Verificação de antecedentes criminais;

b) Verificação de situação de crédito;

c) Verificação de histórico de empregos anteriores; e

d) Comprovação de escolaridade e de residência.

5.3.2.2

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

5.3.3 Requisitos de treinamento

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

a) Princípios e mecanismos de segurança da AC SOLUTI;

b) Sistema de certificação em uso na AC SOLUTI;

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

d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.2.2; e

e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC SOLUTI envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC SOLUTI. Treinamentos de reciclagem são realizados pela AC SOLUTI sempre que necessário.

5.3.5 Frequência e sequência de rodízios de cargos

A AC SOLUTI não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

5.3.6.1

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

5.3.6.2

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

a) relato da ocorrência com “modus operandi”;

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 SOLUTI encaminhará suas conclusões à AC Raiz.

5.3.6.4

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

a) advertência;

b) suspensão por prazo determinado; ou

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

5.3.7 Requisitos para contratação de pessoal

O pessoal da AC SOLUTI, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.3.8 Documentação fornecida ao pessoal

5.3.8.1

A AC SOLUTI disponibiliza para todo o seu pessoal:

a) Esta DPC;

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

c) A Política de Segurança da AC SOLUTI;

d) Documentação operacional relativa às suas atividades;

e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2

Toda a documentação fornecida ao pessoal é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela AC SOLUTI.

5.4 Procedimentos de Log de Auditoria

Nos itens seguintes estão descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC SOLUTI, responsável pela DPC com o objetivo de manter um ambiente seguro.

5.4.1 Tipos de eventos registrados

5.4.1.1

É registrado em arquivos de auditoria todos os eventos relacionados à segurança do sistema de certificação da AC SOLUTI. Entre outros, os seguintes eventos estão 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 SOLUTI;

c) mudanças na configuração da AC SOLUTI ou nas suas chaves;

d) mudanças nas políticas de criação de certificados;

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

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

g) geração de chaves próprias da AC SOLUTI ou de chaves de Titulares de Certificados;

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;

l) operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1

Não se aplica.

5.4.1.2

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

a) registros de acessos físicos;

b) manutenção e mudanças na configuração de seus sistemas;

c) mudanças de pessoal e de perfis qualificados;

d) relatórios de discrepância e comprometimento; e

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

5.4.1.3

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

5.4.1.4

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

5.4.1.5

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

5.4.1.6

A AC SOLUTI, responsável por esta DPC, registrará eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

a) os agentes de registro que realizaram as operações;

b) data e hora das operações;

c) a associação entre os agentes que realizaram a validação e aprovação e o certificado gerado; e

d) a assinatura digital do executante.

5.4.1.7

A AC SOLUTI define que o local de arquivamento das cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados e dos termos de titularidade e responsabilidade, é o mesmo das instalações técnicas da AC SOLUTI.

5.4.2 Frequência de auditoria de registros

Os registros de auditoria da AC SOLUTI serão analisados semanalmente pelo pessoal operacional da AC SOLUTI.

Todos os eventos significativos serão explicados em relatório de auditoria de registros. Tal análise envolverá uma inspeção breve de todos os registros, verificando-se que não foram alterados, em seguida proceder-se-á a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise serão documentadas.

5.4.3 Período de retenção para registros de auditoria

A AC SOLUTI manterá nas instalações da AC SOLUTI os seus registros de auditoria pelo prazo de 2 (dois) meses e, subsequentemente, fará o armazenamento da maneira descrita no item 5.5.

5.4.4 Proteção de registros de auditoria

5.4.4.1

Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.4.4.2

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

conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.4.4.3

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

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

A AC SOLUTI executa procedimentos de backup, de todo o sistema de certificação (SISTEMA OPERACIONAL + APLICAÇÃO DE AC + BANCO DE DADOS) de duas formas:

a) diariamente: cópia de segurança; e

b) semanalmente: cópia armazenada para processos de auditoria.

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

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

5.4.7 Notificação de agentes causadores de eventos

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

5.4.8 Avaliações de vulnerabilidade

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

5.5 Arquivamento de Registros

5.5.1 Tipos de registros arquivados

A AC SOLUTI registra e arquiva as seguintes informações a respeito de:

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 SOLUTI;

g) informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são (de):

a) PERMANENTEMENTE: as LCR referentes a certificados de assinatura digital, para fins de consulta histórica;

b) SETE ANOS: para as cópias dos documentos de identificação apresentados no momento da solicitação e da revogação de certificados, os termos de titularidade e responsabilidade, a contar da data da expiração ou revogação do certificado;

c) SETE ANOS: as demais informações, inclusive arquivos de auditoria.

5.5.3 Proteção de arquivo

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

5.5.4 Procedimentos de cópia de arquivo

5.5.4.1

Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC SOLUTI, e recebem o mesmo tipo de proteção utilizada por ela no arquivo principal.

5.5.4.2

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

5.5.4.3

É feita a verificação da integridade dessas cópias de segurança, periodicamente a cada 6 (seis) meses.

5.5.5 Requisitos para datação de registros

Os servidores da AC SOLUTI são sincronizados com a hora UTC fornecida pela AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em UTC, inclusive os certificados emitidos por esses equipamentos. No caso dos registros feitos manualmente, se não especificado o fuso horário, estes contêm a Hora Oficial do Brasil.

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

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

5.5.7 Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC SOLUTI, 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

A AC de nível imediatamente subsequente ao da AC SOLUTI deverá iniciar, até 3 (três) meses antes da data de expiração do seu certificado, o processo de geração de novo par de chaves e de emissão de novo certificado. Revogado ou expirado o certificado de uma AC de nível imediatamente subsequente ao seu, a AC SOLUTI remove imediatamente esse certificado do diretório e de sua página web, mantendo-o armazenado permanentemente para efeito de consulta histórica.

As chaves privadas usadas para assinar os certificados das ACs subsequentes devem ser mantidas até o momento em que todos os certificados das ACs tenham expirado.

5.6.2

A solicitação de renovação do certificado deverá ser feita pelo responsável pela AC subsequente solicitando por meio eletrônico, assinada digitalmente.

5.7 Comprometimento e Recuperação de Desastre

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

5.7.1 Procedimentos gerenciamento de incidente e comprometimento

5.7.1.1

A AC SOLUTI possui um Plano de Continuidade de Negócios (PCN), de acesso restrito, testado anualmente, garantindo assim a continuidade dos seus serviços críticos. A AC SOLUTI possui também 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

A AC SOLUTI possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

a) é feita a identificação de todos os elementos corrompidos;

b) o instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;

c) é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um backup de segurança até a revogação do certificado da AC SOLUTI.

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado de entidade é revogado

A AC SOLUTI possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que o certificado da AC SOLUTI é revogado, e que podem ser resumidas da seguinte forma:

a) A AC SOLUTI, a AC Raiz e ACs subsequentes serão notificadas por comunicação segura;

b) A AC SOLUTI revoga os certificados por ela emitidos;

c) A AC SOLUTI solicita um novo certificado à AC Raiz:

d) Iniciam-se os procedimentos para emissão dos novos certificados de ACs subsequentes.

5.7.3.2 Chave de entidade é comprometida

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

5.7.4 Capacidade de continuidade de negócio após desastre

A AC SOLUTI possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza.

O propósito deste plano é restabelecer as principais operações da AC SOLUTI quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc. O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC SOLUTI faz parte.

Isto significa que o plano tem como meta primária, restabelecer a AC SOLUTI para tornar acessível os registros lógicos mantidos dentro do software. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo uma ordem de prioridade.

5.8 Extinção da AC

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

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes estão definidas as medidas de segurança implementadas pela AC SOLUTI, responsável pela DPC para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados..

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 da AC SOLUTI é gerado pela própria AC SOLUTI, em módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9], após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2

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

6.1.1.3

Os algoritmos e dispositivos criptográficos a serem utilizados para as chaves criptográficas da AC Raiz estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [9].

6.1.1.4

O processo de geração do par de chaves da AC SOLUTI é feito por hardware com NSH-2, homologado no INMETRO.

6.1.1.5

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

6.1.1.6

A chave privada da AC SOLUTI é gerada, armazenada e utilizada apenas em hardware criptográfico homologado na ICP-Brasil ou certificado pelo INMETRO. O acesso a esse hardware é controlado por meio de chave criptográfica de ativação, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9];

6.1.2 Entrega da chave privada à entidade

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

6.1.3 Entrega da chave pública para emissor de certificado

6.1.3.1

A AC SOLUTI entregará à AC Raiz cópia de sua chave pública, em formato PKCS#10.

6.1.3.2

O representante legal da AC Subsequente entregará a chave pública da AC, em cerimônia específica, em data e hora previamente estabelecidas pela AC SOLUTI. Os detalhes da cerimônia serão registrados para fins de auditoria.

6.1.4 Entrega de chave pública da AC às terceiras partes

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

a) no momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9];

b) diretório;

c) página web da AC SOLUTI (http://ccd.acsoluti.com.br/); e

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

6.1.5 Tamanhos de chave

6.1.5.1

Esta DPC define os tamanhos das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.1.5.2

O tamanho mínimo das chaves criptográficas associadas ao certificado de AC Subsequente é de RSA 4096 bits (V2 e V5) e ECDSA 512 bits (V4), conforme 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 da AC SOLUTI seguem o padrão de Homologação da ICP-Brasil, conforme definido 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

A chave privada de AC Subsequente pode ser utilizada apenas para assinatura dos certificados por ela emitidos e para assinatura de sua LCR.

6.1.7.2

A chave privada da AC SOLUTI 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 chave privada da AC SOLUTI é gerada, armazenada e utilizada apenas em hardware criptográfico homologado na ICP-Brasil ou certificado pelo INMETRO. O acesso a esse hardware é controlado por meio de chave criptográfica de ativação.

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1

O módulo criptográfico de geração de chaves assimétricas da AC SOLUTI utiliza hardware criptográfico, classificado como FIPS 140-2 nível 3. Este padrão está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.2.1.2

O módulo criptográfico de geração de chaves assimétricas das ACs subsequentes utiliza hardware criptográfico, classificado como FIPS 140-2 nível 3. Este padrão está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.2.2 Controle “n de m” para chave privada

6.2.2.1

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

6.2.2.2

É exigido a presença no mínimo de 2 (dois) detentores da chave de ativação (“n”) de um grupo de 5 (cinco) (“m”) para a ativação da chave da AC SOLUTI.

6.2.3 Custódia (escrow) de chave privada

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

6.2.4 Cópia de segurança de chave privada

6.2.4.1

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

6.2.4.2

A AC SOLUTI mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave e aprovado pelo CG da ICP-Brasil, e mantida pelo prazo de validade do certificado correspondente.

6.2.4.3

A AC SOLUTI não mantém cópia de segurança da chave privada de Titular de Certificado de assinatura digital por ela emitido.

6.2.4.4

Em qualquer caso, a cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1

As chaves privadas dos titulares de certificados emitidos pela AC SOLUTI não são arquivadas.

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 SOLUTI 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 da chave privada da AC SOLUTI é implementada por meio de token criptográfico, protegido com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores da AC SOLUTI, seus sócios, diretores ou funcionários designados para essa função. As senhas utilizadas obedecem à política de senhas estabelecida pela AC SOLUTI.

6.2.9 Método de desativação de chave privada

A chave privada da AC SOLUTI, armazenada em módulo criptográfico, é desativada quando não mais é necessária através de mecanismo disponibilizado pelo software de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este

procedimento é implementado por meio de tokens criptográficos, protegidos com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC SOLUTI. As senhas utilizadas obedecem à política de senhas estabelecida pela AC SOLUTI.

6.2.10 Método de destruição de chave privada

Quando a chave privada da AC SOLUTI for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Todas as cópias de segurança da chave privada da AC SOLUTI e os tokens criptográficos dos custodiantes serão eliminados. Os agentes autorizados para realizar estas operações são os administradores e os custodiantes das chaves de ativação da AC SOLUTI.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A AC SOLUTI armazena as chaves públicas da própria AC SOLUTI e das ACs de nível imediatamente subsequente ao seu, bem como as LCRs emitidas, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

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

6.3.2.1

A chave privada da AC SOLUTI e das ACs de nível imediatamente subsequente ao seu, são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC SOLUTI pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos certificados correspondentes.

6.3.2.2

Não se aplica.

6.3.2.3

Não se aplica.

6.3.2.4

O período máximo de validade admitido para o certificado da AC SOLUTI é limitada à validade do certificado da AC que o emitiu.

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 da chave privada da AC SOLUTI são únicos e aleatórios.

6.4.1.2

Não se aplica.

6.4.2 Proteção dos dados de ativação.

6.4.2.1

Os dados de ativação da AC SOLUTI são protegidos contra o uso não autorizado, por tokens criptográficos individuais com senha e pelo armazenamento em ambiente de nível 6 de segurança.

6.4.2.2

Os dados de ativação da chave privada da entidade titular do certificado são protegidos contra uso não autorizado.

6.4.3 Outros aspectos dos dados de ativação

Todos os aspectos acerca dos dados de ativação já foram tratados nos itens anteriores.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.1.1

A AC SOLUTI garante que a geração de seu par de chaves é realizada em ambiente off-line, para impedir o acesso remoto não autorizado durante o processo.

6.5.1.2

Os requisitos gerais de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC SOLUTI estão descritos nesta DPC.

6.5.1.3

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

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

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

c) acesso restrito aos bancos de dados da AC SOLUTI;

d) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

e) geração e armazenamento de registros de auditoria da AC SOLUTI;

f) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;

g) mecanismos para cópias de segurança (backup).

6.5.1.4

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

6.5.1.5

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

6.5.1.6

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

6.5.2 Classificação da segurança computacional

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

6.5.3 Controles de Segurança para as Autoridades de Registro

6.5.3.1

Os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pela ARs para os processos de validação e aprovação de certificados são os estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA ARs DA ICP-BRASIL[1].

6.5.3.2

Nas PSs adotadas foram atendidos os requisitos mínimos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA ARs DA ICP-BRASIL[1].

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistema

6.6.1.1

A AC SOLUTI adota o Sistema de Certificação Digital da AC SOLUTI, desenvolvido em código aberto. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente do CCD avalia e decide quando será a implementação no ambiente de produção.

6.6.1.2

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

6.6.2 Controles de gerenciamento de segurança

6.6.2.1

As ferramentas e os procedimentos empregados pela AC SOLUTI para garantir que os seus sistemas implementem os níveis configurados de segurança são a administração de segurança de sistema que é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

6.6.2.2

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

a) instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;

b) implantação ou modificação de Autoridades Certificadoras com customizações ao nível de certificados, páginas web, scripts, etc.;

c) implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos;

d) instalação de novos serviços na plataforma de processamento.

6.6.3 Controles de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na Geração da LCR

Todas as LCRs geradas pela AC SOLUTI, antes de publicadas, 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 SOLUTI, incluindo firewalls e recursos similares.

6.7.1.2

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

6.7.1.3

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

6.7.1.4

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

6.7.1.5

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

6.7.2 Firewall

6.7.2.1

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

6.7.2.2

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

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1

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

6.7.3.2

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

6.7.3.3

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

6.7.4 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, firewalls ou IDS – são registradas em arquivos para posterior análise, que poderá ser automatizada. O exame dos arquivos de registro é realizado diariamente 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 SOLUTI 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

Todos os certificados emitidos pela AC SOLUTI implementa a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado

Os certificados emitidos pela AC SOLUTI apresentam obrigatoriamente as seguintes extensões:

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

b) **Subject Key Identifier**, não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado (AC Subsequente);

c) **Key Usage**, crítica: somente os bits **keyCertSign** e **CRLSign** estão ativados;

d) **Certificate Policies**, não crítica:

1. o campo **policyIdentifier** deve conter os OIDs das PCs que a AC Subsequente, titular do certificado, implementa;
2. o campo **policyQualifiers** deve conter o endereço Web da DPC da AC SOLUTI: **https://ccd.acsoluti.com.br/docs/dpc-ac-soluti.pdf**;

e) **basicConstraints**, crítica: contém o campo **CA=True**; e

f) **CRL Distribution Points**, não crítica: contém o endereço Web onde se obtém a LCR da AC SOLUTI:

1. Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V2:
   i. **http://ccd.acsoluti.com.br/lcr/ac-soluti-v1.crl**
   ii. **http://ccd2.acsoluti.com.br/lcr/ac-soluti-v1.crl**
   iii. **http://repositorio.icpbrasil.gov.br/lcr/ACSOLUTI/ac-soluti-v1.crl**
2. Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V5:
   i. **http://ccd.acsoluti.com.br/lcr/ac-soluti-v5.crl**
   ii. **http://ccd2.acsoluti.com.br/lcr/ac-soluti-v5.crl**

7.1.3 Identificadores de algoritmo

Os certificados de AC deverão ser assinados com o uso do algoritmo

sha512WithRSAEncryption, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

7.1.4 Formatos de nome

O nome da AC titular de certificado, constante do campo “Subject”, deverá adotar o “Distinguished Name” (DN) do padrão ITU X.500/ISO 9594, como exemplo, da seguinte forma:

a) Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V2:

C = BR
O = ICP-Brasil
OU = Autoridade Certificadora Raiz Brasileira v2
OU = AC SOLUTI
CN = <nome da AC Subsequente>

b) Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V5:

C = BR
O = ICP-Brasil
OU = AC SOLUTI v5
CN = <nome da AC Subsequente>

7.1.5 Restrições de nome

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

a) Não são admitidos sinais de acentuação, trema ou cedilhas;

i. caracteres acentuados devem ser substituídos por seu correspondente sem acento;

ii. o cedilha deve ser substituído pelo caractere 'c';

b) Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

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

7.1.6 OID (Object Identifier) da DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil após a conclusão do processo de credenciamento, é 2.16.76.1.1.46.

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” deverá conter o endereço web (URL) da DPC da AC SOLUTI: **https://ccd.acsoluti.com.br/docs/dpc-ac-soluti.pdf**.

7.1.9 Semântica de processamento para as extensões criticas 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 SOLUTI implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 Extensões de LCR e de suas entradas

7.2.2.1

A LCR emitida pela AC Raiz implementa as seguintes extensões previstas na RFC 5280.

7.2.2.2

A AC SOLUTI adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) “Authority Key Identifier”, não crítica: contém o resumo SHA-1 da chave pública da AC SOLUTI;

b) “CRL Number”, não crítica: contém número sequencial para cada LCR emitida.

7.3 Perfil de OCSP

7.3.1 Número(s) de versão

Não se aplica.

7.3.2 Extensões de OCSP

Não se aplica.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 Frequência e circunstâncias das avaliações

A AC SOLUTI entidade integrante da ICP-Brasil sofre 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, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2].

8.2.2

As auditorias da AC SOLUTI 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

A auditoria da AC SOLUTI é realizada pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizada, 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 da AC SOLUTI estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil e com princípios e critérios definidos pelo WebTrust.

8.4.2

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

8.4.3

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

8.5 Ações tomadas como resultado de uma deficiência

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

8.6 Comunicação dos resultados

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

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 Tarifas

9.1.1 Tarifas de emissão e renovação de certificados

As tarifas referentes aos serviços de emissão e renovação de certificados serão definidas internamente pela AC SOLUTI.

Está facultado à AC SOLUTI usar livremente de todos os meios idôneos e legais disponíveis para parear suas tarifas à concorrência de mercado.

9.1.2 Tarifas de acesso ao certificado

Não há tarifa que incida sobre este serviço.

9.1.3 Tarifas de revogação ou de acesso à informação de status

As tarifas serão definidas internamente pela AC SOLUTI.

9.1.4 Tarifas para outros serviços

As tarifas serão definidas internamente pela AC SOLUTI.

9.1.5 Política de reembolso

Variável, definida internamente pela AC SOLUTI.

9.2 Responsabilidade Financeira

A responsabilidade da AC SOLUTI é verificada conforme previsto na legislação brasileira.

9.2.1 Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2 Outros ativos

Conforme regramento desta DPC.

9.2.3 Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

9.3.1.1

Todas as informações coletadas, geradas, transmitidas e mantidas pela AC SOLUTI são consideradas sigilosas.

9.3.1.2

Como princípio geral, nenhum documento, informação ou registro fornecido à AC deverá ser divulgado.

9.3.2 Informações fora do escopo de informações confidenciais

Os seguintes documentos da AC SOLUTI são considerados documentos não sigilosos:

a) os certificados e as LCR emitidos;

b) informações corporativas ou pessoais que façam parte de certificados, ou de diretórios públicos;

c) a DPC da AC;

d) versões públicas de Políticas de Segurança;

e) a conclusão dos relatórios de auditoria; e

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

9.3.2.1

Certificados, LCR, e informações corporativas ou pessoais que necessariamente façam parte deles, ou de diretórios público são considerados informações não confidenciais.

9.3.2.2

Os seguintes documentos da AC SOLUTI também são considerados não confidenciais:

a) qualquer DPC;

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

c) a conclusão dos relatórios da auditoria.

9.3.2.3

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

9.3.3 Responsabilidade em proteger a informação confidencial

9.3.3.1

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

9.3.3.2

A chave privada de assinatura digital da AC SOLUTI, é gerada e mantida pela própria AC SOLUTI, que é a responsável pelo seu sigilo. A divulgação ou utilização da chave privada de assinatura da AC SOLUTI é de sua inteira responsabilidade.

9.3.3.3

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

9.3.3.4

Não se aplica.

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

A AC SOLUTI assegura a proteção dos 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 SOLUTI é considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma de legislação aplicável.

9.4.3 Informações não consideradas privadas

Informações sobre revogação de usuários finais são fornecidos na LCR da AC SOLUTI.

9.4.4 Responsabilidade para proteger a informação privada

A AC SOLUTI e AR são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5 Aviso e consentimento para usar informações privadas

Qualquer liberação de informação pela AC SOLUTI a terceiros somente será permitida mediante autorização formal do titular do certificado. As formas de autorização são as seguintes:

a) por meio eletrônico, contendo assinatura válida garantida por certificado do titular, reconhecido pela AC SOLUTI; 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 SOLUTI, será fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.

As informações privadas ou confidenciais sob a aguarda da AC SOLUTI, 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 de dados perante terceiros.

9.4.7 Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8 Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro, sob a guarda da AC SOLUTI, será fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizado para fazê-lo e esteja corretamente identificada.

9.5 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, e todos os documentos gerados para a AC SOLUTI (eletrônicos ou não), de acordo com a legislação vigente, pertencem e continuarão sendo propriedade da Soluti – Soluções em Negócios Inteligentes.

9.6 Declarações e Garantias

9.6.1 Declarações e Garantias da AC

A AC SOLUTI declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

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

9.6.1.2 Precisão da informação

A AC SOLUTI 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 imediatamente subsequentes na forma de sua DPC, PCs e normas complementares.

9.6.1.3 Identificação do requerente

A AC SOLUTI implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC SOLUTI, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs imediatamente subsequentes na forma de sua DPC, PCs e normal complementares.

9.6.1.4 Consentimento dos titulares

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

9.6.1.5 Serviço

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

9.6.1.6 Revogação

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

normas da ICP-Brasil e nos documentos *Baseline Requirements*.

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

9.6.3.2

A AC SOLUTI informará 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; e

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

9.6.4.2

O certificado da AC SOLUTI é considerado válido quando:

i. tiver sido emitido pela AC Raiz;

ii. não constar como revogado pela AC Raiz;

iii. não estiver expirado;

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

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 SOLUTI 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 SOLUTI 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

A DPC da AC SOLUTI 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

A DPC da AC SOLUTI vigorá por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.3 Efeitos de rescisão e sobrevivência

Os atos praticados na vigência da DPC da AC SOLUTI são válidos e eficazes para todos os fins de direitos produzindo efeitos mesmo após a sua revogação ou substituição.

9.11 Avisos individuais e comunicações com os participantes

Todas as solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas nessa DPC serão realizadas por iniciativa da AC SOLUTI por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil via e-mail, assinado digitalmente, oficial das pessoas, dos órgãos e instituições envolvidos, ficando sob o crivo da AC SOLUTI a adoção de via postal, quando conveniente ou o meio se mostrar mais adequado.

9.12 Alterações

9.12.1 Procedimento para emendas

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

9.12.2 Mecanismo de notificação e períodos

A AC SOLUTI publica esta DPC, em sua página web acessível pela URL http://ccd.acsoluti.com.br/docs/dpc-ac-soluti.pdf. Sempre que esta DPC for atualizada será alterado o arquivo disponibilizado na web.

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 da AC SOLUTI serão solucionados de acordo com a legislação vigente.

9.13.2

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

9.14 Lei aplicável

Esta DPC da AC SOLUTI 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 SOLUTI 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 da AC SOLUTI representa as obrigações e deveres aplicáveis à AC SOLUTI e AR.

Havendo conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2 Cessão

Os direitos e obrigações previstos nesta DPC da AC SOLUTI 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 da DPC da AC SOLUTI 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
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRATICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[12]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DE TEMPO	DOC-ICP-12
[13]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

10.2

Os documentos abaixo 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 aprovam.

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]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	DOC-ICP-05.03

10.3

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

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

11 REFERÊNCIAS BIBLIOGRÁFICAS

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