



# **Declaração de Práticas de Certificação DPC**

## **Autoridade Certificadora VALID**

***OID 2.16.76.1.1.43***

**DPC da VALID  
Versão 4.0  
Outubro de 2022**

---

## Sumário

1. INTRODUÇÃO .....	11
1.1. Visão Geral.....	11
1.2. Nome do documento e identificação .....	11
1.3. Participantes da ICP-Brasil.....	11
1.3.1. Autoridades Certificadoras .....	11
1.3.2. Autoridades de Registro .....	12
1.3.3. Titulares do Certificado.....	12
1.3.4. Partes Confiáveis .....	12
1.3.5. Outros Participantes .....	12
1.4. Usabilidade do Certificado.....	12
1.4.1. Uso apropriado do certificado.....	12
1.4.2. Uso proibitivo do certificado .....	12
1.5. Política de Administração .....	13
1.5.1. Organização administrativa do documento .....	13
1.5.2. Contatos .....	13
1.5.3. Pessoa que determina a adequabilidade da DPC com a PC .....	13
1.5.4. Procedimentos de aprovação da DPC .....	13
1.6. Definições e Acrônimos.....	13
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO.....	14
2.1. Repositórios .....	14
2.2. Publicação de informações dos certificados.....	15
2.3. Tempo ou Frequência de Publicação.....	15
2.4. Controle de Acesso aos Repositórios .....	16
3. IDENTIFICAÇÃO E AUTENTICAÇÃO .....	16
3.1. Atribuição de Nomes .....	16
3.1.1. Tipos de Nomes .....	16
3.1.2. Necessidade dos nomes serem significativos .....	16
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado .....	16
3.1.4. Regras para interpretação de vários tipos de nomes .....	16
3.1.5. Unicidade de nomes.....	17
3.1.6. Procedimento para resolver disputa de nomes .....	17
3.1.7. Reconhecimento, autenticação e papel de marcas registradas .....	17
3.2. Validação Inicial de Identidade.....	17
3.2.1. Método para comprovar o controle de chave privada .....	18
3.2.2. Autenticação da identificação da organização .....	18

3.2.3. Autenticação da identidade de um indivíduo .....	20
3.2.4. Informações não verificadas do titular do certificado.....	21
3.2.5. Validação das autoridades .....	21
3.2.6 Critérios para interoperação .....	21
3.2.7 Autenticação da identidade de equipamento ou aplicação.....	21
3.2.8. Procedimentos complementares .....	23
3.2.9 Procedimentos específicos.....	24
3.3. Identificação e autenticação para pedidos de novas chaves.....	24
3.4. Identificação e autenticação para novas chaves após a revogação.....	25
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO ..	25
4.1. Solicitação do Certificado .....	25
4.1.1. Quem pode submeter uma solicitação de certificado .....	26
4.1.2. Processo de registro e responsabilidades.....	26
4.2. Processamento de Solicitação de Certificado .....	28
4.2.1. Execução das funções de identificação e autenticação .....	28
4.2.2. Aprovação ou rejeição de pedidos de certificado .....	28
4.2.3. Tempo para processar a solicitação de certificado .....	28
4.3. Emissão de Certificado.....	28
4.3.1. Ações da AC durante a emissão de um certificado.....	28
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado .....	29
4.4. Aceitação de Certificado.....	29
4.4.1. Conduta sobre a aceitação do certificado .....	29
4.4.2. Publicação do certificado pela AC.....	30
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades .....	30
4.5. Usabilidade do par de chaves e do certificado .....	30
4.5.1. Usabilidade da Chave privada e do certificado do titular.....	30
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis .....	30
4.6. Renovação de Certificados .....	31
4.6.1. Circunstâncias para renovação de certificados .....	31
4.6.2. Quem pode solicitar a renovação.....	31
4.6.3. Processamento de requisição para renovação de certificados .....	31
4.6.4. Notificação para nova emissão de certificado para o titular .....	31
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado	31
4.6.6. Publicação de uma renovação de um certificado pela AC .....	31
4.6.7. Notificação de emissão de certificado pela AC para outras entidades...	31

---

4.7. Nova chave de certificado ( <i>Re-key</i> ) .....	31
4.7.1. Circunstâncias para nova chave de certificado .....	31
4.7.2. Quem pode requisitar a certificação de uma nova chave pública .....	31
4.7.3. Processamento de requisição de novas chaves de certificado .....	31
4.7.4. Notificação de emissão de novo certificado para o titular.....	32
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada .....	32
4.7.6. Publicação de uma nova chave certificada pela AC.....	32
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades .....	32
4.8. Modificação de certificado .....	32
4.8.1. Circunstâncias para modificação de certificado .....	32
4.8.2. Quem pode requisitar a modificação de certificado.....	32
4.8.3. Processamento de requisição de modificação de certificado .....	32
4.8.4. Notificação de emissão de novo certificado para o titular.....	32
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado ...	32
4.8.6. Publicação de uma modificação de certificado pela AC .....	32
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades .....	33
4.9. Suspensão e Revogação de Certificado .....	33
4.9.1. Circunstâncias para revogação .....	33
4.9.2. Quem pode solicitar revogação.....	33
4.9.3. Procedimento para solicitação de revogação.....	34
4.9.4. Prazo para solicitação de revogação.....	35
4.9.5. Tempo em que a AC deve processar o pedido de revogação.....	35
4.9.6. Requisitos de verificação de revogação para as partes confiáveis .....	35
4.9.7. Frequência de emissão de LCR .....	35
4.9.8. Latência máxima para a LCR.....	35
4.9.9. Disponibilidade para revogação/verificação de status on-line .....	35
4.9.10. Requisitos para verificação de revogação on-line .....	36
4.9.11. Outras formas disponíveis para divulgação de revogação.....	36
4.9.12. Requisitos especiais para o caso de comprometimento de chave .....	36
4.9.13. Circunstâncias para suspensão .....	36
4.9.14. Quem pode solicitar suspensão .....	36
4.9.15. Procedimento para solicitação de suspensão .....	36
4.9.16. Limites no período de suspensão.....	36
4.10. Serviços de status de certificado.....	36
4.10.1. Características operacionais .....	36

---

4.10.2 Disponibilidade dos serviços .....	36
4.10.3. Funcionalidades operacionais .....	37
4.11. Encerramento de atividades .....	37
4.12. Custódia e recuperação de chave .....	37
4.12.1 Política e práticas de custódia e recuperação de chave.....	37
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão .....	37
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES .....	38
5.1. Controles Físicos .....	38
5.1.1. Construção e localização das instalações .....	38
5.1.2. Acesso físico .....	38
5.1.3. Energia e ar-condicionado.....	41
5.1.4. Exposição à água .....	42
5.1.5. Prevenção e proteção contra incêndio .....	43
5.1.6. Armazenamento de mídia .....	43
5.1.7. Destruição de lixo .....	43
5.1.8. Instalações de segurança ( <i>backup</i> ) externas ( <i>off-site</i> ) para AC.....	43
5.2. Controles Procedimentais .....	43
5.2.1. Perfis qualificados .....	43
5.2.2. Número de pessoas necessário por tarefa.....	45
5.2.3. Identificação e autenticação para cada perfil .....	45
5.2.4. Funções que requerem separação de deveres .....	45
5.3. Controles de Pessoal .....	46
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade.....	46
5.3.2. Procedimentos de Verificação de Antecedentes .....	46
5.3.3. Requisitos de treinamento.....	46
5.3.4. Frequência e requisitos para reciclagem técnica .....	47
5.3.5. Frequência e sequência de rodízios de cargos .....	47
5.3.6. Sanções para ações não autorizadas .....	47
5.3.7. Requisitos para contratação de pessoal.....	47
5.3.8. Documentação fornecida ao pessoal .....	48
5.4. Procedimentos de Log de Auditoria .....	48
5.4.1. Tipos de eventos registrados .....	48
5.4.2. Frequência de auditoria de registros .....	49
5.4.3. Período de retenção para registros de auditoria .....	50
5.4.4. Proteção de registros de auditoria.....	50

---

5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria .....	50
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo) .....	50
5.4.7. Notificação de agentes causadores de eventos .....	50
5.4.8. Avaliações de vulnerabilidade .....	51
5.5. Arquivamento de Registros .....	51
5.5.1. Tipos de registros arquivados .....	51
5.5.2. Período de retenção para arquivo .....	51
5.5.3. Proteção de arquivo .....	51
5.5.4. Procedimentos de cópia de arquivo .....	51
5.5.5. Requisitos para datação de registros .....	52
5.5.6. Sistema de coleta de dados de arquivo (interno e externo) .....	52
5.5.7. Procedimentos para obter e verificar informação de arquivo .....	52
5.6. Troca de chave.....	52
5.7. Comprometimento e Recuperação de Desastre .....	52
5.7.1. Procedimentos de gerenciamento de incidente e comprometimento .....	53
5.7.2. Recursos computacionais, software, e/ou dados corrompidos.....	53
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade .....	53
5.7.4. Capacidade de continuidade de negócio após desastre .....	53
5.8. Extinção da AC.....	54
6. CONTROLES TÉCNICOS DE SEGURANÇA.....	54
6.1. Geração e Instalação do Par de Chaves.....	54
6.1.1. Geração do Par de Chaves .....	54
6.1.2. Entrega da chave privada à entidade.....	55
6.1.3. Entrega da chave pública para emissor de certificado .....	55
6.1.4. Entrega de chave pública da AC às terceiras partes.....	55
6.1.5. Tamanhos de chave .....	55
6.1.6. Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros .....	55
6.1.7. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3) .....	56
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico .....	56
6.2.1. Padrões para módulo criptográfico.....	56
6.2.2. Controle “n de m’ para chave privada .....	56
6.2.3. Recuperação (escrow) de chave privada .....	57
6.2.4. Cópia de segurança (backup) de chave privada .....	57

---

6.2.5. Arquivamento de chave privada .....	57
6.2.6. Inserção de chave privada em módulo criptográfico .....	57
6.2.7. Armazenamento de chave privada em módulo criptográfico .....	57
6.2.8. Método de ativação de chave privada .....	57
6.2.9. Método de desativação de chave privada .....	58
6.2.10. Método de destruição de chave privada .....	58
6.3. Outros Aspectos do Gerenciamento do Par de Chaves .....	58
6.3.1. Arquivamento de chave pública .....	58
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada .....	58
6.4. Dados de Ativação .....	59
6.4.1. Geração e instalação dos dados de ativação .....	59
6.4.2. Proteção dos dados de ativação .....	59
6.4.3. Outros aspectos dos dados de ativação .....	59
6.5. Controles de Segurança Computacional .....	59
6.5.1. Requisitos técnicos específicos de segurança computacional .....	59
6.5.2. Classificação da segurança computacional .....	60
6.5.3. Controle de segurança para as Autoridades de Registro .....	61
6.6. Controles Técnicos do Ciclo de Vida .....	62
6.6.1. Controles de desenvolvimento de sistemas .....	62
6.6.2. Controle de gerenciamento de segurança .....	62
6.6.3. Classificação de segurança de ciclo de vida .....	62
6.6.4. Controles na Geração de LCR .....	62
6.7. Controles de Segurança de Rede .....	62
6.7.1. Diretrizes Gerais .....	62
6.7.2. Firewall .....	63
6.7.3. Sistema de detecção de intrusão (IDS) .....	63
6.7.4. Registro de acessos não-autorizados à rede .....	64
6.8. Carimbo de Tempo .....	64
7. PERFIS DE CERTIFICADO, LCR E OCSP .....	64
7.1. Perfil do Certificado .....	64
7.1.1. Número de versão .....	64
7.1.2. Extensões de certificado .....	64
7.1.3. Identificadores de algoritmo .....	65
7.1.4. Formatos de nome .....	65
7.1.5. Restrições de nome .....	65
7.1.6. OID ( <i>Object Identifier</i> ) da DPC .....	67

---

7.1.7. Uso da extensão “ <i>Policy Constraints</i> ” .....	67
7.1.8. Sintaxe e semântica dos qualificadores de política .....	67
7.1.9. Semântica de processamento para as extensões críticas de PC.....	67
7.2. Perfil de LCR .....	67
7.2.1. Número(s) de versão.....	67
7.2.2. Extensões de LCR e de suas entradas .....	67
7.3. Perfil de OCSP .....	67
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES.....	68
8.1. Frequência e circunstâncias das avaliações .....	68
8.2. Identificação / Qualificação do avaliador .....	68
8.3. Relação do avaliador com a entidade avaliada .....	68
8.4. Tópicos cobertos pela avaliação .....	68
8.5. Ações tomadas como resultado de uma deficiência .....	69
8.6. Comunicação dos resultados .....	69
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS .....	69
9.1. Tarifas .....	69
9.1.1. Tarifas de emissão e renovação de certificados .....	69
9.1.2. Tarifas de acesso ao certificado.....	69
9.1.3. Tarifas de revogação ou de acesso à informação de status .....	69
9.1.4. Tarifas para outros serviços .....	69
9.1.5. Política de reembolso.....	69
9.2. Responsabilidade Financeira .....	70
9.2.1 Cobertura do seguro .....	70
9.2.2 Outros ativos .....	70
9.2.3 Cobertura de seguros ou garantia para entidades finais.....	70
9.3 Confidencialidade da informação do negócio.....	70
9.3.1 Escopo de informações confidenciais .....	70
9.3.2. Informações fora do escopo de informações confidenciais.....	70
9.3.3 Responsabilidade em proteger a informação confidencial .....	71
9.4. Privacidade da informação pessoal.....	72
9.4.1. Plano de privacidade .....	72
9.4.2 Tratamento de informação como privadas .....	72
9.4.3 Informações não consideradas privadas .....	72
9.4.4 Responsabilidade para proteger a informação privadas .....	72
9.4.5 Aviso e consentimento para usar informações privadas .....	72
9.4.6. Divulgação em processo judicial ou administrativo .....	72



---

9.4.7. Outras circunstâncias de divulgação de informação .....	73
9.4.8. Informações a terceiros .....	73
9.5. Direitos de Propriedade Intelectual .....	73
9.6. Declarações e Garantias .....	73
9.6.1 Declarações e Garantias da AC .....	73
9.6.2. Declarações e Garantias da AR .....	74
9.6.3. Declarações e garantias do titular .....	74
9.6.4. Declarações e garantias das terceiras partes .....	74
9.6.5. Representações e garantias de outros participantes .....	75
9.7. Isenção de garantias .....	75
9.8. Limitações de responsabilidades .....	75
9.9. Indenizações .....	75
9.10. Prazo e Rescisão .....	75
9.10.1. Prazo .....	75
9.10.2. Término .....	75
9.10.3. Efeito da rescisão e sobrevivência .....	75
9.11. Avisos individuais e comunicações com os participantes.....	76
9.12. Alterações .....	76
9.12.1. Procedimento para emendas .....	76
9.12.2. Mecanismo de notificação e períodos .....	76
9.12.3. Circunstâncias na qual o OID deve ser alterado .....	76
9.13. Solução de conflitos .....	76
9.14. Lei aplicável.....	76
9.15. Conformidade com a Lei aplicável .....	76
9.16. Disposições Diversas .....	77
9.16.1. Acordo completo .....	77
9.16.2. Cessão .....	77
9.16.3. Independência de disposições .....	77
9.16.4. Execução (honorários dos advogados e renúncia de direitos).....	77
9.17. Outras provisões .....	77
10. DOCUMENTOS REFERENCIADOS.....	77
11. REFERÊNCIAS BIBLIOGRÁFICAS .....	78

**CONTROLE DE ALTERAÇÕES:**

<b>Versão</b>	<b>Data</b>	<b>Resolução que aprova a alteração</b>	<b>Item Alterado</b>	<b>Descrição da Alteração</b>
<b>3.0</b>	16/02/2022	Resolução n.197	Diversos	Adequação para atender resolução
<b>4.0</b>	10/10/2022	Resolução n.204	4.5.1.2	Adequação para atender resolução

## 1. INTRODUÇÃO

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

### 1.1. Visão Geral

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

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

As referências a formulários presentes nesta DPC deverão ser entendidas também como referências a outras formas que a AC VALID possa vir a adotar.

**1.1.3.** Não se aplica.

**1.1.4.** A estrutura desta DPC está baseada na RFC 3647.

**1.1.5.** A AC VALID mantém todas as informações da sua DPC sempre atualizadas.

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

### 1.2. Nome do documento e identificação

**1.2.1.** Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora VALID no âmbito da ICP-Brasil e referida como "DPC da AC VALID", cujo **OID** (*object identifier*) é **2.16.76.1.1.43**.

**1.2.2.** A AC VALID é emissora de certificados para nível imediatamente subsequente (AC Subsequente) ao seu.

### 1.3. Participantes da ICP-Brasil

#### 1.3.1. Autoridades Certificadoras

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

### **1.3.2. Autoridades de Registro**

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pelas ACs subsequentes à AC VALID para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC VALID: (<https://www.validcertificadora.com.br/index.aspx?DID=60>)

- a) Relação de todas as ARs credenciadas; e
- b) Relação de ARs que tenham se descredenciado da cadeia da AC subsequente à AC VALID, com respectiva data do descredenciamento;

### **1.3.3. Titulares do Certificado**

A AC VALID emite certificados para Autoridades Certificadoras de nível imediatamente subsequente ao seu. Os titulares dos certificados são entidades e pessoas jurídicas de direito público e privado.

### **1.3.4. Partes Confiáveis**

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

### **1.3.5. Outros Participantes**

1.3.5.1. A relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC VALID é publicada em serviço de diretório e/ou em página web da AC VALID (<https://www.validcertificadora.com.br/index.aspx?DID=60>)

## **1.4. Usabilidade do Certificado**

### **1.4.1. Uso apropriado do certificado**

Os certificados definidos por esta DPC AC VALID têm sua utilização exclusiva para a assinatura de certificados digitais de AC de nível subsequente ao seu e de Lista de Certificados Revogados (LCR).

### **1.4.2 Uso proibitivo do certificado**

Não se aplica.

## 1.5 Política de Administração

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

### 1.5.1 Organização administrativa do documento

Nome da AC: AC VALID

### 1.5.2 Contatos

**Endereço:** Alameda Rio Claro, 241 - Bela Vista - São Paulo, SP - Brasil

CEP: 01332-010

**Telefone:** (11) 2575-6800

**Página Web:** <http://www.validcertificadora.com.br/>

**E-mail:** [pki.compliance@valid.com](mailto:pki.compliance@valid.com)

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

**Nome:** Marcio Nunes da Silva

**Telefone:** (11) 2575-6800

**E-mail:** [pki.compliance@valid.com](mailto:pki.compliance@valid.com)

**Outros:** <http://www.validcertificadora.com.br/>

### 1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

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

## 1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AGR	Agente de Registro
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
DN	<i>Distinguished Name</i>

<b>DPC</b>	Declaração de Práticas de Certificação
<b>ICP-Brasil</b>	Infraestrutura de Chaves Públicas Brasileira
<b>IEC</b>	<i>International Electrotechnical Commission</i>
<b>INMETRO</b>	Instituto Nacional de Metrologia, Qualidade e Tecnologia
<b>ISO</b>	<i>International Organization for Standardization</i>
<b>ITU</b>	<i>International Telecommunications Union</i>
<b>LCR</b>	Lista de Certificados Revogados
<b>NBR</b>	Norma Brasileira
<b>NIS</b>	Número de Identificação Social
<b>OCSP</b>	<i>Online Certificate Status Protocol</i>
<b>OID</b>	<i>Object Identifier</i>
<b>OU</b>	<i>Organization Unit</i>
<b>PASEP</b>	Programa de Formação do Patrimônio do Servidor Público
<b>PC</b>	Políticas de Certificado
<b>PCN</b>	Plano de Continuidade de Negócio
<b>PIN</b>	Personal Identification Number
<b>PIS</b>	Programa de Integração Social
<b>PS</b>	Política de Segurança
<b>PSBio</b>	Prestador de Serviço Biométrico
<b>PSC</b>	Prestador de Serviço de Confiança
<b>PSS</b>	Prestadores de Serviço de Suporte
<b>PUK</b>	PIN Unblocking Key
<b>RFC</b>	<i>Request For Comments</i>
<b>RG</b>	Registro Geral
<b>SSL</b>	<i>Secure Socket Layer</i>
<b>UF</b>	Unidade de Federação
<b>URL</b>	<i>Uniform Resource Locator</i>

## 2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

### 2.1. Repositórios

2.1.1. A AC VALID mantém disponível repositório atendendo as seguintes obrigações:

- Disponibilizar, logo após a sua emissão, os certificados emitidos pela AC e a sua LCR;
- Estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
- Implementar os recursos necessários para a segurança dos dados nele armazenados.

**2.1.2.** As publicações da AC VALID podem ser consultadas através do protocolo <https://www.validcertificadora.com.br/index.aspx?DID=60>.

Somente a AC VALID, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar atualizações nas informações por ela publicadas no seu repositório.

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

**2.1.4.** A AC VALID disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR.

- <http://icp-brasil.validcertificadora.com.br/ac-valid/lcr-ac-validv5.crl>
- <http://icp-brasil2.validcertificadora.com.br/ac-valid/lcr-ac-validv5.crl>

## **2.2. Publicação de informações dos certificados**

**2.2.1.** As informações descritas abaixo são publicadas em serviço de diretório e/ou em página *web* da AC VALID (<https://www.validcertificadora.com.br/index.aspx?DID=60>), obedecendo as regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC VALID em serviço de diretório e/ou página *web* é de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

**2.2.2.** As seguintes informações são publicadas em serviço de diretório e/ou em página *web* da AC VALID (<https://www.validcertificadora.com.br/index.aspx?DID=60>)

- a) Seu próprio certificado;
- b) Suas LCRs;
- c) Esta DPC;
- d) Não se aplica;
- e) Uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços; e
- f) Uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

## **2.3. Tempo ou Frequência de Publicação**

**2.3.1.** De modo a assegurar a disponibilização sempre atualizada de seus conteúdos:

- a) Os certificados são publicados imediatamente após sua emissão;
- b) A publicação da LCR se dá conforme o item 4.9.7 desta DPC;
- c) As versões ou alterações desta DPC são atualizadas na website da AC VALID após aprovação da AC Raiz da ICP-Brasil; e

- d) Os endereços das AR vinculadas das ACs subsequentes são atualizadas na website da AC VALID.

## **2.4. Controle de Acesso aos Repositórios**

**2.4.1.** Não há nenhuma restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC VALID e aos endereços das AR vinculadas.

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

## **3. IDENTIFICAÇÃO E AUTENTICAÇÃO**

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

### **3.1. Atribuição de Nomes**

#### **3.1.1. Tipos de Nomes**

**3.1.1.1.** O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o “*Distinguished Name*” do padrão ITU X.500, endereços de correio eletrônico, endereço de página *Web* (URL), ou outras informações que permitam a identificação unívoca do titular.

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

#### **3.1.2. Necessidade dos nomes serem significativos**

**3.1.2.1.** Os certificados emitidos pela AC VALID exigem o uso de nomes significativos que possibilitam determinar univocamente a identidade da organização titular do certificado.

#### **3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado**

Não se aplica.

#### **3.1.4. Regras para interpretação de vários tipos de nomes**

**3.1.4.1.** Não se aplica.



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

### **3.1.5. Unicidade de nomes**

Os identificadores “*Distinguished Name*” (DN) são únicos para cada entidade titular de certificado emitido pela AC VALID. 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 VALID se reserva o direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrente da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

### **3.1.7. Reconhecimento, autenticação e papel de marcas registradas**

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

## **3.2. Validação Inicial de Identidade**

Neste item e nos seguintes, a DPC descreve detalhes os requisitos e procedimentos utilizados pelas ARs vinculadas as ACs subsequentes à AC VALID para a realização dos seguintes processos:

a) Identificação do titular do certificado – identificação da pessoa jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2 e 3.2.3, observando quanto segue:

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

b) Emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC. A extensão *Subject Alternative Name* é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o

solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

**Nota:** Nos casos de falecimento dos responsáveis legais por quaisquer empresas de um modo geral, desde que haja decisão judicial com nomeação de inventariante e termo de compromisso de inventariante assinado, e nomeação expressa deste como administrador será admitida a pessoa nomeada na qualidade de responsável legal do Certificado Digital para todos os fins legais e administrativos, de acordo com a legislação vigente.

### **3.2.1. Método para comprovar o controle de chave privada**

A AR verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital, segundo o padrão definido RFC 4210 e 6712 são utilizadas como referência para essa finalidade.

### **3.2.2. Autenticação da identificação da organização**

#### **3.2.2.1. Disposições Gerais**

**3.2.2.1.1.** Neste item devem ser definidos os procedimentos empregados pelas ARs vinculadas as ACs subsequentes à AC VALID para a confirmação da identidade de uma pessoa jurídica.

**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 de seus representantes, nos seguintes termos:

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

**Nota 1:** A AR poderá solicitar uma assinatura manuscrita ao requerente ou responsável pelo uso do certificado em termo específico para a comparação com o documento de identidade ou contrato social. Nesse caso, o termo manuscrito

digitalizado e assinado digitalmente pelo AGR será apensado ao dossiê eletrônico do certificado, podendo o original em papel ser descartado.

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

**3.2.2.1.5** O disposto no item 3.2.2.1.3 poderá ser realizado:

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

### **3.2.2.2. Documentos para efeitos de identificação de uma organização**

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

- a) Relativos à sua habilitação jurídica:
  - I. Se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e 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 oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

**3.2.2.3.** Informações contidas no certificado emitido para uma organização.

Não se aplica.

**3.2.2.4** Não se aplica.

### **3.2.3. Autenticação da identidade de um indivíduo**

A confirmação é realizada mediante a presença física do interessado ou por um dos procedimentos listados nas alíneas abaixo, que asseguraram nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico:

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

#### **3.2.3.1. Documentos para efeitos de identificação de um indivíduo**

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

- a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:
  - i. Registro de Identidade, se brasileiro; ou
  - ii. Título de Eleitor, com foto; ou
  - iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
  - iv. Passaporte, se estrangeiro não domiciliado no Brasil.
- b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

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

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

3.2.3.1.2. Não se aplica.

3.2.3.1.3. Não se aplica.

3.2.3.1.4. Não se aplica.

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.1.7. Não se aplica.

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

3.2.3.1.8.1. Não se aplica.

### **3.2.3.2. Informações contidas no certificado emitido para um indivíduo**

3.2.3.2.1. Não se aplica.

3.2.3.2.1.1 Não se aplica.

3.2.3.2.2. Não se aplica.

3.2.3.2.3. Não se aplica.

3.2.3.2.3.1 Não se aplica.

### **3.2.4. Informações não verificadas do titular do certificado**

Não se aplica.

### **3.2.5. Validação das autoridades**

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

### **3.2.6 Critérios para interoperação**

Não se aplica.

### **3.2.7 Autenticação da identidade de equipamento ou aplicação**

#### **3.2.7.1 Disposições Gerais**

3.2.7.1.1. Não se aplica.

3.2.7.1.2. Não se aplica.

3.2.7.1.3. Não se aplica.

3.2.7.1.4. Não se aplica.

3.2.7.1.5. Não se aplica.

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

3.2.7.2.1. Não se aplica.

3.2.7.2.2. Não se aplica.

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

3.2.7.3.1. Não se aplica.

3.2.7.3.2. Não se aplica.

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

3.2.7.4.1. Não se aplica.

3.2.7.4.2. Não se aplica.

3.2.7.4.3. Não se aplica.

3.2.7.4.4. Não se aplica.

**3.2.7.5. Procedimentos para efeitos de identificação de um equipamento SAT**

3.2.7.5.1. Não se aplica.

**3.2.7.6. Informações contidas no certificado emitido para um equipamento SAT**

3.2.7.6.1. Não se aplica.

3.2.7.6.2. Não se aplica.

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

3.2.7.7.1. Não se aplica.

3.2.7.7.2. Não se aplica.

3.2.7.7.3. Não se aplica.

3.2.7.7.4. Não se aplica.

### **3.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico**

**3.2.7.8.1.** Não se aplica.

### **3.2.7.9. Informações contidas no certificado emitido para um equipamento metrológico**

**3.2.7.9.1.** Não se aplica

**3.2.7.9.2.** Não se aplica.

### **3.2.8. Procedimentos complementares**

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

**3.2.8.2.** Todo o processo de identificação do titular do certificado é registrado possibilita a reconstituição completa dos processos executados para fins de auditoria.

**3.2.8.2.1** Não se aplica.

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

**3.2.8.3.1.** Não se aplica.

**3.2.8.3.2** Não se aplica.

**3.2.8.3.3** Não se aplica.

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

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

**3.2.8.4.2** Não se aplica.

---

### **3.2.9 Procedimentos específicos**

3.2.9.1. Não se aplica.

3.2.9.2. Não se aplica.

3.2.9.3. Não se aplica.

3.2.9.3.1. Não se aplica.

3.2.9.3.2. Não se aplica.

3.2.9.3.3. Não se aplica.

3.2.9.4. Não se aplica.

#### **3.2.9.5. Disposições para a Validação de Solicitação de Certificados do Tipo OM-BR**

Não se aplica.

3.2.9.6. Não se aplica.

3.2.9.7. Não se aplica.

3.2.9.8 Não se aplica.

### **3.3. Identificação e autenticação para pedidos de novas chaves**

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

**3.3.2. Esse processo poderá ser 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) Por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico; ou
- f) Não se aplica.

**3.3.2.1.** Não se aplica.



### 3.3.3. Não se aplica.

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

### 3.4. Identificação e autenticação para novas chaves após a revogação

O solicitante da revogação de certificado deverá ser identificado. Somente os agentes descritos no item 4.9.2 podem solicitar a revogação do certificado da AC VALID.

## 4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

### 4.1. Solicitação do Certificado

Para atender à solicitação de certificado digital à AC VALID, os requisitos e procedimentos deverão compreender, no mínimo:

- a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
- b) Não se aplica.
- c) Um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico;
- d) O atendimento via videoconferência será realizado atendendo os critérios mencionados abaixo:
  - Clientes que possui suas biometrias coletada em um a validação presencial;
  - Certificados vencidos;
  - Clientes que possui um e-mail que tenha acesso;
  - Clientes que possui uma web-cam e internet.

A AC VALID adequou o sistema atual para atendimento a essa modalidade, seguindo requisitos descrito no DOC-ICP-05.05, sendo assim, os clientes deverão atender os requisitos descrito acima para ter o acesso emissão do certificado via videoconferência; e

- e) Não se aplica.

**Nota:** na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados de equipamento, aplicação e outros que façam uso de CSR) será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo certificado,

no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo será necessária a verificação da assinatura contra o documento de identificação.

#### **4.1.1. Quem pode submeter uma solicitação de certificado**

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

**4.1.1.2.** Não se aplica.

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

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

#### **4.1.2. Processo de registro e responsabilidades**

Abaixo são descritas as obrigações gerais das entidades envolvidas.

##### **4.1.2.1. Responsabilidades da AC**

**4.1.2.1.1.** A AC VALID responde pelos danos a que der causa.

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

**4.1.2.1.3.** Não se aplica.

##### **4.1.2.2. Obrigações da AC**

As obrigações da AC VALID são as abaixo relacionadas:

- a) Operar de acordo com a sua DPC;
- b) Gerar e gerenciar os seus pares de chaves criptográficas;
- c) Assegurar a proteção de suas chaves privadas;
- d) Notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

- e) Notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- f) Distribuir o seu próprio certificado;
- g) Emitir, expedir e distribuir os certificados de AC 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 em sua página web sua DPC;
- l) Publicar, em sua página web, as informações definidas no item 2.2.2 deste documento;
- m) Publicar, em página *web*, informações sobre o descredenciamento de AR e AC subsequente;
- n) Utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;
- o) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- p) Adotar as medidas de segurança e controle previstas na DPC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- q) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- r) Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- s) Manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;
- t) Manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, quando esta estiver obrigada a contratá-lo, de acordo com as normas do CG da ICP-Brasil;
- u) Informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
- v) Informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;
- w) Não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
- x) Realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais das ACs subsequentes, diretamente com seus profissionais, ou através de auditorias internas ou

- empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AC subsequente; e
- y) Não se aplica.

#### **4.1.2.3. Responsabilidades da AR**

Não se aplica.

#### **4.1.2.4. Obrigações das ARs**

Não se aplica.

### **4.2. Processamento de Solicitação de Certificado**

#### **4.2.1. Execução das funções de identificação e autenticação**

A AC VALID executa as funções de identificação e autenticação conforme item 3 desta DPC.

#### **4.2.2. Aprovação ou rejeição de pedidos de certificado**

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

**4.2.2.2.** A AC VALID 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 VALID cumpre os procedimentos determinados na ICP-Brasil. Não há tempo máximo para processar as solicitações na ICP-Brasil.

### **4.3. Emissão de Certificado**

#### **4.3.1. Ações da AC durante a emissão de um certificado**

**4.3.1.1.** A emissão de um certificado pela AC VALID é feita em cerimônia específica, com a presença de representantes da AC VALID, da AC habilitada, convidados e testemunhas, na qual são registrados todos os procedimentos executados.

A AC VALID garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 10 (dez) dias

úteis após o recebimento da solicitação.

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

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

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

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

### **4.4. Aceitação de Certificado**

#### **4.4.1. Conduta sobre a aceitação do certificado**

**4.4.1.1.** A AC VALID garante que as informações contidas no certificado emitido para uma AC de nível imediatamente subsequente ao seu foram verificadas de correspondente acordo com esta DPC

Ao aceitar o certificado, a AC titular:

- a) concorda com as responsabilidades, obrigações e deveres a ela impostos pelo Termo de Acordo e a DPC da AC VALID;
- b) garante que com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;
- 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;
- d) aceita as regras e normas da AC VALID para emissão de certificados na sua cadeia de certificação. 4.3.5. A não aceitação do certificado dentro do 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 após a verificação pela AC ou na primeira utilização da chave privada. A AC titular tem o prazo de 2 (dois) dias úteis, contados do seu recebimento, para fazer a verificação dos dados do certificado. Após esse prazo o certificado é considerado aceito.

A não aceitação do certificado dentro do prazo previsto implica a realização de nova cerimônia, onde é feita a revogação do certificado não aceito e a emissão de novo certificado.

**4.4.1.3.** A AC atestará por meio de seus representantes legais, mediante assinatura do “Termo de Acordo”, o recebimento do certificado emitido.

---

#### **4.4.2. Publicação do certificado pela AC**

O certificado da AC VALID 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 deve operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementar, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICPBRASIL [7].

##### **4.5.1. Usabilidade da Chave privada e do certificado do titular**

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

##### **4.5.1.2. Obrigações do Titular do Certificado**

As obrigações dos titulares de certificados emitidos pela AC VALID são as abaixo relacionadas:

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

##### **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 item 3.3 desta DPC.

### **4.6.2. Quem pode solicitar a renovação**

Em acordo com item 3.3 desta DPC.

### **4.6.3. Processamento de requisição para renovação de certificados**

Em acordo com item 3.3 desta DPC.

### **4.6.4. Notificação para nova emissão de certificado para o titular**

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

### **4.6.6. Publicação de uma renovação de um certificado pela AC**

Não se aplica.

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

Em acordo com item 4.3 desta DPC.

## **4.7. Nova chave de certificado (*Re-key*)**

### **4.7.1. Circunstâncias para nova chave de certificado**

Não se aplica.

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

Não se aplica.

### **4.7.3. Processamento de requisição de novas chaves de certificado**

Não se aplica.

---

#### **4.7.4. Notificação de emissão de novo certificado para o titular**

Não se aplica.

#### **4.7.5. Conduta constituindo a aceitação de uma nova chave certificada**

Não se aplica.

#### **4.7.6. Publicação de uma nova chave certificada pela AC**

Não se aplica.

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

Não se aplica.

#### **4.8. Modificação de certificado**

Não se aplica.

##### **4.8.1. Circunstâncias para modificação de certificado**

Não se aplica.

##### **4.8.2. Quem pode requisitar a modificação de certificado**

Não se aplica.

##### **4.8.3. Processamento de requisição de modificação de certificado**

Não se aplica.

##### **4.8.4. Notificação de emissão de novo certificado para o titular**

Não se aplica.

##### **4.8.5. Conduta constituindo a aceitação de uma modificação de certificado**

Não se aplica.

##### **4.8.6. Publicação de uma modificação de certificado pela AC**

Não se aplica.



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

Não se aplica.

### **4.9. Suspensão e Revogação de Certificado**

#### **4.9.1. Circunstâncias para revogação**

**4.9.1.1.** A AC titular, por meio do seu representante legal, pode solicitar a revogação de seu certificado a qualquer tempo, independentemente de qualquer circunstância.

**4.9.1.2.** O certificado deve ser obrigatoriamente revogado:

- a) Quando constatada emissão imprópria ou defeituosa do mesmo;
- b) Quando for necessária a alteração de qualquer informação constante no mesmo;
- c) No caso de dissolução de AC titular do certificado; ou
- d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

**4.9.1.3.** A AC VALID define ainda que:

- a) A AC VALID deve revogar, no prazo definido no item 4.9.3.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e
- b) O CG da ICP-Brasil ou AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

**4.9.1.4.** Não se aplica.

**4.9.1.4.1.** Não se aplica.

**4.9.1.4.2.** Não se aplica.

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

#### **4.9.2. Quem pode solicitar revogação**

A revogação de um certificado de uma AC de nível imediatamente subsequente ao da AC VALID somente poderá ser feita:

- a) Por solicitação do titular do certificado;
- b) Não se aplica.

- c) Não se aplica.
- d) Pela AC VALID emitente;
- e) Não se aplica.
- f) Por determinação do CG da ICP-Brasil ou da AC Raiz; ou
- g) Não se aplica;
- h) Não se aplica;
- i) Não se aplica; ou
- j) Não se aplica;
- k) Por decisão judicial.

### **4.9.3. Procedimento para solicitação de revogação**

**4.9.3.1.** A solicitação de revogação de certificado de AC de nível imediatamente subsequente será feita formalmente por representante legal da AC, que deve apresentá-la pessoalmente.

A solicitação de revogação de certificado de AC subsequente deve ser feita por meio de do formulário SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC. Esse formulário deverá ser assinado pelo representante legal da AC. Se utilizada versão digital do documento, este deverá estar assinado digitalmente. O documento deverá ser entregue pessoalmente na AR VALID CD pelo representante legal da AC subsequente, e, em se tratando de formulário em papel, será assinado no ato da entrega.

**4.9.3.2.** Como diretrizes gerais:

- a) O Solicitante da revogação de um certificado é identificado;
- b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC VALID;
- c) As justificativas para a revogação de um certificado são registradas;
- d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado à base de dados da AC VALID, quando aplicável.

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

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

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

**4.9.3.6.** Não se aplica.

---

#### **4.9.4. Prazo para solicitação de revogação**

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

O prazo para aceitação do certificado pelo seu titular é de 2 (dois) dias úteis, dentro do qual a revogação desse certificado pode ser solicitada sem ônus.

**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 VALID processa a revogação imediatamente após a análise do pedido.

#### **4.9.6. Requisitos de verificação de revogação para as partes confiáveis**

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

#### **4.9.7. Frequência de emissão de LCR**

**4.9.7.1.** A frequência máxima para emissão de LCR referente a certificados de AC de nível imediatamente subsequente ao da AC VALID é de 90(noventa) dias.

**4.9.7.2.** Não se aplica.

**4.9.7.3.** A frequência máxima admitida para a emissão de LCR referente a certificados de AC é de 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC VALID deverá emitir nova LCR no prazo previsto no item 4.9.3.4 e notificar todas as ACs de nível imediatamente subsequente ao seu.

**4.9.7.4.** Não se aplica.

**4.9.7.5.** Não se aplica.

#### **4.9.8. Latência máxima para a LCR**

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

#### **4.9.9 Disponibilidade para revogação/verificação de status on-line**

A AC VALID não disponibiliza recursos para revogação on-line de certificados

---

#### **4.9.10. Requisitos para verificação de revogação on-line**

Não se aplica.

#### **4.9.11. Outras formas disponíveis para divulgação de revogação**

Além das LCRs, a AC VALID poderá utilizar outros meios para divulgação de informações de revogação de certificados de AC de nível imediatamente subsequente ao seu, incluindo publicação na sua página web.

#### **4.9.12. Requisitos especiais para o caso de comprometimento de chave**

**4.9.12.1.** No caso do comprometimento da chave privada de uma AC de nível imediatamente subsequente ao da AC VALID, essa notificará imediatamente à AC VALID.

**4.9.12.2.** A comunicação do comprometimento da chave privada de uma AC poderá ser feita por correio eletrônico assinado digitalmente pelo representante legal da AC.

#### **4.9.13. Circunstâncias para suspensão**

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

#### **4.9.14 Quem pode solicitar suspensão**

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

#### **4.9.15. Procedimento para solicitação de suspensão**

Os procedimentos de solicitação de suspensão serão dados por norma específica da DPC.

#### **4.9.16. Limites no período de suspensão**

Os períodos de suspensão serão estabelecidos por norma específica das DPC .

### **4.10. Serviços de status de certificado**

#### **4.10.1. Características operacionais**

A AC VALID fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR, conforme item 4.9.

#### **4.10.2 Disponibilidade dos serviços**

Ver item 4.9

---

### **4.10.3. Funcionalidades operacionais**

Ver item 4.9

### **4.11. Encerramento de atividades**

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

**4.11.2.** Quando for necessário encerrar as atividades da AC VALID, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevaletentes, inclusive:

- a) notificar a AC Raiz da ICP-Brasil;
- b) notificar todas as entidades subordinadas;
- c) providenciar a transferência de chaves públicas, dos certificados e respectiva documentação para serem armazenados por outra AC, após aprovação da AC Raiz;
- d) transferir progressivamente o serviço e os registros operacionais para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC VALID e AR VALID;
- e) preservar qualquer registro não transferido a um sucessor;
- f) transferir, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas; e
- g) repassar à AC Raiz os documentos referentes aos certificados digitais e as respectivas chaves públicas, caso essas não sejam assumidas por outra AC.

### **4.12. Custódia e recuperação de chave**

#### **4.12.1 Política e práticas de custódia e recuperação de chave**

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

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

A AC VALID não executa tais práticas.

---

## 5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

### 5.1. Controles Físicos

#### 5.1.1. Construção e localização das instalações

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

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

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

Existem sistemas de aterramento e de proteção contra descargas atmosféricas;

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

#### 5.1.2. Acesso físico

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

##### 5.1.2.1 Níveis de Acesso

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

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

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

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

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

**5.1.2.1.5.** O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da AC VALID. Qualquer atividade relativa ao ciclo de vida dos certificados digitais é executada a partir desse nível. Pessoas não envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

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

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

**5.1.2.1.8.** No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC VALID tais como emissão e revogação de certificados e emissão de LCR e a disponibilidade à resposta à consulta OCSP. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível, inclusive o sistema de AR. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver sendo ocupado.

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

quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - possuem proteção contra interferência eletromagnética externa.

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

**5.1.2.1.11.** Na AC VALID, existem ambientes de quarto nível para abrigar e segregar, quando foro caso:

- a) Equipamentos de produção on-line, gabinete reforçado de armazenamento e equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores - (Data Center);
- b) Equipamentos de produção off-line e cofre de armazenamento (Sala de cerimônia).

**5.1.2.1.12.** O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre interior à sala de cerimônia e um gabinete reforçado trancado no Data Center. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

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

- a) confeccionado em aço;
- b) possui tranca com chave.

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

## **5.1.2.2. Sistemas físicos de detecção**

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

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



**5.1.2.2.3.** Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados ininterruptamente.

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

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

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

### **5.1.2.3. Sistema de Controle de Acesso.**

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

### **5.1.2.4. Mecanismos de emergência**

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

**5.1.2.4.2.** Todos os procedimentos referentes aos mecanismos de emergência 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 VALID está dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC VALID e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC VALID.

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

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

**5.1.3.4.** Todos os cabos são catalogados, identificados e periodicamente vistoriados, a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

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

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

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

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

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

**5.1.3.10.** A capacidade de redundância de toda a estrutura de energia e ar-condicionado da AC VALID 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, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

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

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

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

### **5.1.6. Armazenamento de mídia**

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

### **5.1.7. Destruição de lixo**

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

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

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

As instalações de *backup* deverão atender aos requisitos mínimos estabelecidos por este documento. Sua localização deverá ser tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não sejam atingidas e tornem-se totalmente operacionais em condições idênticas em, no máximo, 48 (quarenta e oito) hora.

## **5.2. Controles Procedimentais**

### **5.2.1. Perfis qualificados**

**5.2.1.1.** A AC VALID pratica uma política de segregação de funções, controlando e registrando o acesso físico e lógico às funções críticas do ciclo de vida dos certificados digitais, de forma a garantir a segurança da atividade de certificação

e evitar a manipulação desautorizada do sistema. As ações permitidas são limitadas de acordo com o perfil de cada cargo.

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

Gerência de Operações Data Center:

*Supervisão Operacional:*

- Configuração e manutenção do hardware e do software da AC;
- Gerenciamento e controle da tecnologia empregada nos serviços de certificação da AC;
- Controle de acesso lógico dos funcionários à rede AC;
- Gerenciamento dos operadores da AC;
- Controle de acesso ao sistema de certificação.

*Supervisão de PKI:*

Administração e controle dos componentes criptográficos da AC:

- Verificação dos registros de acesso aos diferentes níveis de proteção das chaves privadas das AC (logs);
- Elaboração das cerimônias de geração de chaves de AC;
- Armazenamento dos registros de auditoria do sistema de certificação;
- Utilização de criptografia para segurança de acesso ao aplicativo de certificação.

Gerência de Segurança:

- Implementação da Política de Segurança da AC;
- Verificação dos registros de auditoria; supervisão do cumprimento das práticas e procedimentos determinados na Política de Segurança da AC;
- Acompanhamento das auditorias de segurança realizadas por terceiros;
- Verificação do cumprimento desta DPC;
- Autorização e concessão de acesso às instalações físicas e autorização de acessos lógicos ao sistema de certificação;
- Utilização de criptografia para a segurança da base de dados de registro de auditoria do sistema de certificação.

Gerência de Operação:

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

**5.2.1.3.** Os operadores do sistema de certificação da AC VALID recebem treinamento específico antes de obter qualquer tipo de acesso ao sistema. O tipo

e o nível de acesso estão determinados, em documento formal (Política de Segurança da AC VALID), com base nas necessidades de cada perfil.

#### **5.2.1.3.1. Não se aplica.**

**5.2.1.4.** Quando um empregado se desligar da AC, suas permissões de acesso são revogadas imediatamente. Quando houver 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 VALID, 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 VALID requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC VALID podem ser executadas por um único empregado.

### **5.2.3. Identificação e autenticação para cada perfil**

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

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

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

- a) são diretamente atribuídos a um único empregado;
- b) não são compartilhados; e
- c) são restritos às ações associadas ao perfil para o qual foram criados.

**5.2.3.3.** A AC VALID implementa um padrão de utilização de “senhas fortes”, definido em conformidade com a Política de Segurança da ICP-Brasil, junto a procedimentos de validação dessas senhas.

### **5.2.4. Funções que requerem separação de deveres**

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

### **5.3. Controles de Pessoal**

Todos os empregados da AC VALID, das AR e PSS vinculados encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

- a) Os termos e as condições do perfil que ocupam;
- b) O compromisso de observar as normas, políticas e regras aplicáveis da AC VALID;
- c) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
- 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 VALID e das AR vinculadas envolvido em atividades diretamente relacionada com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

#### **5.3.2. Procedimentos de Verificação de Antecedentes**

**5.3.2.1.** Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC VALID e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser submetido a:

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

**5.3.2.2.** Não se aplica.

#### **5.3.3. Requisitos de treinamento**

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

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

#### **5.3.4. Frequência e requisitos para reciclagem técnica**

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

#### **5.3.5. Frequência e sequência de rodízios de cargos**

Não estabelecido.

#### **5.3.6. Sanções para ações não autorizadas**

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

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

- a) Relato da ocorrência com “modus 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 VALID 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**

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

### **5.3.8. Documentação fornecida ao pessoal**

**5.3.8.1.** A AC VALID disponibiliza para todo o seu pessoal e para o pessoal das ARs vinculadas as ACs subseqüentes:

- a) A DPC da AC VALID;
- b) Não se aplica;
- c) A Política de Segurança da ICP-Brasil [8];
- d) Documentação operacional relativa às suas atividades; e
- e) Contratos, normas e políticas relevantes para suas atividades.

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

### **5.4. Procedimentos de Log de Auditoria**

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

#### **5.4.1. Tipos de eventos registrados**

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

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

**5.4.1.1.1.** Não se aplica.



**5.4.1.2.** A AC VALID também registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

- a) Registros de acessos físicos;
- b) Manutenção e mudanças na configuração de seus sistemas;
- c) Mudanças de pessoal e 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 VALID são todas as descritas nos itens acima.

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

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

**5.4.1.6.** A AC VALID registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são obrigatoriamente 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.

**5.4.1.6.1** Não se aplica.

**5.4.1.7.** A AC VALID a que esteja vinculada a AR define, em documento a estar disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

## **5.4.2. Frequência de auditoria de registros**

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

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

### **5.4.3. Período de retenção para registros de auditoria**

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

### **5.4.4. Proteção de registros de auditoria**

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

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

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

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

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

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

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

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

### **5.4.7. Notificação de agentes causadores de eventos**

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

#### **5.4.8. Avaliações de vulnerabilidade**

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

#### **5.5. Arquivamento de Registros**

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

##### **5.5.1. Tipos de registros arquivados**

Os tipos de registros arquivados são:

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

##### **5.5.2. Período de retenção para arquivo**

Os períodos de retenção por tipo de registro arquivado são:

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

##### **5.5.3. Proteção de arquivo**

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

##### **5.5.4. Procedimentos de cópia de arquivo**

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

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

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

### **5.5.5. Requisitos para datação de registros**

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

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

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

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

### **5.5.7. Procedimentos para obter e verificar informação de arquivo**

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

## **5.6. Troca de chave**

**5.6.1.** O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico, disponibilizado pela AR Responsável, por onde é encaminhado o processo de fornecimento de novo certificado.

A AR que recebeu e validou o pedido de emissão do certificado envia uma comunicação ao titular do certificado, 30 (trinta) dias antes da data de expiração do mesmo, junto com instruções para a solicitação de um novo certificado.

A comunicação de expiração, junto com as instruções para a solicitação de um novo certificado é realizada através de e-mail enviado ao titular do certificado.

**5.6.2.** Não se aplica.

## **5.7. Comprometimento e Recuperação de Desastre**

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

### **5.7.1. Procedimentos de gerenciamento de incidente e comprometimento**

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

**5.7.1.2** Não se aplica.

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

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

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

#### **5.7.3.1 Certificado de entidade é revogado**

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

#### **5.7.3.2 Chave de entidade é comprometida**

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

- a) Todos os certificados afetados serão revogados e as partes serão notificadas.
- b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a AC VALID estiver encerrando suas atividades.

### **5.7.4. Capacidade de continuidade de negócio após desastre**

Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, o Departamento de Infraestrutura, responsável pela contingência, notifica o Gerente de

Segurança e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:

- a) Garantir a integridade física das pessoas que se encontram nas instalações da AC VALID;
- b) Monitorar e controlar o foco da contingência;
- c) Minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

## **5.8. Extinção da AC**

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

## **6. CONTROLES TÉCNICOS DE SEGURANÇA**

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

### **6.1. Geração e Instalação do Par de Chaves**

#### **6.1.1. Geração do Par de Chaves**

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

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

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

O par de chaves da AC VALID é gerado em módulo criptográfico de hardware no padrão FIPS 140-2 nível 2 (para a cadeia de certificação V1); FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no DOC-ICP-01.01.

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

**6.1.1.3.** Não se aplica.

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

**6.1.1.5.** Não se aplica.

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

### **6.1.2. Entrega da chave privada à entidade**

Não se aplica.

### **6.1.3. Entrega da chave pública para emissor de certificado**

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

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

### **6.1.4. Entrega de chave pública da AC às terceiras partes**

A AC VALID disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web: (<http://www.validcertificadora.com.br/>)

### **6.1.5. Tamanhos de chave**

**6.1.5.1.** O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC VALID é de 4096 bits. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo da ICP Brasil estão em conformidade com o definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

**6.1.5.2.** Não se aplica.

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

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

**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 [1].

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

**6.1.7.1.** As chaves criptográficas dos titulares de certificados emitidos pela AC VALID (ACs subsequentes) poderão ser utilizadas apenas para assinatura dos certificados por elas emitidos e de suas LCRs.

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

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

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

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

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

**6.2.1. Padrões para módulo criptográfico**

**6.2.1.1.** O módulo criptográfico de geração de chaves assimétricas da AC VALID adota o padrão FIPS 140-2 nível 2 (para a cadeia de certificação V1); FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

**6.2.2. Controle “n de m’ para chave privada**

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



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

### **6.2.3. Recuperação (escrow) de chave privada**

A AC VALID não implementa tal prática.

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

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

**6.2.4.2.** A AC VALID mantém cópia de segurança de sua chave privada.

**6.2.4.3.** A AC VALID, não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC.

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

### **6.2.5. Arquivamento de chave privada**

**6.2.5.1.** A AC VALID não arquivacópias de chaves privadas de titulares de certificados.

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

### **6.2.6. Inserção de chave privada em módulo criptográfico**

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

### **6.2.7. Armazenamento de chave privada em módulo criptográfico**

Ver item 6.1.

### **6.2.8. Método de ativação de chave privada**

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

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

#### **6.2.9. Método de desativação de chave privada**

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

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

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

#### **6.2.10. Método de destruição de chave privada**

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

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

### **6.3. Outros Aspectos do Gerenciamento do Par de Chaves**

#### **6.3.1. Arquivamento de chave pública**

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

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

**6.3.2.1.** As chaves privadas dos titulares dos certificados de assinatura digital emitidos pela AC VALID são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo período de tempo determinado pela legislação aplicável,

para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

**6.3.2.2.** Não se aplica.

**6.3.2.3.** Os certificados emitidos pela AC VALID para as ACs de nível imediatamente subsequente ao seu terão validade de no máximo 8 (oito) anos.

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

## **6.4. Dados de Ativação**

Os dados de ativação da chave privada da AC VALID são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em hardware (token ou cartão criptográfico).

### **6.4.1. Geração e instalação dos dados de ativação**

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

**6.4.1.2.** Não se aplica.

### **6.4.2. Proteção dos dados de ativação.**

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

**6.4.2.2.** Não se aplica.

### **6.4.3. Outros aspectos dos dados de ativação**

Não se aplica.

## **6.5. Controles de Segurança Computacional**

### **6.5.1. Requisitos técnicos específicos de segurança computacional**

**6.5.1.1.** A geração do par de chaves da AC VALID é realizada em ambiente próprio para a condução de Cerimônia de Geração de Chaves. O ambiente computacional é mantido off-line de modo a impedir o acesso remoto não autorizado.

**6.5.1.2.** Os requisitos gerais de segurança computacional dos equipamentos utilizados para a geração dos pares de chaves criptográficas das ACs titulares de certificados emitidos pela AC VALID devem ser os mesmos descritos no item abaixo para os computadores servidores da AC VALID.

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

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

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

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

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

## **6.5.2. Classificação da segurança computacional**

A segurança computacional da AC VALID segue as recomendações *Common Criteria*.

### **6.5.3. Controle de segurança para as Autoridades de Registro**

**6.5.3.1.** Neste item estão descritos os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas AR para os processos de validação e aprovação de certificados.

**6.5.3.2.** Os requisitos abaixo correspondem aos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]:

- a) Controle de acesso lógico ao sistema operacional;
- b) Exigência de uso de senhas fortes;
- c) Diretivas de senha e de bloqueio de conta;
- d) Logs de auditoria do sistema operacional ativados, registrando:
  - I. Iniciação e desligamento do sistema;
  - II. Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;
  - III. Mudanças na configuração da estação;
  - IV. Tentativas de acesso (login) e de saída do sistema (logout);
  - V. Tentativas não autorizadas de acesso aos arquivos de sistema;
  - VI. Tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.
- e) Antivírus, antitrojan e *antispyware*, instalados, atualizados e habilitados;
- f) Firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo;
- g) Proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;
- h) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
- i) Utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;
- j) Impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
- k) Utilização de data e hora de Fonte Confiável do Tempo (FCT).

**6.5.3.3** Não se aplica.

---

## **6.6. Controles Técnicos do Ciclo de Vida**

### **6.6.1. Controles de desenvolvimento de sistemas**

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

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

### **6.6.2. Controle de gerenciamento de segurança**

**6.6.2.1.** A AC VALID verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

**6.6.2.2.** Uma metodologia formal de gerenciamento de configuração é usada para a instalação e a contínua manutenção do sistema de certificação da AC

### **6.6.3. Classificação de segurança de ciclo de vida**

Não se aplica.

### **6.6.4. Controles na Geração de LCR**

Antes de publicadas, todas as LCRs geradas pela AC VALID 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 VALID, incluindo firewalls e recursos similares.

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

**6.7.1.3.** Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls, e sistemas de detecção de intrusos (IDS), localizados no segmento de rede que hospeda o sistema de certificação estão localizados e operam em ambiente de nível 4.

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

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

## **6.7.2. Firewall**

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

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

## **6.7.3. Sistema de detecção de intrusão (IDS)**

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

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

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

#### 6.7.4. Registro de acessos não-autorizados à rede

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

#### 6.8. Carimbo de Tempo

Não se aplica.

### 7. PERFIS DE CERTIFICADO, LCR E OCSP

#### 7.1. Perfil do Certificado

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

##### 7.1.1. Número de versão

Os certificados emitidos pela AC VALID implementam 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 VALID, sob esta DPC, obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

- a) “Authority Key Identifier”, não crítica: o campo keyIdentifier contém o resumo (hash) SHA-1 da chave pública da AC VALID;
- b) “Subject Key Identifier”, não crítica: contém o hash da chave pública da AC titular do certificado;
- c) “Key Usage”, crítica: somente os bits e keyCertSign e cRLSign são ativados;
- d) “Certificate Policies”, não crítica:
  - d.1) o campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;
  - d.2) o campo policyQualifiers contém o endereço URL da página web onde se obtém a DPC da AC VALID: <http://icp-brasil.validcertificadora.com.br/ac-valid/dpc-ac-validv5.pdf>
- e) basicConstraints, crítica: contém o campo CA=True; e
- f) “CRL Distribution Points”, não crítica: contém os endereços URL das duas páginas web onde se obtém a LCR da AC VALID:

#### ***Para Certificados da cadeia V2:***



- f.1 <http://icp-brasil.validcertificadora.com.br/ac-valid/lcr-ac-validv2.crj>;
- f.2 <http://icp-brasil2.validcertificadora.com.br/ac-valid/lcr-ac-validv2.crj>;
- f.3 <http://repositorio.icpbrasil.gov.br/lcr/valid/lcr-ac-validv2.crj>;

**Para Certificados da cadeia V5:**

- f.1 <http://icp-brasil.validcertificadora.com.br/ac-valid/lcr-ac-validv5.crj>;
- f.2 <http://icp-brasil2.validcertificadora.com.br/ac-valid/lcr-ac-validv5.crj>.

- g) "Authority Information Access", não crítica, contendo o endereço na Web onde se obtém o arquivo p7b com os certificados da cadeia:

**Para Certificados da cadeia V2:**

<http://icp-brasil.validcertificadora.com.br/ac-valid/ac-validv2.p7b>

**Para Certificados da cadeia V5:**

<http://icp-brasil.validcertificadora.com.br/ac-valid/ac-validv5.p7b>

### 7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC VALID são assinados com o uso do algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [9].

### 7.1.4. Formatos de nome

**7.1.4.1.** Para os certificados emitidos sob a DPC AC VALID, o nome da AC titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

**C**=BR

**O**= ICP-Brasil

**OU**= nome da AC emitente

**CN**= nome da AC titular

O CN deverá estar na forma "AC < nome da AC titular>

No formato os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

### 7.1.5. Restrições de nome

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

- a) não serão utilizados sinais de acentuação, tremas ou cedilhas;  
b) além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

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

---

### 7.1.6. OID (*Object Identifier*) da DPC

O OID desta DPC é 2.16.76.1.1.43.

### 7.1.7. Uso da extensão “*Policy Constraints*”

A extensão “Policy Constraints” poderá ser utilizada, da forma definida na RFC 5280, em certificados emitidos pela AC VALID.

### 7.1.8. Sintaxe e semântica dos qualificadores de política

O campo `policyQualifiers` da extensão "Certificate Policies" contém o endereço web da DPC da AC VALID.

### 7.1.9. Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

## 7.2. Perfil de LCR

### 7.2.1. Número(s) de versão

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

### 7.2.2. Extensões de LCR e de suas entradas

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

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

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

## 7.3. Perfil de OCSP

Não se aplica.

---

## 8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

### 8.1. Frequência e circunstâncias das avaliações

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

### 8.2. Identificação / Qualificação do avaliador

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

**8.2.2.** Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas por empresas de auditoria independentes credenciadas pela AC Raiz, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

### 8.3. Relação do avaliador com a entidade avaliada

As auditorias das entidades integrantes da ICP-Brasil são realizadas por empresas de auditoria independentes credenciadas pela AC Raiz, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

### 8.4. Tópicos cobertos pela avaliação

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

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

**8.4.3.** As entidades da ICP-Brasil diretamente vinculadas à AC VALID (AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC

VALID é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

### **8.5. Ações tomadas como resultado de uma deficiência**

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

### **8.6. Comunicação dos resultados**

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

## **9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS**

### **9.1. Tarifas**

#### **9.1.1. Tarifas de emissão e renovação de certificados**

Variável conforme definição interna Comercial.

#### **9.1.2. Tarifas de acesso ao certificado**

Não são cobradas tarifas de acesso ao certificado digital emitido.

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

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

#### **9.1.4. Tarifas para outros serviços**

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

#### **9.1.5. Política de reembolso**

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

---

## **9.2. Responsabilidade Financeira**

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

### **9.2.1 Cobertura do seguro**

Conforme item 4 desta DPC.

### **9.2.2 Outros ativos**

Conforme regramento desta DPC.

### **9.2.3 Cobertura de seguros ou garantia para entidades finais**

Conforme item 4 desta DPC.

## **9.3 Confidencialidade da informação do negócio**

### **9.3.1 Escopo de informações confidenciais**

**9.3.1.1.** Neste item são identificados os tipos de informações consideradas sigilosas pela AC VALID e pela sua AR, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil

**9.3.1.2.** Como princípio geral, nenhum documento, informação ou registro fornecido à AC VALID ou à sua AR Vinculada deve ser divulgado.

### **9.3.2. Informações fora do escopo de informações confidenciais**

As informações consideradas não sigilosas compreendem:

- a) Os certificados e a LCR emitidos pela AC VALID;
- b) Informações corporativas ou pessoais que façam parte de certificados ou em diretórios públicos;
- c) Não se aplica;
- d) Esta DPC;
- e) Versões públicas da Política de Segurança;
- f) Resultados finais de auditorias; e
- g) Termo de Titularidade ou solicitação de emissão do certificado.

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

- a) Estejam na posse legítima da AC VALID ou da AR a ela vinculada antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;

- b) Posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro(s) com direitos legítimos para divulgação sua sem quaisquer restrições para tal;
- c) Sejam requisitados por determinação judicial ou governamental, desde que a AC VALID ou a AR a ela vinculada comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

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

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

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

- a) Não se aplica;
- b) Qualquer DPC;
- c) Versões públicas de Política de Segurança – PS; e
- d) A conclusão dos relatórios da auditoria.

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

### **9.3.3 Responsabilidade em proteger a informação confidencial**

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

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

**9.3.3.3.** Os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos 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 VALID assegurará a proteção de dados pessoais conforme sua Política de Privacidade.

### **9.4.2 Tratamento de informação como privadas**

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

### **9.4.3 Informações não consideradas privadas**

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

### **9.4.4 Responsabilidade para proteger a informação privadas**

A AC VALID 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**

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

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

Autorizações formais podem ser apresentadas de duas formas:

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

### **9.4.6. Divulgação em processo judicial ou administrativo**

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



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

#### **9.4.7. Outras circunstâncias de divulgação de informação**

Não se aplica.

#### **9.4.8. Informações a terceiros**

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

#### **9.5. Direitos de Propriedade Intelectual**

De acordo com a legislação vigente.

#### **9.6. Declarações e Garantias**

##### **9.6.1 Declarações e Garantias da AC**

A AC VALID declara e garante o quanto segue:

##### **9.6.1.1 Autorização para certificado**

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

##### **9.6.1.2. Precisão da informação**

A AC VALID 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 ARs na forma de suas DPCs, PCs e normas complementares.

##### **9.6.1.3. Identificação do requerente**

A AC VALID implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC VALID,

no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das ARs na forma de suas DPCs, PCs, e normas complementares.

#### **9.6.1.4. Consentimento dos titulares**

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

#### **9.6.1.5. Serviço**

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

#### **9.6.1.6. Revogação**

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

#### **9.6.1.7. Existência Legal**

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

### **9.6.2. Declarações e Garantias da AR**

Em acordo com item 4 desta DPC.

### **9.6.3. Declarações e garantias do titular**

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

**9.6.3.2.** A AC VALID deve informar à AC Raiz qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

### **9.6.4. Declarações e garantias das terceiras partes**

**9.6.4.1.** As terceiras partes devem:

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

**9.6.4.2.** O certificado da AC VALID é considerado válido quando:

- I. Tiver sido emitido pela AC;

- II. Não constar como revogado pela AC;
- III. Não estiver expirado; e
- IV. Puder ser verificado com o uso do certificado válido da AC.

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

#### **9.6.5. Representações e garantias de outros participantes**

Não se aplica.

#### **9.7. Isenção de garantias**

Não se aplica.

#### **9.8. Limitações de responsabilidades**

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

#### **9.10. Prazo e Rescisão**

##### **9.10.1. Prazo**

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

##### **9.10.2. Término**

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

##### **9.10.3. Efeito da rescisão e sobrevivência**

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

---

## **9.11. Avisos individuais e comunicações com os participantes**

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

## **9.12. Alterações**

### **9.12.1. Procedimento para emendas**

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

### **9.12.2. Mecanismo de notificação e períodos**

A AC VALID mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web (<http://icp-brasil.validcertificadora.com.br/ac-valid/dpc-ac-validv5.pdf>)

### **9.12.3. Circunstâncias na qual o OID deve ser alterado**

Não se aplica.

## **9.13. Solução de conflitos**

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

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

## **9.14. Lei aplicável**

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

## **9.15. Conformidade com a Lei aplicável**

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

## 9.16. Disposições Diversas

### 9.16.1. Acordo completo

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

### 9.16.2. Cessão

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

### 9.16.3. Independência de disposições

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

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

De acordo com a legislação vigente.

## 9.17. Outras provisões

Não se aplica.

## 10. DOCUMENTOS REFERENCIADOS

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA 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
[9]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[13]	POLÍTICA TARIFARIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[4]	TERMO DE TITULARIDADE	ADE-ICP-05.B

## 11. REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

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

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

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

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

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