



# **Declaração de Práticas de Certificação DPC**

**Autoridade Certificadora VALID CODESIGNING**

**OID 2.16.76.1.1.145**

## Sumário

1. INTRODUÇÃO .....	12
1.1. Visão Geral .....	12
1.2. Nome do documento e identificação .....	12
1.3. Participantes da ICP-Brasil.....	13
1.3.1 Autoridades Certificadoras.....	13
1.3.2. Autoridade de Registro.....	13
1.3.3 Titulares de Certificado .....	13
1.3.4 Partes Confiáveis .....	13
1.3.5 Outros Participantes.....	13
1.4 Usabilidade do Certificado .....	14
1.4.1 Uso apropriado do certificado .....	14
1.4.2 Uso proibitivo do certificado .....	14
1.5 Política de Administração.....	14
1.5.1 Organização administrativa do documento .....	14
1.5.2 Contatos .....	14
1.5.3 Pessoa que determina a adequabilidade da DPC com a PC .....	14
1.5.4 Procedimentos de aprovação da DPC .....	14
1.6 Definições e Acrônimos .....	15
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO .....	17
2.1 Repositórios .....	17
2.2 Publicação de informações dos certificados .....	17
2.3 Tempo ou Frequência de Publicação .....	17
2.4. Controle de Acesso aos Repositórios .....	18
3 IDENTIFICAÇÃO E AUTENTICAÇÃO .....	18
3.1 Atribuição de Nomes.....	18
3.1.1 Tipos de nomes .....	18
3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado .....	18
3.1.4 Regras para interpretação de vários tipos de nomes .....	18
3.1.5. Unicidade de nomes.....	18
3.1.6 Procedimento para resolver disputa de nomes .....	18
3.1.7. Reconhecimento, autenticação e papel de marcas registradas .....	18
3.2 Validação inicial de identidade .....	18
3.2.1 Método para comprovar o controle de chave privada .....	19

3.2.2 Autenticação da identificação da organização.....	19
3.2.2.2 Documentos para efeitos de identificação de uma organização .....	20
3.2.2.3 Informações contidas no certificado emitido para uma organização.....	20
3.2.3 Autenticação da identidade de um indivíduo .....	20
3.2.3.1 Documentos para efeitos de identificação de um indivíduo.....	21
3.2.4 Informações não verificadas do titular do certificado .....	22
3.2.5 Validação das autoridades .....	22
3.2.6 Critérios para interoperação .....	22
3.2.7 Autenticação da identidade de equipamento ou aplicação.....	22
3.2.8 Procedimentos complementares .....	23
3.2.9 Procedimentos específicos.....	24
3.3 Identificação e autenticação para pedidos de novas chaves .....	24
3.3.1 Identificação e autenticação para rotina de novas chaves antes da expiração .....	24
3.3.2. Identificação e autenticação para novas chaves após a revogação.....	25
3.4 Identificação e Autenticação para solicitação de 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
4.1.2.1 Responsabilidades da AC.....	26
4.1.2.2 Obrigações da AC .....	27
4.1.2.3 Responsabilidades da AR.....	28
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 .....	29
4.3. Emissão de Certificado .....	29
4.3.1 Ações da AC durante a emissão de um 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.....	29
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
4.5.1.2 Obrigações do Titular do Certificado.....	30

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis .....	30
4.6. Renovação de Certificados .....	30
4.6.1 Circunstâncias para renovação de certificados .....	30
4.6.2 Quem pode solicitar a renovação .....	30
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
4.6.7 Notificação de emissão de certificado pela AC para outras entidades .....	31
4.6.6 Publicação de uma renovação de um certificado pela AC.....	31
4.7 Nova chave de certificado (Re-key).....	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 .....	31
4.7.5 Conduta constituindo a aceitação de uma nova chave certificada.....	31
4.7.6 Publicação de uma nova chave certificada pela AC .....	31
4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades.....	31
4.8 Modificação de certificado .....	31
4.8.1 Circunstâncias para modificação de certificado.....	31
4.8.2 Quem pode requisitar a modificação de certificado.....	31
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.....	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.....	32
4.9 Suspensão e Revogação de Certificado.....	32
4.9.1 Circunstâncias para revogação .....	32

4.9.2. Quem pode solicitar revogação.....	35
4.9.3. Procedimento para solicitação de revogação .....	35
4.9.4. Prazo para solicitação de revogação .....	36
4.9.5. Tempo em que a AC deve processar o pedido de revogação .....	36
4.9.6 Requisitos de verificação de revogação para as partes confiáveis.....	36
4.9.7 Frequência de emissão de LCR.....	36
4.9.10. Requisitos para verificação de revogação on-line .....	37
4.9.11. Outras formas disponíveis para divulgação de revogação .....	37
4.9.12. Requisitos especiais para o caso de comprometimento de chave.....	37
4.9.13. Circunstâncias para suspensão.....	37
4.9.14. Quem pode solicitar suspensão .....	37
4.9.15. Procedimento para solicitação de suspensão .....	37
4.9.16. Limites no período de suspensão .....	37
4.10. Serviços de status de certificado .....	38
4.10.2. Disponibilidade dos serviços .....	38
4.10.3 Funcionalidades operacionais .....	38
4.11 Encerramento de atividades .....	38
4.12. Custódia e recuperação de chave.....	39
5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAS.....	39
5.1. CONTROLE FÍSICO.....	39
5.1.1. Construção e localização das instalações.....	39
5.1.2. Acesso físico .....	40
5.1.2.1 Níveis de Acesso .....	40
5.1.3. Energia e ar condicionado.....	42
5.1.4. Exposição à água .....	43
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> ).....	43
5.1.9. Instalações Técnicas de AR.....	44
5.2. CONTROLES PROCEDIMENTAIS.....	44
5.2.1. Perfis qualificados .....	44
5.2.2. Número de pessoas necessário por tarefa.....	45
5.2.3. Identificação e autenticação para cada perfil .....	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.....	48
5.3.8. Documentação disponibilizada 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 .....	49
5.4.4. Proteção de Registros de Auditoria.....	49
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 .....	50
5.5. Arquivamento de Registros .....	50
5.5.1. Tipos de Registros Arquivados .....	50
5.5.2. Período de Retenção para Arquivo .....	50
5.5.3. Proteção de Arquivo.....	51
5.5.4. Procedimentos de cópia de arquivo.....	51
5.5.5. Requisitos para Datação de Registros .....	51
5.5.6. Sistema de Coleta de Dados de Arquivo (Interno e Externo) .....	51
5.5.7. Procedimentos para Obter e Verificar Informação de Arquivo.....	51
5.6. Troca de Chave .....	51
5.7. Comprometimento e Recuperação de Desastre .....	51
5.7.1. Procedimentos de Gerenciamento de Incidente e Comprometimento.....	52
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 .....	55
6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES.....	55
6.1.1. Geração do Par de Chaves.....	55

6.1.2. Entrega da chave privada à entidade titular .....	56
6.1.3. Entrega da chave pública para emissor de certificado .....	56
6.1.4. Disponibilização de chave pública da AC VALID CODESIGNING para usuários .....	56
6.1.5. Tamanhos de chave .....	56
6.1.6. Geração de parâmetros de chaves assimétricas .....	56
6.1.7. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3) .....	57
6.2. PROTEÇÃO DA CHAVE PRIVADA .....	57
6.2.1. Padrões para módulo criptográfico .....	57
6.2.2. Controle “n de m’ para chave privada .....	57
6.2.3. Recuperação (escrow) de chave privada .....	57
6.2.4. Cópia de segurança (backup) de chave privada .....	58
6.2.5. Arquivamento de chave privada .....	58
6.2.6. Inserção de chave privada em módulo criptográfico .....	58
6.2.7. Armazenamento de chave privada em módulo criptográfico .....	58
6.2.8. Método de ativação de chave privada .....	58
6.2.9. Método de desativação de chave privada .....	58
6.2.10. Método de desativação de chave privada .....	58
6.2.11. Método de destruição de chave privada .....	59
6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES .....	59
6.3.1. Arquivamento de chave pública .....	59
6.3.2. Períodos de uso para as chaves pública e privada .....	59
6.4. DADOS DE ATIVAÇÃO .....	60
6.4.1. Geração e instalação dos dados de ativação .....	60
6.4.2. Proteção dos dados de ativação .....	60
6.4.3. Outros aspectos dos dados de ativação .....	60
6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL .....	60
6.5.1. Requisitos técnicos específicos de segurança computacional .....	60
6.5.2. Classificação da segurança computacional .....	61
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 .....	63
6.6.4. Controles na Geração de LCR .....	63
6.7. CONTROLES DE SEGURANÇA DE REDE .....	63

6.7.1. Diretrizes Gerais .....	63
6.7.2. Firewall .....	63
6.7.3. Sistema de detecção de intrusão (IDS).....	64
6.7.4. Registro de acessos não autorizados à rede .....	64
6.8. Carimbo de Tempo.....	64
7.PERFIL DO CERTIFICADO, LCR e OCSP .....	64
7.1 Perfil do Certificado.....	64
7.1.1. Número(s) de versão.....	64
7.1.2. Extensões de certificados.....	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 (Object Identifier) de DPC .....	66
7.1.7. Uso da extensão “Policy Constraints” .....	66
7.1.8. Sintaxe e semântica dos qualificadores de política.....	67
7.1.9. Semântica de processamento para extensões críticas.....	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
7.3.1. Número(s) de versão.....	67
7.3.2. Extensões 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 .....	69
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
9.4.4 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
9.6.1.1 Autorização para certificado .....	73
9.6.1.2 Precisão da informação .....	73
9.6.1.4 Consentimento dos titulares .....	73
9.6.1.5 Serviço .....	73
9.6.1.6 Revogação .....	73
9.6.1.7 Existência Legal .....	73
9.6.2 Declarações e Garantias da AR .....	73
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 .....	74
9.7 Isenção de garantias .....	74
9.8 Limitações de responsabilidades .....	74
9.9 Indenizações .....	74
9.10 Prazo e Rescisão .....	74
9.10.1 Prazo .....	74
9.10.2 Término .....	74

9.10.3 Efeito da rescisão e sobrevivência .....	75
9.11 Avisos individuais e comunicações com os participantes .....	75
9.12. Alterações.....	75
9.12.1. Procedimento para emendas .....	75
9.12.2. Mecanismo de notificação e períodos .....	75
9.12.3. Circunstâncias na qual o OID deve ser alterado.....	75
9.13. Solução de conflitos .....	75
9.14. Lei aplicável .....	75
9.15. Conformidade com a Lei aplicável .....	75
9.16. Disposições Diversas .....	75
9.16.1. Acordo completo.....	75
9.16.2. Cessão .....	75
9.16.3. Independência de disposições .....	75
9.16.4. Execução (honorários dos advogados e renúncia de direitos).....	76
9.17. Outras provisões .....	76
10. DOCUMENTOS REFERENCIADOS .....	76

**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>1.0</b>	14/10/2019	Resolução n. 151	Não se aplica	Criação da Declaração de Práticas de Certificação (DPC) AC VALID CODESIGNING
<b>1.0</b>	23/07/2020	Adequação	-	Criação da Declaração de Práticas de Certificação (DPC) AC VALID CODESIGNING
<b>1.1</b>	15/09/2020	Adequação	-	Ajustes na Declaração de Práticas de Certificação (DPC) AC VALID CODESIGNING
<b>1.2</b>	07/10/2020	Adequação	-	Ajustes na Declaração de Práticas de Certificação (DPC) AC VALID CODESIGNING
<b>1.2</b>	14/01/2021	N/A	-	1.1.3 – inclusão de referência aos documentos CAB/Forum. 1.5.2 – Inclusão de contatos para Revogação de Certificados e Relatos de Problemas de Certificados. 2.2.1 – Inclusão de referência à verificação de registros CAA antes da emissão. 2.2.2 Inclusão de referências às paginas de publicação de modelos de certificados válidos, expirados e revogados. 4.1 Exclusão da modalidade de validação online para certificados SSL EV.4.9.9. Inclusão de informações sobre consulta OCSP.
<b>2.0</b>	02/03/2021	Resolução nº177 e 181	Diversos - 3.2.3.1 e 3.2.3.1.8	Adequação para atender as resoluções
<b>3.0</b>	22/02/2022	Resoluções 196 e 197	Diversos	Adequação para atender as resoluções.

4.0	10/10/2022	Resolução 204	1.6 e 4.5.1.2	Adequação para atender à 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. Este documento estabelece os requisitos mínimos, observados obrigatoriamente pela Autoridade Certificadora VALID CODESIGNING, a AC VALID CODESIGNING integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação - DPC. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução dos seus serviços.

1.1.2. Toda DPC elaborada no âmbito da ICP-Brasil adota obrigatoriamente a mesma estrutura empregada no documento “REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [4]”. As informações sobre a administração e geração dos tipos de certificados emitidos pela AC VALID CODESIGNING , são apresentados nas Políticas de Certificado (PCs) que podem ser consultadas no endereço eletrônico: <https://www.validcertificadora.com.br/index.aspx?did=496>

1.1.3. A AC VALID CODESIGNING segue as atualizações dos documentos do CA/Browser Forum CODESIGNING Working Group, publicados pelo CA Security Council (CASC) sob o título “Baseline Requirements for the Issuance and Management of Publicly-Trusted CODESIGNING Certificates”[4] ([https://cabforum.org/wp-content/uploads/baseline\\_requirements\\_for\\_the\\_issuance\\_and\\_management\\_of\\_code\\_signing.v.2.1.pdf](https://cabforum.org/wp-content/uploads/baseline_requirements_for_the_issuance_and_management_of_code_signing.v.2.1.pdf)) No caso de qualquer inconsistência entre esse documento e os requisitos do CA/Browser Fórum, estes terão precedência sobre o documento.

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

1.1.5. A AC VALID CODESIGNING 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 Este documento denominado “Declaração de Práticas de Certificação da Autoridade Certificadora VALID CODESIGNING” (DPC), comumente referido como “DPC da AC VALID CODESIGNING” identifica procedimentos e práticas empregados no âmbito da ICP-Brasil. O OID (*Object Identifier*) atribuído à esta DPC é o **2.16.76.1.1.145**.

1.2.2 A AC VALID CODESIGNING emissora de certificados para usuários finais é exclusiva e separada de acordo com o propósito de uso de chaves assinatura de código (CODESIGNING).

1.2.3 Os Certificados emitidos pela AC VALID CODESIGNING destinam-se para ser usados para verificar a identidade do titular do certificado (Assinante) e a integridade de seu código. Eles fornecem garantia a um usuário ou provedor de plataforma que o código verificado com o certificado não foi modificado de sua forma original e é distribuído pela entidade legal identificada no certificado de assinatura de código por nome, endereço da empresa, jurisdição de incorporação ou registro e outros informação. Certificados

de assinatura de código podem ajudar a estabelecer a legitimidade do código assinado, ajudar a manter a confiabilidade das plataformas de software, ajuda os usuários a fazer escolhas informadas de software e limita a disseminação de malware.

### **1.3. Participantes da ICP-Brasil**

#### **1.3.1 Autoridades Certificadoras**

Esta DPC refere-se unicamente à AC VALID CODESIGNING , (Avenida Paulista, nº 2064, 15º andar, São Paulo/SP, CEP: 01310-928 sob CNPJ 14.121.957/0001/09), no âmbito da ICP-Brasil, encontra se publicada no seu repositório no seguinte endereço: <https://www.validcertificadora.com.br/index.aspx?did=496>

#### **1.3.2. Autoridade de Registro**

1.3.2.1. No endereço eletrônico <https://www.validcertificadora.com.br/index.aspx?did=496> a Autoridade de Registro (AR) vinculada à AC VALID CODESIGNING, esta responsável nas competências dos processos de recebimento, validação e encaminhamento das solicitações de emissão e revogação dos certificados digitais e na identificação dos seus solicitantes:

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

#### **1.3.3 Titulares de Certificado**

Pessoas físicas ou jurídicas, de direito público ou privado, nacionais ou estrangeiras, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis, podem ser Titulares de Certificado. Os certificados podem ser utilizados por pessoas físicas, pessoas jurídicas.

Em sendo o titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada. Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

#### **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. No endereço eletrônico (<https://www.validcertificadora.com.br/index.aspx?diD=496>) constam 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 CODESIGNING.

1.3.5.2. Outros grupos que participaram do desenvolvimento dos requisitos do Cab/Browser Fórum [15] incluem a AICPA / CICA, que é a força-tarefa do WebTrust for AC e a ETSI ESI. A participação de tais grupos não implica endosso, recomendação ou aprovação do produto final.

### **1.4 Usabilidade do Certificado**

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

A AC VALID CODESIGNING implementa as seguintes Políticas de Certificado Digital:

POLÍTICA DE CERTIFICADO	NOME	OID
Política de Certificado de Assinatura Digital do tipo A1 da AC VALID CODESIGNING	PC A1 da AC VALID CODESIGNING	2.16.76.1.2.1.111
Política de Certificado de Assinatura Digital do tipo A3 da AC VALID CODESIGNING	PC A3 da AC VALID CODESIGNING	2.16.76.1.2.3.105

#### 1.4.2 Uso proibitivo do certificado

Este item, quando cabível, as aplicações para as quais existem restrições ou proibições para o uso desses certificados.

### 1.5 Política de Administração

#### 1.5.1 Organização administrativa do documento

AC VALID CODESIGNING

#### 1.5.2 Contatos

Endereço: Alameda Rio Claro, 241 - Bela Vista - São Paulo, SP - CEP: 01332-010

Telefone: +55 11 2575-6800

Página da Web: <https://www.validcertificadora.com.br/index.aspx?did=496>

Para os casos de Revogação do Certificado, conforme disposto no procedimento interno "Manual de Revogação e Suporte dos Certificados SSL e Codesigning", o cliente conta com os seguintes contatos para relatar um problema ou solicitar a revogação do certificado digital:

- SAC - 3004-3454 para São Paulo ou 0800 725 4565 para demais localidades, equipe especializada das (8h as 20h);
- Suporte N2 - <https://www.validcertificadora.com.br/>, na aba chat ao vivo, em horário comercial das (8h as 19h) ou a qualquer horário pelo <https://www.validcertificadora.com.br/faleconosco>, temos uma equipe especializada para atendimento destes chamados 24 horas, 7 dias na semana;
- Suporte Comercial SSL/ SSL EV e Codesigning - O cliente poderá entrar em contato com o Consultor Responsável pela venda do certificado SSL / SSL EV ou Codesigning pelo e-mail [comercial@valid.com](mailto:comercial@valid.com)

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

Nome: Kamila Burunsizian Marciano

Área: Normas e Compliance

Telefone: +55 11 2575-6906

+55 11 2575-6978

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

#### 1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

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

<b>SIGLA</b>	<b>DESCRIÇÃO</b>
<b>AC</b>	Autoridade Certificadora
<b>AC Raiz</b>	Autoridade Certificadora Raiz da ICP-Brasil
<b>AGR</b>	Agente de Registro
<b>AR</b>	Autoridades de Registro
<b>CEI</b>	Cadastro Específico do INSS
<b>CG</b>	Comitê Gestor
<b>CN</b>	<i>Common Name</i>
<b>CNE</b>	Carteira Nacional de Estrangeiro
<b>CNPJ</b>	Cadastro Nacional de Pessoas Jurídicas
<b>CPF</b>	Cadastro de Pessoas Físicas
<b>DN</b>	<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 CODESIGNING mantém disponível repositório atendendo as seguintes obrigações:

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

2.1.2. As publicações da AC VALID CODESIGNING podem ser consultadas através do protocolo http. Somente a AC VALID CODESIGNING, 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 CODESIGNING está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7(sete) dias por semana.

2.1.4 A AC VALID CODESIGNING deve disponibilizar 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR/OCSP:

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

## 2.2 Publicação de informações dos certificados

2.2.1 As informações descritas abaixo são publicadas e atualizadas em serviço de diretório e/ou em página web da AC VALID CODESIGNING (<https://www.validcertificadora.com.br/index.aspx?DID=496>) obedecendo as regras e os critérios estabelecidos nesta DPC.

A AC VALID CODESIGNING está em conformidade com a versão atual dos Requisitos de Linha de Base para a Emissão e Gerenciamento de Certificados de confiança pública, publicados no documento “*Baseline Requirements for the Issuance and Management of Publicly-Trusted CODESIGNING Certificates*” [https://cabforum.org/wp-content/uploads/baseline\\_requirements\\_for\\_the\\_issuance\\_and\\_management\\_of\\_code\\_signing.v.2.1.pdf](https://cabforum.org/wp-content/uploads/baseline_requirements_for_the_issuance_and_management_of_code_signing.v.2.1.pdf) No caso de qualquer inconsistência entre este documento e esses requisitos, esses têm precedência sobre este documento.

A disponibilidade das informações publicadas pela AC VALID CODESIGNING 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 CODESIGNING (<https://www.validcertificadora.com.br/index.aspx?did=496>):

- a) seus próprio certificado;
- b) suas LCRs/OCSP;
- c) sua DPC;
- d) as PCs que implementa;
- e) uma relação, regularmente atualizada, contendo a AR vinculada e seu respectivo endereço; e
- f) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.
- g) Links para paginas web separadas com certificados válido, revogado e expirado por ela emitidos para que fornecedores de software ou aplicações realizem testes.
- h) Paginas da Web de teste que permitem que os fornecedores de software aplicativos testem seus softwares com Certificados de Assinante. Essas páginas de teste Web são acessíveis nos seguintes URLs:

- Certificados Válidos: <https://approved.vpki.com.br/>
- Certificados Revogados: <https://revoked.vpki.com.br/>
- Certificados Expirados: <https://expired.vpki.com.br/>

### 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 4.4.9 da PC correspondente;
- c) as versões ou alterações desta DPC e da PC são atualizadas na web site da AC VALID CODESIGNING após aprovação da AC Raiz da ICP-Brasil; e
- d) os endereços das AR vinculadas são atualizadas na *web* site da AC VALID CODESIGNING.

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

A AC VALID CODESIGNING revisa sua DPC pelo menos uma vez ao ano e faz as alterações necessárias para que a operação permaneça precisa, transparente e cumprindo com os requisitos.

A AC VALID CODESIGNING monitora de perto as votações que acontecem no Fórum do CA/Browser (<https://cabforum.org/ballots/>) e as atualizações dos Requisitos e implementações da linha de base, mantendo as operações da AC atualizadas com relação a esses Requisitos em tempo hábil.

### 2.4. Controle de Acesso aos Repositórios

2.4.1. Não há qualquer restrição ao acesso para consulta a esta DPC, à LCR da AC VALID CODESIGNING, às PC implementadas 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 CODESIGNING verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os direitos de propriedade intelectual de terceiros. 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 Não se aplica

#### 3.1.2 Necessidade dos Nomes Serem Significativos

3.1.2.1 Os certificados emitidos pela AC VALID CODESIGNING exigem o uso de nomessignificativos que possibilitam de terminar univocamente a identidade da pessoa ou da organização titular do certificado a que se referem, para a identificação dos titulares dos certificados emitidos.

### **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**

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

### **3.1.6 Procedimento para resolver disputa de nomes**

A AC VALID CODESIGNING 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 deve descrever em detalhes os requisitos e procedimentos utilizados pela AR vinculada à AC VALID CODESIGNING para a realização dos seguintes processos:

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

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

b) emissão do certificado: 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.

### 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. Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

### 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 pela AR vinculada 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 da pessoa física, nos seguintes termos:

- a) apresentação do rol de documentos elencados no item 3.2.2.2;
- b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;
- c) 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 responsável pelo certificado em termo específico para a comparação com o documento de identidade ou contrato social. Nesse caso, o termo manuscrito digitalizado e assinado digitalmente pelo AGR será apensado ao dossiê eletrônico do certificado, podendo o original em papel ser descartado.

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

3.2.2.1.5 O disposto no item 3.2.2.1.3 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**

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

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

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

**3.2.2.4 Responsabilidade decorrente do uso do certificado de uma organização**

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

**3.2.3 Autenticação da identidade de um indivíduo**

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**

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

- a) 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 e a etapa de verificação. As evidências desse processo farão parte do dossiê eletrônico do requerente.

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

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

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

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

3.2.3.1.5 Não se aplica.

3.2.3.1.6. Não se aplica.

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

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

3.2.3.2.1.1. Não se aplica.

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

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

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

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

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

3.2.3.2.3.1 Não se aplica.

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

Não se aplica.

### **3.2.5 Validação das autoridades**

Não se aplica.

### **3.2.6 Critérios para interoperação**

Não se aplica.

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

3.2.7.1 Não se aplica.

#### **3.2.7.2 Informações contidas no certificado emitido para um equipamento ou aplicação**

##### **3.2.7.1. Disposição Gerais.**

Não se aplica.

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

Não se aplica.

##### **3.2.7.3 Autenticação de identificação de equipamento para certificado CF-e-SAT**

Não se aplica.

#### **3.2.7.4 Procedimentos para efeitos de identificação de um equipamento SAT**

Não se aplica.

#### **3.2.7.5 Informações contidas no certificado emitido para um equipamento SAT**

Não se aplica.

#### **3.2.7.6 Autenticação de identificação de equipamentos para certificado OM-BR**

Não se aplica.

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

Não se aplica.

#### **3.2.7.8 Informações contidas no certificado emitido para um equipamento metrológico**

Não se aplica.

### **3.2.8 Procedimentos complementares**

3.2.8.1 A AC VALID CODESIGNING 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, bem como os documentos do CA/Browser Forum aplicáveis.

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

3.2.8.2.1 Não se aplica.

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

3.2.8.3.1 Não se aplica.

3.2.8.3.2. Não se aplica.

3.2.8.3.3 Não se aplica.

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

3.2.8.4.1 Na hipótese de identificação positiva no processo biométrico da ICP-Brasil, fica dispensada a



apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação conforme item 3.2.3.1.

3.2.8.4.2 Não se aplica.

### **3.2.9 Procedimentos específicos**

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 CODESIGNING 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) doção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3;
- b) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;
- c) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido de uma organização, do tipo A3 ou superior, para o qual tenham sido coletados os dados biométricos do responsável pelo certificado, desde que, mantido nessa condição, apresente documento digital verificável por meio de barramento ou aplicação oficial dos entes federativos, que comprove poder de representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;
- d) solicitação por meio eletrônico dada nas alíneas 'b' e 'c', acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação da AC-Raiz ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;
- e) Não se aplica;
- f) Não se aplica.

3.3.2.1 Não se aplica.

3.3.3. Não se aplica.

3.3.4 Não se aplica.

## **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 de uma AC de nível imediatamente subsequente ao da AC Raiz.

O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.9.3. Solicitações de revogação de certificados devem ser registradas.

## 4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

### 4.1 Solicitação do certificado

Neste item são descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC VALID CODESIGNING e pela AR a ela vinculada para as solicitações de emissão de certificado. Esses requisitos e procedimentos compreendem todas as ações necessárias tanto do indivíduo solicitante quanto das AC e AR no processo de solicitação de certificado digital e contemplam:

- a. A comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
- b. O uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados;
- c. Um termo de titularidade assinado pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico ACORDO DE ASSINANTES. Para a emissão de certificados Codesigning somente são realizadas validações presenciais do representante da organização solicitante do certificado; e
- d. Não se aplica.

**Nota 1:** o termo de titularidade para certificados de usuários finais com propósito de uso CS deve seguir o padrão adotado no documento CS Guidelines.

**Nota 2:** na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados SSL, de equipamento, aplicação, codesign 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

A submissão da solicitação deve ser sempre por intermédio da AR.

4.1.1.1. Não se aplica.

4.1.1.2. Não se aplica.

4.1.1.3. Não se aplica.

4.1.1.4. Não se aplica.

#### 4.1.2 Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1. Responsabilidades da AC.

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

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

4.1.2.1.3 Não se aplica.

#### 4.1.2.2 Obrigações da AC

As obrigações da AC VALID CODESIGNING são as abaixo relacionadas:

- a) operar de acordo com a sua DPC e com as PCs que implementa;
- 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 AR a ela vinculadas e de usuários finais;
- h) informar a emissão do certificado ao respectivo solicitante;
- i) revogar os certificados por ela emitidos;
- j) emitir, gerenciar e publicar suas LCRs e, quando aplicável, disponibilizar consulta on-line de situação do certificado (OCSP - *On-line Certificate Status Protocol*);
- k) publicar em sua página web sua DPC e as PCs aprovadas que implementa;
- 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;
- n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
- o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
- t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;
- u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;

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

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

A AR será responsável pelos danos a que der causa.

#### **4.1.2.4 Obrigações das ARs**

As obrigações da AR vinculada à AC VALID CODESIGNING são abaixo relacionadas:

- a) receber solicitações de emissão ou de revogação de certificados;
- b) confirmar a identidade do solicitante e a validade da solicitação;
- c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC VALID CODESIGNING utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1];
- d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC VALID CODESIGNING e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1], bem como Princípios e Critérios WebTrust para AR [5];
- f) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
- g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2 e 3.2.3; e
- h) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios WebTrust para AR [5].

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

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

Não se aplica.

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

4.2.2.1 Não se aplica.

4.2.2.2 A AC VALID CODESIGNING e AR podem, 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 CODESIGNING cumpre os procedimentos determinados na ICP-Brasil. Não haverá tempo máximo para processar as solicitações na ICP-Brasil.

### **4.3. Emissão de Certificado**

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

4.3.1.1 A emissão de certificado depende do correto preenchimento de formulário de solicitação, da assinatura do “Termo de Titularidade”, no caso de certificados de pessoas jurídicas, ou aplicações e dos demais documentos exigidos. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido e Titular é notificado da emissão e do método para a retirada do certificado.

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

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

O Titular é notificado da emissão e do método para a retirada do certificado.

## **4.4. Aceitação de Certificado**

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

4.4.1.1 O titular do certificado ou pessoa física responsável verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação dele. Ao aceitar o certificado, o titular do certificado:

- a) concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;
- b) garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;
- c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4.1.2 A aceitação de todo certificado emitido é declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

4.4.1.3 Eventuais termos de acordo, ou instrumentos similares, se necessários, são descritos neste item da PC correspondente.

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

O certificado da AC VALID CODESIGNING 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**

O titular do certificado para usuário final emitido pela AC VALID CODESIGNING deve operar de acordo com esta Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) aplicáveis, estabelecidas em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

4.5.1.1 A AC VALID CODESIGNING deve utilizar sua chave privada e garantir a proteção dessa chave

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

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

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

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

#### **4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis**

Em acordo com o item 9.6.4 desta DPC.

#### **4.6. Renovação de Certificados**

Em acordo com item 3.3 desta DPC.

##### **4.6.1 Circunstâncias para renovação de certificados**

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Não se aplica.

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

Em acordo com item 4.3 desta DPC.

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

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

Não se aplica

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

Não se aplica

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

Não se aplica

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

Não se aplica

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

## **4.8 Modificação de certificado**

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

Não se aplica

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

Não se aplica

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

Não se aplica

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

Não se aplica

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

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

O titular e o responsável pelo certificado, a AR ou a AC VALID CODESIGNING pode solicitar a revogação. Além disso, Assinantes, Terceiros de Confiança, Fornecedores de Software de Aplicativos e outros terceiros podem enviar Relatórios de Problemas de Certificado, informando a AC VALID CODESIGNING da causa razoável para revogar o certificado.

4.9.1.1. O titular e o responsável pelo certificado podem solicitar a revogação de seu certificado a qualquer tempo, independentemente de qualquer circunstância.

4.9.1.2. O certificado CODESIGNING deve ser obrigatoriamente revogado:

- a) Quando constatada emissão imprópria ou defeituosa dele;
- b) Quando for necessária a alteração de qualquer informação constante no mesmo;
- c) Não se aplica;
- d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora;

##### **4.9.1.2.1. Revogação com base na solicitação de um fornecedor de aplicativo de software**

Se o Fornecedor de software de aplicativo solicitar a revogação para AC VALID CODESIGNING porque o Fornecedor de Software de Aplicativo acredita que um atributo de certificado é fraudulento ou que o certificado está sendo usado para malware, pacote de mercadorias, software indesejado ou algum outro objetivo ilícito, o fornecedor de software de aplicativo pode solicitar que a AC VALID CODESIGNING revogue o certificado.

Dentro de dois (2) dias úteis após o recebimento da solicitação, a AC VALID CODESIGNING deve revogar o certificado ou informar o fornecedor do software de aplicativo que está conduzindo uma investigação.



Caso a AC VALID CODESIGNING decida conduzir uma investigação, deve informar o fornecedor do software aplicativo revogará ou não o Certificado, dentro de dois (2) dias úteis.

#### 4.9.1.2.2. Revogação com base na solicitação do assinante

A AC VALID CODESIGNING irá revogar um certificado de CODESIGNING dentro de um (1) dia útil se o assinante solicitar por escrito que o certificado será revogado ou notifique a AC que a solicitação do certificado original não foi autorizada e não concede autorização retroativamente.

#### 4.9.1.2.3. Revogação com base em comprometimento relatado ou detectado ou uso em malware

Para todos os incidentes envolvendo malware, as autoridades de certificação revogarão o certificado de assinatura de código de acordo com e dentro dos seguintes prazos máximos. Não há impeditivo caso a AC VALID CODESIGNING decida revogar o certificado antes dos prazos previstos.

A AC VALID CODESIGNING entra em contato com o editor do software dentro de um (1) dia útil após o incidente.

- 1) A AC VALID CODESIGNING informa o volume de terceiros confiáveis que são impactados (por exemplo, com base nos logs do OCSP) dentro de 72 horas após serem informados do incidente.
- 2) A AC VALID CODESIGNING solicita que o editor do software envie uma confirmação para a AC dentro de 72 horas após o recebimento da solicitação
  - a. Se o editor responder dentro de 72 horas, a AC VALID CODESIGNING e o editor determinam uma "data razoável" para revogar o certificado com base em discussões com a AC VALID CODESIGNING.
  - b. Se a AC VALID CODESIGNING não receber uma resposta, ela deverá notificar o editor que a AC VALID CODESIGNING revogará em 7 dias se nenhuma resposta adicional for recebida.
    - i. Se o editor do software responder dentro de 7 (sete) dias, a AC e o editor determinarão uma "data razoável" para revogar o certificado.
    - ii. Se nenhuma resposta for recebida após 7 dias, a AC VALID CODESIGNING revogará o certificado, exceto se a AC tiver provas documentadas (por exemplo, logs do OCSP) de que isso causará um impacto significativo ao público em geral.

A AC VALID CODESIGNING revogará o certificado após identificar que estava associado ao código suspeito assinado ou a outra conduta fraudulenta ou ilegal fornecerá todas as informações e indicadores de risco relevantes para outras ACs ou grupos do setor. A AC VALID CODESIGNING indica se sua investigação constatou que o Código de Suspeito era um falso positivo ou uma assinatura inadvertida.

#### 4.9.1.2.4 Investigação da AC VALID CODESIGNING

A AC VALID CODESIGNING inicia a análise os relatórios de problemas com certificados dentro de vinte e quatro horas após o recebimento, e decide se a revogação ou outra ação apropriada é justificada com base, pelo menos, nos seguintes critérios:

1. A natureza do problema :(adware, spyware, malware, bug de software etc.),
2. O número de relatórios de problemas com certificados recebidos,
3. A entidade que faz o relatório (por exemplo, uma notificação de uma organização antimalware ou de uma agência de aplicação da lei) e
4. Legislação aplicável.

4.9.1.3. A AC VALID CODESIGNING deve observar ainda que:

- a) A AC VALID CODESIGNING irá 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. Todo certificado deve ter a sua validade verificada, na respectiva LCR ou OCSP, antes de ser utilizado.

4.9.1.4.1 ACs que emitem certificados CS devem suportar requisições OCSP em conformidade com a RFC 6960 e/ou RFC5019 e requisitos do CAB Forum. Para certificados CS, a resposta OCSP deve ter validade mínima de um dia e máxima de uma semana, sendo que a próxima atualização deve estar disponível a cada quatro dias.

4.9.1.4.2 A AC VALID CODESIGNING provê garantias que uma LCR pode ser baixada em não mais do que três segundos por uma linha de telefone analógica, sobre uma condição normal de rede.

4.9.1.5 A autenticidade da LCR/OCSP é confirmada por meio das verificações da assinatura da AC VALID CODESIGNING e do período de validade da LCR/ OCSP.

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

A revogação de um certificado somente poderá ser feita:

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

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

4.9.3.1. Uma solicitação de revogação é necessária para que AR responsável inicie o processo de revogação. O solicitante da revogação habilitado pode solicitar facilmente e a qualquer tempo a revogação de certificado, evitando assim a utilização indevida do certificado.

Instruções para a solicitação de revogação do certificado são obtidas em página web disponibilizada pela AC VALID CODESIGNING ou pela AR Responsável.

A revogação é realizada através de Formulário on-line contendo o motivo da solicitação de revogação mediante o fornecimento de dados e da frase de identificação indicada na solicitação de emissão do

Caso o Titular ou o Responsável no caso de certificados de pessoas jurídicas ou aplicações - não recorde a frase de identificação ou quando a revogação é solicitada diretamente pelo Titular sem a participação do Responsável, o Formulário de revogação é impresso e assinado e entregue na AR Responsável.

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 CODESIGNING;
- c) As justificativas para a revogação de um certificado são registradas;
- d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado e com a atualização do status do certificado na resposta OCSP à base de dados da AC VALID CODESIGNING, quando aplicável.

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

4.9.3.4. Não se aplica.

4.9.3.5. A AC VALID CODESIGNING 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 7 (sete) dias, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa de revogação.

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 CODESIGNING processa a revogação imediatamente após a análise do pedido.

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

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

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

4.9.7.1 A frequência de emissão de LCR referente a certificados de usuários finais pela AC VALID CODESIGNING é de 1 hora.

4.9.7.2 A frequência máxima admitida para a emissão de LCR para os certificados de usuários finais é de

4.9.7.3 Não se aplica.

4.9.7.4 Não se aplica.

4.9.7.5 Para certificados emitidos pela AC VALID CODESIGNING as frequências de emissão de LCR são implementadas e descritas em suas PCs, no item correspondente, em conformidade com os requisitos do CAB Fórum.

4.9.8. Latência máxima para a LCR

A LCR da AC VALID CODESIGNING 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 CODESIGNING suporta os processos de revogação de certificados de forma on-line quando aplicável por força de contratação específica

A AC VALID CODESIGNING suporta verificação da situação de estado de certificados de forma on-line quando aplicável por força de contratação específica.

A verificação da situação de um certificado deverá ser feita diretamente na AC VALID CODESIGNING, por meio do protocolo OCSP (On-line Certificate Status Protocol).

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

Não se aplica.

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

Não se aplica.

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

4.9.12.1. O titular de certificado deve notificar imediatamente, através de solicitação on-line de revogação de certificado, à AR responsável caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.9.12.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente na AR Responsável, assinando formulário de solicitação de revogação, observado o item 4.4.3 desta DPC. Todos os documentos e relatórios relativos são arquivados após a conclusão deste processo.

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

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

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

A AC VALID CODESIGNING 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 das DPC e PCs

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

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

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

4.10.1. Características operacionais A AC VALID CODESIGNING deve fornecer um serviço de status de certificado na forma de um ponto de distribuição da LCR no certificado ou OCSP, 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 credenciamento do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICPBRASIL [6], este item da DPC descreve os requisitos e os procedimentos que são adotados nos casos de extinção ou encerramento dos serviços da AC VALID CODESIGNING, de uma AR, PSS ou PSBios a ela vinculados.

4.11.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC VALID segue os requisitos e procedimentos descritos no documento Plano de Encerramento. Esse plano tem abordagem multidisciplinar envolvendo aspectos de várias áreas da companhia, como jurídico, comercial, técnicos/tecnológicos, entre outros. De acordo com esse plano a AC VALID CODESIGNING:

- a) Comunicará publicamente a extinção dos serviços da AC VALID CODESIGNING, através de publicação em jornal de grande circulação.
- b) Revogará todos os certificados gerados pela AC VALID CODESIGNING nos prazos estipulados nas PC implementadas após a publicação e comunicará às partes afetadas através de mensagem eletrônica.
- c) Extinguirá os serviços de emissão de certificados.
- d) Extinguirá os serviços de revogação, como emissão da LCR e/ou conservação dos serviços de status on-line após a revogação completa de todos os certificados.
- e) Destruirá a chave privada da AC VALID CODESIGNING extinta seguindo o procedimento descrito na DPC Item 6.2.9.
- f) Transferirá os dados e gravações da AC VALID CODESIGNING para a Autoridade Certificadora sucessora, aprovada pela AC Raiz.
- g) Transferirá as chaves públicas dos certificados emitidos pela AC VALID CODESIGNING para serem armazenadas por outra AC aprovada pela AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC VALID CODESIGNING. Caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.
- h) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC VALID CODESIGNING.

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

No caso de falência, extinção da AR ou encerramento das atividades como AR vinculada a AC VALID CODESIGNING a AR deverá seguir os seguintes requisitos e procedimentos:

- a) Comunicará publicamente a extinção dos serviços de AR vinculada AC VALID CODESIGNING, através de publicação em jornal de grande circulação e
- b) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados.

No caso de encerramento das atividades como PSS vinculada a AC VALID CODESIGNING, a AC VALID CODESIGNING, diretamente ou por intermédio da AR, deverá seguir os seguintes requisitos e procedimentos:

- a) Publicará, em sua página web, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso; e
- b) Manterá a guarda de toda a documentação comprobatória em seu poder.

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

4.12.1. Política e práticas de custódia e recuperação de chave A AC VALID CODESIGNING 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 CODESIGNING não executa tais práticas.

### **5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAS**

Nos itens seguintes estão descritos os controles de segurança implementados pela AC VALID CODESIGNING e pela AR vinculadas para executar, de modo seguro, suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros. Os requisitos estipulados no CA/Browser Forum Network(<https://cabforum.org/wp-content/uploads/CA-Browser-Forum-Network-Security-Controlsv1.3.pdf>) estão também incorporados nas descrições a seguir.

#### **5.1. CONTROLE FÍSICO**

Nos itens seguintes estão descritos os controles físicos referentes às instalações que abrigam os sistemas da AC VALID CODESIGNING e instalações da AR vinculadas.

##### **5.1.1. Construção e localização das instalações**

5.1.1.1. A operação da AC VALID CODESIGNING é executada dentro de um ambiente físico seguro em área de instalação altamente protegida. A localização e o sistema de certificação utilizado para a operação da AC VALID CODESIGNING não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Nas instalações da AC VALID CODESIGNING, foram implementados, entre outros, os seguintes controles de segurança física:

- a) instalações de equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, nobreaks, baterias, quadros de distribuição de energia e de telefonia, retificadores, estabilizadores e

b) instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas;

c) iluminação de emergência.

### 5.1.2. Acesso físico

O acesso físico às dependências da AC VALID CODESIGNING é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso. O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes. O sistema de certificação da AC VALID CODESIGNING está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

#### 5.1.2.1 Níveis de Acesso

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

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

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido no ambiente onde estão instalados os equipamentos utilizados na operação da AC VALID CODESIGNING, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *paggers*, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

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

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

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

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

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

5.1.2.1.9. No quarto nível, todas as paredes, o piso e o 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 a chamada sala-cofre - possuem proteção contra interferência eletromagnética externa.

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

5.1.2.1.11. A AC VALID CODESIGNING possui um único ambiente para abrigar os equipamentos de produção *online*, os equipamentos de produção *off-line*, o cofre de armazenamento e os equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

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

5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre obedece às seguintes especificações:

a) é feito em aço;

b) possui tranca com chave.

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

## 5.1.2.2. Sistema físico de detecção

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

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

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. Onde houver, a partir do nível 2, vidros separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado 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, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar de ser satisfeito, ocorre a reativação automática dos sensores de presença.

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

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

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

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

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

5.1.2.4.1. Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC VALID CODESIGNING em emergências. 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 emergências.

### **5.1.3. Energia e ar condicionado**

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

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

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

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

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

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

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

de climatização é independente e tolerante 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 é garantida por meio de:

- a) geradores de porte compatível;
- b) geradores de reserva;
- c) sistemas de “nobreaks” 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. Todas as instalações da AC VALID CODESIGNING possuem sistemas de prevenção contra incêndio. Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

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

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

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

#### **5.1.6. Armazenamento de mídia**

A AC VALID CODESIGNING 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)**

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

### 5.1.9. Instalações Técnicas de AR

As instalações técnicas de AR atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARS DA ICP-BRASIL [1].

## 5.2. CONTROLES PROCEDIMENTAIS

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

### 5.2.1. Perfis qualificados

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

5.2.1.2. A AC VALID CODESIGNING estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as ações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema e atribuídos às seguintes áreas:

- Gerência de Operações Data Center:

#### o 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.

#### o 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;
- 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.

- 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.

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

5.2.1.3.1. A AC VALID CODESIGNING realiza um exame, para emissão de certificados em cadeia do tipo CODESIGNING, nos operadores do sistema de certificação da AC VALID CODESIGNING, de acordo com os princípios e critérios WebTrust aplicáveis.

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

## **5.2.2. Número de pessoas necessário por tarefa**

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC VALID CODESIGNING, 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 CODESIGNING necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da AC VALID CODESIGNING. As demais tarefas da AC poderão ser executadas por um único empregado.

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

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

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

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

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

5.2.3.3. A AC VALID CODESIGNING implementa um padrão de utilização de "senhas fortes", definido em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

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

A AC VALID CODESIGNING deve impor a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

### 5.3. CONTROLES DE PESSOAL

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC VALID CODESIGNING e pela AR vinculada em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Todos os empregados da AC VALID CODESIGNING e da AR VALID, 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 CODESIGNING;
- c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

#### 5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC VALID CODESIGNING envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC VALID CODESIGNING e na Política de Segurança da ICP-Brasil [8].

#### 5.3.2. Procedimentos de Verificação de Antecedentes

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

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

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

#### 5.3.3. Requisitos de treinamento

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

- a) princípios e mecanismos de segurança da AC VALID CODESIGNING e da AR vinculada;
- b) sistema de certificação em uso na AC VALID CODESIGNING;
- c) procedimentos de recuperação de desastres e de continuidade do negócio;
- d) reconhecimento de assinaturas e da validade dos documentos apresentados, na forma dos itens 3.2.2 e 3.2.3; e
- e) ameaças comuns ao processo de verificação de informações (incluindo *phishing* e outras táticas de engenharia social); e
- f) outros assuntos relativos a atividades sob sua responsabilidade.

A VALID CODESIGNING mantém registros desses treinamentos e garante que pessoal da AC VALID CODESIGNING e da AR vinculada, mantenha um nível de habilidade que lhes permita desempenhar essas tarefas de maneira satisfatória.

A AC VALID CODESIGNING documenta que o pessoal da AC VALID CODESIGNING e da AR vinculada possuem as habilidades exigidas para os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.

A AC VALID CODESIGNING exige que todo o pessoal da AC VALID CODESIGNING e da AR vinculada sejam aprovados nos treinamentos fornecidos.

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

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

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

A AC VALID CODESIGNING não implementa rodízio de cargos.

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

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC VALID CODESIGNING suspenderá o seu acesso ao sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima conterà, 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 CODESIGNING 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 AC VALID CODESIGNING e da ICP-Brasil.

#### **5.3.7. Requisitos para contratação de pessoal**

O pessoal da AC VALID CODESIGNING e das AR, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, será contratado conforme o estabelecido nas Política de Segurança da ICP-Brasil [8] e na Política de Segurança da AC VALID CODESIGNING.

### 5.3.8. Documentação disponibilizada ao pessoal

5.3.8.1. A AC VALID CODESIGNING disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas:

- a) esta DPC;
- b) as PC que implementa;
- c) a Política de Segurança da ICP-Brasil;
- d) documentação operacional relativa às suas atividades; e
- e) contratos, normas e políticas relevantes para suas atividades.

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

## 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 CODESIGNING com o objetivo de manter um ambiente seguro.

### 5.4.1. Tipos de Eventos Registrados

5.4.1.1. A AC VALID CODESIGNING 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 CODESIGNING;
- c) Mudanças na configuração dos sistemas AC VALID CODESIGNING ou nas suas chaves;
- d) Mudanças nas políticas de criação de certificados;
- e) Tentativas de acesso (login) e de saída do sistema (logout);
- f) Tentativas não autorizadas de acesso aos arquivos do sistema;
- g) Geração de chaves próprias da AC VALID CODESIGNING 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. A AC VALID CODESIGNING controla rigorosamente sua qualidade de serviço, realizando auto auditorias contínuas contra uma amostra selecionada aleatoriamente de pelo menos 6% (seis por cento) dos certificados de assinatura de código emitidos no período imediatamente após a coleta da última amostra. A análise é realizada mensalmente.

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

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

**5.4.1.3.** As informações registradas pela AC VALID CODESIGNING 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 CODESIGNING é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

**5.4.1.6.** A AC VALID CODESIGNING 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 CODESIGNING 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 CODESIGNING 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 CODESIGNING 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 CODESIGNING, 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 CODESIGNING 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 CODESIGNING 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 CODESIGNING, 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 CODESIGNING, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC VALID CODESIGNING 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 CODESIGNING e pela AR a ela vinculada.

#### **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 CODESIGNING; 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 CODESIGNING estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC VALID CODESIGNING, 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 CODESIGNING 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 CODESIGNING 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 CODESIGNING, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

## **5.6. Troca de Chave**

**5.6.1.** O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico. A AC VALID CODESIGNING fornece novo certificado a usuário final utilizando o mesmo procedimento utilizado para emissão do certificado inicial.

A AC VALID CODESIGNING comunica o titular do certificado, 13 (treze) meses antes da expiração do certificado, junto com instruções para a solicitação de um novo certificado.

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

**5.6.2.** Não se aplica.

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

Nos itens seguintes da DPC estão descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no PCN da AC VALID CODESIGNING, 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 CODESIGNING 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 um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.

A AC VALID CODESIGNING documenta os procedimentos de continuidade de negócios e recuperação de desastre projetados para notificar e proteger os fornecedores, assinantes e terceiros de software de aplicativos no caso de um desastre, comprometimento da segurança ou falha nos negócios. A AC VALID CODESIGNING não é obrigada a divulgar publicamente seus Planos de Continuidade de Negócios, para fins de auditoria a AC divulga, mediante solicitação.

No tratamento constante nos Planos acima deve ser considerado:

- a) comprometimento da chave privada das entidades;
- b) invasão do sistema e da rede interna da entidade;
- c) incidentes de segurança física e lógica;

- d) indisponibilidade da Infraestrutura;
- e) fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de certificados;
- f) comprometimento de controle de segurança em qualquer evento referenciado no PCN;
- g) notificação à comunidade de usuários, se for o caso;
- h) revogação dos certificados afetados, se for o caso; i) procedimentos para interrupção ou suspensão de serviços e investigação;
- j) análise e monitoramento de trilhas de auditoria; e
- k) com o público e com meios de comunicação, se for o caso.

Todo pessoal envolvido com o PCN da AC VALID CODESIGNING deve receber um treinamento específico para poder enfrentar estes incidentes.

5.7.1.2. Os procedimentos previstos no PCN da AR vinculada para recuperação, total ou parcial das atividades da AR, contém as seguintes informações:

- a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;
- b) Identificação e concordância de todas as responsabilidades e procedimentos de emergência;
- c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários;
- d) Documentação dos processos e procedimentos acordados;
- e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;
- f) Teste e atualização dos planos;
- g) Avaliação dos danos;
- h) Estimativa do prazo de retorno;
- i) Notificação do problema à área de Gestão Operacional da AC VALID CODESIGNING; e
- j) Tomada de decisão sobre a declaração ou não da contingência.

Os planos de contingência da AR estão organizados em estrutura hierárquica contendo as seguintes fases:

1. Fraude ou erro no processo de validação e emissão de certificados;
2. Impossibilidade de revogação de certificados pela AR;
3. Fraude ou erro no processo de validação e emissão de certificados; e
4. Impossibilidade de revogação de certificados pela AR.

### **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 CODESIGNING, 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 ele 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 CODESIGNING o Gerente de Segurança, juntamente com a Supervisão de PKI da AC VALID CODESIGNING, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados. A AC VALID CODESIGNING 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 CODESIGNING, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com a Supervisão de PKI da AC VALID CODESIGNING, 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 CODESIGNING 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 CODESIGNING;
- 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

**5.8.1.** O descredenciamento da AC VALID CODESIGNING ocorre em relação a todas as PCs para qual tenha sido credenciada ou em relação a PC específicas. O descredenciamento da AC VALID CODESIGNING para todas as PCs credenciadas enseja a revogação do correspondente certificado e o descredenciamento de todas as entidades que lhe sejam operacionalmente vinculadas.

**5.8.2.** O descredenciamento da AC VALID CODESIGNING, ocorre nas seguintes hipóteses:

- a) quando da expiração do prazo de validade de certificado da AC, sem que haja a emissão de novo certificado para substituí-lo;
- b) quando do descredenciamento da AC de nível imediatamente superior;
- c) quando do descredenciamento de PSS único vinculado, que desempenhe atividades descritas nas DPCs e PCs da AC, de modo a inviabilizar a continuidade de operação da AC, sem que haja a solicitação de credenciamento de novo PSS e sem que a AC passe a desempenhar, ela própria, as atividades antes executadas pelo PSS;

d) a pedido da própria AC, mediante requerimento, em relação às suas atividades;

e) por determinação da AC Raiz, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

**5.8.3.** Em caso de extinção da AC VALID CODESIGNING irá realizar os seguintes processos:

i. as chaves públicas dos certificados por ela emitidos deverão ser armazenadas por outra AC, após aprovação da AC Raiz;

ii. quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas aquela indicada pela AC que encerra as suas atividades;

iii. a AC VALID CODESIGNING transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas; e

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

Conforme DOC ICP 03 V.6.0 - Credenciamento das Entidades Integrantes da ICP-Brasil

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

Nos itens seguintes, a DPC define as medidas de segurança implantadas pela AC VALID CODESIGNING 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 CODESIGNING e pela AR vinculada na execução de suas funções operacionais.

### **6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES**

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

6.1.1.1. O par de chaves criptográficas da AC VALID CODESIGNING é gerado pela própria AC VALID CODESIGNING, 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 CODESIGNING é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC VALID CODESIGNING, treinados para a função.

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

O par de chaves da AC VALID CODESIGNING é gerado em módulo criptográfico de hardware no padrão FIPS 140-2 nível 3 e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V11), conforme definido no DOC-ICP01.01.

Somente os titulares dos certificados emitidos pela AC VALID CODESIGNING geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC VALID CODESIGNING.

6.1.1.3. As PCs implementadas pela AC VALID CODESIGNING definem o meio utilizado para

armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

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

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

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

Item não aplicável. A DPC da AC VALID CODESIGNING informa que a geração e a guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

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

6.1.3.1. Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, a AC VALID CODESIGNING fará uso do padrão PKCS#10, em data e hora previamente estabelecidas pela AC-Raiz da ICP- Brasil.

6.1.3.2. Chaves públicas de usuários finais são entregues à AC VALID CODESIGNING por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC VALID CODESIGNING.

A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital, realizada com a chave privada correspondente à chave pública contida na solicitação.

### **6.1.4. Disponibilização de chave pública da AC VALID CODESIGNING para usuários**

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC VALID CODESIGNING compreendem:

- a) No momento da disponibilização de um certificado para seu titular; usando formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil;
- b) Diretório;
- c) na página *web*: <https://www.validcertificadora.com.br/index.aspx?DID=496>
- d) outros meios seguros aprovados pelo CG da ICP-Brasil.

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

6.1.5.1. Cada PC implementada pela AC VALID CODESIGNING define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.5.2. Não se aplica.

### **6.1.6. Geração de parâmetros de chaves assimétricas**

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

[9].

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

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

6.1.7.1 Os certificados de assinatura emitidos pela AC VALID CODESIGNING têm ativado o bit digitalSignature.

Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC VALID CODESIGNING, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC que implementa.

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

## **6.2. PROTEÇÃO DA CHAVE PRIVADA**

As chaves privadas da AC VALID CODESIGNING são armazenadas de forma cifrada nos mesmos componentes seguros de *hardware* utilizados para sua geração. O acesso a esses componentes é controlado por meio de chave criptográfica de ativação.

A AC VALID CODESIGNING 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 CODESIGNING 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 CODESIGNING, 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 CODESIGNING adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V11) e no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO), 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. Cada PC implementada descreve os padrões do módulo criptográfico a ser utilizado pela entidade titular de certificado.

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

6.2.2.1. A chave criptográfica de ativação do componente seguro de *hardware* que armazena a chave privada da AC VALID CODESIGNING é dividida em 8 (oito) partes e distribuídas por 8 (oito) custodiantes designados pela AC VALID CODESIGNING (m).

6.2.2.2. É necessária a presença de no mínimo 2 (dois) custodiantes (n) para a ativação do componente e a consequente utilização da chave privada.

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

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

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

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

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

6.2.4.3. A AC VALID CODESIGNING não mantém cópia de segurança das chaves privadas de certificado de assinatura digital por ela emitido. Cada PC implementada define os requisitos específicos aplicáveis.

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

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

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

A AC VALID CODESIGNING 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 da AC VALID CODESIGNING é implementada por meio do módulo criptográfico, após identificação dos operadores responsáveis. Esta identificação é realizada por meio de senha e de tokens ou cartões criptográficos, após a identificação de 2 (dois) dos 8 (oito) custodiantes da chave criptográfica de ativação. Os custodiantes da chave de ativação são funcionários indicados pelo representante legal da AC VALID CODESIGNING. Cada PC implementada descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

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

A chave privada da AC VALID CODESIGNING, armazenada em módulo criptográfico é desativada, quando não mais necessária, por meio de mecanismo disponibilizado pelo *software* de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de tokens ou cartões criptográficos, protegidos com senha, após a identificação de 2 (dois) dos 8 (oito) custodiantes da chave criptográfica de ativação.

Quando a chave privada da AC VALID CODESIGNING for desativada, em decorrência de expiração ou revogação, ela deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estiver armazenada, deve ser sobrescrito.

Todas as cópias de segurança da chave privada da AC VALID CODESIGNING e os cartões criptográficos dos



custodiantes serão destruídos. Os agentes autorizados para realizar estas operações são os administradores e os custodiantes das chaves de ativação da AC VALID CODESIGNING.

A chave privativa da AC VALID CODESIGNING, 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 CODESIGNING. 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 CODESIGNING contendo fotografia, nome, e departamento do funcionário.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

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

A Supervisão de PKI da AC VALID CODESIGNING, de posse da chave privada original e suas cópias de segurança a serem destruídas, acompanhado do representante legal da AC VALID CODESIGNING, 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 remanescente sensíveis nessas mídias.

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

Cada PC implementada descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

### **6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES**

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

As chaves públicas da própria AC VALID CODESIGNING e dos titulares dos certificados de assinatura digital por ela emitidos, bem como as LCR emitidas e sistemas de OCSP 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. A chave privada da AC VALID CODESIGNING bem como as chaves privadas dos titulares dos certificados por ela emitidos deverão ser utilizadas apenas durante o período de validade do certificado correspondente. As correspondentes chaves públicas poderão ser utilizadas durante todo o período determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Não se aplica.

6.3.2.3. Cada PC implementada pela AC VALID CODESIGNING define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICPBRASIL [7].

6.3.2.4 A validade admitida para certificados da AC VALID CODESIGNING é limitada à validade do

certificado da AC que o emitiu, desde que mantido o padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

#### **6.4. Dados de ativação**

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

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

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

6.4.1.2. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

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

6.4.2.1. Os dados de ativação das chaves privadas da AC VALID CODESIGNING são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra o uso não autorizado.

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

Item não aplicável.

#### **6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL**

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

6.5.1.1. A AC VALID CODESIGNING garante que a geração de seu par de chaves é realizada em ambiente *seguro*, para impedir o acesso remoto não autorizado.

6.5.1.2. Os requisitos gerais de segurança computacional dos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC VALID CODESIGNING são descritos em cada PC implementada.

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

- a) controle de acesso aos serviços e perfis da AC VALID CODESIGNING;
- b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC VALID CODESIGNING;
- 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 CODESIGNING;
- e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- f) mecanismos para cópias de segurança (*backup*).

6.5.1.4. Essas características são implementadas pelo sistema operacional ou por meio da combinação

deste com o sistema de certificação e com mecanismos de segurança física.

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

6.5.1.6. Equipamento incorporado à AC VALID CODESIGNING é preparado e configurado como previsto na política de segurança implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

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

A AC VALID CODESIGNING aplica configurações de segurança definidas como EAL3, baseadas no Common Criteria e desenvolvidas para o sistema operacional Red Hat Enterprise Linux. O fabricante disponibiliza as atualizações do sistema operacional utilizado nos servidores do Sistema de Certificação Digital da AC VALID CODESIGNING.

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

6.5.3.1. A AC VALID CODESIGNING implementa requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pela AR Vinculada 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 (logoff);
  - 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 antispysware, 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 AGR;

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);

l) equipamentos de coleta biométrica, em atendimento aos padrões da ICP-Brasil; e

m) equipamentos que exijam a identificação biométrica do agente de registro durante a identificação biométrica do requerente do certificado.

**6.5.3.3** Não se aplica.

## **6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA**

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

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

6.6.1.1. A AC VALID CODESIGNING adota sistema de certificação desenvolvido em código aberto; todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após a conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, a gerência de infraestrutura da AC VALID CODESIGNING avalia e decide quando será a implementação no ambiente de produção.

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

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

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

- a) a AC VALID CODESIGNING opera em equipamento fisicamente protegido em ambiente de nível 4;
- b) a administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional e pelos papéis confiados descritos no item 5.2.1.

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

- a) instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;
- b) implantação ou modificação de Autoridades Certificadoras com customizações de certificados, páginas *web*, *scripts* etc.;
- c) implantação de novos procedimentos operacionais relacionados com a plataforma de

- processamento incluindo módulos criptográficos; e
- d) instalação de novos serviços na plataforma de processamento.

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

Item não aplicável.

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

Antes de publicadas todas as LCR geradas pela AC VALID CODESIGNING são cheçadas quanto á consistência de seu conteúdo, comparando-a com o conteúdo esperado em relação ao 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 CODESIGNING, incluindo firewalls e recursos similares.

6.7.1.2. Os servidores do sistema de certificação da AC VALID CODESIGNING, 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 CODESIGNING.

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. PERFIL DO CERTIFICADO, LCR e OCSP**

### **7.1 Perfil do Certificado**

Todos os certificados emitidos pela AC VALID CODESIGNING 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. O conteúdo e perfis dos certificados emitidos nas cadeias CS seguem os estabelecidos nos documentos CS Guidelines.

#### **7.1.1. Número(s) de versão**

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

#### **7.1.2. Extensões de certificados**

Não se aplica.

#### **7.1.3. Identificadores de Algoritmo**

Não se aplica.

#### **7.1.4. Formatos de nome**

Não se aplica.

#### **7.1.5. Restrições de nome**

Não se aplica.

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

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC VALID CODESIGNING após conclusão do processo de seu credenciamento, é **2.16.76.1.1.145**.

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

Item não aplicável

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

Não se aplica.

#### **7.1.9. Semântica de processamento para extensões críticas.**

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 CODESIGNING implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

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

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

7.2.2.2. As LCR da AC VALID CODESIGNING 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 CODESIGNING;

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

### 7.3. Perfil de OCSP

#### 7.3.1. Número (s) de versão

Os serviços de respostas OCSP da AC **VALID** CODESIGNING implementam a versão 1. do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

#### 7.3.2. Extensões de OCSP

Os serviços de respostas OCSP da AC **VALID** CODESIGNING estão em conformidade com a RFC 6960.

## 8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

### 8.1. Frequência e circunstâncias das avaliações

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

### 8.2. Identificação/Qualificação do avaliador

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

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

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

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

#### **8.4. Tópicos cobertos pela avaliação**

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

A auditoria da AC VALID CODESIGNING é realizada por um auditor qualificado. Um auditor qualificado significa uma pessoa singular, Jurídica Entidade, ou grupo de pessoas físicas ou jurídicas que possuam as seguintes qualificações e habilidades:

1. Independência do objeto da auditoria;
2. A capacidade de realizar uma auditoria que atenda aos critérios estabelecidos pela ICP-BRASIL e WebTrust;
3. Emprega indivíduos com conhecimento em tecnologia de Infraestrutura de Chave Pública, ferramentas e técnicas de segurança, auditoria e tecnologia da informação; e
4. Para auditorias realizadas de acordo com o padrão WebTrust) licenciado pelo WebTrust.

A AC VALID CODESIGNING realiza a contratação das auditorias apenas para empresas devidamente credenciadas junto a ICP-BRASIL e WebTrust.

8.4.2. A AC VALID CODESIGNING 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 CODESIGNING (AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC VALID CODESIGNING 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 CODESIGNING 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].

Para os casos de não conformidades durante a auditoria, a AC VALID CODESIGNING elabora um plano de ação, contendo os itens de não conformidade, ação a ser tomada para correção da não conformidade e o prazo para correção.

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

A AC VALID CODESIGNING 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].

A AC VALID CODESIGNING, comunica a AC RAIZ para corrigir as não-conformidades com a legislação ou com as políticas, normas, práticas e regras estabelecidas. Tais regularizações serão comunicadas formalmente.



## **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 CODESIGNING, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC VALID CODESIGNING, será emitido gratuitamente outro certificado em substituição.

### **9.2 Responsabilidade Financeira**

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

#### **9.2.1 Cobertura do seguro**

Conforme item 4 desta DPC.

#### **9.2.2 Outros ativos**

Conforme regramento desta DPC.

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

Conforme item 4 desta DPC.

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

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

9.3.1.1 Como princípio geral, todo documento, informação ou registro fornecido à AC ou às AR é sigiloso.

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

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

As informações consideradas não sigilosas compreendem:

- a) os certificados e a LCR/OCSP emitidos pela AC VALID CODESIGNING;
- b) informações corporativas ou pessoais que façam parte dos certificados ou em diretórios públicos;
- c) a PC correspondente;
- d) esta DPC;
- e) versões públicas da Política de Segurança;

f) resultados de auditorias; e

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

A AC VALID CODESIGNING 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 CODESIGNING 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 paratal;

c) sejam requisitados por determinação judicial ou governamental, desde que a AC VALID CODESIGNING 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 CODESIGNING 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/OCSP, 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 CODESIGNING também são considerados documentos não confidenciais:

a) qualquer PC aplicável;

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 CODESIGNING 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 CODESIGNING 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, terão as atribuições de geração, manutenção e 9.3.3 Responsabilidade em proteger a informação confidencial.

9.3.3.4. Não se aplica.

## **9.4 Privacidade da informação pessoal**

### **9.4.1 Plano de privacidade**

A AC VALID CODESIGNING assegurará a proteção de dados pessoais conforme sua Política de Privacidade, disponível em: <https://www.validcertificadora.com.br/politicadeprivacidade> e a Lei Geral de Proteção de Dados Pessoais (LGPD).

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

Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC VALID CODESIGNING será tratado, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

**Nota 1:** A Lei Geral de Proteção de Dados (LGPD), entrará em vigor em agosto de 2020.

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

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

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

A AC VALID CODESIGNING 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 CODESIGNING poderão ser utilizadas ou divulgadas a terceiros mediante o fornecimento de consentimento pelo titular de certificado e representante legal, 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, mediante ao seu consentimento.

Autorizações formais podem ser apresentadas de duas formas:

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

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

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC VALID CODESIGNING 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 CODESIGNING 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 CODESIGNING 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 CODESIGNING declara e garante o quanto segue:

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

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

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

A AC VALID CODESIGNING 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 processo AR na forma de suas DPCs, PCs e normas complementares.

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

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

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

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

#### **9.6.1.5 Serviço**

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

#### **9.6.1.6 Revogação**

A AC irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos documentos CS Guidelines.

#### **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 CODESIGNING, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6.3.2 A AC VALID CODESIGNING 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 CODESIGNING é considerado válido quando:

- i. tiver sido emitido pela AC VALID CODESIGNING;
- ii. não constar como revogado pela AC VALID CODESIGNING;
- 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

### **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 CODESIGNING 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 CODESIGNING 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 CODESIGNING 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-validcodesigning/dpc-ac-validcodesigningv11.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 CODESIGNING 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 CODESIGNING 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 CODESIGNING e AR e outras entidades citadas. Havendo conflito entre esta PC 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 listados a seguir 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
[1]	DIRETRIZES DA POLÍTICA TARIFÁRIA 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.iti.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.

[14] WebTrust Principles and Criteria for Registration Authorities

[15] WebTrust Principles and Criteria for Certification Authorities

[16] WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES –PUBLICLY TRUSTED CODESIGNING CERTIFICATES Version 1.0.1

Disponível:

<https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria>

[17] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted [18] Certificates Versão 1.6.6

[19] CA/Browser Forum Guidelines for The Issuance and Management of Extended Validation CODESIGNING Certificates versão 1.4

[20] Baseline Requirements for the Issuance and Management of Publicly Trusted CODESIGNING Certificates versão 1.2

Disponível: <https://cabforum.org/baseline-requirements-documents/>