

**Declaração de Práticas de Certificação  
da  
Autoridade Certificadora  
do  
SERPRO SSL**

Autenticação de SSL/TLS

(DPC AC SERPRO SSL)

**Versão 7.0 de Julho 2025**



## Sumário

|                                                                        |    |
|------------------------------------------------------------------------|----|
| Controle de Alterações.....                                            | 9  |
| 1. INTRODUÇÃO.....                                                     | 10 |
| 1.1. Visão Geral.....                                                  | 10 |
| 1.2. Identificação.....                                                | 10 |
| 1.3. Participantes da ICP-Brasil.....                                  | 10 |
| 1.3.1. Autoridades Certificadoras.....                                 | 10 |
| 1.3.2. Autoridades de Registro.....                                    | 10 |
| 1.3.3. Titulares de Certificado.....                                   | 11 |
| 1.3.4. Partes Confiáveis.....                                          | 11 |
| 1.3.5. Outros Participantes.....                                       | 11 |
| 1.4. Usabilidade do Certificado.....                                   | 11 |
| 1.4.1. Uso apropriado do certificado.....                              | 11 |
| 1.4.2. Uso proibitivo do certificado.....                              | 11 |
| 1.5. Política de Administração.....                                    | 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. Siglas e Acrônimos:.....                                          | 13 |
| 2. DISPOSIÇÕES GERAIS.....                                             | 14 |
| 2.1. Obrigações do Repositório.....                                    | 14 |
| 2.2. Publicação de informações dos certificados.....                   | 15 |
| 2.3. Tempo ou Frequência de Publicação.....                            | 16 |
| 2.4. Controle de Acesso aos Repositórios.....                          | 16 |
| 3. IDENTIFICAÇÃO E AUTENTICAÇÃO.....                                   | 17 |
| 3.1. Atribuição de Nomes.....                                          | 17 |
| 3.1.1. Tipos de nomes.....                                             | 17 |
| 3.1.2. Necessidade de nomes significativos.....                        | 17 |
| 3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado.....       | 17 |
| 3.1.4. Regras para interpretação de vários tipos de nomes.....         | 17 |
| 3.1.5. Unicidade de nomes.....                                         | 17 |
| 3.1.6. Procedimento para resolver disputa de nomes.....                | 17 |
| 3.1.7. Reconhecimento, autenticação e papel de marcas registradas..... | 17 |
| 3.2. Validação inicial de identidade.....                              | 17 |
| 3.2.1. Método para comprovar o controle da chave privada.....          | 18 |
| 3.2.2. Autenticação da Identidade de uma organização.....              | 18 |
| 3.2.3. Autenticação da identidade de um indivíduo.....                 | 20 |
| 3.2.4. Informações não verificadas do titular do certificado.....      | 22 |
| 3.2.5. Validação das autoridades.....                                  | 22 |
| 3.2.6. Critérios para interoperação.....                               | 22 |

|                                                                                          |    |
|------------------------------------------------------------------------------------------|----|
| 3.2.7. Autenticação da Identidade de um equipamento ou aplicação.....                    | 22 |
| 3.2.8. Procedimentos complementares.....                                                 | 24 |
| 3.2.9. Procedimentos específicos.....                                                    | 24 |
| 3.3. Identificação e autenticação para pedidos de novas chaves.....                      | 24 |
| 3.4. Identificação e Autenticação para solicitação de revogação.....                     | 25 |
| 4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO.....                          | 25 |
| 4.1. Solicitação de Certificado.....                                                     | 25 |
| 4.1.1. Quem pode submeter uma solicitação de certificado.....                            | 26 |
| 4.1.2. Processo de registro e responsabilidades.....                                     | 26 |
| 4.2. Processamento de Solicitação de Certificado.....                                    | 28 |
| 4.2.1. Execução das funções de identificação e autenticação.....                         | 28 |
| 4.2.2. Aprovação ou rejeição de pedidos de certificado.....                              | 29 |
| 4.2.3. Tempo para processar a solicitação de certificado.....                            | 29 |
| 4.3. Emissão de Certificado.....                                                         | 29 |
| 4.3.1. Ações da AC durante a emissão de um certificado.....                              | 29 |
| 4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado..... | 29 |
| 4.4. Aceitação de Certificado.....                                                       | 30 |
| 4.4.1. Conduta sobre a aceitação do certificado.....                                     | 30 |
| 4.4.2. Publicação do certificado pela AC.....                                            | 30 |
| 4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades.....     | 30 |
| 4.5. Usabilidade do par de chaves e do certificado.....                                  | 30 |
| 4.5.1. Usabilidade da Chave privada e do certificado do titular.....                     | 30 |
| 4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis.....          | 31 |
| 4.6. Renovação de Certificados.....                                                      | 31 |
| 4.6.1. Circunstâncias para renovação de certificados.....                                | 31 |
| 4.6.2. Quem pode solicitar a renovação.....                                              | 31 |
| 4.6.3. Processamento de requisição para renovação de certificados.....                   | 31 |
| 4.6.4. Notificação para nova emissão de certificado para o titular.....                  | 31 |
| 4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado.....          | 31 |
| 4.6.6. Publicação de uma renovação de um certificado pela AC.....                        | 31 |
| 4.6.7. Notificação de emissão de certificado pela AC para outras entidades.....          | 31 |
| 4.7. Nova chave de certificado (Re-key).....                                             | 31 |
| 4.7.1. Circunstâncias para nova chave de certificado.....                                | 31 |
| 4.7.2. Quem pode requisitar a certificação de uma nova chave pública.....                | 32 |
| 4.7.3. Processamento de requisição de novas chaves de certificado.....                   | 32 |
| 4.7.4. Notificação de emissão de novo certificado para o titular.....                    | 32 |
| 4.7.5. Conduta constituindo a aceitação de uma nova chave certifica.....                 | 32 |
| 4.7.6. Publicação de uma nova chave certificada pela AC.....                             | 32 |
| 4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades.....      | 32 |
| 4.8. Modificação de certificado.....                                                     | 32 |
| 4.8.1. Circunstâncias para modificação de certificado.....                               | 32 |
| 4.8.2. Quem pode requisitar a modificação de certificado.....                            | 32 |
| 4.8.3. Processamento de requisição de modificação de certificado.....                    | 32 |
| 4.8.4. Notificação de emissão de novo certificado para o titular.....                    | 32 |

|                                                                                             |    |
|---------------------------------------------------------------------------------------------|----|
| 4.8.5. Conduta constituindo a aceitação de uma modificação de certificado.....              | 32 |
| 4.8.6. Publicação de uma modificação de certificado pela AC.....                            | 32 |
| 4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades.....         | 32 |
| 4.9. Suspensão e Revogação de Certificado.....                                              | 32 |
| 4.9.1. Circunstâncias para revogação.....                                                   | 32 |
| 4.9.3. Procedimento para solicitação de revogação.....                                      | 34 |
| 4.9.4. Prazo para solicitação de revogação.....                                             | 35 |
| 4.9.5. Tempo em que a AC deve processar o pedido de revogação.....                          | 35 |
| 4.9.6. Requisitos de verificação de revogação para as partes confiáveis.....                | 36 |
| 4.9.7. Frequência de emissão de LCR.....                                                    | 36 |
| 4.9.8. Latência máxima para a LCR.....                                                      | 36 |
| 4.9.9. Disponibilidade para revogação/verificação de status on-line.....                    | 36 |
| 4.9.10. Requisitos para verificação de revogação on-line.....                               | 36 |
| 4.9.11. Outras formas disponíveis para divulgação de revogação.....                         | 36 |
| 4.9.12. Requisitos especiais para o caso de comprometimento de chave.....                   | 37 |
| 4.9.13. Circunstâncias para suspensão.....                                                  | 37 |
| 4.9.14. Quem pode solicitar suspensão.....                                                  | 37 |
| 4.9.15. Procedimento para solicitação de suspensão.....                                     | 37 |
| 4.9.16. Limites no período de suspensão.....                                                | 37 |
| 4.10. Serviços de status de certificado.....                                                | 37 |
| 4.10.1. Características operacionais.....                                                   | 37 |
| 4.10.2. Disponibilidade dos serviços.....                                                   | 37 |
| 4.10.3. Funcionalidades operacionais.....                                                   | 37 |
| 4.11. Encerramento de atividades.....                                                       | 37 |
| 4.12. Custódia e recuperação de chave.....                                                  | 38 |
| 4.12.1. Política e práticas de custódia e recuperação de chave.....                         | 38 |
| 4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão.....         | 38 |
| 5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES.....                              | 38 |
| 5.1. Controle Físico.....                                                                   | 38 |
| 5.1.1. Construção e localização das instalações de AC.....                                  | 38 |
| 5.1.2. Acesso físico.....                                                                   | 39 |
| 5.1.3. Energia e ar-condicionado.....                                                       | 41 |
| 5.1.4. Exposição à água.....                                                                | 42 |
| 5.1.5. Prevenção e proteção contra incêndio.....                                            | 42 |
| 5.1.6. Armazenamento de mídia.....                                                          | 43 |
| 5.1.7. Destruição de lixo.....                                                              | 43 |
| 5.1.8. Instalações de segurança ( <i>backup</i> ) externas ( <i>off-site</i> ) para AC..... | 43 |
| 5.2. Controles Procedimentais.....                                                          | 43 |
| 5.2.1. Perfis qualificados.....                                                             | 43 |
| 5.2.2. Número de pessoas necessário por tarefa.....                                         | 44 |
| 5.2.3. Identificação e autenticação para cada perfil.....                                   | 44 |
| 5.3. Controles de Pessoal.....                                                              | 44 |
| 5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade.....              | 45 |
| 5.3.2. Procedimentos de verificação de antecedentes.....                                    | 45 |

|                                                                                               |    |
|-----------------------------------------------------------------------------------------------|----|
| 5.3.3. Requisitos de treinamento.....                                                         | 45 |
| 5.3.4. Frequência e requisitos para reciclagem técnica.....                                   | 45 |
| 5.3.5. Frequência e sequência de rodízios de cargos.....                                      | 45 |
| 5.3.6. Sanções para ações não autorizadas.....                                                | 46 |
| 5.3.7. Requisitos para contratação de pessoal.....                                            | 46 |
| 5.3.8. Documentação fornecida ao pessoal.....                                                 | 46 |
| 5.4. Procedimentos de <i>Log</i> de auditoria.....                                            | 47 |
| 5.4.1. Tipos de Evento Registrados.....                                                       | 47 |
| 5.4.2. Frequência de auditoria de registros ( <i>logs</i> ).....                              | 48 |
| 5.4.3. Período de Retenção para registros de auditoria.....                                   | 48 |
| 5.4.4. Proteção de registros de auditoria.....                                                | 48 |
| 5.4.5. Procedimentos para cópia de segurança ( <i>backup</i> ) de registros de auditoria..... | 49 |
| 5.4.6. Sistema de coleta de dados de auditoria(interno ou externo).....                       | 49 |
| 5.4.7. Notificação de agentes causadores de eventos.....                                      | 50 |
| 5.4.8. Avaliações de vulnerabilidade.....                                                     | 50 |
| 5.5. Arquivamento de Registros.....                                                           | 50 |
| 5.5.1. Tipos de registros arquivados.....                                                     | 50 |
| 5.5.2. Período de retenção para arquivo.....                                                  | 50 |
| 5.5.3. Proteção de arquivos.....                                                              | 51 |
| 5.5.4. Procedimentos para cópia de arquivos.....                                              | 51 |
| 5.5.5. Requisitos para datação de registros.....                                              | 51 |
| 5.5.6. Sistema de coleta de dados de arquivo(interno e externo).....                          | 51 |
| 5.5.7. Procedimentos para obter e verificar informação de arquivo.....                        | 52 |
| 5.6. Troca de chave.....                                                                      | 52 |
| 5.7. Comprometimento e Recuperação de Desastre.....                                           | 52 |
| 5.7.1. Procedimentos gerenciamento de incidente e comprometimento.....                        | 52 |
| 5.7.2. Recursos computacionais, software e/ou dados corrompidos.....                          | 52 |
| 5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade.....             | 53 |
| 5.7.4. Capacidade de continuidade de negócio após desastre.....                               | 53 |
| 5.8. Extinção da AC.....                                                                      | 53 |
| 6. Controles Técnicos de Segurança.....                                                       | 54 |
| 6.1. Geração e Instalação do Par de chaves.....                                               | 54 |
| 6.1.1. Geração do Par de Chaves.....                                                          | 54 |
| 6.1.2. Entrega da chave privada à entidade titular.....                                       | 54 |
| 6.1.3. Entrega da chave pública para emissor de certificado.....                              | 54 |
| 6.1.4. Disponibilização de chave pública da AC para usuários.....                             | 54 |
| 6.1.5. Tamanhos de chave.....                                                                 | 55 |
| 6.1.6. Geração de parâmetros de chaves assimétricas.....                                      | 55 |
| 6.1.7. Propósitos de uso de chave (conforme campo “ <i>Key usage</i> ” na X.509 v3).....      | 55 |
| 6.2. Proteção da Chave Privada.....                                                           | 55 |
| 6.2.1. Padrões para módulo criptográfico.....                                                 | 55 |
| 6.2.2. Controle “ <i>n</i> de <i>m</i> ’ para chave privada.....                              | 55 |
| 6.2.3. Custódia ( <i>escrow</i> ) de chave privada.....                                       | 56 |
| 6.2.4. Cópia de segurança ( <i>backup</i> ) de chave privada.....                             | 56 |

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| 6.2.5. Arquivamento de chave privada.....                               | 56 |
| 6.2.6. Inserção de chave privada em módulo criptográfico.....           | 56 |
| 6.2.7. Armazenamento de chave privada em módulo criptográfico.....      | 56 |
| 6.2.8. Método de ativação de chave privada.....                         | 56 |
| 6.2.9. Método de desativação de chave privada.....                      | 56 |
| 6.2.10. Método de destruição de chave privada.....                      | 57 |
| 6.3. Outros Aspectos do Gerenciamento do Par de Chaves.....             | 57 |
| 6.3.1. Arquivamento de chave pública.....                               | 57 |
| 6.3.2. Períodos de uso para as chaves pública e privada.....            | 57 |
| 6.4. Dados de ativação.....                                             | 57 |
| 6.4.1. Geração e instalação dos dados de ativação.....                  | 57 |
| 6.4.2. Proteção dos dados de ativação.....                              | 58 |
| 6.4.3. Outros aspectos dos dados de ativação.....                       | 58 |
| 6.5. Controles de Segurança dos computadores.....                       | 58 |
| 6.5.1. Requisitos técnicos específicos de segurança computacional.....  | 58 |
| 6.5.2. Classificação da segurança computacional.....                    | 59 |
| 6.5.3. Controle de segurança para a Autoridade de Registro.....         | 59 |
| 6.6. Controles Técnicos do Ciclo de Vida.....                           | 59 |
| 6.6.1. Controles de desenvolvimento de sistemas.....                    | 59 |
| 6.6.2. Controle de gerenciamento de segurança.....                      | 59 |
| 6.6.3. Classificação de segurança de ciclo de vida.....                 | 60 |
| 6.6.4. Controles na Geração de LCR.....                                 | 60 |
| 6.7. Controles de Segurança de Rede.....                                | 60 |
| 6.7.1. Diretrizes Gerais.....                                           | 60 |
| 6.7.2. Firewall.....                                                    | 61 |
| 6.7.3. Sistema de detecção de intrusão (IDS):.....                      | 61 |
| 6.7.4. Registro de acessos não autorizados à rede.....                  | 61 |
| 6.8. Carimbo de Tempo.....                                              | 61 |
| 7. PERFIS DE CERTIFICADO, LCR E OCSP.....                               | 62 |
| 7.1. Perfil do Certificado.....                                         | 62 |
| 7.1.1. Número de versão.....                                            | 62 |
| 7.1.2. Extensões de certificado.....                                    | 62 |
| 7.1.3. Identificadores de algoritmo.....                                | 62 |
| 7.1.4. Formatos de nome.....                                            | 62 |
| 7.1.5. Restrições de nome.....                                          | 62 |
| 7.1.6. OID (Object Identifier) da DPC.....                              | 62 |
| 7.1.7. Uso da extensão “Policy Constraints”.....                        | 62 |
| 7.1.8. Sintaxe e semântica dos qualificadores de política.....          | 62 |
| 7.1.9. Semântica de processamento para as extensões críticas de PC..... | 62 |
| 7.2. Perfil de LCR.....                                                 | 62 |
| 7.2.1. Número(s) de versão.....                                         | 62 |
| 7.2.2. Extensões de LCR e de suas entradas.....                         | 63 |
| 7.3. Perfil de OCSP.....                                                | 63 |
| 7.3.1. Número(s) de versão.....                                         | 63 |

|                                                                      |    |
|----------------------------------------------------------------------|----|
| 7.3.2. Extensões de OSCP.....                                        | 63 |
| 8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES.....                 | 63 |
| 8.1. Frequência e circunstâncias das avaliações.....                 | 63 |
| 8.2. Identificação/Qualificação do avaliador.....                    | 63 |
| 8.3. Relação do avaliador com a entidade avaliada.....               | 64 |
| 8.4. Tópicos cobertos pela avaliação.....                            | 64 |
| 8.5. Ações tomadas como resultado de uma deficiência.....            | 64 |
| 8.6. Comunicação dos resultados.....                                 | 64 |
| 9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....                         | 64 |
| 9.1. Tarifas.....                                                    | 64 |
| 9.1.1. Tarifas de emissão e renovação de certificados.....           | 64 |
| 9.1.2. Tarifas de acesso ao certificado.....                         | 65 |
| 9.1.3. Tarifas de revogação ou de acesso à informação de status..... | 65 |
| 9.1.4. Tarifas para outros serviços.....                             | 65 |
| 9.1.5. Política de reembolso.....                                    | 65 |
| 9.2. Responsabilidade Financeira.....                                | 65 |
| 9.2.1. Cobertura do seguro.....                                      | 65 |
| 9.2.2. Outros ativos.....                                            | 65 |
| 9.2.3. Cobertura de seguros ou garantia para entidades finais.....   | 65 |
| 9.3. Confidencialidade da informação do negócio.....                 | 65 |
| 9.3.1. Escopo de informações confidenciais.....                      | 65 |
| 9.3.2. Informações fora do escopo de informações confidenciais.....  | 65 |
| 9.3.3. Responsabilidade em proteger a informação confidencial.....   | 66 |
| 9.4. Privacidade da informação pessoal.....                          | 66 |
| 9.4.1. Plano de privacidade.....                                     | 66 |
| 9.4.2. Tratamento de informação como privadas.....                   | 66 |
| 9.4.3. Informações não consideradas privadas.....                    | 66 |
| 9.4.4. Responsabilidade para proteger a informação privadas.....     | 67 |
| 9.4.5. Aviso e consentimento para usar informações privadas.....     | 67 |
| 9.4.6. Divulgação em processo judicial ou administrativo.....        | 67 |
| 9.4.7. Outras circunstâncias de divulgação de informação.....        | 67 |
| 9.4.8. Informações a terceiros.....                                  | 67 |
| 9.5. Direitos de Propriedade Intelectual.....                        | 67 |
| 9.6. Declarações e Garantias.....                                    | 67 |
| 9.6.1. Declarações e Garantias da AC.....                            | 67 |
| 9.6.2. Declarações e Garantias da AR.....                            | 68 |
| 9.6.3. Declarações e garantias do titular.....                       | 68 |
| 9.6.4. Declarações e garantias das terceiras partes.....             | 69 |
| 9.6.5. Representações e garantias de outros participantes.....       | 69 |
| 9.7. Isenção de garantias.....                                       | 69 |
| 9.8. Limitações de responsabilidades.....                            | 69 |
| 9.9. Indenizações.....                                               | 69 |
| 9.10. Prazo e Rescisão.....                                          | 69 |
| 9.10.1. Prazo.....                                                   | 69 |

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| 9.10.2. Término.....                                                    | 69 |
| 9.10.3. Efeito da rescisão e sobrevivência.....                         | 69 |
| 9.11. Avisos individuais e comunicações com os participantes.....       | 70 |
| 9.12. Alterações.....                                                   | 70 |
| 9.12.1. Procedimento para emendas.....                                  | 70 |
| 9.12.2. Mecanismo de notificação e períodos.....                        | 70 |
| 9.12.3. Circunstâncias na qual o OID deve ser alterado.....             | 70 |
| 9.13. Solução de conflitos.....                                         | 70 |
| 9.14. Lei aplicável.....                                                | 70 |
| 9.15. Conformidade com a Lei aplicável.....                             | 70 |
| 9.16. Disposições Diversas.....                                         | 70 |
| 9.16.1. Acordo completo.....                                            | 70 |
| 9.16.2. Cessão.....                                                     | 70 |
| 9.16.3. Independência de disposições.....                               | 70 |
| 9.16.4. Execução (honorários dos advogados e renúncia de direitos)..... | 71 |
| 9.17. Outras provisões.....                                             | 71 |
| 10. Documentos referenciados.....                                       | 71 |
| 11. REFERÊNCIAS BIBLIOGRÁFICAS.....                                     | 72 |



### Controle de Alterações

| Versão | Data          | Responsável        | Motivo         | Descrição                                                                                                                                              |
|--------|---------------|--------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0    | 01/09/2019    | Lucia Castelli     | Versão Inicial | Versão Inicial                                                                                                                                         |
| 1.0    | 01/09/2019    | Osni Bunn          | Aprovação      |                                                                                                                                                        |
| 1.1    | 22/11/2019    | Lucia Castelli     | Revisão        | Inclusão requisitos CabForum 1.6.6.                                                                                                                    |
| 1.1    | 22/11/2019    | Osni Bunn          | Aprovação      |                                                                                                                                                        |
| 1.2    | 21/01/2020    | Lucia Castelli     | Revisão        | Alteração item 3.2.3.1.3.(Res. 154);                                                                                                                   |
| 1.2    | 21/01/2020    | Osni Bunn          | Aprovação      |                                                                                                                                                        |
| 1.3    | 05/02/2020    | Lucia Castelli     | Revisão        | Inclusão item 4.2.1 – Certificados de Alto Risco, Inclusão das páginas de testes – item, 2.2.2 letra “h”)                                              |
| 1.3    | 05/02/2020    | Osni               | Aprovação      |                                                                                                                                                        |
| 1.4    | 26/02/2020    | Lucia Castelli     | Revisão        | Acerto link onde se encontra a DPC                                                                                                                     |
| 1.4    | 26/02/2020    | Alice Vasconcellos | Aprovação      |                                                                                                                                                        |
| 2.0    | 28/04/2020    | Lucia Castelli     | Aprovação      | Alteração versão do certificado da AC; Alterações – Res.155.                                                                                           |
| 2.0    | 28/04/2020    | Alice Vasconcellos | Aprovação      |                                                                                                                                                        |
| 3.0    | 12/05/2020    | Lucia Castelli     | Revisão        | Inclusão das Resoluções 164 e 167(4.9.3.3) e apontamentos ITI;                                                                                         |
| 3.0    | 12/05/2020    | Alice Vasconcellos | Aprovação      |                                                                                                                                                        |
| 3.1    | 01/06/2020    | Lucia Castelli     | Revisão        | Complementação das informações da validação do domínio SSL, item 3.2.7.2.1; Item 6.2.3 não se aplica; 6.7.1.1.b – correções; item 6.8 – não se aplica. |
| 3.1    | 01/06/2020    | Alice Vasconcellos | Aprovação      |                                                                                                                                                        |
| 4.0    | Novembro/2020 | Lucia Castelli     | Revisão        | Atualização conforme Resolução 177                                                                                                                     |
| 4.0    | Novembro/2020 | Alice Vasconcellos | Aprovação      |                                                                                                                                                        |
| 5.0    | Junho/2022    | Lucia Castelli     | Revisão        | Atualização conforme Resolução 181 e 197; Atualização quanto aos métodos a serem utilizados para validação do domínio(item3.2.7.2.1).                  |
| 5.0    | Junho/2022    | Alice Vasconcellos | Aprovação      |                                                                                                                                                        |

| <b>Versão</b> | <b>Data</b>   | <b>Responsável</b> | <b>Motivo</b> | <b>Descrição</b>                                                                                                                         |
|---------------|---------------|--------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 6.0           | Setembro/2022 | Fernando Morgado   | Atualização   | Atualização conforme as resoluções 197 e 204                                                                                             |
| 6.0           | Setembro/2022 | Alice Vasconcellos | Aprovação     |                                                                                                                                          |
| 7.0           | Julho/2025    | Fernando Morgado   | Alteração     | A AC deixou de emitir certificados do tipo SSL/TLS com os requisitos CAB Forum. Exclusão a referências à WebTrust BR SSL e/ ou CABForum. |
| 7.0           | Julho/2025    | Alice Vasconcellos | Aprovação     |                                                                                                                                          |

## 1. INTRODUÇÃO

### 1.1. Visão Geral

1.1.1. Esta Declaração de Práticas de Certificação(DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora do SERPRO SSL (AC SERPRO SSL), AC integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, na execução dos seus serviços.

1.1.2. Esta DPC adota a mesma estrutura empregada no documento DOC-ICP-05 da ICP-Brasil.

1.1.3. AAC SERPRO SSL observa e descreve os princípios e critérios WebTrust.

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

1.1.5. AAC SERPRO SSL mantém todas as informações dessa DPC sempre atualizadas.

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

### 1.2. Identificação

1.2.1. Esta DPC é chamada de “Declaração de Práticas de Certificação da Autoridade Certificadora do SERPRO SSL”, integrante da ICP-Brasil, e comumente referida como “DPC AC SERPRO SSL”.

O Identificador de Objeto (OID) adquirido após credenciamento é **2.16.76.1.1.137**.

1.2.2. A AC SERPRO SSL, emissora de certificados para usuários finais devem ser exclusivas e separadas de acordo com os seguintes propósitos de uso de chaves:

- a) autenticação de servidor (SSL/TLS);
- b) não se aplica;
- c) não se aplica;
- d) não se aplica.

De acordo com a Resolução CG ICP-BRASIL Nº 209, de 7 de agosto de 2024:

- Art. 1º Fica vedada a emissão de certificados digitais destinados à autenticação de servidor (SSL/TLS) na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, excetuado o disposto no art. 2º;
- Art. 2º Fica mantida a cadeia v10 da AC Raiz da ICP-Brasil para emissão exclusiva de certificados digitais SSL/TLS para uso restrito em aplicações específicas;
- Parágrafo único. Consideram-se aplicações específicas aquelas realizadas entre entidades dentro de um ecossistema fechado, onde as autenticações são mútuas e limitadas aos intervenientes conhecidos.

### 1.3. Participantes da ICP-Brasil

#### 1.3.1. Autoridades Certificadoras

Esta DPC se refere unicamente à Autoridade Certificadora da SERPRO SSL, integrante da ICP-Brasil.

#### 1.3.2. Autoridades de Registro

1.3.2.1. O endereço da página *web* (URL) da AC é <https://certificados.serpro.gov.br/serprossl>

Neste endereço está publicado dados referentes à Autoridade de Registro responsável pelo processo de recebimento, identificação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

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

A Autoridade de Registro, envolvida na emissão de certificados SSL, atende e segue os requisitos estabelecidas nas seções 4.2 e 5.3 desse documento.

#### 1.3.3. Titulares de Certificado

Os Titulares de Certificados são pessoas jurídicas autorizadas pela AR a receber um certificado digital emitido pela AC.

Em sendo o titular de certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada.

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

#### 1.3.4. Partes Confiáveis

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

#### 1.3.5. Outros Participantes

A AC utiliza o Serviço Federal de Processamento de dados (SERPRO) como Prestador de Serviço de Suporte – PSS, Prestador de Serviço Biométrico – PSBio e Prestador de Serviço de Confiança – PSC, conforme disponibilizado no endereço: <https://certificados.serpro.gov.br/serprossl>.

### 1.4. Usabilidade do Certificado

#### 1.4.1. Uso apropriado do certificado

A Política de Certificado (PC) implementada pela AC é: **PC AC SERPRO SSL A1** que após credenciamento adquiriu o OID **2.16.76.1.2.1.105**.

Na PC está relacionada as aplicações para as quais são adequados os certificados emitidos por essa AC.

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

As aplicações para as quais são adequados os certificados emitidos pela AC estão relacionadas na Política de Certificado correspondente.

Não existem restrições ou proibições para o uso dos certificados emitidos por essa AC.

Os certificados SSL, emitidos sob esta DPC, não garantem que o equipamento, no qual o certificado foi instalado, não esteja isento de defeitos, malware ou vírus.

### **1.5. Política de Administração**

Esta DPC é administrada pelo Centro de Certificação Digital do SERPRO (CCD-SERPRO).

#### **1.5.1. Organização Administrativa do documento**

Autoridade Certificadora do SERPRO SSL

#### **1.5.2. Contatos**

##### **a) Administrativo:**

Nome: Pedro Moacir Rigo Motta

Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

E-mail: [certificados@serpro.gov.br](mailto:certificados@serpro.gov.br)

Telefone: (61) 2021-7957

##### **b) Suporte / Fraudes**

Nome: Central de Serviços SERPRO

Página Web: <https://atendimento.serpro.gov.br/certificacaodigital>

E-mail: [css.serpro@serpro.gov.br](mailto:css.serpro@serpro.gov.br)

Telefone: 0800 7282323

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

Nome: Pedro Moacir Rigo Motta

Telefone: (61) 2021-7957

E-mail: [certificados@serpro.gov.br](mailto:certificados@serpro.gov.br)

#### 1.5.4. Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

As alterações feitas nesse documento serão identificados dentro do Controle de Alterações.

#### 1.6. Siglas e Acrônimos:

| SIGLA      | DESCRIÇÃO                                                                  |
|------------|----------------------------------------------------------------------------|
| AC         | Autoridade Certificadora                                                   |
| ACME       | Automatic Certificate Management Environment                               |
| AC Raiz    | Autoridade Certificadora Raiz da ICP-Brasil                                |
| AICPA      | American Institute of Certified Public Accountants                         |
| AGR        | Agente de Registro                                                         |
| AR         | Autoridades de Registro                                                    |
| CAA        | Certification Authority Authorization                                      |
| CEI        | Cadastro Específico do INSS                                                |
| CF-e       | Cupom Fiscal Eletrônico                                                    |
| CG         | Comitê Gestor                                                              |
| CICA       | Canadian Institute of Chartered Accountants                                |
| CN         | <i>Common Name</i>                                                         |
| CNE        | Carteira Nacional de Estrangeiro                                           |
| CNPJ       | Cadastro Nacional de Pessoas Jurídicas                                     |
| CPF        | Cadastro de Pessoas Físicas                                                |
| DN         | <i>Distinguished Name</i>                                                  |
| DNS        | Domain Name System                                                         |
| DPC        | Declaração de Práticas de Certificação                                     |
| ETSI       | European Telecommunications Standards Institute                            |
| ESI        | Electronic Signatures and Infrastructures                                  |
| FIPS       | (US Government) Federal Information Processing Standard                    |
| FQDN       | Fully Qualified Domain Name                                                |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira                               |
| IDS        | <i>Intrusion Detection System</i>                                          |
| IEC        | <i>International Electrotechnical Commission</i>                           |
| IETF PKIX  | <i>Internet Engineering Task Force - Public-Key Infrastructure (X.509)</i> |
| ISO        | <i>International Organization for Standardization</i>                      |
| ITU        | <i>International Telecommunications Union</i>                              |

|       |                                                        |
|-------|--------------------------------------------------------|
| LCR   | Lista de Certificados Revogados                        |
| NBR   | Norma Brasileira                                       |
| NIS   | Número de Identificação Social                         |
| OCSP  | <i>Online Certificate Status Protocol</i>              |
| OID   | Object Identifier                                      |
| OM-BR | Objetos Metrológicos ICP-Brasil                        |
| OU    | Organization Unit                                      |
| OV    | Organization Validation                                |
| PASEP | Programa de Formação do Patrimônio do Servidor Público |
| PC    | Políticas de Certificado                               |
| PCN   | Plano de Continuidade do Negócio                       |
| PIN   | Personal Identification Number                         |
| PIS   | Programa de Integração Social                          |
| POP   | <i>Proof of Possession</i>                             |
| PRD   | Plano de Recuperação de Desastres                      |
| PRI   | Plano de Recuperação de Incidentes                     |
| PS    | Política de Segurança                                  |
| PSBio | Prestador de Serviço Biométrico                        |
| PSS   | Prestadores de Serviço de Suporte                      |
| PUK   | PIN Unblocking key                                     |
| RFC   | Request For Comments                                   |
| RG    | Registro Geral                                         |
| SAT   | Sistema Autenticador e Transmissor                     |
| SNMP  | <i>Simple Network Management Protocol</i>              |
| SSL   | <i>Secure Socket Layer</i>                             |
| TLS   | <i>Transport Layer Security</i>                        |
| UF    | Unidade de Federação                                   |
| URL   | Uniform Resource Locator                               |
| ZDM   | Zona Desmilitarizada                                   |

## 2. DISPOSIÇÕES GERAIS

### 2.1. Obrigações do Repositório

#### 2.1.1. Repositórios:

- a) AAC disponibiliza, logo após a sua emissão, os certificados emitidos por ela e a sua LCR;
- b) AAC disponibiliza para consulta, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e

c) A AC implementa os recursos necessários para garantir a segurança dos dados nele armazenados.

2.1.2. Os requisitos aplicáveis aos repositórios da AC estão abaixo descritos:

a) Localização Física: Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

b) Disponibilidade – aquela definida no item 2.6.1;

c) Protocolos de acesso – HTTP e HTTPS;

d) Requisitos de segurança – obedece aos requisitos definidos no item 5.

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

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

<http://certificados2.serpro.gov.br/lcr/>  
<https://repositorio.serpro.gov.br/lcr/>

## 2.2. Publicação de informações dos certificados

2.2.1. A AC publica e mantém disponível em sua página *web* as informações descritas no item 2.2.2. no endereço <https://certificados.serpro.gov.br/serprossl>. A disponibilidade da página é de no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2. As seguintes informações são publicadas na página *web*:

- a) seu próprio certificado;
- b) suas LCRs;
- c) sua DPC;
- d) as PCs que implementam essa AC;
- e) relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços;
- f) relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.
- g) *links* para páginas *web* separadas com certificados válido, revogado e expirado por ela emitidos para que fornecedores de software ou aplicações realizem testes.

## 2.3. Tempo ou Frequência de Publicação

2.3.1. A frequência de publicação de LCRs e a frequência de atualização de registros OCSP são especificadas nas Seções 4.9.7 e 4.9.9 deste documento.

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



A AC revisa sua DPC pelo menos uma vez ao ano e faz as alterações necessárias para que a operação da AC permaneça precisa, transparente e cumprindo com os requisitos listados na Seção 8 deste documento.

A Tabela de revisão na Seção 1.2. Indicam as revisões e atualizações feitas nesta DPC adicionando uma data de registro de alterações e incremento do número da versão da DPC, mesmo que nenhuma outra alteração seja feita no documento.

Versões novas ou modificadas desta DPC são publicadas logo após o envio para o ITI.

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

Não existe nenhuma restrição ao acesso para consulta a esta DPC, às suas PCs, aos certificados emitidos e a LCR da AC.

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

## **3. IDENTIFICAÇÃO E AUTENTICAÇÃO**

### **3.1. Atribuição de Nomes**

#### **3.1.1. Tipos de nomes**

3.1.1.1. Os tipos de nomes admitidos para os titulares de certificados da AC é o “*distinguished name*” do padrão ITU X.500, endereços de correios eletrônicos, endereço de página *Web* (URL), ou outras informações que permitam a identificação unívoca do titular.

3.1.1.2. Não se aplica.

#### **3.1.2. Necessidade de nomes significativos**

Para identificação dos titulares dos certificados emitidos, a AC faz uso de nomes significativos que possibilitam determinar a identidade da organização a que se referem.

#### **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. Os requisitos e procedimentos específicos, quando aplicáveis, estão detalhados na PC implementada.

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

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

Os identificadores do tipo “*Distinguished name*” (DN) são únicos para cada titular de certificados emitidos pela AC. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

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

A AC reserva-se o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes. Durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

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

De acordo com a legislação em vigor.

## **3.2. Validação inicial de identidade**

Os procedimentos e os requisitos para a primeira identificação e cadastramento junto à ICP-Brasil de pessoas físicas titulares ou responsáveis por certificados digitais, compreendem os seguintes processos:

a) identificação e cadastro iniciais do titular do certificado – identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3 e 3.2.7, observado o quanto segue:

i. Para certificados de pessoa física: Não se aplica.

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

b) emissão do certificado: após a conferência dos dados da solicitação de certificado com os constantes dos documentos e biometrias apresentados, na etapa de identificação, é liberada a emissão do certificado no sistema da AC. A extensão Subject Alternative Name é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

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

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

### **3.2.2. Autenticação da Identidade de uma organização**

A AC faz a verificação da identidade do solicitante e a autenticidade de seu representante legal usando processo de verificação que atende o item 3.2.2.1. e também verifica se os documentos apresentados são verdadeiros ou não.

### 3.2.2.1. Disposições Gerais

3.2.2.1.1. Os procedimentos empregados pela AR vinculada para a confirmação da identidade de uma pessoa jurídica é feita mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

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

3.2.2.1.3. Deverá ser feita a confirmação da identidade da organização e da pessoa física, responsável pelo certificado, nos seguintes termos:

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

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

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

3.2.2.1.4. Não se aplica;

3.2.2.1.5. O disposto no item 3.2.2.1.3 poderá ser realizado:

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

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

a) Relativos a sua habilitação jurídica:

- i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do CNPJ;
- ii. se entidade privada:

1. Certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e
  2. Documentos da eleição de seus representantes legais, quando aplicável;
- b) Relativos a sua habilitação fiscal:
- i. Prova de inscrição no cadastro nacional de Pessoas Jurídicas - CNPJ; ou
  - ii. Prova de inscrição no cadastro Específico do INSS – CEI.

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

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

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

- a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;
- b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
- c) Nome completo do responsável pelo certificado, sem abreviações;<sup>3</sup> e d) Data de nascimento do responsável pelo certificado.

3.2.2.3.2. A PC define, como obrigatório, o preenchimento de outros campos, o responsável pelo certificado, mediante declaração expressa no termo de titularidade.

### 3.2.2.4. Responsabilidade decorrente do uso do certificado de uma organização

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

### 3.2.3. Autenticação da identidade de um indivíduo

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

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

#### 3.2.3.1. Documentos para efeito de identificação de um indivíduo

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

a) Apresentação da seguinte documentação, em sua versão original, física o digital:

- I. Registro de identidade ou passaporte se brasileiro; ou
- II. Título de Eleitor com foto; ou
- III. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
- IV. Passaporte, se estrangeiro não domiciliado no Brasil;

b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

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

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

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

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

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

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

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.1.7. Não se aplica.

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

3.2.3.1.8.1. Não se aplica.

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

#### 3.2.3.2.1. Não se aplica

##### 3.2.3.2.1.1. Não se aplica.

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

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

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

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

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

Não se aplica.

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

Não se aplica.

### **3.2.6. Critérios para interoperação**

Não se aplica.

### **3.2.7. Autenticação da Identidade de um equipamento ou aplicação**

#### 3.2.7.1. Disposições Gerais

3.2.7.1.1. Em se tratando de certificado emitido para equipamento, o titular será a pessoa jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

##### 3.2.7.1.2. Não se aplica.

3.2.7.1.3. Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e da pessoa física responsável pelo certificado, na forma do item 3.2.2.

##### 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

3.2.7.2.1. Para certificados de equipamento que utilizem URL na identificação do titular, deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele endereço. Nesse caso deve ser apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

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. É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nos documentos apresentados:

- a) URL ou nome da aplicação<sup>1</sup>;
- b) nome completo do responsável pelo certificado, sem abreviações<sup>2</sup>;
- c) data de nascimento do responsável pelo certificado<sup>3</sup>;
- d) nome empresarial constante do CNPJ(Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o titular for pessoa jurídica<sup>4</sup>;
- e) Cadastro Nacional de Pessoa Jurídica (CNPJ), se o titular for pessoa jurídica<sup>5</sup>.

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

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

---

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

2 No campo Subject Alternative Name, OID 2.16.76.1.3.2.

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

4 No campo Subject Alternative Name, OID 2.16.76.1.3.8.

5 No campo Subject Alternative Name, OID 2.16.76.1.3.3.

Não se aplica.

### **3.2.8. Procedimentos complementares**

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

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

3.2.8.2.1. Não se aplica.

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

3.2.8.3.1. Não se aplica.

3.2.8.3.2. Não se aplica.

3.2.8.3.3. Não se aplica.

3.2.8.4. As AC devem disponibilizar, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

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

3.2.8.4.2. Não se aplica.

### **3.2.9. Procedimentos específicos**

Não se aplica.

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

3.3.1. Neste item a DPC estabelece os processos de identificação e confirmação do cadastro do solicitante, utilizados pela AC SERPRO SSL, 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, 3.2.3 ou 3.2.7;
- b) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;
- c) Não se aplica;
- d) Não se aplica;
- e) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico; ou
- f) não se aplica.

3.3.2.1. Não se aplica.

3.3.3. Não existem procedimentos específicos nas PCs implementadas.

3.3.4. Não se aplica.

#### **3.4. Identificação e Autenticação para solicitação de revogação**

A solicitação de revogação de certificado é realizada através de formulário específico na página da AR emissora do certificado, permitindo a identificação inequívoca do solicitante.

A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas.

O procedimento para solicitação de revogação de certificado emitido pela AC está descrito no item 4.9.2. desta DPC.

As razões para revogação do certificado sempre serão informadas para o seu titular.

As solicitações de revogação de certificados serão registradas.

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

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

#### **4.1. Solicitação de 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) Mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; e

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] específico;

d) Não se aplica.

Nota 1: Não se aplica.

Nota 2: Na impossibilidade técnica de assinatura digital do termo de titularidade, como certificados SSL, de equipamento, de aplicação, será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil, do titular do certificado ou responsável pelo certificado, no caso de certificado de pessoa jurídica.

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

A AC utilizará o sistema SAF do próprio ITI, onde se tem acesso a uma base de dados com informações a respeito de fraudes, como também a lista de exceções do sistema do PsBIO.

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

A submissão da solicitação deve ser sempre por intermédio da AR e por pessoa jurídica.

4.1.1.1. Não se aplica.

4.1.1.2. Não se aplica.

4.1.1.3. Não se aplica.

4.1.1.4. Não se aplica.

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

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

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

4.1.2.1.1. AAC responde pelos danos a que der causa.

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

4.1.2.1.3. Não se aplica.

##### **4.1.2.2. Obrigações da AC**

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

a) operar de acordo com DPC da AC e com a PC que a implementa;

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

c) assegurar a proteção de suas chaves privadas;

- d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;
- e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- f) distribuir o seu próprio certificado;
- g) emitir, expedir e distribuir os certificados de AR a ela vinculadas e de usuários finais;
- h) informar a emissão do certificado ao respectivo solicitante;
- i) revogar os certificados por ela emitidos;
- j) emitir, gerenciar e publicar suas LCR e, disponibilizar consulta on-line de situação do certificado (OCSP - *On-line Certificate Status Protocol*), quando aplicável;
- k) publicar na página *web* a DPC e a PC aprovada, que a implementa;
- l) publicar, na página *web*, as informações definidas no item 2.2.2. deste documento;
- m) publicar, na página *web*, informações sobre o descredenciamento de AR;
- n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;
- o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementa, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- s) manter e testar anualmente seu Plano de continuidade do Negócio - PCN;
- t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;
- u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;

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

#### 4.1.2.3. Responsabilidades da AR

AAR será responsável pelos danos a que der causa.

#### 4.1.2.4. Obrigações da AR

As obrigações das ARs vinculadas à AC estão abaixo relacionadas:

- a) receber solicitações de emissão ou de revogação de certificados;
- b) confirmar a identidade do solicitante e a validade da solicitação;
- c) encaminhar a solicitação de emissão ou de revogação de certificado à AC utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-Brasil[1];
- d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1], bem como no documento WEBTRUST PRINCIPLES AND CRITERIA FOR REGISTRATION AUTHORITIES(Referências Bibliográficas);
- f) manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;
- g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2., 3.2.3. e 3.2.7; e
- h) divulgar suas práticas, relativas a cada cadeia de AC ao qual se vincular, em conformidade com o documento WEBTRUST PRINCIPLES AND CRITERIA FOR REGISTRATION AUTHORITIES(Referências Bibliográficas).

## 4.2. Processamento de Solicitação de Certificado

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

AAC e AR executam 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. Não se aplica.

4.2.2.2. A AC e AR podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC..

#### **4.2.3. Tempo para processar a solicitação de certificado**

A AC deve cumprir os procedimentos determinados na ICP-Brasil. Não haverá tempo máximo para processar as solicitações na ICP-Brasil.

### **4.3. Emissão de Certificado**

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

4.3.1.1. Os certificados são emitidos pela AC de acordo com os seguintes passos:

- a) O responsável pela AR verifica o completo e correto preenchimento da solicitação do certificado, bem como a documentação do solicitante, como também o controle do domínio pelo solicitante;
- b) O responsável pela AR aprova a solicitação, disponibilizando o certificado para a instalação por seu solicitante;
- c) O software de AC emite automaticamente um *e-mail* informando ao solicitante que o certificado está disponível para instalação.
- d) O certificado dessa AC só poderá ser emitido com uma declaração do órgão solicitante.

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

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

O software de AC emite automaticamente um e-mail informando ao solicitante que o certificado está disponível para instalação.

### **4.4. Aceitação de Certificado**

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

4.4.1.1. O recebimento de um certificado pelo Titular de Certificado e o uso subsequente das chaves e certificado, constitui aceitação do certificado por parte do Titular de Certificado. Aceitando um certificado, o Titular de Certificado:

- a) Concorde estar de acordo com as responsabilidades contínuas, obrigações e deveres impostas a ele pelo Termo de responsabilidade e PC implementada pela AC e esta DPC;
- b) Garante que por seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado;
- c) Afirma que as informações de certificado fornecidas durante o processo de solicitação são verdadeiras e foram publicadas dentro do certificado com precisão.

4.4.1.2. A aceitação de todo certificado emitido é garantida pela assinatura do Termo de Titularidade pelo respectivo titular.

No caso dessa AC, os certificados são emitidos para equipamentos e, portanto, a aceitação é feita pela pessoa física, que representa a pessoa jurídica e responsável pelo uso subsequente ao recebimento do certificado.

4.4.1.3. Não se aplica.

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

O certificado da AC são publicados de acordo com item 2.2. desta DPC.

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

Não se aplica.

#### **4.5. Usabilidade do par de chaves e do certificado**

O titular do certificado para usuário final devem operar de acordo com a DPC dessa AC e com a Políticas de Certificado (PC) que implementa, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

4.5.1.1. A AC utiliza sua chave privada e garante a proteção dessa chave conforme o previsto nesta DPC.

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

As obrigações do titular de certificado emitido de acordo com esta DPC e constantes dos termos de titularidade de que trata o item 4.1, são as abaixo relacionadas:

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

Nota: Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, estas obrigações se aplicam ao responsável pelo certificado.

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

Em acordo com o item 9.6.4 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

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

Não se aplica.

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

Em acordo com item 4.3 desta DPC.

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

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

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

4.9.1.1. A AC pode revogar um certificado em até 24 horas, por ela emitido, por um ou todos os motivos listados:

- a) Solicitação de revogação corretamente preenchida pelo Titular do Certificado;
- b) Solicitação de revogação enviada à AC por um terceiro autorizado, por exemplo, uma determinação judicial;
- c) Solicitação de revogação feita por uma pessoa com procuração do Titular do Certificado;
- d) Titular de Certificado deixa a comunidade de interesses sob a qual seu certificado foi emitido, por exemplo:
  - Titular de Certificado organizacional deixa o emprego;
  - Ocorre o falecimento do Titular de Certificado;

4.9.1.2. Um certificado é revogado obrigatoriamente pelos seguintes motivos.

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

4.9.1.3. Em relação à revogação, deve ainda ser observado que:

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



- b) O CG da ICP-Brasil ou a AC Raiz determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.
- c) O certificado não está em conformidade com os requisitos dos itens 6.1.5. e 6.1.6;
- d) O certificado foi utilizado incorretamente pelo Titular do Certificado, violando uma de suas obrigações por ele assina no Termo do certificado;
- e) Quando a AC está ciente de uma mudança material nas informações contidas no certificado;
- f) Quando o certificado não foi emitido de acordo com os Requisitos ou a Política de Certificação ou Declaração de Prática de Certificação dessa AC;
- g) A AC determina ou está ciente de que qualquer informação exibida no certificado está imprecisa;

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

4.9.1.4.1. A AC suporta requisições OCSP em conformidade com a RFC 6960 e/ou RFC5019 e requisitos do documento WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES[14]. A resposta OCSP deve ter validade mínima de um dia e máxima de uma semana, sendo que a próxima atualização deve estar disponível a cada quatro dias.

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

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

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

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

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

- h) Não se aplica
- i) Não se aplica.
- j) Não se aplica.

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

4.9.3.1. O procedimento para a solicitação de uma revogação varia dependendo de quem a origina e a AC terá um prazo de até 24 horas após a solicitação de responder a revogação.

As solicitações de revogação de certificado podem ser realizadas das formas abaixo e estão disponíveis 24 x 7:

- a) Através da página de solicitação do certificado na opção “Revogar”;
- b) Envio do formulário específico disponibilizado na página de solicitação de certificados, preenchidos como os dados do solicitante e assinado;
- c) Por Denúncia de Fraude, através dos canais de atendimento do item 1.5.2, “b”.

4.9.3.2. Como diretrizes gerais, fica estabelecido que:

- a) O solicitante da revogação de um certificado será identificado;
- b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas;
- c) As justificativas para a revogação de um certificado são documentadas; e
- d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.9.3.3. O 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 Não se aplica.

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

4.9.3.6. Caso sejam requeridos procedimentos de revogação específicos para a PC implementada, os mesmos devem ser descritos na PC, no item correspondente.

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

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

4.9.4.2. A AC estabelece o prazo de 7 (sete) dias úteis para a aceitação do certificado solicitado por seu titular, dentro dos quais a revogação do certificado poderá ser solicitada sem cobrança de tarifa pela AC.

#### **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 deve processar a revogação imediatamente após a análise do pedido.

Dentro de 24 horas após o recebimento de um relatório de problemas com o certificado, a AC investigará os fatos e circunstâncias relacionadas nesse Relatório fornecerá um relatório preliminar ao titular do certificado.

Depois de analisar os fatos e as circunstâncias, a AC notificará o titular do certificado e o período desde o recebimento do relatório de problemas não excederá o prazo estabelecido no item 4.9.1.1.

A data selecionada pela AC considerará os seguintes critérios para avaliação:

1. A natureza do problema alegado (escopo, contexto, gravidade, magnitude, risco de dano);
2. As consequências da revogação (impactos diretos e colaterais aos titulares);
3. O número de Relatórios de Problemas com Certificados que já foram recebidos sobre um determinado certificado;
4. A entidade que fez a denúncia (por exemplo, uma denúncia de um oficial da justiça ou não, de que um site está envolvido em atividades ilegais) e
5. Legislação relevante.

#### **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 identificadas em cada certificado na cadeia de certificação.

A autenticidade da LCR deve também ser confirmada por meio da verificação da assinatura da AC e do período de validade da LCR.

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

4.9.7.1. A frequência de emissão de LCR referentes a certificados de usuários finais é de 1 (uma) hora.

4.9.7.2. A frequência máxima admitida para a emissão de LCR para os certificados de usuário finais é de 6 (seis) horas.

4.9.7.3. Não se aplica.

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 suporta o processo de verificação da situação de estado de certificados de forma on-line (OCSP).

O processo de revogação on-line está disponível ao Titular do Certificado, conforme descrito no item 3.4.

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

A AC disponibiliza diretório on-line(OCSP) para verificar o estado dos certificados emitidos, como também a LCR.

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

4.9.11.1. A AC não suporta outras formas para divulgação da revogação que não através da publicação de LCR e no diretório OCSP.

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, o Titular do Certificado deverá comunicar imediatamente a AC.

4.9.12.2. A comunicação a AC deverá ser através de formulário específico disponibilizado na página (Solicitação de Revogação) da AC, como também nos canais disponíveis no item 1.5.2.

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

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

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

AAC, aprovados pelo Comitê Gestor.

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

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

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

Os períodos de suspensão serão estabelecidos por norma específica da DPC e PC associada.

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

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

AAC fornece um serviço de status de certificado na forma de um ponto 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. Caso seja necessária a extinção dos serviços da AC ou AR, a AC SERPRO SSL efetuará os procedimentos aplicáveis descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-Brasil [6].

4.11.2. Os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivos, incluem:

- a) Notificação para o e-mail do titular do certificado.
- b) Transferência progressiva do serviço e dos registros operacionais para um sucessor que tenha os mesmos requisitos de segurança da entidade extinta;
- c) Preservação de quaisquer registros não transferidos a um sucessor.
- d) As chaves públicas dos certificados emitidos pela AC dissolvida serão armazenadas por outra AC após aprovação da AC Raiz.
- e) Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC SERPRO ACF.
- f) A AC SERPRO ACF, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.
- g) Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

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

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

Não se aplica.

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

Não se aplica.

## **5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES**

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

### **5.1. Controle Físico**

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

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

5.1.1.2. Todos os aspectos de construção das instalações da AC, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos abaixo:

- a) Todas as instalações de equipamentos de apoio, tais como: máquinas de ar-condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, retificadores e estabilizadores e similares;
- b) Instalações para sistemas de telecomunicações;
- c) Sistema de aterramento e de proteção contra descargas atmosféricas; e
- d) Iluminação de emergência.

#### **5.1.2. Acesso físico**

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

##### **5.1.2.1. Níveis de Acesso**

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

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

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

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro nível e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC. 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 – é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

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

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

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

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

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

5.1.2.1.11. São três os tipos de serviço abrigados no ambiente de quarto nível:

- a) Equipamentos de produção *online* e cofre de armazenamento;
- b) Equipamentos de produção *offline* e cofre de armazenamento;
- c) Equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

5.1.2.1.12. O quinto nível – ou nível 5 – é interno aos ambientes de nível 4, e compreende cofres e gabinetes reforçados trancados. 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 ou o gabinete obedecem às seguintes especificações mínimas:

- a) Ser feito em aço ou material de resistência equivalente; e
- b) Possuir tranca com chave.

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

#### 5.1.2.2. Sistema físico de detecção

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

5.1.2.2.2. As mídias de armazenamento 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 mídia) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma mídia referente a cada semana. Essas mídias são armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. Onde houver, a partir do nível 2, vidros separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado ininterruptamente.

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

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

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

#### 5.1.2.3. Sistema de Controle de Acesso

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

#### 5.1.2.4. Mecanismos de emergência

5.1.2.4.1. Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com



controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

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

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

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

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

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

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

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

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

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

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

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

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

- a) Geradores de porte compatível;
- b) Geradores de reserva;
- c) Sistemas de *no-breaks* redundantes;
- d) Sistemas redundantes de ar-condicionado.

#### **5.1.4. Exposição à água**

A estrutura inteira 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 das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

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

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

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

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

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

#### **5.1.7. Destruição de lixo**

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

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

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

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

### **5.2. Controles Procedimentais**

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

#### **5.2.1. Perfis qualificados**

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

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

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

5.2.1.3.1. A AC realiza um exame, para emissão de certificados em cadeia do tipo SSL, nos operadores do sistema de certificação da AC, de acordo com os requisitos de princípios e critérios WebTrust Baseline[14].

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

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

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

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

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

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

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

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

5.2.3.3. A AC implementa um padrão de utilização de "*senhas fortes*", definido em seu Manual de Segurança e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], junto a procedimentos de validação dessas senhas.

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

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC, pelas AR e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. A DPC garante que todos os empregados da AC e das AR e PSS vinculados, encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

- a) Os termos e as condições do perfil que ocupam;
- b) O compromisso de observar as normas, políticas e regras aplicáveis da AC;
- c) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e
- d) O compromisso de não divulgar informações sigilosas a que tenham acesso.

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

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

#### **5.3.2. Procedimentos de verificação de antecedentes**

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

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

5.3.2.2. AAC poderá definir requisitos adicionais para a verificação de antecedentes.

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

Todo o pessoal da AC e da AR vinculada, envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, com provas ao final do treinamento quando se atribui um conceito que atribui domínio dos seguintes temas:

- a) Princípios e mecanismos de segurança da AC e da AR vinculada;
- b) Sistema de certificação em uso na AC;

- c) Procedimentos de recuperação de desastres e de continuidade do negócio;
- d). Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.2.2, 3.2.3. e 3.2.7; e
- e) Outros assuntos relativos a atividades sob sua responsabilidade.

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

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

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

AAC não implementa rodízio de cargos.

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

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

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

- a) Relato da ocorrência com “*modus operandis*”;
- b) Identificação dos envolvidos;
- c) Eventuais prejuízos causados;
- d) Punições aplicadas, se for o caso; e
- e) Conclusões.

5.3.6.3. Concluído o processo administrativo, a AC encaminhará suas conclusões à AC Raiz.

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

- a) Advertência;
- b) Suspensão por prazo determinado; ou
- c) Impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

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

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

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

5.3.8.1. AAC disponibiliza para todo o seu pessoal, para a AR vinculada:

- a) Esta DPC;
- b) A PC que implementa;
- c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8];
- d) A Política de Segurança da AC;
- e) Documentação operacional relativa às suas atividades; e
- f) Contratos, normas e políticas relevantes para suas atividades.

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

#### **5.4. Procedimentos de Log de auditoria**

Nos itens seguintes esta DPC descreve os aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC com o objetivo de manter um ambiente seguro.

##### **5.4.1. Tipos de Evento Registrados**

5.4.1.1. Todas as ações executadas pelo pessoal da AC, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou. A AC registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

- a) Iniciação e desligamento do sistema de certificação;
- b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC;
- c) Mudanças na configuração da AC ou nas suas chaves;
- d) Mudanças nas políticas de criação de certificados;
- e) Tentativas de acesso (*login*) e de saída do sistema (*logout*);
- f) Tentativas não-autorizadas de acesso aos arquivos de sistema;
- g) Geração de chaves próprias da AC ou de chaves de usuários finais;
- h) Emissão e revogação de certificados;
- i) Geração de LCR, das listas de revogação de certificados e de entrada do diretório OCSP;
- 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. Essa AC tem a possibilidade de auditar até 6% dos certificados SSL emitidos.

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

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

5.4.1.3. Os registros de auditoria mínimos a serem mantidos pela AC incluem além dos acima:

- a) Registros de solicitação, inclusive registros relativos a solicitações rejeitadas;
- b) Pedidos de geração de certificado, mesmo que a geração não tenha êxito;
- c) Registros de solicitação de emissão de LCR.

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

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

5.4.1.6. A AR vinculada à AC SERPRO SSL, pela DPC, 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 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.

5.4.1.6.1. Não se aplica.

5.4.1.7. AAC armazena, eletronicamente, as cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados e dos termos de titularidade.

#### **5.4.2. Frequência de auditoria de registros (logs)**

A periodicidade de auditoria de registros não será superior a uma semana, sendo que os registros de auditoria são analisados pelo pessoal operacional da AC. Todos os eventos significativos são

explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando-se que não foram alterados. Em seguida procede-se a 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 mantém localmente, nas instalações do SERPRO, os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, faz o armazenamento da maneira descrita no item 5.5.

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

5.4.4.1. Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação.

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

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

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

A AC executa procedimentos de backup, de todo o sistema de certificação (sistemas operacionais, aplicação e banco de dados) de duas formas:

- a) Diariamente: cópia de segurança; e
- b) Semanalmente: cópia armazenada para processos de auditoria.

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

O sistema de coleta de dados de auditoria da AC é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação da AC, pelo sistema de controle de acesso e pelo pessoal operacional. A localização dos recursos se encontra na tabela abaixo:

| Tipo de evento                                                                                    | Sistema de coleção | Registrado por      |
|---------------------------------------------------------------------------------------------------|--------------------|---------------------|
| Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional    | Automático         | Sistema operacional |
| Início e parada de aplicação                                                                      | Automático         | Sistema operacional |
| Sucesso e fracasso de tentativas de log-in e log-out                                              | Automático         | Sistema operacional |
| Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema               | Automático         | Sistema operacional |
| Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados | Automático         | Sistema operacional |



|                                                                                                       |                     |                                                              |
|-------------------------------------------------------------------------------------------------------|---------------------|--------------------------------------------------------------|
| Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados  | Automático          | <i>Software</i> de AC ou AR                                  |
| Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado | Automático          | <i>Software</i> de AR                                        |
| <i>Logs</i> de <i>Backup</i> e restauração                                                            | Automático e manual | Sistema operacional e pessoal de operações                   |
| Mudanças de configuração de sistema                                                                   | Manual              | Pessoal de operações                                         |
| Atualizações de <i>software</i> e <i>hardware</i>                                                     | Manual              | Pessoal de operações                                         |
| Manutenção de sistema                                                                                 | Manual              | Pessoal de operações                                         |
| Mudanças de pessoal                                                                                   | Manual              | Pessoal de operações                                         |
| Registros de acessos físicos                                                                          | Automático e manual | <i>Software</i> de controle de acesso e pessoal de operações |

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

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

#### 5.4.8. Avaliações de vulnerabilidade

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

Além disso, o programa de segurança da AC inclui uma Avaliação de Risco anual que:

1. Identifica ameaças internas e externas previsíveis que podem resultar em acesso não autorizado, divulgação, uso indevido, alteração ou destruição de quaisquer dados do certificado ou no próprio ciclo de vida do mesmo;
2. Avalia a probabilidade e o possível dano dessas ameaças, levando em consideração a sensibilidade dos dados do certificado e o processo de gerenciamento dos mesmos; e
3. Avalia as políticas, procedimentos, sistemas de informação, tecnologia e outros acordos que a AC possui para combater essas ameaças.

### 5.5. Arquivamento de Registros

Nos itens seguintes é descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC e pela AR vinculada.

#### 5.5.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC:

- 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; e
- g) Informações de auditoria previstas no item 5.4.1.

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

Os períodos de retenção para cada registro arquivado são os seguintes:

- a) As LCR referentes a certificados de assinatura digital são retidas 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 arquivos**

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

### **5.5.4. Procedimentos para cópia de arquivos**

5.5.4.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo à AC e recebem o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

5.5.4.3. É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

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

Os servidores da AC são sincronizados com a hora fornecida pela AC RAIZ por meio de sua Fonte Confiável do Tempo – FCT conforme DOC-ICP 07 [16]. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.

No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

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

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

| Tipo de evento                                     | Sistema de coleção  | Registrado por                           |
|----------------------------------------------------|---------------------|------------------------------------------|
| Solicitações de certificados                       | Automático e manual | Software de AC/AR e pessoal de operações |
| Solicitações de revogação de certificados          | Automático e manual | Software de AC/AR e pessoal de operações |
| Notificações de comprometimento de chaves privadas | Manual              | Pessoal de operações                     |
| Emissões e revogações de certificados              | Automático          | Software de AC/AR                        |
| Emissões de LCR                                    | Automático          | Software de AC/AR                        |
| Correspondências formais                           | Manual              | Pessoal de operações                     |

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

A integridade dos arquivos da AC e da AR vinculada é verificada na ocasião em que o arquivo é preparado, ou diariamente com a execução automática de *script*.

### 5.6. Troca de chave

5.6.1. A AC comunica aos Titulares de Certificado, por e-mail, a necessidade de renovação do certificado, com antecedência de 30 dias, com instruções para a renovação do mesmo.

5.6.2. Detalhes dos procedimentos estão descritos na PC implementada.

### 5.7. Comprometimento e Recuperação de Desastre

A AC declara que os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres estão descritos no PCN – Plano de Continuidade de Negócio da AC - conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], garantindo a continuidade dos seus serviços críticos.

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

5.7.1.1. O Plano de Continuidade de Negócio(PCN), é de acesso restrito, testado pelo menos uma vez por ano, garantindo a continuidade de serviços críticos. Possui ainda o Plano de Respostas a Incidentes (PRI) e Plano de Recuperação de Desastres(PRD). O PCN, PRD e PRI estão disponíveis para verificação pelos Auditores Qualificados, quando solicitado.

5.7.1.2. Os procedimentos no PCN da AR vinculada para recuperação, total ou parcial das atividades da AR, são os seguintes:

- Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;
- Identificação e concordância de todas as responsabilidades e procedimentos de emergência;

- c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários.
- d) Documentação dos processos e procedimentos acordados;
- e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e
- f) Teste e atualização dos planos.

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

A AC possui o Plano de continuidade de Negócio, que contém ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos e que podem ser resumidas no seguinte:

- a) É feita a identificação de todos os elementos corrompidos;
- b) O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
- c) É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um backup de segurança até a revogação do certificado da AC.

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

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

AAC possui um PCN que especifica as ações a serem tomadas no caso em que o certificado da AC é revogado, e que podem ser resumidas da seguinte forma:

- a) A AC SERPRO, a AC Raiz e os Titulares de Certificados serão notificadas por comunicação segura;
- b) AAC revoga os certificados por ela emitidos;
- c) AAC solicita um novo certificado;
- d) Iniciam-se os procedimentos para emissão dos novos certificados para os usuários.

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

AAC possui um PCN que especifica as ações a serem tomadas no caso de comprometimento de sua chave privada. Após a identificação da crise são notificados os gestores do processo de certificação digital que acionam as equipes envolvidas, para ativar o site de contingência.

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

A AC possui um PRD que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da AC quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.

O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a AC para tornar acessível os registros lógicos mantidos dentro do software. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo uma ordem de prioridade.

## **5.8. Extinção da AC**

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

## **6. Controles Técnicos de Segurança**

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

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

6.1.1.1. O par de chaves da AC é gerado pela própria AC, em módulo criptográfico de *hardware* com padrão de segurança FIPS 140-1 level 3, utilizando algoritmo RSA para geração do par de chaves e algoritmo 3-DES para sua proteção, após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito da ICP-Brasil. A geração é através de uma cerimônia com a participação do pessoal da AC com função confiável para execução do script de geração da chave e participação dos auditores qualificados para tal.

6.1.1.2. Pares de chaves são gerados somente pelo Titular do Certificado correspondente. Os procedimentos específicos estão descritos em cada PC implementada.

6.1.1.3. A PC implementada pela AC define o meio utilizado para armazenamento das respectivas chaves privadas, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.1.4. O processo de geração do par de chaves da AC utiliza módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

6.1.1.6. A chave privada da AC é gerada, armazenada e utilizada apenas em hardware criptográfico específico. O módulo criptográfico da AC segue o padrão “Homologação da ICP-Brasil NSH-3”.

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

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

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

6.1.3.1. A AC SERPRO SSL entregará à AC Raiz, cópia de sua chave pública, em formato PKCS#10. Essa entrega será feita por representante legal da AC, em cerimônia específica, em data e hora previamente estabelecida pela AC.

6.1.3.2. Chaves públicas são entregues ao emissor de certificado por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC.

### 6.1.4. Disponibilização de chave pública da AC para usuários

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

- a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9];
- b) Página *web* da AC <https://certificados.serpro.gov.br/serprossl>.
- c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

### 6.1.5. Tamanhos de chave

6.1.5.1. A PC implementada pela AC definirá os tamanhos das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento “REQUISITOS MINIMOS PARA AS POLITICAS DE CERTIFICADO NA ICP-BRASIL (7)”.

6.1.5.2. Não se aplica.

### 6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC seguem o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

6.1.7.1. Os certificados emitidos pela AC têm no campo “Key usage” (2.5.29.15) ativado os bits digitalSignature e keyAgreement. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC, bem como as possíveis restrições cabíveis em conformidade com as aplicações definidas para os certificados correspondentes, estão especificados em cada PC que implementa.

6.1.7.2. A chave privada da AC é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCRs.

## 6.2. Proteção da Chave Privada

A chave privada da AC é gerada, armazenada e utilizada apenas em *hardware* criptográfico específico, não havendo portanto tráfego da mesma em nenhum momento.

### **6.2.1. Padrões para módulo criptográfico**

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC adota o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. Os módulos de geração de chaves criptográficas dos Titulares de Certificados são aqueles definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9] - Cada PC implementada especifica os requisitos adicionais aplicáveis.

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

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

6.2.2.2. É exigido a presença no mínimo de 2 (dois) detentores da chave de ativação (“n”) de um grupo de 15 (quinze) (“m”) para a ativação da chave da AC.

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

Não se aplica.

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

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

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

6.2.4.3. A AC não mantém cópia de segurança da chave privada de Titular de Certificado de assinatura digital.

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

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

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

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

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

A chave privada da AC é inserida no módulo criptográfico de acordo com o estabelecido na RFC 4210 e 6712.

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

Ver item 6.1.

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

A ativação da chave privada da AC é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de 2 dos custodiantes da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC.

As senhas utilizadas obedecem à política de senhas estabelecida pela AC.

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

A chave privada da AC, armazenada em módulo criptográfico, é desativada quando não mais é necessária através de mecanismo disponibilizado pelo *software* de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação de 2 dos custodiantes da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC. As senhas utilizadas obedecem à política de senhas estabelecida pela AC.

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

Quando a chave privada da AC for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estiver armazenada, deve ser sobrescrito. Todas as cópias de segurança da chave privada da AC e os cartões criptográficos dos custodiantes serão destruídos. Os agentes autorizados para realizar estas operações são os administradores e os custodiantes das chaves de ativação da AC.

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

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

A AC armazena as chaves públicas da própria AC e dos titulares de certificados, 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 uso para as chaves pública e privada**

6.3.2.1. A chave privada da AC e dos titulares de certificados por ela emitidos, são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC pode ser utilizada 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. Cada PC implementada pela AC define o período máximo de validade do certificado que define, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLITICAS DE CERTIFICADO NA ICP-BRASIL [7].



6.3.2.4. A validade admitida para certificados da AC é limitada à validade do certificado da AC, 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, estão descritos os requisitos gerais de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

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

6.4.1.1. Os dados de ativação da chave privada da AC são únicos e aleatórios.

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

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

6.4.2.1. Os dados de ativação da AC são protegidos contra o uso não autorizado, por cartões criptográficos individuais com senha, e são armazenados em ambiente de nível 6 de segurança.

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

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

Não se aplica.

#### **6.5. Controles de Segurança dos computadores**

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

6.5.1.1. A AC 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 do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC estão descritos na PC implementada.

6.5.1.3. Os computadores servidores, utilizados pela AC, 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;
- b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC;
- c) Acesso restrito aos bancos de dados da AC;
- d) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

- e) Geração e armazenamento de registros de auditoria da AC;
- f) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- g) Mecanismos para cópias de segurança (*backup*).

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

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

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

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

Não se aplica.

#### **6.5.3. Controle de segurança para a Autoridade de Registro**

6.5.3.1. São os estabelecidos no documento “CARACTERISTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs da ICP-Brasil[1]”.

6.5.3.2. São os estabelecidos no documento “CARACTERISTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs da ICP-Brasil[1]”, no item 6.5.32 “Estações de Trabalho”.

6.5.3.3. Não se aplica.

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

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

6.6.1.1. A AC adota o Sistema de Certificação Digital do SERPRO (Serviço Federal de Processamento de Dados), desenvolvido em código aberto. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluído os testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente do CCD avalia e decide quando será a implementação no ambiente de produção.

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

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

6.6.2.1. A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

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

- a) Instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;
- b) Implantação ou modificação de Autoridades Certificadoras com customizações de certificados, páginas *web*, *scripts* etc;
- c) Implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos; e
- d) Instalação de novos serviços na plataforma de processamento.

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

Não se aplica.

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

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

## **6.7. Controles de Segurança de Rede**

### **6.7.1. Diretrizes Gerais.**

6.7.1.1. Os controles implementados para garantir a confidencialidade, integridade e disponibilidade dos serviços da AC são os seguintes:

- a) Infraestrutura de conectividade:
  - i. Alojamento seguro de equipamento de comunicação;
  - ii. *Firewall* seguro e serviços de roteador;
  - iii. Serviço de LAN seguro;
  - iv. Serviço *back office* seguro; e
  - v. Serviço de internet seguro e redundante.
- b) Prevenção incidente e avaliação:
  - i. Descoberta de intrusão;

- ii. Análise de vulnerabilidade;
- iii. Configuração segura de servidor; e
- iv. Auditorias técnicas.

c) Administração de Infraestrutura:

- i. Monitoramento de servidor;
- ii. Monitoramento de rede;
- iii. Monitoramento de URL; e
- iv. Relatórios de largura da banda.

6.7.1.2. Nos servidores e elementos de Infraestrutura e proteção de rede utilizado pela AC, somente os serviços estritamente necessários são habilitados.

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

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

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

## **6.7.2. Firewall**

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

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

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

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

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

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

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

As tentativas de acesso não autorizado – em roteadores, *firewall* ou IDS – são registradas em arquivos para análise, são automatizadas. A frequência de exame dos arquivos de registro são diárias ou quando ocorrer algum evento, e todas as ações tomadas em decorrência desse exame são documentadas.

### **6.8. Carimbo de Tempo**

Não se aplica.

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

### **7.1. Perfil do Certificado**

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

#### **7.1.1. Número de versão**

Todos os certificados emitidos pela AC, segundo esta PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

#### **7.1.2. Extensões de certificado**

Referido no mesmo item da PC.

#### **7.1.3. Identificadores de algoritmo**

Referido no mesmo item da PC.

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

Referido no mesmo item da PC.

#### **7.1.5. Restrições de nome**

Referido no mesmo item da PC.

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

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil após a conclusão do processo de credenciamento, é **2.16.76.1.1.137**.

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

Não se aplica.

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

Não se aplica.

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

Extensões críticas devem ser interpretadas conforme a RFC 5280.

## 7.2. Perfil de LCR

### 7.2.1. Número(s) de versão

As LCRs geradas pela AC SERPRO SSL 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. Esta AC implementa as extensões de LCR definidas como obrigatória, conforme item 7.2.2.2.

7.2.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

- a) **“Authority Key Identifier”**: deve conter o hash SHA-1 da chave pública da AC que assina a LCR; e
- b) **“CRL Number”, não crítica**: deve conter um número sequencial para cada LCR emitida pela AC.

## 7.3. Perfil de OCSP

### 7.3.1. Número(s) de versão

Serviços de respostas OCSP implementam a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

### 7.3.2. Extensões de OCSP

O campo **“Authority Information Access”**, não crítica, contém o método de acesso *id-ad-ca/issuer*, que utiliza o protocolo de acesso HTTP para a recuperação da cadeia do certificado;

A segunda entrada desse campo contém o método de acesso *id-ad-ocsp*, com o respectivo endereço <http://ocsp.serpro.gov.br/acserprossl1>

do respondedor OCSP, utilizando o protocolo de acesso, HTTP e **OID: 1.3.6.1.5.5.7.48.1**.

## 8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

### 8.1. Frequência e circunstâncias das avaliações

A AC sofre auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento.

A partir dos requisitos da CA/Browser Forum[5], uma auditoria anual é realizada por um auditor externo independente para avaliar a conformidade da AC com os requisitos estabelecidos. Um período de auditoria não deve exceder um ano de duração.

## **8.2. Identificação/Qualificação do avaliador**

8.2.1. As fiscalizações da AC 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 da AC 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 for CA(11. Referências Bibliográficas)*.

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

8.4.3. As entidades da ICP-Brasil vinculadas (AC, AR e PSS), também receberam auditoria prévia, para fins de credenciamento, e que a AC é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

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

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

## **8.6. Comunicação dos resultados**

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

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

### **9.1. Tarifas**

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

As tarifas de emissão e de renovação de certificado pela AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [13].

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

Não se aplica.

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

Não há tarifa de revogação ou de acesso à informação de status de certificado.

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

Tarifas para outros serviços da AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [13].

#### **9.1.5. Política de reembolso**

Não se aplica.

### **9.2. Responsabilidade Financeira**

A responsabilidade da AC 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. Todas as informações coletadas, geradas, transmitidas e mantidas pela AC e a AR vinculada são consideradas sigilosas, exceto aquelas informações citadas no item 9.3.2.

9.3.1.2. Como princípio geral, nenhum documento, informação ou registro fornecido à ou AR vinculada deverá ser divulgado.

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

Os seguintes documentos da AC e AR vinculada são considerados documentos não confidenciais:



- a) os certificados e as LCRs/OCSP emitidos pela AC;
- b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
- c) a PC implementada pela AC;
- d) a DPC da AC;
- e) versão pública da PS; e
- f) a conclusão dos relatórios de auditoria.

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 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 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 recebem ou tem acesso a informações confidenciais possuem mecanismos que asseguram 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 SERPRO SSL foi gerada e é mantida pela própria AC, que é responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC será de sua inteira responsabilidade.

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

9.3.3.4. Não se aplica.

## **9.4. Privacidade da informação pessoal**

### **9.4.1. Plano de privacidade**

AAC assegura 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 será considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

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

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

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

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

#### **9.4.5. Aviso e consentimento para usar informações privadas**

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

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

Autorizações formais podem ser apresentadas de duas formas:

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

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

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC 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 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**

Nenhum documento, informação ou registro sob a guarda da AR ou da AC SERPRO SSL, 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**

AAC declara e garante o quanto segue, como também os requisitos do CA/Browser Forum[5]:

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

AAC implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC.

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

A AC implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC.

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

AAC, 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**

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

#### **9.6.1.5. Serviço**

A AC mantém 24x7 acesso ao seu repositório com a informação do seu próprio certificado e das LCRs/OCSP.

#### **9.6.1.6. Revogação**

AAC revogará certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos documentos do CA/Browser Forum[5].

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

9.6.3.2. A AC informa à AC Raiz qualquer comprometimento de sua chave privada e solicita 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 é considerado válido quando:

- i. tiver sido emitido pela AC;
- ii. não constar como revogado pela AC;
- iii. não estiver expirado; e
- iv. puder ser verificado com o uso do certificado válido da AC.

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

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

Não se aplica.

### **9.7. Isenção de garantias**

Não se aplica.

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

A AC 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 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 para AC Raiz.

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

Mudança nesta DPC será publicado no site da AC.

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

### **9.16.2. Cessão**

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

### **9.16.3. Independência de disposições**

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

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

De acordo com a legislação vigente.

## **9.17. Outras provisões**

Não se aplica

## **10. Documentos referenciados**

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

| <b>Ref</b> | <b>Nome do documento</b>                                                                        | <b>Código</b>     |
|------------|-------------------------------------------------------------------------------------------------|-------------------|
| <b>[2]</b> | CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL             | <b>DOC-ICP-09</b> |
| <b>[3]</b> | CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL | <b>DOC-ICP-08</b> |
| <b>[6]</b> | CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL           | <b>DOC-ICP-03</b> |
| <b>[7]</b> | REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE                                                         | <b>DOC-ICP-04</b> |

|             |                                                                                                                   |                   |
|-------------|-------------------------------------------------------------------------------------------------------------------|-------------------|
|             | CERTIFICADO NA ICP-BRASIL                                                                                         |                   |
| <b>[8]</b>  | POLÍTICA DE SEGURANÇA DA ICP-BRASIL                                                                               | <b>DOC-ICP-02</b> |
| <b>[12]</b> | REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL              | <b>DOC-ICP-12</b> |
| <b>[13]</b> | POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL                                                 | <b>DOC-ICP-06</b> |
| <b>[16]</b> | DIRETRIZES PARA SINCRONIZAÇÃO DE FREQUÊNCIA E DE TEMPO NA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA ICP-BRASIL | <b>DOC-ICP 07</b> |

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

| <b>Ref</b>  | <b>Nome do documento</b>                                                                                                                                            | <b>Código</b>        |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>[1]</b>  | CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL                                                                                                       | <b>DOC-ICP-03.01</b> |
| <b>[9]</b>  | PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL                                                                                                                   | <b>DOC-ICP-01.01</b> |
| <b>[10]</b> | PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL                         | <b>DOC-ICP-05.02</b> |
| <b>[11]</b> | PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASILPROCEDIMENTOS DE CONFIRMAÇÃO DE CADASTRO DE REQUERENTE DE CERTIFICADO DIGITAL POR MEIO DE VIDEOCONFERÊNCIA | <b>DOC-ICP-05.03</b> |
| <b>[16]</b> | PROCEDIMENTOS DE CONFIRMAÇÃO DE CADASTRO DE REQUERENTE DE CERTIFICADO DIGITAL POR MEIO DE VIDEOCONFERÊNCIA                                                          | <b>DOC-ICP-05.05</b> |

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

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

## 11. REFERÊNCIAS BIBLIOGRÁFICAS

WEBTRUST PRINCIPLES AND CRITERIA FOR REGISTRATION AUTHORITIES, disponível em <http://www.webtrust.org>

PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES FOR CA, disponível em <http://www.webtrust.org>

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

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

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

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

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

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

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