www.serpro.gov.br

Política de Certificados

SERPROACF do tipo A1

(PC SERPROACFA1)

Credenciada pela ICP-Brasil

Versão 1.2 de 12 de dezembro de 2005

Soluções para um Brasil de Todos SERPRO

ÍNDICE

1. Introdução

1.1 Visão Geral

Esta Política de Certificado Digital (PC) refere-se exclusivamente a Certificados de Assinatura Digital do Tipo A1, emitido pela Autoridade Certificadora do SERPRO Final (SERPROACF) credenciada pela ICP-Brasil e implementada sob a Declaração de Práticas de Certificação da SERPROACF.

1.2 Identificação

Esta PC obedece às recomendações da ICP-Brasil para a emissão de certificados de assinatura do tipo A1.

O OID deste documento é: 2.16.76.1.2.1.16

1.3 Comunidade e Aplicabilidade

1.3.1 SERPROACF

O Serviço Federal de Processamento de Dados (SERPRO) opera nas instalações do Centro de Certificação Digital do SERPRO (CCD-SERPRO) a Autoridade Certificadora do SERPRO Final (SERPROACF) como uma das Autoridades Certificadoras que compõem a Infra-estrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora do SERPRO (ACSERPRO).

Esta PC é implementada pela SERPROACF cuja DPC (DPC da SERPROACF) encontra-se publicada na página *Web* da mesma, conforme item 2.6.1.

1.3.2 Autoridades de Registro

As AR vinculadas à SERPROACF são:

- AR SERPRO
- AR ANOREG

Os endereços estão publicados na página *https://ccd.serpro.gov.br/serproacf/.*

É função da AR verificar, autorizar e submeter requisições de certificados e requisições de revogação de certificados, sempre em conformidade com esta Política de Certificado. Também é sua função receber, conferir e autenticar a documentação exigida conforme item 3.1.9 desta PC, além de orientar os Titulares de Certificados nos processos de solicitação de seus certificados.

O operador da AR acata as obrigações a ele impostas por esta Política de Certificados e pela Declaração de Práticas de Certificação da SERPROACF, DPC da SERPROACF, as quais descrevem em linhas gerais todos os seus procedimentos.

A PC será atualizada sempre que houver o credenciamento de mais uma AR vinculada à SERPROACF.

1.3.3 Titulares de Certificado

Os Titulares de Certificados desta PCSERPROACF A1 são pessoas físicas ou jurídicas autorizadas pela AR a receber um certificado digital emitido pela SERPROACF, para sua própria utilização.

Em sendo o titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será a detentora da chave privada.

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

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

1.3.4 Aplicabilidade

Os certificados emitidos sob esta PC pela SERPROACF estão definidos na tabela a seguir:

Nome do Certificado	Tipo	Apropriado para
Usuário Pessoa Física	A1	Pessoas Físicas
Usuário Pessoa Jurídica	A1	Pessoa Jurídica
Servidor	A1	Equipamentos ou aplicação

Esses certificados se destinam à utilização em assinatura digital, não repúdio, garantia de integridade da informação, autenticação de seu titular.

As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigoroso, emitido por qualquer Autoridade Certificadora credenciada pela AC-Raiz.

1.3.4.1 Aplicações Apropriadas

Os certificados emitidos sob esta PC pela SERPROACF são apropriados ao uso apenas nas aplicações apresentadas na tabela descrita a seguir (tabela 2).

Tabela 2 – Aplicações Apropriadas

Política de Certificado	Aplicações apropriadas
PCSERPROACF A1	Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas aplicações abaixo: • Confirmação de Identidade na Web; • Correio Eletrônico; • Transações on-line; • Redes privadas virtuais (VPN);

	• Transações eletrônicas; • Cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.4.2 Aplicações Proibidas

O uso de certificados e chaves privadas emitidas sob esta PC está limitado às aplicações especificadas no item 1.3.4.1. Todas as demais aplicações são proibidas.

1.4 Dados de Contato

Esta PC é administrada pelo Centro de Certificação Digital do SERPRO, CCD-SERPRO localizado no seguinte endereço;

Rua Pacheco Leão Número 1235 – Fundos
Bairro. Jardim Botânico CEP. 22.460.030
Rio de Janeiro – RJ Brasil.

Pessoas de Contato.

Nome: Márcia Paulina Souza
Telefone: (21) 2159-3611 ou 2159-3612
Fax: (21) 2159-3360
(encaminhar aos cuidados do CCD SERPRO)

Email de Contato.

ccdserpro@serpro.gov.br

2. Disposições Gerais

2.1 Obrigações e Direitos

2.1.1 Obrigações da Autoridade Certificadora

A SERPROACF deve:

1. Operar de acordo com:
   - esta PC;
   - a DPC da SERPROACF;
   - a Política de Segurança da SERPROACF;
   - a Política de Segurança da ICP-Brasil.
2. Gerar e gerenciar o seu par de chaves criptográficas;
3. Assegurar a proteção de suas chaves privadas;
4. Notificar a AC Raiz e a ACSERPRO, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado;
5. Notificar os seus usuários quando ocorrer suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado, ou o encerramento de suas atividades;
6. Distribuir o seu próprio certificado;
7. Emitir, expedir e distribuir os certificados de AR vinculadas e os certificados dos usuários finais;
8. Informar a emissão do certificado ao respectivo solicitante;
9. Revogar, quando necessário, os certificados por ela emitidos;
10. Emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR);
11. Manter os processos, procedimentos e atividades em conformidade com a legislação vigente e com as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
12. Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
13. Publicar em sua página Web a DPC da SERPROACF e suas PC aprovadas;
14. Adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança da SERPROACF, envolvendo seus processos, procedimentos e atividades, observada as normas, critérios, práticas e procedimentos da ICP-Brasil;
15. Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
16. Manter e testar regulamento seu Plano de Continuidade do Negócio;
17. Armazenar, pelo prazo estipulado pela ICP-Brasil, cópia dos certificados dos Titulares;
18. Tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
19. Informar às terceiras partes e titulares de certificados acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC;
20. Não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
21. 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 Comitê Gestor da ICP-Brasil.

2.1.2 Obrigações das AR

Pela adesão às práticas descritas nesta PC, os responsáveis pela AR ficam cientes das obrigações a que estão submetidos.

São obrigações dos responsáveis das AR:

1) Operar de acordo com;
   - esta PC:
   - a DPC da SERPROACF;
   - a Política de Segurança da SERPROACF.
2) Receber as solicitações de emissão ou de renovação de certificados;
3) Confirmar a identidade dos solicitantes de certificado de seu domínio, de acordo com os requisitos estabelecidos pelos itens 3 e 4 da PC;
4) Receber e guardar as cópias dos documentos de identificação solicitados dos Titulares de Certificado conforme indicado no item 3.1.9 desta PC;
5) Receber o Termo de Responsabilidade ou Termo de Titularidade assinado pelo Titular do Certificado;
6) Encaminhar a solicitação de emissão ou de revogação de certificado à SERPROACF utilizando VPN (virtual private network – rede privativa virtual), SSL (secure socket layer – protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade;
7) Utilizar VPN (virtual private network – rede privativa virtual), SSL (secure socket layer – protocolo de comunicação segurança) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
8) Informar aos respectivos Titulares de Certificado a emissão ou a revogação de seus certificados;
9) Disponibilizar os certificados emitidos pela SERPROACF aos seus respectivos solicitantes;
10) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
11) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pelo CG da ICP-Brasil;
12) Manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil;
13) Oferecer treinamento aos seus agentes de registro, especialmente quanto ao reconhecimento de assinaturas e validade dos documentos apresentados na forma dos itens 3.1.8 e 3.1.9.

2.1.3 Obrigações de Titulares de Certificado

Aceitando as práticas descritas nesta Política de Certificados (PCSERPROACF A1) , os Titulares de Certificado ficam cientes das obrigações a eles impostas pela mesma. Os Titulares de Certificado, incluindo os responsáveis pela AR e pela SERPROACF, são responsáveis por:

1) Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
2) Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
3) Utilizar os seus certificados e chaves privadas em aplicações aprovadas e de modo apropriado, conforme o previsto nesta PC;

4) Conhecer os seus direitos e obrigações, contemplados por esta PC, pela DPC da SERPROACF e por outros documentos aplicáveis da ICP-Brasil;
5) Notificar imediatamente a AR de qualquer erro ou defeito nos certificados , ou de qualquer mudança subseqüente na informação do certificado;
6) Informar à SERPROACF, através de sua AR, qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
7) Estar ciente das obrigações e responsabilidades estipuladas nesta Política de Certificados sob a qual seu certificado é emitido, assinando o Termo de Responsabilidade.

Nota: Em se tratando de certificado emitido para equipamentos ou aplicação, esta obrigações se aplicam ao responsável pelo uso do certificado.

2.1.4 Direitos do Usuário de Certificado (Terceira Parte Confiável)

Considera-se Usuário de Certificado a entidade que confia no teor, validade e aplicabilidade do certificado digital.

Constituem direitos do Usuário de Certificado:

1) Recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;
2) Verificar, a qualquer tempo, a validade do certificado. Um certificado emitido pela SERPROACF é considerado válido quando:
   - não constar da LCR da SERPROACF;
   - não estiver expirado; e
   - puder ser verificado com o uso de certificado válido da SERPROACF;

O não exercício desses direitos não afasta a responsabilidade da SERPROACF e do titular do certificado.

É recomendável que os Usuários de Certificados:

1) Se familiarizem com esta Política de Certificado;
2) Utilizem certificados emitidos sob esta PC pela SERPROACF em aplicações aprovadas e em propósitos apropriados descritos no item 1.3.4.1 desta PC;
3) Validem os certificados, manual ou automaticamente, antes da utilização das chaves públicas neles contidas;
4) Verifiquem a LCR, manual ou automaticamente, e somente utilizar chaves públicas contidas em certificados que não tenham sido revogados.

2.1.5 Obrigações do Repositório

Não há repositório de certificados implementado. O repositório da LCR é o indicado pelo endereço: http://ccd.serpro.gov.br/lcr/serproacfv1.crl. O mesmo está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

O repositório está instalado em sala com controle de acesso biométrico, há controle de acesso lógico dual, o sistema possui sistema de configuração para eliminação de vulnerabilidades, conforme orientações dos fabricantes e de instituições de segurança reconhecidas. Existe sistema de identificação de intrusão na rede em que o equipamento está conectado, como também há proteção por firewall. O sistema interno de arquivos e diretório do repositório possui controle de permissão de acesso.

2.2 Responsabilidades

2.2.1 Responsabilidades da SERPROACF

A SERPROACF responde pelos danos a que der causa.

2.2.2 Responsabilidades das AR

A AR será responsável pelos danos a que der causa.

2.3 Responsabilidade Financeira

2.3.1 Indenização devida pelos Usuários de Certificados

Não existe situação específica de utilização do certificado da SERPROACF que requeira prática de indenização pelos Usuários de Certificados.

2.3.2 Relações Fiduciárias

A SERPROACF ou AR vinculada indenizará integralmente os danos o que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3 Processos Administrativos

Será seguida a legislação específica uma vez que os Titulares e Usuários de Certificados são funcionários públicos.

2.4 Interpretação e Execução

2.4.1 Legislação Governamental

A PCSERPROACFA1 obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2200-2, de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil.

2.4.2 Forma de interpretação e notificação

No caso de uma ou mais das disposições desta PC ser, por qualquer razão, considerada inválida, ilegal, ou não aplicável, somente essa disposição será afetada, todas as demais permanecem válidas dentro do escopo de abrangência deste documento. A SERPROACF promoverá a correção do item em desacordo, no prazo de 05 dias.

As práticas descritas nesta PC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

As notificações, solicitações ou quaisquer outras comunicações necessárias, sujeitas às práticas descritas na PCSERPROACF A1, são realizadas pela SERPROACF e AR vinculadas por E-mail a ser enviado ao endereço eletrônico fornecido pelo solicitante na solicitação do certificado. O E-mail é considerado como recebido quando enviado a esse endereço..

2.4.3 Procedimentos de resolução de disputas

No caso de um conflito entre esta PC e outras políticas, planos, acordos, contratos ou procedimentos onde o assunto da disputa está entre esta PC e:

1) Um acordo operacional, o acordo operacional prevalecerá;
2) Um Termo de Responsabilidade ou de Titularidade, esta PC prevalecerá;
3) Qualquer política, plano, procedimentos ou qualquer outra documentação operacional ou documentação de práticas, esta PC prevalecerá.

No caso de um conflito entre esta PC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pelo CG da ICP-Brasil.

2.5 Tarifas de Serviço

Como não há tarifas previstas a serem cobradas dos Titulares ou Usuários de Certificados, todos os itens serão relacionados como não aplicáveis. Os serviços da SERPROACF são cobrados através de contratos específicos para este fim celebrados com seus clientes.

2.5.1 Tarifas de emissão ou renovação de certificados

Não há tarifa que incida sobre este serviço.

2.5.2 Tarifas de acesso aos certificados

Não há tarifa que incida sobre este serviço.

2.5.3 Tarifas de revogação ou acesso à informação de estado

Não há tarifa que incida sobre este serviço.

2.5.4 Tarifas para outros serviços como informação de política

Não há tarifa que incida sobre este serviço.

2.5.5 Política de reembolso

Não há política de reembolso uma vez que não há tarifas definidas.

2.6 Publicação e Repositórios

2.6.1 Publicação de informações da SERPROACF

A SERPROACF mantém página *Web* https://ccd.serpro.gov.br/serproacf/ que contém as seguintes informações:

1) PC SERPRO A1: https://ccd.serpro.gov.br/serproacf/docs/pcserproacfa1.pdf;
2) DPC SERPROACF: https://ccd.serpro.gov.br/serproacf/docs/dpcserproacf.pdf
3) LCR: http://ccd.serpro.gov.br/lcr/serproacfv1.crl

4) Certificado da SERPROACF;
5) Certificado da ACSERPRO;
6) Certificado da AC Raiz da ICP-Brasil;
7) Os endereços das instalações técnicas das AR vinculadas.

A disponibilidade da página *Web* é de, no mínimo, de 99% (noventa e nove por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.2 Freqüência da publicação

As publicações das informações descritas no item anterior são;

- As versões mais recentes desta PC e da DPC serão publicadas logo após sua aprovação pela AC-Raiz;
- A LCR é publicada a cada 1 hora;
- Os certificados são publicados logo após a sua geração;
- Os endereços das instalações técnicas da AR são publicados sempre que ocorrer alguma mudança.

2.6.3 Controle de acesso

Não há nenhum controle de acesso de leitura das informações especificadas no item 2.6.1.

Os acessos para modificações dessas informações são feitos por funcionários da SERPROACF, com a utilização de senhas de acesso aos diretórios onde estão arquivadas.

2.6.4 Repositórios

A SERPROACF adota como repositório de LCR uma página *Web* (*http://ccd.serpro.gov.br/lcr/serproacfv1.crl*), que atende aos seguintes requisitos:

1) Disponibilidade – aquela definida no item 2.6.1;
2) Protocolos de acesso – HTTP e HTTPS;
3) Requisitos de segurança – obedece aos requisitos definidos no item 5.

2.7 Auditoria de Conformidade

A SERPROACF, de nível imediatamente subseqüente ao da ACSERPRO, para fins de continuidade do credenciamento, apresenta anualmente relatório de auditoria fornecido por empresa de auditoria especializada e independente, contratada pela SERPROACF e autorizada pela AC Raiz. A SERPROACF realiza auditorias de conformidade anuais nas AR operacionais e disponibiliza à ACSERPRO os relatórios destas auditorias.

A auditoria de conformidade obedece aos requisitos especificados no item 2.7 da DPC da SERPROACF, que inclui os tópicos: freqüência de auditoria de conformidade, identidade e qualificações do auditor, relação entre auditor e parte auditada, tópicos cobertos pela auditoria, medidas adotadas em caso de não conformidade e comunicação de resultados.

A descrição dos tópicos descritos acima estão no item 2.7 da DPC da SERPROACF.

Auditorias intempestivas podem ser executadas por qualquer das entidades acima descritas a qualquer uma das entidades à ela subordinadas.

2.8 Sigilo

A SERPROACF é responsável pela geração, manutenção e sigilo de sua chave privada bem como por sua divulgação ou utilização indevida.

A chave privada de assinatura digital da SERPROACF é mantida pelo CCD-SERPRO, que é responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura da SERPROACF será de inteira responsabilidade da SERPROACF.

Os Titulares de certificados emitidos nesta PC , têm as atribuições de geração e manutenção de suas respectivas chaves criptográficas. Além, disso, responsabilizam-se pela divulgação ou utilização indevida das chaves.

Os titulares de certificados ou os responsáveis pelo uso do certificado devem observar procedimentos básicos de segurança, tais como;

- Nunca fornecer a senha a terceiros;
- Utilizar senhas de, no mínimo, 8 caracteres;
- Montar senhas com caracteres numéricos e alfanuméricos;
- Memorizar a senha e não escrevê-la;
- Guardar a mídia principal e cópia de segurança em lugar seguro.

O certificado emitido sob esta PC não é um certificado de sigilo.

2.8.1 Tipos de Informação Sigilosa

Todas as informações coletadas, geradas, transmitidas e mantidas pela SERPROACF são consideradas sigilosas, exceto os descritos no item 2.8.2.

Como princípio geral, todo documento, informação ou registro fornecido à SERPROACF ou às AR vinculadas será sigiloso.

2.8.2 Tipos de Informação não sigilosas

As informações não sigilosas que podem ser divulgadas pela SERPROACF incluem:

1) os certificados e as LCR emitidos;
2) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
3) esta PC;
4) a DPC da SERPROACF;
5) versões públicas de Políticas de Segurança;
6) resultados finais de auditorias.

2.8.3 Divulgação de Informação de Revogação/Suspensão de Certificados

Informações de estado de certificados são fornecidos através de consulta à LCR aplicável.

O razão para revogação de um certificado sempre será informado para o seu titular, e serão tornadas públicas desde que haja autorização expressa deste.

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

2.8.4 Quebra de sigilo por motivos legais

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da SERPROACF e suas AR é divulgado a entidades legais ou seus funcionários, exceto quando:

1) Exista uma ordem judicial corretamente constituída; e
2) Esteja corretamente identificado o representante da lei.

2.8.5 Informações a terceiros

Nenhum documento, informação ou registro sob a guarda da SERPROACF e suas AR será 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.

2.8.6 Divulgação por solicitação do titular

O Titular do Certificado, ou seu representante legal, poderá ter acesso a quaisquer dos seus dados ou identificações, ou poderá autorizar a divulgação de seus registros a outras pessoas. Para tanto, a solicitação da liberação da informação deverá ser encaminhada a SERPROACF através de E-mail assinado digitalmente pelo Titular do Certificado, ou de carta entregue a um AR da SERPROACF assinada pelo Titular do Certificado.

2.8.7 Outras circunstâncias de divulgação de informação

Não estão previstas outras circunstâncias em que poderão ser divulgadas informações sigilosas.

2.9 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual inclusive todos os direitos autorais em todos os certificados e todos os documentos gerados para a SERPROACF (eletrônico ou não) pertencem e continuarão sendo propriedade do SERPRO.

O Titular de Certificado concede à SERPROACF, o direito de publicar e divulgar em página *web* a chave pública que corresponde à chave privada que está sob posse do Titular de Certificado. Esta publicação ocorrerá pela incorporação da chave pública em certificado emitido pela SERPROACF. Nada nesta cláusula concede ao Titular de Certificado qualquer direito em relação ao formato ou estrutura do certificado que acompanha sua chave pública.

Direitos sobre Identificadores de Objeto (OID) atribuídos à SERPROACF após o processo de credenciamento, cabem única e exclusivamente ao ITI, designado como a AC Raiz da ICP-Brasil.

3. Identificação e Autenticação

3.1 Registro Inicial

A AR realizará a autenticação da identidade de uma organização (item 3.1.8) e a autenticação da identidade de um indivíduo (item 3.1.9) por meio de, no mínimo, dois agentes de registro responsáveis pelo recolhimento e verificação da validade dos documentos apresentados.

O Certificado emitido para pessoa jurídica possui o nome da pessoa física responsável pelo uso.

3.1.1 Tipos de Nomes

No domínio da SERPROACF, o atributo sujeito nos certificados emitidos para Titulares de Certificado , é do tipo *Distinguished Name*, contendo sempre o nome no formato previsto pelo padrão ITU X.500.

Os certificados emitidos para pessoa jurídica incluem o nome da pessoa física responsável pelo seu uso. Para todos os efeitos legais, os certificados e as respectivas chaves de assinatura são de titularidade do responsável constante do certificado.

3.1.2 Necessidade de Nomes Significativos

Para os certificados de pessoa física, o campo Common Name é composto do nome do Titular do Certificado.

Para os certificados de pessoa jurídica, o campo Common Name é composto do nome empresarial da pessoa jurídica.

Os certificados gerados para certificar equipamentos ou aplicações utilizam a informação do nome do Domain Name System (DNS) no campo Common Name.

Em um dos campos OU (Organizational Unit), contém a organização a que pertence o Titular do Certificado.

3.1.3 Regras para interpretação de vários tipos de nomes

Não existem regras específicas para interpretação de nomes no âmbito da SERPROACF.

3.1.4 Unicidade de Nomes

Esta PC estabelece que identificadores do tipo "*Distinguished Name" (DN)* serão únicos para cada titular de certificado, no âmbito da SERPROACF. Números ou letras adicionais podem ser incluídos ao nome do Titular para assegurar a unicidade do campo.

As AR podem propor e aprovar nomes distintos para candidatos de certificado e, para verificar que um nome distinto proposto é único, devem submeter a aprovação do certificado e o *software* retornará mensagem de erro caso o nome não seja único em seu domínio.

3.1.5 Procedimento para resolver disputa de nomes

A SERPROACF se reserva o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes de certificados. Durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

Não se aplica aos certificados emitidos sob esta política.

3.1.7 Método para comprovar a posse da Chave Privada

O sistema de certificação, implementado no CCD-SERPRO e utilizado pela SERPROACF no gerenciamento do ciclo de vida de seus certificados, controla e garante, de forma automática, a entrega do certificado somente ao detentor da chave privada correspondente à chave pública constante do certificado.

A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital da mesma, realizada com a chave privada correspondente à chave pública contida na solicitação. Ao recebê-la o software de certificação (SGC) procede a verificação automática da assinatura digital com uso da chave pública incluída nessa solicitação. Esse teste confirma a posse da chave privada pelo requisitante. A solicitação é então armazenada no banco de dados do SGC e possui, associado, um número de identificação. Este número é impresso no Termo de Responsabilidade ou de Titularidade junto com os dados da entidade solicitante. Os dados são autenticados pela AR através de documentos oficiais, efetivando a vinculação da solicitação e chave privada à entidade autenticada pela AR.

3.1.8 Autenticação da Identidade de uma Organização

A confirmação da identidade de pessoa jurídica é feita mediante a apresentação dos seguintes documentos;

- Registro comercial, no caso de empresa individual;
- Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores; e
- Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- Prova de inscrição no Cadastro Específico do INSS (CEI), **se aplicável**;

A pessoa física responsável referida no item 3.1.1 é identificada, na forma descrita no item seguintes.

3.1.9 Autenticação da Identidade do Indivíduo

O processo de autenticação da identidade dos Titulares de Certificado prevista nesta PC é feito por Autoridade de Registro vinculadas à SERPROACF, que farão a checagem mediante a presença física do interessado e dos documentos de identificação legalmente aceitos.

Quando o titular do certificado for pessoa jurídica, deverá ser feita a confirmação de sua identidade, na forma do item 3.1.8; e de seu representante legal, mediante a apresentação dos documentos descritos no item 3.1.9.1. Neste caso, o representante legal da pessoa jurídica

assinará “Termo de Titularidade”, e a pessoa física indicada como responsável pelo certificado assinará “Termo de Responsabilidade”.

Tanto a pessoa jurídica titular do certificado, como a pessoa física designada como responsável pelo certificado, serão responsáveis, pela correta utilização deste conforme as normas da ICP-Brasil. Será feita ainda a confirmação da identidade da pessoa física responsável pelo uso do certificado.

São mantidos arquivos com o tipo e os detalhes dos procedimentos de identificação utilizados em cada caso.

3.1.9.1. Documentos para identificação

Devem ser apresentados, acompanhados de duas cópias, no mínimo os seguintes documentos;

- Uma foto recente;
- Cédula de Identidade ou Passaporte, se estrangeiro;
- Cadastro de Pessoa Física (CPF);
- Comprovante de Residência;
- Número de identificação Social-NIS (Cadastro do Programa de Integração Social-PIS, Cadastro do Programa de Formação do Patrimônio do Servidor Público-PASEP ou Cadastro de Contribuintes Individuais do INSS-CI), **se aplicável**;
- Cadastro Especifico do INSS-CEI, **se aplicável**;
- Titulo de eleitor, **se aplicável**;
- Os documentos acima relacionados do responsável, caso o solicitante seja incapaz.

NOTA: Entende-se por cédula de identidade as carteiras instituídas por lei, desde que contenham foto e às mesmas seja atribuída fé pública em todo o território nacional, tais como: Carteira de Identidade emitida pela Secretaria de Segurança Pública, Carteira Nacional de Habilitação, Carteira de Identidade Funcional, Carteira de Identidade Profissional;

3.1.9.2 Certificado Emitido para Pessoa Física.

Deverá ser feita a confirmação de sua identidade, na forma do item 3.1.9.1, e esta assinará Termo de Titularidade.

3.1.9.3 Certificado Emitido para Pessoa Jurídica.

Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos;

- Apresentação do rol de documentos elencados no item 3.1.8;
- Apresentação do rol de documentos elencados no item 3.1.9.1 do representante legal da pessoa jurídica e do responsável pelo uso do certificado;
- Presença física do responsável pelo uso do certificado e assinatura do Termo de Responsabilidade; e
- Presença física do representante legal da pessoa jurídica e assinatura do Termo de Titularidade.

3.1.9.4 Certificado Emitido para Equipamentos ou Aplicação.

Se o titular for pessoa física, deverá ser feita a confirmação de sua identidade, na forma do item 3.1.9.1, e esta assinará Termo de Titularidade.

Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

- Apresentação do rol de documentos elencados no item 3.1.8;
- Apresentação do rol de documentos elencados no item 3.1.9.1 do representante legal da pessoa jurídica e do responsável pelo uso do certificado;
- Presença física do responsável pelo uso do certificado e assinatura do Termo de Responsabilidade; e
- Presença física do representante legal da pessoa jurídica e assinatura do Termo de Titularidade, ou outorga de procuração atribuindo poderes para solicitação de certificado para equipamento ou aplicação e assinatura do respectivo Termo de Titularidade.

3.2 Geração de novo par de chaves antes da expiração do atual

Os Titulares de Certificado serão comunicados da necessidade da renovação com uma antecedência mínima de 30 dias pela SERPROACF. As solicitações de renovação de certificados serão feitas pelos próprios Titulares de Certificado quando do recebimento dessa notificação, por meio eletrônico e assinado digitalmente com o uso de certificado vigente de mesmo nível de segurança, podendo repetir esse procedimento por 3 (três) ocorrências sucessivas.

Para os certificados de equipamento e aplicações não há o processo de renovação. Os procedimentos a ser adotado são os mesmos para a solicitação inicial de certificado, item 3.1.9.

3.3 Geração de novo par de chaves após revogação

Os procedimentos utilizados para confirmação da identidade de uma entidade solicitante de novo certificado, após a revogação do certificado dessa entidade, são os mesmos executados quando da solicitação do certificado.

3.4 Solicitação de revogação

Solicitações de revogação de certificados devem ser feitas da seguinte forma;

- Página *Web* da SERPROACF, onde o próprio usuário revoga seu certificado, apresentando seu certificado ainda válido ou informando sua "Frase-Senha";
- Através de contato telefônico ao AR, onde o usuário deve informar sua "Frase Senha". Caso a "Frase Senha" informada pelo usuário não corresponda a "Frase Senha" cadastrada no sistema, o AR não executará a revogação do certificado.
- Formulário específico, disponibilizado na página *Web* da SERPROACF, que deve ser preenchido, assinado pelo Titular do Certificado e entregue pessoalmente a um AR.
- Solicitação via documento formal (memorando, ofício ou E-mail assinado) informando o número da solicitação ou número de série do certificado, mais a "Frase Senha" informada na solicitação do certificado.

A confirmação da identidade do Titular do Certificado pela AR deve ser feita com base em um dos documentos de identidade descritos no item 3.1.9 desta PC, ou pela “Frase Senha” informada.

As solicitações de revogação ficam arquivadas pelos AR.

4. Requisitos Operacionais

4.1 Solicitação de Certificados

Os seguintes passos devem ser seguidos pelos Titulares de Certificado para a solicitação de certificados:

1) O solicitante de certificado acessa a página *Web* https://ccd.serpro.gov.br/serproacf da SERPROACF, seleciona uma das opções constantes em "Certificados A1" ("Pessoa Física", "Pessoa Jurídica" ou "Equipamento"), lê as instruções constantes nesta página, seleciona "Avançar" na parte inferior direita da página e então seleciona a opção "Solicitar Certificado". Preenche então os dados solicitados, imprime em duas vias o Termo de Responsabilidade para Certificado de Usuário, pessoa física ou jurídica, ou o Termo de Titularidade para o Certificado de Servidor, e envia a sua solicitação;
2) No formulário da solicitação que será preenchido será solicitada a criação de uma "Frase Senha" que será utilizada posteriormente para a busca e instalação do certificado;
3) O solicitante preenche no Termo de Responsabilidade ou de Titularidade o número de sua solicitação recebido após o envio da mesma, e se dirige a uma das AR indicadas pela SERPROACF munido dos documentos exigidos para comprovação dos atributos de identificação constantes do certificado;

Os Agentes de Registro responsável pela solicitação da emissão ou da revogação do certificado executam os seguintes procedimentos;

1. A comprovação dos atributos de identificação constantes do certificado conforme o item 3.1;
2. Utilizam para sua autenticação certificado de nível A3;
3. Validam e assinam as duas vias do Termo de Titularidade ou Termo de Responsabilidade, devolve uma das vias ao solicitante e arquiva a outra junto com as cópias dos documentos entregue pelo solicitante.

4.2 Emissão de Certificados

Os certificados são emitidos pela SERPROACF de acordo com os seguintes passos:

1) O responsável pela AR verifica o completo e correto preenchimento da solicitação do certificado;
2) O responsável pela AR aprova a solicitação, disponibilizando o certificado para a instalação por seu solicitante.
3) O software de AC emite automaticamente uma notificação ao solicitante informando que o certificado está disponível para busca.

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

4.3 Aceitação de Certificados

Os certificados são instalados de acordo com os seguintes passos:

1) O solicitante de certificado acessa a página *Web* https://ccd.serpro.gov.br/serproacf/ da SERPROACF, seleciona uma das opções constantes em "Certificados A1" ("Pessoa Física", "Pessoa Jurídica" ou "Equipamento"), lê as instruções constantes nesta página, seleciona "Avançar" na parte inferior direita da página;
2) O solicitante seleciona a opção "Buscar Certificado" e informa o número da sua solicitação e a "Frase Senha" definida no processo de solicitação do certificado;
3) O solicitante instala o certificado na sua estação, conferindo seus dados impresso no certificado;
4) O Titular do Certificado exporta o certificado com a chave privativa para um disquete, token ou smart card.

O recebimento de um certificado pelo Titular de Certificado e o uso subseqüente das chaves e certificado, constitui aceitação deste certificado.

Aceitando um certificado, o Titular do Certificado:

1) Concorda estar de acordo com as responsabilidades, obrigações e deveres impostos a ele pelo Termo de Responsabilidade e Titularidade, por esta PC e pela DPC da SERPROACF;
2) Garante que por seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado;
3) Afirma que as informações do certificado fornecidas durante o processo de solicitação são verdadeiras e foram publicadas dentro do certificado com precisão.

4.4 Suspensão e Revogação de Certificados

4.4.1 Circunstâncias para revogação

A SERPROACF deve revogar um certificado por ela emitido pelos seguintes motivos

1) Descritos no item 4.4.1 da DPC da SERPROACF;
2) Emissão imprópria ou defeituosa do certificado;
3) Uma informação contida no certificado foi alterada ou não é mais válida;
4) Comprometimento ou suspeita de comprometimento de chaves privadas ou senhas;
5) Comprometimento ou suspeita da mídia armazenadora de chaves privadas;
6) Exoneração ou suspensão do Titular;
7) Falha do Titular do certificado no cumprimento de suas obrigações ou qualquer compromisso, regulamento ou lei em vigor;
8) Solicitação de Revogação pelo Titulara (item 3.4 da PC)
9) Certificado da SERPROACF, da ACSERPRO ou da AC Raiz da ICP-Brasil é revogado.

O prazo para revogação dos certificados da SERPROACF do tipo A1 está definido no item 4.4.3.

4.4.2 Quem Pode Solicitar a Revogação

Revogação de certificados somente podem ser feitas por;

1) Solicitação do Titular do Certificado;
2) Solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
3) Solicitação de empresa ou órgão, quando o titular do certificado for seu empregado, funcionário ou servidor;

4) Pela SERPROACF;
5) Um pedido validado e recebido de um terceiro autorizado, por exemplo:
   - Uma determinação judicial.
6) Um pedido feito por uma pessoa com procuração do Titular do Certificado;
7) Por uma AR vinculada; ou
8) Por determinação do CG da ICP-Brasil, da ACSERPRO ou da AC Raiz.

4.4.3 Procedimentos para a Revogação

Como diretriz geral, fica estabelecido que:

- A SERPROACF garante que todos os agentes habilitados, conforme especificado no item 4.4.2, podem solicitar facilmente e a qualquer tempo um revogação de seu próprio certificado, bastando para isso enviar uma solicitação à SERPROACF, utilizando o formulário disponível na página *https://ccd.serpro.gov.br/serproacf/* ou por meio de um documento formal (memorando, ofício ou E-mail assinado com o seu próprio certificado);
- O solicitante da revogação de um certificado será identificado, conforme item 3.4;
- As solicitações de revogação, bem como as ações delas decorrentes, realizadas pela SERPROACF e AR vinculadas serão registradas e armazenadas;
- As justificativas para a revogação de um certificado serão documentadas e arquivadas;
- O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, é de 72 horas, conforme especificado para certificados de assinatura tipo A1 pelo CG da ICP-Brasil.

A SERPROACF provê, durante 24 horas por dia, 7 dias por semana, serviço que permita ao titular do certificado solicitar a revogação do mesmo.

A SERPROACF 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.

4.4.4 Prazo para solicitação de revogação

Os Titulares de Certificados ou as entidades descritas no item 4.4.2 devem fazer a solicitação de revogação imediatamente quando configuradas as circunstâncias definidas no item 4.4.1.

O Titular do Certificado tem até 3 dias, após o recebimento da notificação da aprovação da solicitação do certificado, para encaminhar à SERPROACF declaração de não aceitação do certificado. Dentro deste prazo a revogação desse certificado poderá ser solicitada sem cobrança de tarifa.

4.4.5 Circunstâncias para suspensão

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

4.4.6 Quem pode solicitar suspensão

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

4.4.7 Procedimento para solicitação de suspensão

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

4.4.8 Limites no período de suspensão

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

4.4.9 Freqüência de emissão de LCR

A Lista de Certificados Revogados (LCR) da SERPROACF é atualizada em sua entrada a cada 1 hora.

Os números de série de certificados de qualquer entidade final que estejam revogados devem aparecer na LCR. Estes números permanecem nas LCR emitidas até a data de expiração dos certificados ser atingida, sendo removidos na primeira LCR emitida após a data de suas expirações.

São emitidas LCR na freqüência determinada neste item, mesmo quando não houver nenhuma mudança ou atualização, para assegurar a periodicidade da informação.

4.4.10 Requisitos para verificação de LCR

Todos os certificados revogados no domínio da SERPROACF são listados na LCR que pode ser acessada na página da SERPROACF ou no endereço URL contido no próprio certificado.

Antes de aceitar um certificado, Usuários de Certificados (partes confiáveis) devem verificar a situação do mesmo na LCR corrente. Também deve ser verificada a autenticidade da LCR por meio das verificações de assinatura e do seu período de validade. Os Usuários devem utilizar aplicações cliente que atendam a estas especificações.

4.4.11 Disponibilidade para revogação ou verificação de status *on-line*

A SERPROACF não 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.

4.4.12 Requisitos para a verificação de revogação *on-line*

A SERPROACF não suporta os processos de verificação de revogação de forma *on-line*.

4.4.13 Outras formas disponíveis para divulgação de revogação

A SERPROACF não suporta outras formas para divulgação da revogação que não através da publicação de LCR.

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

A SERPROACF não suporta qualquer outra forma de verificação de situação de certificados que não seja a consulta à LCR.

4.4.15 Requisitos especiais para o caso de comprometimento de chave

Todas as ocorrências de comprometimento ou suspeita de comprometimento de chaves devem ser comunicadas imediatamente à SERPROACF, por E-mail ou carta. O relato deve incluir o nome do Titular do Certificado e as circunstâncias sob a qual o comprometimento ocorreu.

A AR da SERPROACF irá investigar todos os relatos e tomar as ações apropriadas. Os resultados destas investigações e ações tomadas são registrados juntamente com o relato do Titular e devem ser arquivados conforme especificado na DPC da SERPROACF.

4.5 Procedimentos de Auditoria de Segurança

Os itens a seguir estão definidos na DPC SERPROACF sob a mesma numeração. O leitor deve obter a cópia atualizada da DPC da SERPROACF e referir-se ao item de mesmo número.

4.5.1 Tipos de eventos registrados

Vide item de mesmo número na DPC da SERPROACF.

4.5.2 Freqüência de auditoria de registros (*logs*)

Vide item de mesmo número na DPC da SERPROACF.

4.5.3 Período de retenção para registros (*logs*) de auditoria

Vide item de mesmo número na DPC da SERPROACF.

4.5.4 Proteção de registro (*log*) de auditoria

Vide item de mesmo número na DPC da SERPROACF.

4.5.5 Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria

Vide item de mesmo número na DPC da SERPROACF.

4.5.6 Sistema de coleta de dados de auditoria

Vide item de mesmo número na DPC da SERPROACF.

4.5.7 Notificação de agentes causadores de eventos

Vide item de mesmo número na DPC da SERPROACF.

4.5.8 Avaliações de vulnerabilidade

Vide item de mesmo número na DPC da SERPROACF.

4.6 Arquivamento de Registros

Os itens a seguir estão definidos na DPC da SERPROACF sob a mesma numeração. O leitor deve obter a cópia atualizada da DPC e referir-se ao item de mesmo número.

4.6.1 Tipos de registros arquivados

Vide item de mesmo número na DPC da SERPROACF.

4.6.2 Período de retenção para arquivo

Vide item de mesmo número na DPC da SERPROACF.

4.6.3 Proteção de arquivo

Vide item de mesmo número na DPC da SERPROACF.

4.6.4 Procedimentos para cópia de segurança (*backup*) de arquivo

Vide item de mesmo número na DPC da SERPROACF.

4.6.5 Requisitos para datação (*time-stamping*) de registros

Vide item de mesmo número na DPC da SERPROACF.

4.6.6 Sistema de coleta de dados de arquivo

Vide item de mesmo número na DPC da SERPROACF.

4.6.7 Procedimentos para obter e verificar informação de arquivo

Vide item de mesmo número na DPC da SERPROACF.

4.7 Troca de chave

A SERPROACF se encarrega de avisar o Titular de Certificado via E-mail cadastrado na solicitação do certificado, no prazo de 30 dias, antes da expiração do mesmo para que o Titular proceda a geração de um novo para de chaves do mesmo Tipo de Certificado, no caso A1.

Depois de comunicado o Titular deverá gerar o novo par de chaves, acessando a página https://ccd.serpro.gov.br/serproacf/ na opção Renovar, e com o certificado antigo solicitar uma renovação de certificado.

4.8 Comprometimento e Recuperação de Desastre

Os itens a seguir estão definidos na DPC da SERPROACF sob a mesma numeração. O leitor deve obter a cópia atualizada da DPC e referir-se ao item de mesmo número para informações sobre o processo de recuperação de desastre da SERPROACF.

4.8.1 Recursos computacionais, *software* ou dados são corrompidos

Vide item de mesmo número na DPC da SERPROACF.

4.8.2 Certificado de entidade é revogado

Vide item de mesmo número na DPC da SERPROACF.

4.8.3 Chave de entidade é comprometida

Vide item de mesmo número na DPC da SERPROACF.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

Vide item de mesmo número na DPC da SERPROACF.

4.9 Extinção da SERPROACF

Vide item de mesmo número na DPC da SERPROACF.

5. Controles de Segurança Física, Procedimental e de Pessoas

Os itens a seguir estão definidos na DPC da SERPROACF sob a mesma numeração. O leitor deve obter a cópia atualizada da DPC e referir-se ao item de mesmo número para quaisquer informações sobre os controles de seguranças físicas, procedimentais e de pessoas no âmbito da SERPROACF.

5.1 Controles Físicos

5.1.1 Construção e localização das instalações

Vide item de mesmo número na DPC da SERPROACF.

5.1.2 Acesso físico

Vide item de mesmo número na DPC da SERPROACF.

5.1.3 Energia e ar condicionado

Vide item de mesmo número na DPC da SERPROACF.

5.1.4 Exposição à água

Vide item de mesmo número na DPC da SERPROACF.

5.1.5 Prevenção e proteção contra incêndio

Vide item de mesmo número na DPC da SERPROACF.

5.1.6 Armazenamento de mídia

Vide item de mesmo número na DPC da SERPROACF.

5.1.7 Destruição de lixo

Vide item de mesmo número na DPC da SERPROACF.

5.1.8 Instalações de segurança (*backup*) externas (*off-site*)

Vide item de mesmo número na DPC da SERPROACF.

5.2 Controles Procedimentais

5.2.1 Perfis qualificados

Vide item de mesmo número na DPC da SERPROACF.

5.2.2 Número de pessoas necessário por tarefa

Vide item de mesmo número na DPC da SERPROACF.

5.2.3 Identificação e autenticação para cada perfil

Vide item de mesmo número na DPC da SERPROACF.

5.3 Controles de Pessoal

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

Vide item de mesmo número na DPC da SERPROACF.

5.3.2 Procedimentos de verificação de antecedentes

Vide item de mesmo número na DPC da SERPROACF.

5.3.3 Requisitos de treinamento

Vide item de mesmo número na DPC da SERPROACF.

5.3.4 Freqüência e requisitos para reciclagem técnica

Vide item de mesmo número na DPC da SERPROACF.

5.3.5 Freqüência e seqüência de rodízio de cargos

Vide item de mesmo número na DPC da SERPROACF.

5.3.6 Sanções para ações não autorizadas

Vide item de mesmo número na DPC da SERPROACF.

5.3.7 Requisitos para contratação de pessoal

Vide item de mesmo número na DPC da SERPROACF.

5.3.8 Documentação fornecida ao pessoal

Vide item de mesmo número na DPC da SERPROACF.

6. Controles Técnicos de Segurança

Nos itens seguintes, são descritas as medidas de segurança necessárias para proteger as chaves criptográficas dos Titulares de Certificados emitidos segundo esta PC. Também são definidos outros controles técnicos de segurança utilizados pela SERPROACF e pelas AR vinculadas na execução de suas funções operacionais.

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

O par de chaves criptográficas é gerado pelo próprio Titular do Certificado através de CSP (Cryptographic Service Provider) existentes na estação do solicitante, apresentados pelo browser Microsoft ou Netscape e, quando da geração, a chave privada é armazenada no HD da estação. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(s), a pessoa responsável pela geração dos pares de chaves criptográficos e pelo uso do certificado.

A chave privada poderá ser armazenada utilizando os seguintes dispositivos.

HD.
Para certificados de pessoa física, na solicitação do certificado pelo Internet Explorer deve ser definido o nível de segurança do repositório como alto. Na solicitação pelo Netscape também deve ser definida senha de proteção à chave privada. A chave privada deve ser exportada e armazenada (cópia de segurança) em CD/disquete, evitando assim perda do certificado caso a estação do usuário precise ser formatada. A segurança da chave privada repousa, nesse caso, na proteção da mídia e da senha de acesso ao CD/disquete, cópia de segurança, e na proteção da senha de acesso à chave privada armazenada no HD. A SERPROACF recomenda ao Titular do Certificado a remoção do certificado do browser de sua estação, após sua utilização, caso o equipamento seja compartilhado com outros usuários.
Para certificados de equipamentos, a proteção da chave privada está na proteção da senha de logon do usuário responsável pelo serviço.

Token.
O certificado com a chave privada deverá ser exportado para o Token. A SERPROACF recomenda ao usuário a remoção do certificado do browser de sua estação após a exportação.

Smart Card.
O certificado com a chave privada deverá ser exportado para o Smart Card. A SERPROACF recomenda ao usuário a remoção do certificado do browser de sua estação após a exportação.

Para certificados de equipamento ou aplicação o par de chaves é gerado em equipamento próprio através dos recursos disponíveis para esse fim.

A tecnologia utilizada assegura, por meios técnicos e procedimentais adequados, que:

1. A chave privada é única e seu sigilo é suficientemente assegurado;
2. A chave privada não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;

3. A chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros;
4. A entrega do certificado somente ocorre ao detentor da chave privada correspondente à chave pública constante do certificado.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

Ao ser gerada, a chave privada da entidade titular deverá ser gravada cifrada por algoritmo simétrico 3-DES, IDEA, SAFER+ ou outro aprovado pelo CG da ICP-Brasil, no meio de armazenamento definido para o tipo de certificado A1 objeto desta PC.
A chave privada deverá trafegar cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.
A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do Titular do Certificado e do órgão solicitante, conforme especificado no Termo de Responsabilidade para certificados de pessoa física, e no Termo de Titularidade para certificados de equipamentos ou aplicações.

6.1.2 Entrega da chave privada à entidade titular

Item não aplicável uma vez que é o próprio Titular que gera seu par de chaves.

6.1.3 Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à SERPROACF por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da SERPROACF.

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

6.1.4 Disponibilização de chave pública da AC para usuários

O certificado da SERPROACF e demais certificados de sua cadeia de certificação são disponibilizados, para todos usuários da SERPROACF, segundo as formas abaixo:

1) Formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu Titular;
2) Página *Web* da SERPROACF.

6.1.5 Tamanhos de chave

O tipo de certificado emitido sob esta PC pela SERPROACF é o A1, que exige para o tamanho das chaves de seus certificados o mínimo de 1024 bits.

6.1.6 Geração de parâmetros de chaves assimétricas

Os Titulares de certificados devem garantir que os parâmetros de geração do seu par de chaves assimétricas, relativo ao certificado emitido sob esta PC pela SERPROACF, seguem o padrão FIPS (*Federal Information Processing Standards*) 140-1.
O CSP (*Cryptographic Service Provider*) que será utilizado para esta finalidade poderá ser validado, quanto ao padrao FIPS 140 level 1, no seguinte endereço: http://csrc.nist.gov/cryptval/140-1.htm, através de um arquivo disponibilizado para download contendo os módulos criptográficos certificados pelos laboratórios credenciados pelo NIST.

6.1.7 Verificação da qualidade dos parâmetros

A qualidade dos parâmetros pode ser verificada de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program*) do NIST (*National Institute of Standards and Technology*) uma vez que este é o programa que determina as normas para validação do padrao FIPS 140 level 1.

6.1.8 Geração de chave por *hardware ou software*

O processo de geração do par de chaves dos Titulares do Certificado é feito por software.

Esta PC caracteriza o processo utilizado para a geração de chaves criptográficas dos Titulares de Certificados, com base nos requisitos aplicáveis estabelecidos pelo documento “Requisitos Mínimos para Políticas de Certificados na ICP-Brasil”.

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

As chaves privadas dos Titulares de Certificados emitidos pela SERPROACF serão utilizadas conforme descrito no item 1.3.4.1.

6.2 Proteção da Chave Privada

Nos itens seguintes são definidos os requisitos para a proteção das chaves privadas dos Titulares de Certificados emitidos segundo a PC.

6.2.1 Padrões para módulo criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS (*Federal Information Processing Standards*) 140-1 – requerido pela SERPROACF para os certificados emitidos sob esta PC.

O CSP (*Cryptographic Service Provider*) que será utilizado para esta finalidade poderá ser validado, quanto ao padrao FIPS 140 level 1, no seguinte endereço: http://csrc.nist.gov/cryptval/140-1.htm, através de um arquivo disponibilizado para download contendo os módulos criptográficos certificados pelos laboratórios credenciados pelo NIST.

6.2.2 Controle “n de m” para chave privada

Item não aplicável.

6.2.3 Recuperação (*escrow*) de chave privada

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

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

A SERPROACF não mantém a cópia da chave privada do certificado tipo A1, emitidos sob desta PC.

Titulares de Certificado podem possuir cópia de segurança de suas chaves criptográficas. Neste caso, a cópia de segurança deverá ser armazenada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

Item não aplicável, uma vez que a ICP-Brasil não admite o arquivamento de chaves privadas de assinatura digital.

6.2.6 Inserção de chave privada em módulo criptográfico

Os Titulares de Certificados poderão optar por utilizar um hardware criptográfico sem capacidade de geração de chave, cartão inteligente ou token, para armazenar sua chave privada após a aceitação do certificado.

6.2.7 Método de ativação de chave privada

A chave privada, é ativada mediante senha solicitada pelo CSP (*Cryptographic Service Provider*) existente nas estações. Os critérios para escolha da senha devem obedecer aos descritos no item 2.8 desta PC. A senha deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo.

Os Titulares de Certificados podem alterar suas senhas a qualquer momento, sendo recomendável que o façam no mínimo a cada 3 meses.

6.2.8 Método de desativação de chave privada

A desativação da chave privada ocorre em função da expiração do certificado correspondente ou em função de sua revogação. A desativação é feita utilizando-se uma função de software de AC cujo acesso se da por meio da utilização de um certificado de AR da SERPROACF.

6.2.9 Método de destruição de chave privada

A eliminação da chave da mídia armazenadora do certificado deve ser feita através de software disponibilizado pelo fabricante da mídia, que permite apagar todas as informações nela contida, utilizando para isso a senha de acesso do titular do certificado a mídia armazenadora.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A SERPROACF armazena os certificados contendo as chaves públicas dos Titulares de Certificados de assinatura digital por ela emitidos, após a expiração dos certificados correspondentes, por 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2 Períodos de uso para as chaves pública e privada

As chaves privadas dos respectivos Titulares deverão ser utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados, que é de 1 ano para o certificado do tipo A1.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Item não aplicável.

6.4.2 Proteção dos dados de ativação

Item não aplicável.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

Os equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados devem dispor de mecanismos mínimos que garantam a segurança computacional, como, proteção do equipamento com Senha.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

Item não aplicável pois a SERPROACF não exige um *software* específico para a utilização dos certificados emitidos segundo esta PC.

6.6.1 Controles de desenvolvimento de sistema

Item não aplicável.

6.6.2 Controles de gerenciamento de segurança

Item não aplicável.

6.6.3 Classificações de segurança de ciclo de vida

Item não aplicável.

6.7 Controles de Segurança de Rede

Item não aplicável.

6.8 Controles de Engenharia do Módulo Criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS (*Federal Information Processing Standards*) 140-1 – requerido pela SERPROACF para os certificados emitidos sob esta PC.

O CSP (*Cryptographic Service Provider*) que será utilizado para esta finalidade poderá ser validado, quanto ao padrao FIPS 140 level 1, no seguinte endereço: http://csrc.nist.gov/cryptval/140-1.htm, através de um arquivo disponibilizado para download contendo os módulos criptográficos certificados pelos laboratórios credenciados pelo NIST.

7. Perfis de Certificado e LCR

Os itens seguintes especificam os formatos dos certificados e das LCR gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1 Perfil do Certificado

Todos os certificados emitidos pela SERPROACF, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 v3, especificado pelo CG da ICP-Brasil.

7.1.1 Número de versão

Todos os certificados emitidos pela SERPROACF, segundo esta PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.1.2 Extensões de certificado

A SERPROACF implementa para os certificados emitidos segundo esta PC, as seguintes extensões definidas como obrigatórias pela ICP-Brasil:

1) "*Authority Key Identifier*", não crítica: o campo **keyIdentifier** contém o resumo SHA-1 da chave pública da SERPROACF;
2) **"***Key Usage***"**, crítica: somente os bits **digitalSignature**, **nonRepudiation** e **keyEncipherment** são ativados;
3) "*Certificate Policies*", não crítica: contém o OID desta PC e o endereço *URL* da página *Web* *https://ccd.serpro.gov.br/serproacf/docs/dpcserproacf.pdf* da SERPROACF com a DPC da SERPROACF;
4) "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *Web* *http://ccd.serpro.gov.br/lcr/serproacfv1.crl* onde se obtém a LCR da SERPROACF;
5) "*Subject Alternative Name*", não crítica e com os seguintes formatos para certificados:

Para certificados de pessoa física os seguintes OtherName:

- OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato *ddmmaaaa*; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subseqüentes, o Número de Identificação Social- NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação.
- OID = 2.16.76.1.3.5 e conteúdo nas primeiras 11 (onze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subseqüentes, a Zona Eleitoral;nas 4 (quatro) posições seguintes, a Seção; nas 22 posições subseqüentes, o município e a UF do Título de Eleitor.
- OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado.

Para certificados de pessoa jurídica, de equipamento ou aplicação, os seguintes OtherName:

- OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o Número de Identificação Social- NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;

- OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

- OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica;

- OID = 2.16.76.1.3.7 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.

A SERPROACF implementa também, para os certificados de pessoa física emitidos sob esta PC:

- a sub-extensão "*rfc822Name*", parte da extensão obrigatória "*Subject Alternative Name*", contendo o endereço e-mail do titular do certificado. Esta sub-extensão é definida como opcional pela ICP-Brasil.
- a extensão "*Extended-key-usage*" contendo os valores "*client authentication*" (OID 1.3.6.1.5.5.7.3.2) e "*E-mail protection*" (OID 1.3.6.1.5.5.7.3.4). Esta extensão é definida como opcional pela ICP-Brasil.

A SERPROACF implementa também, para os certificados de pessoa jurídica emitidos sob esta PC:

- a sub-extensão "*rfc822Name*", parte da extensão obrigatória "*Subject Alternative Name*", contendo o endereço e-mail do titular do certificado. Esta sub-extensão é definida como opcional pela ICP-Brasil.
- a extensão "*Extended-key-usage*" contendo os valores "*client authentication*" (OID 1.3.6.1.5.5.7.3.2) e "*E-mail protection*" (OID 1.3.6.1.5.5.7.3.4). Esta extensão é definida como opcional pela ICP-Brasil.
- A extensão opcional "*Extended-key-usage",* não crítica, contendo o valor "*code signing*" (OID 1.3.6.1.5.5.7.3.3).

A SERPROACF implementa também, para os certificados de equipamento ou aplicação emitidos sob esta PC:

- a sub-extensão "*rfc822Name*", parte da extensão obrigatória "*Subject Alternative Name*", contendo o endereço e-mail do responsável pelo certificado. Esta sub-extensão é definida como opcional pela ICP-Brasil.
- a extensão opcional "*Extended-key-usage*" contendo os valores "*server authentication*" (OID 1.3.6.1.5.5.7.3.1).
- a extensão opcional "*Basic Constraints*", não crítica: o campo **SubjectType** contém o valor False (EndEntity).

Para o correto preenchimento dos campos *othername* deve ser observado o seguinte:

- O conjunto de informações definido em cada campo otherName é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING.

- Quando o número de CPF,NIS(PIS, PASEP ou CI), RG, CNPJ, CEI ou Titulo de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchido com caracteres “zero”.
- Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor.
- Todas informações de tamanhos variáveis referentes a número, tais como RG, devem ser preenchidas com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível.
- As 6 (seis) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor.
- Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer informação.

Campos *OtherName* adicionais, contendo informações especificas e formas de preenchimento e armazenamento definidas pela SERPROACF, poderão ser utilizadas com OID atribuídos ou aprovados pela AC-Raiz.

Os outros campos que compõem a extensão *“Subject Alternative Name”* poderão ser utilizados, na forma e com os propósitos definidos na RFC 2459.

7.1.3 Identificadores de algoritmo

O OID (*Object Identifiers*) do algoritmo criptográfico utilizado pela SERPROACF e admitido no âmbito da ICP-Brasil é o seguinte: SHA-1[1] com RSA, OID = 1.2.840.113549.1.1.5.

7.1.4 Formatos de nome

O nome do titular do certificado, constante do campo “*Subject*”, adota o “*Distinguished Name”* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma, para os certificados pessoa física:

C = BR
O = ICP-Brasil
OU = *sigla do órgão de trabalho*
OU = Pessoa Física A1
CN = *nome do titular do certificado*

Para os certificados de pessoa jurídica, o nome do titular do certificado constante do campo “*Subject*” adota o “*Distinguished Name”* (DN), do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR
O = ICP-Brasil
OU = *sigla do órgão de trabalho*
OU = Pessoa Jurídica A1
L = Cidade
S = Estado (UF)

[1] A função *hash* SHA-1 está descrita em FIPS 180-1.

CN = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica)

Para o certificado de equipamento ou aplicação, o identificador CN conterá o URL correspondente da máquina.

C = BR
O = ICP-Brasil
OU = *sigla do órgão de trabalho*
OU = Equipamento A1
CN = *nome DNS oficial do equipamento (para servidores WWW)*

Nota: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.5 Restrições de nome

São as seguintes as restrições aplicáveis para os nomes dos Titulares de Certificados no âmbito da SERPROACF:

1) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas;
2) além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

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

Tabela 3 - Caracteres especiais admitidos em nomes

7.1.6 OID (*Object Identifier*) de Política de Certificado

O OID atribuído à esta Política de Certificado é: 2.16.76.1.2.1.16

7.1.7 Uso da extensão *"Policy Constraints"*

Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo **policyQualifiers** da extensão "*Certificate Policies*" contém o endereço da página *Web* (URL) com a DPC da SERPROACF.

7.1.9 Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 2459.

7.2 Perfil de LCR

7.2.1 Número de versão

As LCR geradas pela SERPROACF, segundo esta PC, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2 Extensões de LCR e de suas entradas

A SERPROACF adota as seguintes extensões de LCR previstas pela ICP-Brasil:

1) **"***Authority Key Identifier*": contém o resumo SHA-1 da chave pública da SERPROACF.
2) "*CRL Number*", não crítica: contém número seqüencial para cada LCR emitida.

8. Administração de Especificação

Os itens seguintes definem como será mantida e administrada esta PC.

8.1 Procedimentos de mudança de especificação

As alterações nas especificações desta PC são realizadas pela SERPROACF. Quaisquer modificações são submetidas à aprovação da ACSERPRO que as submeterá ao CG da ICP-Brasil.

8.2 Políticas de publicação e notificação

A cada nova versão, esta PC é publicada na página *Web* da SERPROACF.

8.3 Procedimentos de aprovação

Esta PC foi submetida à aprovação da ACSERPRO, que por sua vez submeteu ao CG da ICP-Brasil, durante o processo de credenciamento da SERPROACF, conforme o estabelecido no documento "Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil". Como parte desse processo, além da conformidade com os documentos definidos pela ICP-Brasil, deverá ser verificada a compatibilidade entre esta PC e a DPC da SERPROACF.