Declaração de Práticas de Certificação da Autoridade Certificadora Prodemge

(DPC AC PRODEMGE BR)

OID: 2.16.76.1.1.125

Classificação: Pública

Versão 4.0

Julho de 2021

prodemge

Companhia de Tecnologia
da Informação do Estado
de Minas Gerais

CONTROLE DE ALTERAÇÕES E VERSÕES

VERSÃO	DATA	RESOLUÇÃO QUE APROVOU A ALTERAÇÃO	ITEM ALTERADO	DESCRIÇÃO DA ALTERAÇÃO
1.0	07/06/2018	-	-	Versão inicial
2.0	03/09/2019	Resolução 151	Diversos	Adequação Resolução 151
2.1	03/04/2020	Resolução 151	1.2.2, 1.3.2.1, 2.1.4, 3.2, 3.2.2.1.3, 3.2.2.2, 3.2.2.3.2, 3.2.3.1.1, 3.2.3.1.2, 3.2.3.1.3, 3.2.3.1.4, 3.2.3.1.5, 3.2.3.1.6, 3.2.3.1.7, 3.2.3.1.8, 3.2.3.1.9, 3.2.7.1.4, 3.2.7.1.5, 3.2.8.1, 3.2.8.2, 3.2.8.4, 3.2.8.4.1, 3.3.1.3, 3.3.2.1, 3.3.2.3, 3.3.2.4, 4.1, 4.1.2.2, 4.1.2.4, 4.3.2, 4.4.1.1, 4.5.1.2, 4.9.1.4, 4.9.1.5, 4.9.2, 4.9.6, 4.9.7.1, 5.1.2.1.8, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.6.1, 5.3.7, 5.3.8.1, 5.7.1.2, 6.1.5.1, 6.3.2.3 e 9.16.1.	A partir de apontamentos do ITI para correções da V2.0
2.2	28/08/2020	Mudança de estrutura organizacional na Prodemge	1.5.2; 1.5.3	Alteração de contatos e responsabilidades
3.0	09/09/2020	Resoluções 164 e 167	1.1.5, 3.2.2.4, 3.2.3.2, 3.2.3.2.1, 3.2.3.2.2, 3.2.3.2.3, 3.2.9.3.3, 3.2.9.6, 4.9.3.3, 4.9.3.4, 4.9.7.1, 4.9.7.2, 4.9.7.3, 4.9.7.4, 4.9.7.5, 4.9.13, 5.1.2.2.2, 7.1.1, 7.1.2, 7.1.4.1, 7.1.5, 7.2.1, 7.2.2.2, 7.3, 7.3.1, 7.3.2	Altera prazos de emissão de LCR e de revogação de certificado, tempo de armazenamento de vídeo e outros apontamentos do ITI
4.0	23/07/2021	Resolução 177e 181	1.1.1; 1.1.6; 1.3.1; 1.3.2; 1.3.2.1; 1.3.3; 1.3.5; 1.3.5.1; 1.4.1; 1.4.2; 1.5.2; 1.6; 2.1.2; 2.2.2; 2.3; 2.3.1; 2.4; 2.4.1; 3; 3.1.1.2; 3.1.2; 3.1.2.1; 3.1.4; 3.1.4.1; 3.1.4.2; 3.2; 3.2.1; 3.2.2.1.3; 3.2.2.1.4; 3.2.2.1.5; 3.2.2.2; 3.2.2.3.1; 3.2.3.1; 3.2.3.1.1; 3.2.3.1.2; 3.2.3.1.3; 3.2.3.1.8; 3.2.7.4.1.1; 3.2.7.4.1.2; 3.2.7.4.1.3; 3.2.7.4.2; 3.2.7.4.3; 3.2.7.4.4; 3.2.7.5; 3.2.7.5.1; 3.2.7.7.1.1; 3.2.7.7.1.2; 3.2.7.7.1.3; 3.2.7.7.2; 3.2.7.7.3; 3.2.7.7.4; 3.2.7.8; 3.2.7.8.1; 3.2.8.3; 3.2.8.3.2; 3.2.9.3.4; 3.2.9.5; 3.2.9.5.1; 3.2.9.7; 3.2.9.8; 3.3.1; 3.3.1.1; 3.3.1.2; 3.3.1.2.1; 3.3.1.3; 3.3.2; 3.3.2.2; 3.3.2.3; 3.3.2.4; 3.3.4; 4.1; 4.1.1; 4.1.1.3; 4.1.2.3; 4.2; 4.2.1; 4.3.1.1; 4.4.1.1; 4.4.1.2; 4.4.1.3; 4.5.1.1; 4.5.1.2; 4.9.1.5; 4.9.2; 4.9.3.2; 4.9.3.4; 4.9.7.3; 4.9.11.1; 4.9.12.1; 4.9.12.2; 5; 5.1; 5.1.1.2; 5.1.2.2.2; 5.2; 6.1.5.2; 6.1.6.1; 6.1.6.2; 6.2.1.1; 6.2.1.2;	(181) Inclui a previsão de batimento biométrico e biográfico, realizado em base oficial nacional, no processo de identificação de requerente de certificado digital ICP-Brasil. (177) Revisão e consolidação do DOC-ICP-05. Adequação de clausulas compatíveis com AC de primeiro nível.

VER SÃO	DATA	RESOLUÇÃO QUE APROVOU A ALTERAÇÃO	ITEM ALTERADO	DESCRIÇÃO DA ALTERAÇÃO
			6.2.4.4; 6.6; 6.7; 6.7.1; 6.7.1.1; 6.7.1.3; 6.7.1.4; 6.7.1.5; 6.7.2.1; 6.7.2.2; 6.7.3.1; 6.7.3.2; 6.7.3.3; 6.7.4; 7.1.3; 10.1; 10.2; 10.3; 11	

SUMÁRIO

1. INTRODUÇÃO 11
1.1. Visão Geral 11
1.2. Nome do documento e Identificação 11
1.3. Participantes da ICP-Brasil 11
1.3.1. Autoridades Certificadoras 11
1.3.2. Autoridades de Registro 11
1.3.3. Titulares do Certificado 11
1.3.4. Partes Confiáveis 12
1.3.5. Outros Participantes 12
1.4. Usabilidade do Certificado 12
1.4.1. Uso apropriado do certificado 12
1.4.2. Uso proibitivo do certificado 12
1.5. Política de Administração 12
1.5.1. Organização administrativa do documento 12
1.5.2. Contatos 12
1.5.3. Pessoa que determina a adequabilidade da DPC com a PC 12
1.5.4. Procedimentos de aprovação da DPC 12
1.6. Definições a Acrônimos 13
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 14
2.1. Repositórios 14
2.2. Publicação de informações dos certificados 14
2.3. Tempo ou Frequência de Publicação 15
2.4. Controle de Acesso aos Repositórios 15
3. IDENTIFICAÇÃO E AUTENTICAÇÃO 15
3.1. Atribuição de Nomes 15
3.1.1. Tipos de nomes 15
3.1.2. Necessidade dos nomes serem significativos 16
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado 16
3.1.4. Regras para interpretação de vários tipos de nomes 16
3.1.5. Unicidade de nomes 16
3.1.6. Procedimento para resolver disputa de nomes 16
3.1.7. Reconhecimento, autenticação e papel de marcas registradas 16
3.2. Validação inicial de identidade 16
3.2.1. Método para comprovar a posse de chave privada 17
3.2.2. Autenticação da identificação da organização 17
3.2.3. Autenticação da identidade de um indivíduo 19
3.2.4. Informações não verificadas do titular do certificado 20
3.2.5. Validação das autoridades 20

3.2.6. Critérios para interoperação 20
3.2.7. Autenticação da identidade de equipamento ou aplicação 20
3.2.8. Procedimentos complementares 21
3.2.9. Procedimentos específicos 22
3.3. Identificação e autenticação para pedidos de novas chaves 22
3.4. Identificação e Autenticação para solicitação de revogação 22
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 23
4.1. Solicitação do certificado 23
4.1.1. Quem pode submeter uma solicitação de certificado 23
4.1.2. Processo de registro e responsabilidades 23
4.2. Processamento de Solicitação de Certificado 24
4.2.1. Execução das funções de identificação e autenticação 25
4.2.2. Aprovação ou rejeição de pedidos de certificado 25
4.2.3. Tempo para processar a solicitação de certificado 25
4.3. Emissão de Certificado 25
4.3.1. Ações da AC durante a emissão de um certificado 25
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado 25
4.4. Aceitação de Certificado 26
4.4.1. Conduta sobre a aceitação do certificado 26
4.4.2. Publicação do certificado pela AC 26
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades 26
4.5. Usabilidade do par de chaves e do certificado 26
4.5.1. Usabilidade da Chave privada e do certificado do titular 26
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis 27
4.6. Renovação de Certificados 27
4.6.1. Circunstâncias para renovação de certificados 27
4.6.2. Quem pode solicitar a renovação 27
4.6.3. Processamento de requisição para renovação de certificados 27
4.6.4. Notificação para nova emissão de certificado para o titular 27
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado 27
4.6.6. Publicação de uma renovação de um certificado pela AC 27
4.6.7. Notificação de emissão de certificado pela AC para outras entidades 27
4.7. Nova chave de certificado (Re-key) 27
4.7.1. Circunstâncias para nova chave de certificado 27
4.7.2. Quem pode requisitar a certificação de uma nova chave pública 28
4.7.3. Processamento de requisição de novas chaves de certificado 28
4.7.4. Notificação de emissão de novo certificado para o titular 28
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada 28
4.7.6. Publicação de uma nova chave certificada pela AC 28
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades 28
4.8. Modificação de certificado 28
4.8.1. Circunstâncias para modificação de certificado 28

4.8.2. Quem pode requisitar a modificação de certificado 28
4.8.3. Processamento de requisição de modificação de certificado 28
4.8.4. Notificação de emissão de novo certificado para o titular 28
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado 28
4.8.6. Publicação de uma modificação de certificado pela AC 28
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades 28
4.9. Suspensão e Revogação de Certificado 29
4.9.1. Circunstâncias para revogação 29
4.9.2. Quem pode solicitar revogação 29
4.9.3. Procedimento para solicitação de revogação 29
4.9.4. Prazo para solicitação de revogação 30
4.9.5. Tempo em que a AC deve processar o pedido de revogação 30
4.9.6. Requisitos de verificação de revogação para as partes confiáveis 30
4.9.7. Frequência de emissão de LCR 30
4.9.8. Latência máxima para a LCR 31
4.9.9. Disponibilidade para revogação/verificação de status on-line 31
4.9.10. Requisitos para verificação de revogação on-line 31
4.9.11. Outras formas disponíveis para divulgação de revogação 31
4.9.12. Requisitos especiais para o caso de comprometimento de chave 31
4.9.13. Circunstâncias para suspensão 31
4.9.14. Quem pode solicitar suspensão 31
4.9.15. Procedimento para solicitação de suspensão 31
4.9.16. Limites no período de suspensão 31
4.10. Serviços de status de certificado 32
4.10.1. Características operacionais 32
4.10.2. Disponibilidade dos serviços 32
4.10.3. Funcionalidades operacionais 32
4.11. Encerramento de atividades 32
4.12. Custódia e recuperação de chave 32
4.12.1. Política e práticas de custódia e recuperação de chave 32
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão 33
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES 33
5.1. Controles Físicos 33
5.1.1. Construção e localização das instalações de AC 33
5.1.2. Acesso físico 33
5.1.3. Energia e ar condicionado 36
5.1.4. Exposição à água 36
5.1.5. Prevenção e proteção contra incêndio 37
5.1.6. Armazenamento de mídia 37
5.1.7. Destruição de lixo 37
5.1.8. Instalações de segurança (backup) externas (off-site) para AC 37
5.2. Controles Procedimentais 37

5.2.1. Perfis qualificados 37
5.2.2. Número de pessoas necessário por tarefa 38
5.2.3. Identificação e autenticação para cada perfil 38
5.2.4. Funções que requerem separação de deveres 38
5.3. Controles de Pessoal 38
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade 39
5.3.2. Procedimentos de verificação de antecedentes 39
5.3.3. Requisitos de treinamento 39
5.3.4. Frequência e requisitos para reciclagem técnica 39
5.3.5. Frequência e sequência de rodízio de cargos 39
5.3.6. Sanções para ações não autorizadas 39
5.3.7. Requisitos para contratação de pessoal 40
5.3.8. Documentação fornecida ao pessoal 40
5.4. Procedimentos de Log de Auditoria 40
5.4.1. Tipos de eventos registrados 40
5.4.2. Frequência de auditoria de registros 41
5.4.3. Período de retenção para registros de auditoria 42
5.4.4. Proteção de registros de auditoria 42
5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria 42
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo) 42
5.4.7. Notificação de agentes causadores de eventos 42
5.4.8. Avaliações de vulnerabilidade 42
5.5. Arquivamento de Registros 42
5.5.1. Tipos de registros arquivados 42
5.5.2. Período de retenção para arquivo 43
5.5.3. Proteção de arquivo 43
5.5.4. Procedimentos de cópia de arquivo 43
5.5.5. Requisitos para datação de registros 43
5.5.6. Sistema de coleta de dados de arquivo (interno e externo) 43
5.5.7. Procedimentos para obter e verificar informação de arquivo 43
5.6. Troca de chave 43
5.7. Comprometimento e Recuperação de Desastre 44
5.7.1. Procedimentos de gerenciamento de incidente e comprometimento 44
5.7.2. Recursos computacionais, software, e/ou dados corrompidos 44
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade 44
5.7.4. Capacidade de continuidade de negócio após desastre 44
5.8. Extinção da AC 44
6. CONTROLES TÉCNICOS DE SEGURANÇA 44
6.1. Geração e Instalação do Par de Chaves 44
6.1.1. Geração do par de chaves 44
6.1.2. Entrega da chave privada à entidade 45
6.1.3. Entrega da chave pública para emissor de certificado 45

6.1.4. Entrega de chave pública da AC às terceiras partes 45
6.1.5. Tamanhos de chave 45
6.1.6. Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros45
6.1.7. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3) 46
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico 46
6.2.1. Padrões e controle para módulo criptográfico 46
6.2.2. Controle "n de m" para chave privada 46
6.2.3. Custódia (escrow) de chave privada 46
6.2.4. Cópia de segurança de chave privada 46
6.2.5. Arquivamento de chave privada 47
6.2.6. Inserção de chave privada em módulo criptográfico 47
6.2.7. Armazenamento de chave privada em módulo criptográfico 47
6.2.8. Método de ativação de chave privada 47
6.2.9. Método de desativação de chave privada 47
6.2.10. Método de destruição de chave privada 48
6.3. Outros Aspectos do Gerenciamento do Par de Chaves 48
6.3.1. Arquivamento de chave pública 48
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada 48
6.4. Dados de Ativação 48
6.4.1. Geração e instalação dos dados de ativação 48
6.4.2. Proteção dos dados de ativação 49
6.4.3. Outros aspectos dos dados de ativação 49
6.5. Controles de Segurança Computacional 49
6.5.1. Requisitos técnicos específicos de segurança computacional 49
6.5.2. Classificação da segurança computacional 49
6.5.3. Controles de Segurança para as Autoridades de Registro 50
6.6. Controles Técnicos do Ciclo de Vida 50
6.6.1. Controles de desenvolvimento de sistema 50
6.6.2. Controles de gerenciamento de segurança 50
6.6.3. Controles de segurança de ciclo de vida 50
6.6.4. Controles na Geração de LCR 50
6.7. Controles de Segurança de Rede 50
6.7.1. Diretrizes Gerais 50
6.7.2. Firewall 51
6.7.3. Sistema de detecção de intrusão (IDS) 51
6.7.4. Registro de acessos não autorizados à rede 51
6.8. Carimbo de Tempo 51
7. PERFIS DE CERTIFICADO, LCR E OCSP 51
7.1. Perfil do Certificado 51
7.1.1. Número de versão 51
7.1.2. Extensões de certificado 51
7.1.3. Identificadores de algoritmo 52

7.1.4. Formatos de nome 52
7.1.5. Restrições de nome 52
7.1.6. OID (Object Identifier) da DPC....53
7.1.7. Uso da extensão "Policy Constraints" 53
7.1.8. Sintaxe e semântica dos qualificadores de política....53
7.1.9. Semântica de processamento para as extensões críticas de PC 53
7.2. Perfil de LCR 53
7.2.1. Número(s) de versão 53
7.2.2. Extensões de LCR e de suas entradas....53
7.3. Perfil de OCSP....53
7.3.1. Número(s) de versão 53
7.3.2. Extensões de OCSP 54
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES 54
8.1. Frequência e circunstâncias das avaliações....54
8.2. Identificação/Qualificação do avaliador 54
8.3. Relação do avaliador com a entidade avaliada....54
8.4. Tópicos cobertos pela avaliação 54
8.5. Ações tomadas como resultado de uma deficiência 54
8.6. Comunicação dos resultados 55
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS 55
9.1. Tarifas....55
9.1.1. Tarifas de emissão e renovação de certificados....55
9.1.2. Tarifas de acesso ao certificado....55
9.1.3. Tarifas de revogação ou de acesso à informação de status 55
9.1.4. Tarifas para outros serviços....55
9.1.5. Política de reembolso 55
9.2. Responsabilidade Financeira....55
9.2.1. Cobertura do seguro....55
9.2.2. Outros ativos 55
9.2.3. Cobertura de seguros ou garantia para entidades finais 55
9.3. Confidencialidade da informação do negócio 55
9.3.1. Escopo de informações confidenciais 55
9.3.2. Informações fora do escopo de informações confidenciais....56
9.3.3. Responsabilidade em proteger a informação confidencial....56
9.4. Privacidade da informação pessoal....56
9.4.1. Plano de privacidade 56
9.4.2. Tratamento de informação como privadas....56
9.4.3. Informações não consideradas privadas 57
9.4.4. Responsabilidade para proteger a informação privadas....57
9.4.5. Aviso e consentimento para usar informações privadas 57
9.4.6. Divulgação em processo judicial ou administrativo 57

9.4.7. Outras circunstâncias de divulgação de informação 57
9.4.8. Informações a terceiros 57
9.5. Direitos de Propriedade Intelectual 57
9.6. Declarações e Garantias 57
9.6.1. Declarações e Garantias da AC 57
9.6.2. Declarações e Garantias da AR 58
9.6.3. Declarações e garantias do titular 58
9.6.4. Declarações e garantias das terceiras partes 59
9.6.5. Representações e garantias de outros participantes 59
9.7. Isenção de garantias 59
9.8. Limitações de responsabilidades 59
9.9. Indenizações 59
9.10. Prazo e Rescisão 59
9.10.1. Prazo 59
9.10.2. Término 59
9.10.3. Efeito da rescisão e sobrevivência 59
9.11. Avisos individuais e comunicações com os participantes 60
9.12. Alterações 60
9.12.1. Procedimento para emendas 60
9.12.2. Mecanismo de notificação e períodos 60
9.12.3. Circunstâncias na qual o OID deve ser alterado 60
9.13. Solução de conflitos 60
9.14. Lei aplicável 60
9.15. Conformidade com a Lei aplicável 60
9.16. Disposições Diversas 60
9.16.1. Acordo completo 60
9.16.2. Cessão 60
9.16.3. Independência de disposições 61
9.16.4. Execução (honorários dos advogados e renúncia de direitos) 61
9.17. Outras provisões 61
10. DOCUMENTOS REFERENCIADOS 61
11. REFERÊNCIAS BIBLIOGRÁFICAS 62

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos mínimos obrigatoriamente observados pela Autoridade Certificadora de 1º.nível - AC PRODEMGE BR - integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil na elaboração de sua Declaração de Práticas de Certificação – DPCs. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução de seus serviços.

1.1.2. Esta DPC está em conformidade com a estrutura definida no documento do Comitê Gestor da ICP-Brasil REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [9].

1.1.3. Não se aplica.

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

1.1.5. A AC PRODEMGE BR mantém todas as informações da sua DPC sempre atualizadas, disponível no endereço web:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_br/dpc_ac_prodemge_br.pdf

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

1.2. Nome do documento e Identificação

1.2.1. Esta DPC é chamada "Declaração de Práticas de Certificação da Autoridade Certificadora PRODEMGE BR", integrante da ICP-Brasil, e conhecida como "DPC AC PRODEMGE BR". O Object Identifier (OID) desta DPC, atribuído pela AC Raiz, após conclusão de seu processo de credenciamento, é **2.16.76.1.1.125**.

1.2.2. Não se aplica

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

Esta DPC refere-se unicamente à AC PRODEMGE BR.

1.3.2. Autoridades de Registro

A atividade de identificação e cadastramento das ACs de nível imediatamente subsequente ao da AC PRODEMGE BR será realizada junto com o processo de credenciamento, não havendo Autoridades de Registro - AR no âmbito da AC PRODEMGE BR.

1.3.2.1. Não se aplica.

1.3.3. Titulares do Certificado

Os certificados emitidos pela AC PRODEMGE BR têm como titulares as ACs de nível imediatamente subsequente ao seu.

1.3.4. Partes Confiáveis

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

1.3.5. Outros Participantes

A Companhia de Tecnologia da Informação e Comunicação do Paraná - Celepar é um participante prestando o serviço de suporte à AC PRODEMGE BR, disponibilizando infraestrutura física e lógica (ambiente de contingência).

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do certificado

Os certificados emitidos pela AC PRODEMGE BR têm como objetivo único identificar as ACs de nível imediatamente subsequente ao seu e divulgar suas chaves públicas de forma segura.

1.4.2. Uso proibitivo do certificado

Os certificados emitidos pela AC PRODEMGE BR não podem identificar ou verificar qualquer entidade ou assinatura além dos propósitos descritos nesta DPC.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

Nome da AC:	AC PRODEMGE BR

1.5.2. Contatos

Endereço:	Rua da Bahia, 2277 – Bairro de Lourdes – Belo Horizonte – MG – CEP: 30.160-012
Telefone:	(31) 3339-1213 / (31) 3339-1336 / (31) 3339-1283
Fax:	Não se aplica
Página web:	https://wwws.prodemge.gov.br/
E-mail:	acprodemge@prodemge.gov.br
Empresa:	Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE

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

Nome:	Danielle Leite Santana Carrilho
Telefone:	(31) 3339-1213 / (31) 98462-0530
E-mail:	acprodemge@prodemge.gov.br
Área:	Gerência de Controle de Níveis de Serviço

1.5.4. Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

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

1.6. Definições a Acrônimos

Sigla	Descrição
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro de Pessoa Física
CS	Code Signing
CSR	Certificate Signing Request
DMZ	Zona Desmilitarizada
DN	Distinguished name
DPC	Declaração de Práticas de Certificação
DETRAN	Departamento Nacional de Trânsito
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCI	Política de Classificação de Informação
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
PJ	Pessoa Jurídica
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PRD	Plano de Recuperação de Desastres
PSC	Prestador de Serviço de Confiança
Prodemge	Companhia de Tecnologia da Informação do Estado de Minas Gerais
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments

Sigla	Descrição
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SIGEPE	Sistema de Gestão de Pessoal da Administração Pública Federal
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TLS	Transport Layer Security
TSDM	Trusted Software Development Methodology
TSE	Tribunal Superior Eleitoral
UF	Unidade de Federação
URL	Uniform Resource Locator

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios

2.1.1. A AC PRODEMGE BR mantem disponível repositório atendendo as seguintes obrigações:

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

2.1.2. O repositório da AC PRODEMGE BR é acessível publicamente através dos endereços web informados no item 2.1.4 e está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do tempo do mês.

As publicações da AC PRODEMGE BR podem ser consultadas através do protocolo http.

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 se encontra em nível 4 de segurança física e requer uma senha de acesso.

Somente a AC PRODEMGE BR, 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 PRODEMGE BR está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.4. A AC PRODEMGE BR disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR:

(1) http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_br/lcr_ac_prodemge_br.crl

(2) http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_br/lcr_ac_prodemge_br.crl

2.2. Publicação de informações dos certificados

2.2.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC PRODEMGE BR http://icp-brasil.ac.prodemge.gov.br/repositorio, obedecendo as regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC PRODEMGE BR 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 pela AC PRODEMGE BR em serviço de diretório e/ou em página web da AC PRODEMGE BR https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2:

a) seu próprio certificado;
b) suas LCRs;
c) esta DPC;
d) não se aplica;
e) não se aplica; e
f) uma relação, regularmente atualizada, contendo o PSS vinculado.

2.3. Tempo ou Frequência de Publicação

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 imediatamente após sua emissão;
c) as versões ou alterações desta DPC são atualizadas no web site da AC PRODEMGE BR após aprovação da AC Raiz da ICP-Brasil.

2.4. Controle de Acesso aos Repositórios

Não há qualquer restrição ao acesso público para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC PRODEMGE BR.

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

3.1. Atribuição de Nomes

3.1.1. Tipos de nomes

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

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

3.1.2. Necessidade dos nomes serem significativos

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

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 PRODEMGE BR. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6. Procedimento para resolver disputa de nomes

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

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

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

3.2. Validação inicial de identidade

A identificação e o cadastramento das ACs de nível imediatamente subsequente à AC PRODEMGE BR são realizados junto ao processo de credenciamento, não havendo Autoridades de Registro - AR vinculada à AC PRODEMGE BR.

Neste e nos itens seguintes estão descritos em detalhes os requisitos e procedimentos utilizados pela AC PRODEMGE BR para a realização dos seguintes processos:

a) Identificação do titular do certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3 e 3.2.7
    i. Para certificados de pessoa física: não se aplica;
    ii. Para certificados de pessoa jurídica: comprovação de que os documentos apresentados se referem 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 da AC Subsequente no sistema da AC PRODEMGE BR.

3.2.1. Método para comprovar a posse de chave privada

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

3.2.2. Autenticação da identificação da organização

3.2.2.1. Disposições Gerais

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

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

3.2.2.1.3. A confirmação da identidade da organização e da pessoa física responsável pelo certificado é feita 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 AC PRODEMGE BR 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 representante da AC PRODEMGE BR e é 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) não se aplica.

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

A confirmação da identidade da pessoa jurídica é 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 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 administradores, 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.

Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

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

3.2.2.3. **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;[1]
b) Cadastro Nacional de Pessoa Jurídica (CNPJ);[2]
c) nome completo do responsável pelo certificado, sem abreviações;[3] e
d) data de nascimento do responsável pelo certificado.[4]

3.2.2.3.2. Não se aplica

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.

[1] No campo Subject, como parte do Common Name, que compõe o Distinguished Name

[2] No campo Subject Alternative Name, OID 2.16.76.1.3.3

[3] No campo Subject Alternative Name, OID 2.16.76.1.3.2

[4] No campo Subject Alternative Name, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.4

3.2.3. Autenticação da identidade de um indivíduo

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

3.2.3.1. Procedimento para identificação de um indivíduo

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

a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:
   i. Registro de Identidade, se brasileiro; ou
   ii. Título de Eleitor, com foto; ou
   iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
   iv. Passaporte, se estrangeiro não domiciliado no Brasil.
b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz:
   i. Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[11]; e
   ii. Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[11].

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

3.2.3.1.1. 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 serão 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, serão verificados:

a) por pessoal da AC PRODEMGE BR devidamente qualificado para executar o processo de verificação;
b) não se aplica; 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. Não se aplica.

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.1.7. Não se aplica.

3.2.3.1.8. A verificação biométrica do requerente poderá ser realizada por meio de batimento dos dados em base oficial nacional, conforme regulamentado em Instrução Normativa editada pela AC Raiz da ICP-Brasil, que

deverá dispor acerca dos procedimentos e das bases oficiais admitidas para tal finalidade.

3.2.3.2. Informações contidas no certificado emitido para um indivíduo

3.2.3.2.1. Não se aplica.

3.2.3.2.2. Não se aplica.

3.2.3.2.3. Não se aplica.

3.2.4. Informações não verificadas do titular do certificado

Não se aplica.

3.2.5. Validação das autoridades

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

3.2.6. Critérios para interoperação

Não se aplica.

3.2.7. Autenticação da identidade de equipamento ou aplicação

3.2.7.1. Disposições Gerais

3.2.7.1.1. Não se aplica.

3.2.7.1.2. Não se aplica.

3.2.7.1.3. Não se aplica.

3.2.7.1.4. Não se aplica.

3.2.7.1.5. Não se aplica.

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

3.2.7.2.1. Não se aplica.

3.2.7.2.2. Não se aplica.

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

3.2.7.3.1. Não se aplica.

3.2.7.3.2. Não se aplica.

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

3.2.7.4.1. Disposições Gerais

3.2.7.4.1.1. Não se aplica.

3.2.7.4.1.2. Não se aplica.

3.2.7.4.1.3. Não se aplica.

3.2.7.5. Procedimentos para efeitos de identificação de um equipamento SAT

Não se aplica.

3.2.7.6. Informações contidas no certificado emitido para um equipamento SAT

3.2.7.6.1. Não se aplica.

3.2.7.6.2. Não se aplica.

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

3.2.7.7.1. Disposições gerais

3.2.7.7.1.1. Não se aplica.

3.2.7.7.1.2. Não se aplica.

3.2.7.7.1.3. Não se aplica.

3.2.7.8. Procedimentos para efeitos de identificação de um equipamento metrológico

Não se aplica.

3.2.7.9. Informações contidas no certificado emitido para um equipamento metrológico

3.2.7.9.1. Não se aplica.

3.2.7.9.2. Não se aplica.

3.2.8. Procedimentos complementares

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

3.2.8.2. Não se aplica.

3.2.8.3. É mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.3.1. Não se aplica.

3.2.8.3.2. Não se aplica.

3.2.8.4. Não se aplica.

3.2.8.4.1. Não se aplica

3.2.9. Procedimentos específicos

3.2.9.1. Não se aplica.

3.2.9.2. Não se aplica.

3.2.9.3. Não se aplica.

3.2.9.3.1. Não se aplica.

3.2.9.3.2. Não se aplica.

3.2.9.3.3. Não se aplica.

3.2.9.3.4. Não se aplica.

3.2.9.4. Não se aplica.

3.2.9.4.1. Não se aplica.

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

Não se aplica.

3.2.9.6. Não se aplica.

3.2.9.7. Não se aplica.

3.2.9.8. Não se aplica.

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. Neste item estão estabelecidos os processos de identificação do solicitante pela AC PRODEMGE BR para a geração de novo par de chaves, e de seu correspondente novo certificado.

3.3.2. Esse processo poderá ser conduzido segundo uma das seguintes possibilidades:

a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3.

3.3.2.1. Não se aplica.

3.3.3. Não se aplica.

3.3.4. Para os casos específicos de expiração ou revogação de um certificado de AC de nível imediatamente subsequente ao da AC PRODEMGE BR, responsável por esta DPC, a AC PRODEMGE BR executará os processos regulares de geração de seu novo par de chaves.

3.4. Identificação e Autenticação para solicitação de 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

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

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
b) Não se aplica;
c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4]

4.1.1. Quem pode submeter uma solicitação de certificado

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

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

4.1.1.2. Não se aplica.

4.1.1.3. Nos casos previstos no item 4.1.1.1, a AC subsequente deverá encaminhar a solicitação de certificado à AC PRODEMGE BR por meio de seus representantes legais, utilizando o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

4.1.2. Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1. Responsabilidades da AC

4.1.2.1.1. A AC PRODEMGE BR responde pelos danos a que der causa.

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

4.1.2.1.3. Não se aplica.

4.1.2.2. Obrigações da AC

As obrigações da AC PRODEMGE BR são as abaixo relacionadas:

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

e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) distribuir o seu próprio certificado;
g) emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCRs;
k) publicar em sua página web sua DPC;
l) publicar, em sua página web, as informações definidas no item 2.2.2 deste documento;
m) Não se aplica;
n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
p) adotar as medidas de segurança e controle previstas na DPC, 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 pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;
u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
x) não se aplica; e
y) não se aplica.

4.1.2.3. Responsabilidades da AR

Não se aplica.

4.1.2.4. Obrigações das ARs

Não se aplica

4.2. Processamento de Solicitação de Certificado

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

A AC de nível subsequente deve encaminhar a solicitação de seu certificado à AC PRODEMGE BR por meio de

seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

A AC PRODEMGE BR não recebe solicitações de certificados para usuários finais, de acordo com a MP 2.220-2, de 24 de agosto de 2001.

4.2.1. Execução das funções de identificação e autenticação

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

4.2.2. Aprovação ou rejeição de pedidos de certificado

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

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

4.2.3. Tempo para processar a solicitação de certificado

A AC PRODEMGE BR cumpre os procedimentos determinados na ICP-Brasil.

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

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

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

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

A emissão de certificados pela AC PRODEMGE BR para as ACs de nível imediatamente subsequente estará condicionada:

a) a apresentação de apólice de 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
b) ao pagamento da tarifa a que se refere o parágrafo 2 do documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [1].

A AC PRODEMGE BR entrega o certificado emitido, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10], para o representante legal da AC credenciada presente à cerimônia.

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

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

A AC de nível imediatamente subsequente declara, através de seus representantes legais, mediante assinatura do Termo de Titularidade, que aceita o certificado emitido. A aceitação implica que o solicitante reconhece a veracidade dos dados contidos no certificado.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

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

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

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

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

Ao aceitar o certificado, a AC titular:

a) concorda com as responsabilidades, obrigações e deveres a ela impostas pelo Termo de Acordo e esta DPC;
b) garante que com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado; e
c) afirma que todas as informações de certificado fornecidas durante o processo de credenciamento são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

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

4.4.1.3. A Aceitação do certificado é formalizada através da assinatura de Termo de Acordo onde são descritas as responsabilidades e obrigações da AC titular para com o certificado emitido.

4.4.2. Publicação do certificado pela AC

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

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

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

4.5. Usabilidade do par de chaves e do certificado

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

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.1.1. A AC titular do certificado emitido pela AC PRODEMGE BR deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto na sua própria DPC.

4.5.1.2. Obrigações do Titular do Certificado

As obrigações da AC Titular incluem no mínimo os itens abaixo:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme documentos aplicáveis da ICP-Brasil;
d) conhecer os seus direitos e obrigações, contemplados por documentos aplicáveis da ICP-Brasil; e
e) informar à AC PRODEMGE BR qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Nota: Não se aplica.

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

Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Em acordo com item 3.3 desta DPC.

4.6.1. Circunstâncias para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.2. Quem pode solicitar a renovação

Em acordo com item 3.3 desta DPC.

4.6.3. Processamento de requisição para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.4. Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

4.6.6. Publicação de uma renovação de um certificado pela AC

Não se aplica.

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

Em acordo com item 4.3 desta DPC.

4.7. Nova chave de certificado (Re-key)

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica.

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

Não se aplica.

4.7.3. Processamento de requisição de novas chaves de certificado

Não se aplica.

4.7.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica.

4.7.6. Publicação de uma nova chave certificada pela AC

Não se aplica.

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

Não se aplica.

4.8. Modificação de certificado

4.8.1. Circunstâncias para modificação de certificado

Não se aplica.

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3. Processamento de requisição de modificação de certificado

Não se aplica.

4.8.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica.

4.8.6. Publicação de uma modificação de certificado pela AC

Não se aplica.

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

Não se aplica.

4.9. Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

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

4.9.1.2. O certificado deve ser obrigatoriamente revogado:

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

4.9.1.3. A AC PRODEMGE BR define ainda que:

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

4.9.1.4. Todo certificado tem a sua validade verificada, na respectiva LCR, antes de ser utilizado.

4.9.1.4.1. Não se aplica

4.9.1.4.2. Não se aplica

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

4.9.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

a) Por solicitação da AC titular do certificado;
b) não se aplica;
c) não se aplica;
d) Pela AC PRODEMGE BR, emitente do certificado;
e) não se aplica;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz;
g) não se aplica;
h) não se aplica;
i) não se aplica; ou
j) não se aplica.

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. A solicitação de revogação de certificado de AC subsequente, emitida pela AC PRODEMGE BR, deve ser realizada através do envio de ofício assinado por pessoa autorizada devidamente qualificada, informando nome da AC e razão da revogação. O ofício deve ser enviado ao contato informado no item 1.5.3. A AC PRODEMGE BR tomará providências para confirmar a solicitação de revogação e tomar as providências necessárias.

4.9.3.2. Como diretrizes gerais, o processo de revogação de um certificado de AC é precedido, quando for o caso, do recebimento pela AC PRODEMGE BR da solicitação de revogação e termina quando uma nova LCR, contendo o certificado revogado, é emitida e publicada pela AC PRODEMGE BR. Concluído esse processo, a AC PRODEMGE BR informa à AC Raiz e à AC afetada a revogação do certificado.

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

4.9.3.4. O prazo para a revogação de certificado de AC de nível imediatamente subsequente ao da ACP RODEMGE BR é de no máximo 24 (vinte e quatro) horas. O prazo será contato a partir do recebimento pela AC PRODEMGE BR da solicitação de revogação da AC titular do certificado ou da determinação de revogação emitida pela própria AC PRODEMGE BR.

4.9.3.5. A AC PRODEMGE BR 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 PRODEMGE BR processa a revogação imediatamente após a análise do pedido.

4.9.6. Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7. Frequência de emissão de LCR

4.9.7.1. Neste item está definida a frequência de emissão da LCR referente a certificados de AC de nível imediatamente subsequente ao da AC PRODEMGE BR.

4.9.7.2. Não se aplica.

4.9.7.3. A frequência máxima admitida para a emissão de LCR referente a certificados de AC é de 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC PRODEMGE BR emitirá nova LCR no prazo previsto no item 4.9.3.4 e notificará à AC Raiz e a todas as ACs de nível imediatamente subsequente ao seu.

4.9.7.4. Não se aplica.

4.9.7.5. Não se aplica.

4.9.8. Latência máxima para a LCR

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

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

A AC PRODEMGE BR não suporta os processos de revogação de certificados de forma on-line. A AC PRODEMGE BR não suporta o processo de verificação da situação de estado de certificados de forma on-line (OCSP). A única forma de consulta on-line de status de certificado é a realizada por meio da LCR

4.9.10. Requisitos para verificação de revogação on-line

A AC PRODEMGE BR não disponibiliza diretório on-line ou um servidor de OCSP para verificar o estado dos certificados emitidos pela AC PRODEMGE BR.

4.9.11. Outras formas disponíveis para divulgação de revogação

4.9.11.1. Informações de revogação de certificado de AC de nível imediatamente subsequente ao da AC PRODEMGE BR também podem ser divulgadas por meio de sua publicação no Diário Oficial da União e na página web da AC Raiz.

4.9.11.2. Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. Quando houver comprometimento ou suspeita de comprometimento da chave privada de uma AC de nível imediatamente subsequente à AC PRODEMGE BR, a AC Titular do Certificado deverá comunicar imediatamente a AC PRODEMGE BR, observando o previsto no item 4.9.3.

4.9.12.2. Uma AC Titular do Certificado deve garantir que a sua DPC contenha determinações que definam os meios que serão utilizados para se notificar um comprometimento ou suspeita de comprometimento da sua chave privada, observando o item 4.9.3 desta DPC.

4.9.13. Circunstâncias para suspensão

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

4.9.14. Quem pode solicitar suspensão

A AC PRODEMGE BR 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 associadas.

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 PRODEMGE BR disponibiliza um serviço de status de certificado na forma de dois pontos de distribuição da LCR.

4.10.2. Disponibilidade dos serviços

Ver item 4.9

4.10.3. Funcionalidades operacionais

Ver item 4.9

4.11. Encerramento de atividades

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

4.11.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC PRODEMGE BR 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 PRODEMGE BR:

a) Revogará todos os certificados gerados pela AC PRODEMGE BR após a publicação e comunicação às partes afetadas através de mensagem eletrônica.
b) Extinguirá os serviços de emissão de certificados.
c) 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.
d) Destruirá a chave privada da AC PRODEMGE BR extinta seguindo o procedimento descrito na DPC Item 6.2.9.
e) Transferirá os dados e gravações da AC PRODEMGE BR para a Autoridade Certificadora sucessora, aprovada pela AC Raiz.
f) Transferirá as chaves públicas dos certificados emitidos pela AC PRODEMGE BR 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 PRODEMGE BR. 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.
g) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC PRODEMGE BR.
h) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

A AC PRODEMGE BR 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 PRODEMGE BR não executa tais práticas.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens seguintes são descritos os controles de segurança implementados pela AC PRODEMGE BR para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1. Controles Físicos

Nos itens seguintes da DPC são descritos os controles físicos referentes às instalações que abrigam os sistemas da AC PRODEMGE BR.

5.1.1. Construção e localização das instalações de AC

5.1.1.1. A localização e o sistema de certificação da AC PRODEMGE BR não são publicamente identificados.

Não há identificação pública externa das instalações e, internamente, não existem ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Neste item estão descritos aspectos de construção das instalações da AC PRODEMGE BR, relevantes para os controles de segurança física, compreendendo entre outros:

a) As instalações para equipamentos de apoio, tais como máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares ficam em ambiente seguro.
b) As instalações para sistemas de telecomunicações, subestações e retificadores ficam em ambiente seguro com entrada e saída controlada.
c) Existem sistemas de aterramento e de proteção contra descargas atmosféricas
d) Existe iluminação de emergência em todos os ambientes de nível 4, além das áreas cobertas por câmeras de monitoramento.

5.1.2. Acesso físico

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

5.1.2.1. Níveis de acesso

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

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

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

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

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

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

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

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC PRODEMGE BR 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, inclusive o sistema de AR. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver sendo ocupado.

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

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

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

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

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre interior à sala de cerimônia e um gabinete reforçado trancado no Data Center. Materiais criptográficos tais como chaves, dados

de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

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

a) confeccionado em aço ou material de resistência equivalente; e
b) possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) constitui-se de pequenos depósitos localizados no interior do cofre da sala de cerimônia (Nível 5). Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da chave privada da AC PRODEMGE BR são armazenados nesses depósitos.

5.1.2.2. Sistemas físicos de detecção

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

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) 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. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados ininterruptamente.

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

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

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

5.1.2.3. Sistema de controle de acesso

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

5.1.2.4. Mecanismos de emergência

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

5.1.2.4.2. Todos os procedimentos referentes aos mecanismos de emergência são documentados. Os

mecanismos e procedimentos de emergência são verificados, semestralmente, por meio de simulação de situações de emergência.

5.1.3. Energia e ar condicionado

5.1.3.1. A infraestrutura do ambiente de certificação da AC PRODEMGE BR está dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC PRODEMGE BR e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC PRODEMGE BR.

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

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

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

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

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

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

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

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

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

a) gerador de porte compatível;
b) gerador de reserva;
c) sistemas de no-breaks redundantes;
d) sistemas redundantes de ar condicionado.

5.1.4. Exposição à água

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

5.1.5. Prevenção e proteção contra incêndio

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

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

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

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

5.1.6. Armazenamento de mídia

A AC PRODEMGE BR atende às normas NBR 11.515 e NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados “).

5.1.7. Destruição de lixo

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

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

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

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

5.2. Controles Procedimentais

Nos itens seguintes desta DPC estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC PRODEMGE BR, com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, são também estabelecidos o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

5.2.1.1. A AC PRODEMGE BR segrega tarefas para funções críticas, com o intuito de evitar que qualquer empregado utilize indevidamente o sistema de certificação digital sem que seja detectado. As ações de cada empregado estão limitadas em função de seu perfil.

5.2.1.2. A AC PRODEMGE BR estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo-os em:

a) operações cotidianas do sistema;
b) gerenciamento e auditoria dessas operações;
c) gerenciamento de mudanças substanciais no sistema

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

5.2.1.3.1. Não se aplica

5.2.1.4. A AC PRODEMGE BR possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos empregados. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o empregado devolve à AC PRODEMGE BR no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. O controle multiusuário é requisito para a geração e a utilização da chave privada da AC PRODEMGE BR, 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 PRODEMGE BR necessitam da presença de no mínimo 2 (dois) de seus empregados com perfil qualificado. As demais tarefas da AC PRODEMGE BR podem ser executadas por um único empregado com perfil qualificado da AC PRODEMGE BR.

5.2.3. Identificação e autenticação para cada perfil

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

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

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

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

5.2.3.3. A AC PRODEMGE BR implementa um padrão de utilização de “senhas fortes”, definido da sua PS e em conformidade com o documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com os procedimentos de validação dessas senhas.

5.2.4. Funções que requerem separação de deveres

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

5.3. Controles de Pessoal

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

a) os termos e as condições do perfil que ocupam;
b) compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;

c) o compromisso de não divulgar informações sigilosas a que têm acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC PRODEMGE BR envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é admitido conforme o estabelecido no documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3.2. Procedimentos de verificação de antecedentes

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

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

5.3.2.2. Não se aplica.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC PRODEMGE BR envolvidos 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 PRODEMGE BR;
b) sistema de certificação em uso na AC PRODEMGE BR;
c) procedimentos do Plano de Recuperação de Desastres (PRD);
d) procedimentos do Plano de Continuidade de Negócios (PCN);
e) reconhecimento de assinaturas e da validade dos documentos apresentados, na forma dos itens 3.2.2 e 3.2.3; e
f) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC PRODEMGE BR e das AC Subsequentes, envolvidos 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 PRODEMGE BR.

5.3.5. Frequência e sequência de rodízio de cargos

A AC PRODEMGE BR não implementa o rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, suspeita ou real, realizada por pessoa encarregada de processo operacional da AC PRODEMGE BR, o acesso do empregado ao seu sistema de certificação é suspenso imediatamente, e um Processo Administrativo para apuração dos fatos é instaurado e adotadas as medidas legais cabíveis.

5.3.6.2. O Processo Administrativo, indicado em 5.3.6.1 contém os seguintes itens:

a) relato da ocorrência com “modus operandis”;
b) identificação dos envolvidos;
c) eventuais prejuízos causados;
d) punições aplicadas, se for o caso;
e) conclusões.

5.3.6.3. Concluído o Processo Administrativo, a AC PRODEMGE BR encaminha suas conclusões à AC Raiz.

5.3.6.4. As punições passíveis de aplicação, em decorrência de Processo Administrativo, são:

a) advertência;
b) suspensão por prazo determinado;
c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

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

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC PRODEMGE BR disponibiliza para todos os seus empregados:

a) a DPC da AC PRODEMGE BR;
b) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];
c) toda a documentação operacional relativa às suas atividades; e
d) todos os contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. A documentação fornecida é classificada segundo a Política de Classificação de Informação (PCI) definida pela AC PRODEMGE BR e é mantida atualizada.

5.4. Procedimentos de Log de Auditoria

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

5.4.1. Tipos de eventos registrados

5.4.1.1. A AC PRODEMGE BR 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 PRODEMGE BR;
c) mudanças na configuração dos sistemas AC PRODEMGE BR ou nas suas chaves;
d) mudanças nas políticas de criação de certificados;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não autorizadas de acesso aos arquivos do sistema;
g) geração de chaves próprias da AC PRODEMGE BR ou de chaves de seus usuários finais;

h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
l) operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1. Não se aplica

5.4.1.2. A AC PRODEMGE BR 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 PRODEMGE BR 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 PRODEMGE BR é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.4.1.6. A AC PRODEMGE BR 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;
d) a assinatura digital do executante.

5.4.1.7. A AC PRODEMGE BR define, em documento disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos, utilizados para identificação apresentados no momento da solicitação e revogação de certificados, e dos termos de titularidade.

5.4.2. Frequência de auditoria de registros

A periodicidade com que os registros de auditoria da AC PRODEMGE BR 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 PRODEMGE BR 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.

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 PRODEMGE BR, em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

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

A AC PRODEMGE BR executa, automaticamente pelo sistema ou manualmente pelos administradores do sistema, o procedimento de backup dos registros de auditoria semanalmente, ou sempre que houver alguma utilização desses equipamentos quando em ambiente offline.

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

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

5.4.7. Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas da auditoria da AC PRODEMGE BR não são notificados 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 PRODEMGE BR, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC PRODEMGE BR 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 PRODEMGE BR e pelas ARs a ela vinculadas.

5.5.1. Tipos de registros arquivados

Os tipos de registros arquivados são:

a) Solicitações de certificados;
b) Solicitações de revogação de certificados;
c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;
e) Emissões de LCR;
f) Trocas de chaves criptográficas da AC responsável; e
g) Informações de auditoria previstas no item 5.4.1.

5.5.2. Período de retenção para arquivo

Os períodos de retenção por tipo de registro arquivado são:

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

5.5.3. Proteção de arquivo

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

5.5.4. Procedimentos de cópia de arquivo

5.5.4.1. A AC PRODEMGE BR estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC PRODEMGE BR, 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 PRODEMGE BR verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para datação de registros

Os servidores da AC PRODEMGE BR são sincronizados com a hora fornecida pela AC RAIZ por meio de sua Fonte Confiável do Tempo – FCT conforme DOC-ICP 07 [12].

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 PRODEMGE BR em seus procedimentos operacionais são internos.

5.5.7. Procedimentos para obter e verificar informação de arquivo

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

5.6. Troca de chave

5.6.1. A AC PRODEMGE BR comunicará à AC subsequente, com 90 (noventa) dias de antecedência, o vencimento do seu certificado, incluindo neste comunicado as informações necessárias para a solicitação de uma nova chave.

5.6.2. Não se aplica.

5.7. Comprometimento e Recuperação de Desastre

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

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento

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

5.7.1.2. Não se aplica.

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

Procedimentos descritos no PCN da AC PRODEMGE BR.

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

5.7.3.1. Certificado de entidade é revogado

Procedimentos descritos no PCN da AC PRODEMGE BR.

5.7.3.2. Chave de entidade é comprometida

Procedimentos descritos no PCN da AC PRODEMGE BR.

5.7.4. Capacidade de continuidade de negócio após desastre

Procedimentos descritos no PCN da AC PRODEMGE BR.

5.8. Extinção da AC

Conforme CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICPBRASIL[6].

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPC define as medidas de segurança implantadas pela AC PRODEMGE BR 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 PRODEMGE BR 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 PRODEMGE BR é gerado pela própria AC PRODEMGE BR, em hardware específico, conforme detalhado em 6.1.8, 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 PRODEMGE BR é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC PRODEMGE BR, treinados para a função. A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

6.1.1.3. Não se aplica.

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

6.1.1.5. O par de chaves criptográficas de uma AC de nível imediatamente subsequente ao da AC PRODEMGE BR é gerado somente pelo titular do certificado correspondente. É gerado em módulo criptográfico homologado conforme o padrão ICP-Brasil NSH3, 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 PRODEMGE BR são os indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.2. Entrega da chave privada à entidade

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

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Os procedimentos utilizados pela AC PRODEMGE BR para a entrega de sua chave pública à AC de nível hierárquico superior encarregada da emissão de seu certificado são definidos pela AC superior.

6.1.3.2. A AC de nível imediatamente subsequente ao da AC PRODEMGE BR entrega à AC PRODEMGE BR cópia de sua chave pública, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8]. Essa entrega é feita por representante legalmente constituído da AC subsequente, em cerimônia específica, em data e hora previamente estabelecidas pela AC PRODEMGE BR. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

6.1.4. Entrega de chave pública da AC às terceiras partes

A AC PRODEMGE BR disponibiliza o seu certificado e todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através endereços web:

Para certificados emitidos na AC PRODEMGE BR

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_br/ac_prodemge_br.p7c.

6.1.5. Tamanhos de chave

6.1.5.1. Não se aplica.

6.1.5.2. O tamanho mínimo das chaves criptográficas associadas a certificados de AC subsequentes é de RSA 4096 (quatro mil e noventa e seis) bits, observando o disposto em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

6.1.6.1. Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e

algoritmos criptográficos da ICP-Brasil.

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

6.1.7.1. A chave privada das AC Subsequentes é utilizada apenas para a assinatura dos certificados por ela emitidos e da sua LCR.

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

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

A chave privada da AC PRODEMGE BR é gerada, armazenada e utilizada apenas em hardware criptográfico com padrão de segurança de acordo com o documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC PRODEMGE BR adotará o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.1.2. O módulo criptográfico utilizado na geração e utilização das chaves criptográficas das AC de nível imediatamente subsequentes segue os padrões definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil - requeridos para os módulos de geração de chaves.

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 PRODEMGE BR é dividida em "05" (cinco) partes e distribuídas por "05" (cinco) custodiantes designados pela AC PRODEMGE BR (m).

6.2.2.2. É exigido a presença de 2 (dois) custodiantes (n), formalmente designados pela AC PRODEMGE BR, para a ativação do componente e a consequente utilização da chave privada.

6.2.3. Custódia (escrow) de chave privada

A AC PRODEMGE BR não implementa tal prática.

6.2.4. Cópia de segurança de chave privada

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

6.2.4.2. A AC PRODEMGE BR mantém cópia de segurança de sua própria chave privada. Esta cópia está 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 PRODEMGE BR, não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC. Por solicitação do respectivo titular ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC PRODEMGE BR poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido.

6.2.4.4. Em qualquer caso a cópia de segurança é armazenada cifrada por algoritmo AES-256 bits CBC, conforme definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas das AC subordinadas à AC PRODEMGE BR não são arquivadas pela AC PRODEMGE BR.

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 PRODEMGE BR 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

Para a ativação das chaves privadas exige-se um número mínimo de pessoas. A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. Esse número mínimo é:

a) 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco) pessoas para utilização das suas chaves privadas criadas na cadeia V5.

A AC PRODEMGE BR não emite certificados para usuários finais, logo, não há 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 PRODEMGE BR está instalada em ambiente físico com nível de segurança 4, onde só é permitido o acesso por pelo menos 2 (dois) funcionários autorizados. Sua desativação é feita por meio de comandos executados pelos funcionários de confiança, identificados e autorizados através de mecanismos nativos do sistema operacional.

A AC PRODEMGE BR não emite certificados para usuários finais, logo, não há procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.10. Método de destruição de chave privada

Para a destruição das chaves privadas da AC PRODEMGE BR exige-se um número mínimo de pessoas. A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. Esse número mínimo é:

a) 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco) pessoas para utilização das suas chaves privadas criadas na cadeia V5.

As mídias de armazenamento das chaves privadas são reinicializadas de forma a não restarem nelas informações sensíveis.

A AC PRODEMGE BR não emite certificados para usuários finais, logo, não há 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

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

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

6.3.2.1. A chave privada da AC PRODEMGE BR e dos titulares de certificados por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. As chaves públicas correspondentes, podem ser utilizadas durante todo o período de tempo 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. Não se aplica.

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

6.4. Dados de Ativação

Nos itens seguintes desta DPC são descritos os requisitos 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.

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. A AC PRODEMGE BR garante que os dados de ativação da sua chave privada são únicos e aleatórios, instalados fisicamente em dispositivos criptográficos de controle de acesso.

6.4.1.2. Não se aplica.

6.4.2. Proteção dos dados de ativação

6.4.2.1. Os dados de ativação da chave privada da AC PRODEMGE BR são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Não se aplica.

6.4.3. Outros aspectos dos dados de ativação

Não se aplica

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

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

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

6.5.1.3. Os computadores servidores, utilizados pela AC PRODEMGE BR, 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 PRODEMGE BR;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC PRODEMGE BR;
c) uso de criptografia para segurança de base de dados;
d) geração e armazenamento de registros de auditoria da AC PRODEMGE BR;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;
f) mecanismos para cópias de segurança (backup).

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

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde residem os equipamentos utilizados para operação da AC PRODEMGE BR, 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 PRODEMGE BR. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC PRODEMGE BR é preparado e configurado como previsto na PS implementada, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A AC PRODEMGE BR aplica configurações de segurança definida como Evaluated Configuration Guide for Red Hat Enterprise Linux - EAL3, baseada na Common Criteria, que disponibiliza as atualizações deste sistema operacional utilizado nos servidores do Sistema de Certificação Digital.

6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.

6.5.3.2. Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

Nos itens seguintes estão descritos, quando aplicáveis, os controles implementados pela AC PRODEMGE BR no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC PRODEMGE BR utiliza o Processo de Software Prodemge fundamentado nos modelos de referências: Unified Process – UP e Melhoria do Processo de Software Brasileiro – MPS.BR. Contém as abordagens: tradicional e ágil e utiliza os padrões de engenharia de software aplicáveis ao contexto da Prodemge. É iterativo, incremental, adaptativo, configurável e com foco na qualidade de software, possibilitando o desenvolvimento e a manutenção de software em diferentes plataformas tecnológicas.

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

6.6.2. Controles de gerenciamento de segurança

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

6.6.2.2. A AC PRODEMGE BR utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3. Controles de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

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

6.7. Controles de Segurança de Rede

O computador servidor da AC PRODEMGE BR que hospeda o sistema de certificação opera off-line, fisicamente desconectado de qualquer rede.

6.7.1. Diretrizes Gerais

6.7.1.1. Não se aplica.

6.7.1.2. Nos servidores do sistema de certificação da AC PRODEMGE BR somente os serviços estritamente

necessários para o funcionamento da aplicação são habilitados.

6.7.1.3. Não se aplica.

6.7.1.4. Não se aplica.

6.7.1.5. Não se aplica.

6.7.2. Firewall

6.7.2.1. Não se aplica.

6.7.2.2. Não se aplica.

6.7.3. Sistema de detecção de intrusão (IDS)

6.7.3.1. Não se aplica.

6.7.3.2. Não se aplica.

6.7.3.3. Não se aplica.

6.7.4. Registro de acessos não autorizados à rede

Não se aplica.

6.8. Carimbo de Tempo

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR E OCSP

7.1. Perfil do Certificado

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

7.1.1. Número de versão

O certificado da AC Prodemge BR implementa a versão 3 de certificado do padrão ITU-T X.509.

Os certificados das AC's de nível imediatamente subsequente ao da AC PRODEMGE BR implementam a versão 3 de certificado do padrão ITU-T X.509.

7.1.2. Extensões de certificado

O certificado da AC PRODEMGE BR implementa as seguintes extensões obrigatórias definidas pela ICP-Brasil:

a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC PRODEMGE BR.
b) "Subject Key Identifier", não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado.
c) "Key Usage", crítica: somente os bits keyCertSign e cRLSign estão ativados;
d) "Certificate Policies", não crítica:
   d.1) o campo policyIdentifier contém: os OID das PCs que a AC titular do certificado implementa;
   d.2) o campo policyQualifiers contém o endereço Web da DPC da AC que emite o certificado:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_br/dpc_ac_prodemge_br.pdf

e) "Basic Constraints", crítica: contém o campo cA=True

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

http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_br/lcr_ac_prodemge_br.crl

http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_br/lcr_ac_prodemge_br.crl

7.1.3. Identificadores de algoritmo

O certificado de AC de nível subsequente ao da AC PRODEMGE BR é assinado com o uso de algoritmo definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

7.1.4. Formatos de nome

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

C = BR
O = ICP-Brasil
OU AC PRODEMGE BR
CN = nome da AC titular

7.1.5. Restrições de nome

Não são admitidos caracteres especiais ou de acentuação nos campos do DN.

As restrições aplicáveis para os nomes de AC titulares de certificados, estão em conformidade com as restrições gerais estabelecidas pela ICP-Brasil no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

Além dos caracteres alfanuméricos, são utilizados somente os seguintes caracteres especiais:

Caractere	Código / NBR9611 / (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E

Caractere	Código / NBR9611 / (hexadecimal)
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6. OID (Object Identifier) da DPC

O OID desta DPC é **2.16.76.1.1.125**.

7.1.7. Uso da extensão "Policy Constraints"

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço web da DPC da AC PRODEMGE BR:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_br/dpc_ac_prodemge_br.pdf

7.1.9. Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC Prodemge BR 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 PRODEMGE BR e sua criticalidade.

7.2.2.2. A LCR emitida pela AC PRODEMGE BR implementa as extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) "Authority Key Identifier": contendo o hash SHA-1 da chave pública da AC PRODEMGE BR; e
b) "CRL Number", não crítica: contendo um número sequencial para cada LCR emitida pela AC.

7.3. Perfil de OCSP

A AC PRODEMGE BR não implementa os serviços de respostas OCSP.

7.3.1. Número(s) de versão

Não se aplica.

7.3.2. Extensões de OCSP

Não se aplica.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. Frequência e circunstâncias das avaliações

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

8.2. Identificação/Qualificação do avaliador

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

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

8.3. Relação do avaliador com a entidade avaliada

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 definidos pelo WebTrust.

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

8.4.3. As entidades da ICP-Brasil diretamente vinculadas à AC PRODEMGE BR (AC, AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC PRODEMGE BR 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 PRODEMGE BR age de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

8.6. Comunicação dos resultados

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

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

Variável conforme definição interna Comercial.

9.1.2. Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

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

Variável conforme definição interna Comercial.

9.1.4. Tarifas para outros serviços

Variável conforme definição interna Comercial.

9.1.5. Política de reembolso

Variável conforme definição interna Comercial.

9.2. Responsabilidade Financeira

A responsabilidade da AC PRODEMGE BR 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 vinculadas é sigiloso.

9.3.1.2. Nenhum documento, informação ou registro fornecido pelos titulares de certificado à AC PRODEMGE BR ou AR vinculada será divulgado.

9.3.2. Informações fora do escopo de informações confidenciais

As informações consideradas não sigilosas compreendem:

a) os certificados e a LCR emitidos pela AC PRODEMGE BR;
b) informações corporativas ou pessoais que façam parte do certificados ou em diretórios públicos;
c) a PC correspondente;
d) esta DPC;
e) versões públicas da Política de Segurança;
f) resultados finais de auditorias; e
g) informações requisitadas por determinação judicial

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

9.3.2.2. Os seguintes documentos da AC PRODEMGE BR 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 PRODEMGE BR também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados ou carimbos de tempo emitidos no âmbito da ICP-Brasil.

9.3.3. Responsabilidade em proteger a informação confidencial

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

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

9.3.3.3. Não se aplica.

9.3.3.4. Não se aplica.

9.4. Privacidade da informação pessoal

9.4.1. Plano de privacidade

A AC PRODEMGE BR assegurará a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2. Tratamento de informação como privadas

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

9.4.3. Informações não consideradas privadas

Informações sobre revogação de certificados de AC de nível imediatamente subsequente ao da AC são fornecidas na LCR da AC PRODEMGE BR.

9.4.4. Responsabilidade para proteger a informação privadas

A AC PRODEMGE BR é responsável 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 PRODEMGE BR poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo representante legal, conforme legislação aplicável.

O representante legal terá amplo acesso a quaisquer dos seus próprios dados e identificações, e poderá autorizar a divulgação de seus registros a outras pessoas.

Autorizações formais podem ser apresentadas de duas formas:

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

9.4.6. Divulgação em processo judicial ou administrativo

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

9.6.1.1. Autorização para certificado

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

9.6.1.2. Precisão da informação

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

9.6.1.3. Identificação do requerente

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

9.6.1.4. Consentimento dos titulares

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

9.6.1.5. Serviço

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

9.6.1.6. Revogação

A AC irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos documentos Baseline Requirements, EV SSL Guidelines e/ou EV 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 PRODEMGE BR, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6.3.2. A AC PRODEMGE BR 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 PRODEMGE BR ou um certificado de AC de nível imediatamente subsequente ao da AC PRODEMGE BR é considerado válido quando:

a) tiver sido emitido pela AC PRODEMGE BR;
b) não constar como revogado pela AC PRODEMGE BR;
c) não estiver expirado; e
d) puder ser verificado com o uso do certificado válido da AC PRODEMGE BR.

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

9.6.5. Representações e garantias de outros participantes

Não se aplica.

9.7. Isenção de garantias

Não se aplica.

9.8. Limitações de responsabilidades

A AC PRODEMGE BR 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 PRODEMGE BR 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 PRODEMGE BR disponibiliza página específica com a versão corrente desta DPC para consulta pública, nos endereços Web:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_br/dpc_ac_prodemge_br.pdf

http://icp-brasil2.acprodemge.com.br/repositorio/dpc/ac_prodemge_br/dpc_ac_prodemge_br.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 PRODEMGE BR 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 PRODEMGE BR 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 PRODEMGE BR. Havendo conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2. Cessão

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

9.16.3. Independência de disposições

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

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

De acordo com a legislação vigente.

9.17. Outras provisões

Não se aplica.

10. DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[1]	DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL Aprovado pela Resolução nº 10, de 14 de fevereiro de 2002	DOC-ICP-06
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 25, de 24 de outubro de 2003	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 29 de agosto de 2003	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pela Resolução nº 02, de 25 de setembro de 2001	DOC-ICP-02
[9]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	DOC-ICP-12
[12]	DIRETRIZES PARA SINCRONIZAÇÃO DE FREQUENCIA E TEMPO MA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA ICP-BRASIL Aprovado pela Resolução nº 16, de 10 de junho de 2002	DOC-ICP 07

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

Ref.	Nome do documento	Código
[4]	TERMOS DE TITULARIDADE	ADE-ICP-05.B
[10]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[11]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMETRICA NA ICP-Brasil	DOC-ICP-05.03

11. REFERÊNCIAS BIBLIOGRÁFICAS

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 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