www.serpro.gov.br

Declaração de Práticas de Certificação
da
Autoridade Certificadora do SERPRO

(DPC ACSERPRO)

Versão 1.0

Soluções para um Brasil de Todos

SUMÁRIO

1. INTRODUÇÃO

1.1 VISÃO GERAL

Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora do SERPRO (ACSERPRO) integrante da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços.
A ACSERPRO possui um certificado de nível intermediário na ICP-Brasil, sendo este certificado assinado pela AC Raiz da ICP-Brasil. O certificado da ACSERPRO contém a chave pública correspondente à chave privada utilizada para assinar os certificados das AC de nível imediatamente subseqüente ao seu e a sua LCR (Lista de Certificados Revogados).
A ACSERPRO utiliza o ambiente e os serviços do Centro de Certificação Digital do SERPRO (CCD SERPRO), para hospedar, operar e dar manutenção à ACSERPRO.
A estrutura desta DPC ACSERPRO está baseada nas resoluções do Comitê Gestor da ICP-Brasil (CG ICP-Brasil) e na RFC 2527 (Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Framework).

1.2 IDENTIFICAÇÃO

Esta DPC é chamada “Declaração de Práticas de Certificação da Autoridade Certificadora do SERPRO, integrante da ICP-Brasil”, e comumente referida como “DPC ACSERPRO”. O Identificador de Objeto **(OID)** desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.2**.

1.3 COMUNIDADE E APLICABILIDADE

1.3.1 Autoridades Certificadoras

Esta DPC refere-se unicamente à Autoridade Certificadora do SERPRO (ACSERPRO) e encontra-se publicada na página https://ccd.serpro.gov.br/acserpro/docs/dpcacserpro.pdf.
Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a mesma mantém a DPC correspondente publicada na página https://thor.serpro.gov.br/ACSERPRO/docs/DPCACSERPRO.pdf.

1.3.2 Autoridades de Registro

Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência da ACSERPRO através de sua Autoridade de Registro, doravante chamada de AR-ACSERPRO.

A PC operada pela ACSERPRO no âmbito da ICP-Brasil possui sua própria Autoridade de Registro identificada neste mesmo item.

1.3.3 Titulares de Certificado

A ACSERPRO emite certificados para Autoridades Certificadoras de nível imediatamente subseqüente ao seu.
Os titulares dos certificados são as entidades pessoas jurídicas, autorizadas pela AR-ACSERPRO a receberem certificados digitais emitidos pela ACSERPRO, cujos nomes aparecem no certificado digital, no campo "D*istinguished Name (DN)".*
Preferencialmente, será designado como responsável pelo certificado, o dirigente máximo do Órgão, o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.4 Aplicabilidade

Os certificados definidos por esta DPC ACSERPRO têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR).

As Políticas de Certificado (PC) implementadas pela ACSERPRO são:

1. PC ACSERPRO OID 2.16.76.1.2.201.6

As aplicações para as quais são adequados os certificados emitidos pela ACSERPRO e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso destes certificados, estão relacionadas na Política de Certificado correspondente.

1.4 DADOS DE CONTATO

Esta DPC 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.

Pessoas de Contato.

Nome: Márcia Paulina Souza
Telefone: (21) 2529-3611 ou 2529-3612
Fax: (21) 2529-3360
(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 ACSERPRO

As obrigações da ACSERPRO são as abaixo relacionadas:

- Operar de acordo com esta DPC e com a PC implementada;
- Adotar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
- Gerar e gerenciar o seu par de chaves criptográficas;
- Assegurar a proteção de sua chave privada;
- Notificar a AC Raiz da ICP-Brasil, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
- Notificar as AC de nível imediatamente subseqüente ao seu quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- Distribuir o seu próprio certificado;
- Emitir, expedir e distribuir os certificados das AC de nível imediatamente subseqüente ao seu e os certificados da AR-SERPRO .
- Informar a emissão do certificado ao respectivo solicitante;
- Revogar os certificados por ela emitidos;
- Emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR);
- Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil (CG ICP-Brasil);
- Publicar em sua página *web* http://ccd.serpro.gov.br/acserpro/ a DPC ACSERPRO e a PC ACSERPRO aprovadas e implementadas. Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a mesma mantém a DPC e PC correspondentes publicadas na página https://thor.serpro.gov.br/ACSERPRO/;
- Adotar as medidas de segurança e controle previstas na DPC, PC e política de segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios e procedimentos da ICP-Brasil;
- Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- Manter e testar regularmente seu Plano de Continuidade do Negócio;

- Não emitir certificados com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.
- Publicar os certificados por ela emitidos;
- Investigar comprometimento e suspeitas de comprometimento de sua chave privada.
- Fiscalizar e auditar as AC, as AR e os prestadores de serviço, habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor (CG) da ICP-Brasil; e
- Informar as terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC.

2.1.2 Obrigações da AR-ACSERPRO

As obrigações da AR-ACSERPRO são as abaixo relacionadas:

- Receber solicitações de emissão e revogação de certificados e respectivos documentos de identificação armazenado-os conforme critérios estabelecidos pelo CG da ICP-Brasil;
- Confirmar a identidade do solicitante e a validade da solicitação, de acordo com os requisitos estabelecidos pelos itens 3 e 4 desta DPC ACSERPRO;
- Encaminhar a solicitação de emissão e de revogação de certificado à ACSERPRO 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;
- Utilizar 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, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;
- Informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- Disponibilizar os certificados emitidos pela ACSERPRO aos seus respectivos solicitantes;
- Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasi;
- Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela ACSERPRO;
- Manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP –Brasil;
- 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; e

2.1.3 Obrigações do Titular do Certificado

As obrigações do titular de certificado emitido de acordo com esta DPC ACSERPRO são as abaixo relacionadas:

- Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- Utilizar os seus certificados e suas respectivas chaves privadas de modo apropriado, conforme o previsto na PC ACSERPRO;
- Conhecer os seus direitos e obrigações, contemplados na PC da ACSERPRO, nesta DPC e em outros documentos aplicáveis da ICP-Brasil;
- Informar à ACSERPRO qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
- operar de acordo com a sua DPC e com a PC que implementa;
- emitir, expedir e distribuir os certificados de seus solicitantes;
- informar a emissão do certificado ao respectivo solicitante;
- revogar os certificados por ele emitidos;
- emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR);
- publicar em sua página *web* sua DPC e a PC aprovada e implementada;
- fiscalizar e auditar as AR e os prestadores de serviço habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor (CG) da ICP-Brasil; e
- identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil.

Por se tratar de certificado emitido para AC (Órgãos públicos ou pessoas jurídicas), estas obrigações se aplicam ao responsável pelo uso do certificado.

2.1.4 Direitos da Terceira Parte (*Relying Party*)

Considera-se terceira parte, a parte usuária que confia no teor, validade e aplicabilidade do certificado digital. Constituem direitos da terceira parte:

- utilizar o certificado para os propósitos previstos nesta DPC, bem como para outros fins lícitos;
- verificar a qualquer tempo a validade do certificado, sendo este considerado válido quando:
  - puder ser verificado com o uso de certificado válido da ACSERPRO;
  - não constar da LCR da ACSERPRO;
  - não estiver expirado; e
  - recusar a utilização do certificado para fins diversos dos previstos na PC correspondente.

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

2.1.5 Obrigações do Repositório

- disponibilizar, logo após a sua emissão, os certificados emitidos pela ACSERPRO e a sua LCR;
- estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e

- implementar os recursos necessários para a segurança dos dados nele armazenados.

2.2 RESPONSABILIDADES

2.2.1 Responsabilidades da ACSERPRO

A Autoridade Certificadora do SERPRO responde pelos danos a que der causa.
A ACSERPRO responde solidariamente pelos atos das AC da cadeia a ela subordinada.

2.2.2 Responsabilidades da AR

A AR-SERPRO será responsável pelos danos a que der causa.
A ACSERPRO responde solidariamente pelos atos da AR-SERPRO.

2.3 RESPONSABILIDADE FINANCEIRA

2.3.1 Indenizações devidas pela terceira parte usuária (*Relying Party*)

Não existe situação específica de utilização do certificado da ACSERPRO que requeira prática de indenização pelos Usuários de Certificados, exceto na prática de ato ilícito.

2.3.2 Relações Fiduciárias

A ACSERPRO ou a AR-SERPRO indenizará integralmente os danos a 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 legislação específica uma vez que a ACSERPRO é administrada pelo Serviço Federal de Processamento de Dados – SERPRO, empresa vinculada ao Ministério da Fazenda.

2.4 INTERPRETAÇÃO E EXECUÇÃO

2.4.1 LEGISLAÇÃO

A DPC ACSERPRO 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. Além disto, é apoiada em uma estrutura contratual entre SERPRO e Titulares de Certificados.

2.4.2 Forma de interpretação e notificação

Caso uma ou mais disposições desta DPC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento. Nesse caso, o corpo técnico, da ACSERPRO, examinará a disposição inválida e proporá à Comissão Técnica, no prazo máximo de 30 dias, nova redação ou retirada da disposição afetada.As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.
Todas solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas na PC serão realizadas por iniciativa da ACSERPRO por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil e às AC´s subseqüentes se for o caso.

2.4.3 Procedimentos de solução de disputa

No caso de um conflito entre esta DPC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nesta situação esta DPC será alterada para a solução da disputa.

2.5 TARIFAS DE SERVIÇO

Não há tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.1 Tarifas de emissão e renovação de certificados

Não há tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.2 Tarifas de acesso ao certificado

Não há tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.3 Tarifas de revogação ou de acesso à informação de status

Não há tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.4 Tarifas para outros serviços, tais como informação de política

Não há tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.5 Política de reembolso

Não há política de reembolso prevista pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.6 PUBLICAÇÃO E REPOSITÓRIO

2.6.1 Publicação de informação da ACSERPRO

São publicados em página *web* da ACSERPRO, http://ccd.serpro.gov.br/acserpro/ :

- O certificado da ACSERPRO;
- sua LCR;
- esta DPC e a PC que implementa;
- os certificados das AC de nível imediatamente subseqüente ao seu;
- a lista das Autoridades Certificadoras subordinadas à ACSERPRO ;
- a legislação aplicável a esta AC e às suas AC subseqüentes;
- o endereço da instalação técnica da AR-SERPRO; e
- o leiaute dos certificados emitidos pela ACSERPRO.

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a mesma mantém os documentos correspondentes listados acima publicados na página https://thor.serpro.gov.br/ACSERPRO/.

A disponibilidade das informações publicadas pela ACSERPRO em página *web*, tais como certificados, sua LCR, sua DPC, entre outras, é de 99,00% (noventa e nove por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

A ACSERPRO inclui nos certificados emitidos a identificação da sua página *web* .(no certificado consta o endereço da LCR e da DPC).

2.6.2 Freqüência de publicação

Os certificados e a LCR são publicados imediatamente após sua primeira emissão pela ACSERPRO. A LCR que será publicada a cada 15 dias independentemente de haver alteração. Esta DPC ACSERPRO, a PC ACSERPRO e o leiaute dos certificados da ACSERPRO são publicadas após aprovação pela AC Raiz da ICP-Brasil e sempre que sofrerem atualizações.
As demais informações mencionadas no item 2.6.1 serão publicadas sempre que sofrerem alterações.

2.6.3 Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, à sua PC, aos certificados emitidos e à LCR da ACSERPRO.
Acessos para escrita nos locais de armazenamento e publicação serão permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controle de acesso incluirão identificação pessoal para acesso aos equipamentos, utilização de senhas.

2.6.4 Repositórios

O repositório da ACSERPRO está disponível para consulta, em no mínimo 99% (noventa e nove por cento), durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e atende aos seguintes requisitos:

- localização: http://ccd.serpro.gov.br/acserpro/;
- disponibilidade: aquela definida no item 2.6.1 desta DPC ACSERPRO;
- protocolos de acesso: HTTP e HTTPS;
- requisitos de segurança: obedece aos requisitos definidos no item 5 desta DPC ACSERPRO.

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a mesma mantém os documentos correspondentes publicados na página https://thor.serpro.gov.br/ACSERPRO/.

2.7 AUDITORIA DE CONFORMIDADE

A AC Raiz da ICP-Brasil é a responsável pela auditoria dos processos, procedimentos e atividades de todas as AC integrantes da ICP-Brasil e das AR e prestadores de serviço de suporte a elas vinculadas. A AC Raiz audita a ACSERPRO no âmbito da ICP-Brasil. A auditoria é realizada com o objetivo de verificar a conformidade com suas respectivas DPC, PC, PS (Política de Segurança) e demais normas e procedimentos estabelecidos pela ICP-Brasil.
Os serviços de auditoria poderão ser executados:

- por empresas independentes, autorizadas pela AC Raiz e contratadas pela AC auditada; ou
- pela ACSERPRO, em AR´s e PSS (prestadores de serviço de suporte) vinculados, de acordo com os procedimentos estabelecidos pela ICP-Brasil.

2.7.1 Freqüência de auditoria de conformidade de entidade

As AC credenciadas pelo CG da ICP-Brasil, subordinadas à ACSERPRO, suas AR e seus prestadores de serviço sofrem auditoria:

- previamente ao seu credenciamento pela AC-Raiz e à sua habilitação pela ACSERPRO;
- anuais, em data a ser designada pela AC-Raiz ou pela ACSERPRO; e
- a qualquer tempo, sem aviso prévio, pela AC Raiz.

Adicionalmente, as AC de nível imediatamente subseqüente ao da ACSERPRO, para fins de continuidade do credenciamento, apresentarão anualmente relatório de auditoria.
A ACSERPRO conduz anualmente auditorias de conformidade na AR-SERPRO , podendo também executar, a qualquer momento, auditorias não programadas.

2.7.2 Identidade/Qualificações do Auditor

A auditoria será executada por empresa de auditoria independente e especializada, com comprovada experiência em serviços de auditoria e tecnologias de certificação, de acordo com os procedimentos estabelecidos pela ICP-Brasil.
As auditorias nas AR e prestadores de serviço vinculadas, poderão ser executadas pela ACSERPRO.

2.7.3 Relação entre auditor e parte auditada

No caso de contratação de auditoria, o auditor deve ser totalmente independente da AC auditada. Ao auditor, sem prejuízo do disposto nesta PC, aplicam-se, no que couber, as regras de impedimento e suspeição estabelecidas nos arts. 134 e 135 do Código de Processo Civil.
O auditor, tanto no caso de contratação de auditoria independente como nas auditorias realizada pela ACSERPRO, será declarado impedido de realizar auditoria, quando:

- houver motivo de foro íntimo declarado;
- for amigo íntimo ou inimigo capital de membros da AC auditada;
- for credor ou devedor da AC auditada ou de um de seus membros;
- tiver recebido, nos últimos 5 anos, da AC auditada, pagamentos referentes à prestação de serviços de outra natureza;
- tiver interesse no resultado da auditoria da AC auditada; e
- houver relacionamento, de fato ou de direito, como cônjuge, parente, consangüíneo ou afim, com algum dos membros da AC auditada, em linha reta ou na colateral até o terceiro grau.

O auditor firmará declaração, sob as penas da lei, de que não se enquadra em qualquer dessas ou outras causas de impedimento. Declarará, ainda, em outro documento, o seu compromisso de manter em sigilo todas e quaisquer informações que obtiver no curso dos trabalhos, mesmo depois do término destes, sendo responsável civil e criminalmente pela divulgação indevida.

2.7.4 Tópicos cobertos pela auditoria

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.
Todos os eventos significativos ocorridos em um sistema de AC ou de AR serão armazenados em trilhas seguras de auditoria, onde cada entrada possua o registro de data, hora e tipo de evento, com assinatura, para garantir que as entradas não possam ser falsificadas.
Os tópicos cobertos por uma auditoria de conformidade incluem, entre outros:

- Política de Segurança;
- Segurança física;
- Avaliação de tecnologia;
- Administração dos serviços;
- Investigação de pessoal;
- PC e DPC utilizadas;
- Contratos; e
- Considerações de sigilo.

2.7.5 Medidas a serem adotadas em caso de não conformidade

Cabe à entidade auditada cumprir, no menor dos prazos estipulados, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. O não cumprimento das recomendações, no prazo estipulado, acarretará a revogação do seu certificado pela ACSERPRO.
A ACSERPRO, em casos de iminente dano irreparável ou de difícil reparação a terceiros, poderá suspender cautelarmente, no todo ou em parte, a emissão de certificados pela AC de nível imediatamente subseqüente ao seu.

2.7.6 Comunicação de resultados

Os auditores somente informam os resultados da auditoria à entidade auditada, à ACSERPRO e à AC Raiz da ICP-Brasil, nos termos da declaração que firmarem, como exigida pelo item 2.7.3.

2.8 SIGILO

A chave privada de assinatura digital da ACSERPRO foi gerada e é mantida pela própria ACSERPRO, que é responsável pelo seu sigilo.
A divulgação ou utilização indevida da chave privada de assinatura pela ACSERPRO é de sua inteira responsabilidade.
Os titulares de certificados emitidos pela ACSERPRO, ou os responsáveis pelo seu uso, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, são responsáveis pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1 Tipos de informações sigilosas

Todas as informações coletadas, geradas, transmitidas e mantidas pela ACSERPRO e a AR-SERPRO são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.2.
Essas informações serão arquivadas de acordo com sua classificação que será especificada na Política de Segurança.
Como princípio geral, nenhum documento, informação ou registro fornecido à ACSERPRO ou AR-SERPRO deverá ser divulgado.

2.8.2 Tipos de informações não sigilosas

Certificados, LCR e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não sigilosas.
Os seguintes documentos da ACSERPRO e AR-SERPRO são considerados documentos não sigilosos:

- qualquer PC aplicável;
- qualquer DPC;
- versões públicas de Políticas de Segurança; e
- resultados finais de auditoria.

2.8.3 Divulgação de informação de revogação/suspensão de certificado

A ACSERPRO disponibiliza permanentemente em sua página **http://ccd.serpro.gov.br/lcr/acserpro.crl**, lista de certificados revogados.
Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a mesma mantém a LCR correspondente publicada na página http://thor.serpro.gov.br/LCR/ACSERPRO.crl.

As razões para revogação do certificado sempre serão informadas para o seu titular.
Os motivos que justificaram a revogação são mantidos confidenciais pela ACSERPRO e pela AR-SERPRO , exceto quando:

- o titular do certificado revogado autorizar expressamente a sua divulgação a terceiros;
- esses motivos tenham sido publicados, ou sejam ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida da ACSERPRO ou da AR-SERPRO ;

- tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a ACSERPRO ou a AR-SERPRO , se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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 ACSERPRO e suas AR é divulgado a entidades legais ou seus funcionários, exceto quando:

- Exista uma ordem judicial corretamente constituída; e
- Esteja corretamente identificado o representante da lei.

2.8.5 Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro, sob a guarda da ACSERPRO, será fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

2.8.6 Divulgação por solicitação do titular

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:

- por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ACSERPRO; ou
- por meio de pedido escrito com firma reconhecida.

Nenhuma liberação de informação é permitida sem autorização formal do titular do certificado, exceto nos casos do item 2.8.4.

2.8.7 Outras circunstâncias de divulgação de informação

Nenhuma outra liberação de informação, que não as expressamente descritas nesta DPC, é permitida.

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 ACSERPRO (eletrônicos ou não) pertencem e continuarão sendo propriedade do Serviço Federal de Processamento de Dados – SERPRO.
O Titular de Certificado concede à ACSERPRO, 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.
Direitos sobre Identificadores de Objeto (OID) atribuídos à ACSERPRO 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

Neste item e nos seguintes a DPC descreve os requisitos e os procedimentos gerais utilizados pela AR-SERPRO , vinculada à ACSERPRO, responsável no processo inicial de identificação dos solicitantes de certificado.
A AR-SERPRO realiza 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.

3.1.1 Tipos de nomes

As AC de nível imediatamente subseqüente ao da ACSERPRO, titulares de certificados de AC habilitada, terão um nome que as identifique univocamente no âmbito da ACSERPRO, no padrão ITU X.500, não incluindo no certificado o nome da pessoa física responsável pelo mesmo.
A ACSERPRO segue as regras de identificação de nomes da AC Raiz da ICP-Brasil.

3.1.2 Necessidade de nomes significativos

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

3.1.3 Regras para interpretação de vários tipos de nomes

Item não aplicável.

3.1.4 Unicidade de nomes

Os identificadores "*Distinguished Name"* (DN) são únicos para cada AC de nível imediatamente subseqüente ao da ACSERPRO. Para cada AC, números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.509.
A extensão "*Unique Identifiers*" não será admitida para diferenciar as AC com nomes idênticos.

3.1.5 Procedimento para resolver disputa de nomes

A ACSERPRO reserva-se o direito de tomar todas as decisões referentes a disputas de nomes das AC de nível imediatamente subseqüente ao seu. Durante o processo de confirmação de identidade, a AC solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.7 Método para comprovar a posse de chave privada

A confirmação que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, item 2.3.

3.1.8 Autenticação da Identidade de uma organização

A confirmação da identidade de uma AC subordinada é feita com base nos "CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL", conforme aprovados pela Resolução nº 6, de 22 de novembro de 2001, do Comitê Gestor da ICP.

A confirmação da identidade de pessoa jurídica responsável pela solicitação de certificado da AC subseqüente 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;
- Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- Prova de inscrição no Cadastro Especifico do INSS (CEI), se aplicável.

A pessoa física responsável pela AC subordinada será identificada na forma descrita no item seguinte.

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.
A PC ACSERPRO definirá os documentos exigidos com base nos requisitos aplicáveis estabelecidos pelo documento "Requisitos Mínimos para Certificados da ICP-Brasil".

As solicitações de certificados, para a AC subordinada, devem ser realizadas por pessoa física legalmente responsável.

Cabe a AR-SERPRO verificar a autorização atribuída ao solicitante, bem como a presença dos documentos exigidos. Os procedimentos utilizados pela AR-SERPRO , para identificação e verificação da autorização do solicitante, estão descritos na PC ACSERPRO.

Todos os documentos de identificação exigidos serão arquivados pela AR-SERPRO , conforme definido na PC ACSERPRO.

O representante legal da AC subordinada assina o termo de titularidade denominado "Termo de Titularidade" e é, para todos os efeitos legais, titular do certificado emitido.
A pessoa física indicada como responsável pelo certificado assina o "Termo de Responsabilidade".

Os Termos de Titularidade e de Responsabilidade serão mantidos junto à documentação exigida neste item.

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, assim como pelos danos a que derem causa pelo uso indevido do certificado.

É mantido arquivo contendo o tipo e os detalhes do procedimento de identificação utilizado pela AR-SERPRO .

3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

Pode ser solicitado um novo certificado antes da expiração do atual, observando os mesmos requisitos e procedimentos exigidos inicialmente.

3.3 CRIAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO

Após a revogação de seu certificado, uma AC deve executar os processos regulares de geração de novo par de chaves.

3.4 SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado da ACSERPRO será feita formalmente pelo representante da ACSERPRO à AC-Raiz.
A solicitação de revogação de certificado de AC imediatamente subseqüente será feita formal pelo representante da AC imediatamente subseqüente, e a com a presença física do mesmo, a fim de possibilitar a sua identificação inequívoca.

A solicitação de revogação poderá ainda ser feita por decisão judicial, ou determinação da AC-Raiz.

4. REQUISITOS OPERACIONAIS

4.1 SOLICITAÇÃO DE CERTIFICADO

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

1) A comprovação de atributos de identificação constantes do certificado;
2) Para a aprovação de certificados a chave da ACSERPRO é ativada com a presença de no mínimo 2 (dois) dos custodiantes da chave de ativação;
3) Assinatura do Termo de Titularidade e de Responsabilidade (item 3.1.9.1);

A solicitação de certificado para AC de nível imediatamente subseqüente ao da ACSERPRO somente é possível após o deferimento do pedido de credenciamento e a respectiva autorização de

funcionamento da AC em questão pela AC-Raiz.

Nesse caso, aquela AC deve encaminhar a solicitação de seu certificado à ACSERPRO por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10 (Public Key Cryptographic Standards).

4.2 EMISSÃO DE CERTIFICADO

A emissão de um certificado pela ACSERPRO é feita em cerimônia específica, com a presença dos representantes da ACSERPRO, da AC habilitada, de auditores e convidados, na qual são registrados todos os procedimentos executados.
A ACSERPRO garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subseqüente ao seu ocorre em, no máximo, 10 (dez) dias úteis após a autorização de funcionamento da AC em questão pela AC-RAIZ.
A ACSERPRO entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC habilitada.
A emissão dos certificados das AC de nível imediatamente subseqüente à ACSERPRO é feita em equipamentos que operam *off-line*.
O certificado é considerado válido a partir do momento de sua emissão.

4.3 ACEITAÇÃO DE CERTIFICADO

A AC de nível imediatamente subseqüente irá declarar, através de seus representantes legais, mediante assinatura do “Termo de Acordo”, que aceita o certificado emitido. A aceitação implica que o solicitante reconhece a veracidade dos dados contidos no certificado. A PC correspondente detalha os procedimentos referentes à aceitação do certificado.

4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1 Circunstâncias para revogação

Um certificado de AC de nível imediatamente subseqüente ao da ACSERPRO pode ser revogado a qualquer momento nas seguintes circunstâncias: por solicitação da AC titular do certificado, por decisão da ACSERPRO , do CG da ICP-Brasil ou da AC Raiz.
Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

- quando constatada emissão imprópria ou defeituosa;
- quando for necessária a alteração de qualquer informação constante no mesmo;
- no caso de dissolução da AC titular do certificado;
- no caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora; ou
- por decisão judicial.

Em relação à revogação, deve ainda ser observado que:

- A ACSERPRO revogará, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil;

- 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.

4.4.2 Quem pode solicitar revogação

A revogação do certificado de uma AC de nível imediatamente subseqüente ao da ACSERPRO somente pode ser feita:

- pela ACSERPRO;
- pela AR-SERPRO ;
- pela AC Titular do Certificado;
- pelo CG da ICP-Brasil;
- pela AC Raiz;
- **por decisão judicial**.

4.4.3 Procedimento para solicitação de revogação

Uma solicitação de revogação é necessária para que a ACSERPRO inicie o processo de revogação.
O processo de revogação é acessível e ágil para evitar a utilização indevida do certificado.
O solicitante da revogação é identificado. Somente os agentes descritos no item 4.4.2 acima podem solicitar a revogação de certificado.

Os procedimentos detalhados de solicitação de revogação estão descritos na correspondente PC.

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a mesma mantém formulário específico publicado na página https://thor.serpro.gov.br/ACSERPRO/.

Como diretrizes gerais, fica estabelecido que:

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

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

4.4.4 Prazo para solicitação de revogação

A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1.
A PC implementada pela ACSERPRO estabelece os prazos dentro dos quais a revogação do certificado poderá ser solicitada, sem ônus.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

4.4.9 Freqüência de emissão de LCR

O prazo máximo admitido para a emissão de LCR referente a certificados de AC subordinadas é de 15 (quinze) dias.

Na revogação de certificado de AC de nível imediatamente subseqüente ao seu, a ACSERPRO deverá emitir nova LCR no prazo máximo de 24 (vinte e quatro) horas e notificar todas as AC de nível imediatamente subseqüente ao seu.

São emitidas LCR na freqüência determinada na PC, 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 ACSERPRO são listados na LCR que pode ser acessada no endereço *web* contido no próprio certificado.
Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.
Os números de série de certificados revogados, das AC de nível imediatamente subseqüente, aparecem na LCR emitida pela ACSERPRO. Estes números permanecem nas LCR emitidas até a data de expiração dos certificados ser atingida, sendo removidos na primeira LCR emitida após essa data.

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

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

A ACSERPRO não disponibiliza recursos para revogação ou verificação *on-line* de estado de certificados.

4.4.12 Requisitos para verificação de revogação *on-line*

A ACSERPRO não disponibiliza diretório *on-line* ou um servidor de OCSP para verificar o estado dos

certificados emitidos pela ACSERPRO.

4.4.13 Outras formas disponíveis para divulgação de revogação

Informações de revogação de certificado de AC de nível imediatamente subseqüente ao da ACSERPRO serão divulgadas por meio de página *web* **http://ccd.serpro.gov.br/acserpro/.**

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a ACSERPRO 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

item não aplicável.

4.4.15 Requisitos especiais para o caso de comprometimento de chave

No caso do comprometimento da chave privada de uma AC de nível imediatamente subseqüente ao da ACSERPRO, a mesma deve notificar imediatamente à ACSERPRO, solicitando a revogação de seu certificado, conforme descrito no item 4.4.3 desta DPC.

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a mesma mantém formulário específico para solicitação de revogação publicado na página https://thor.serpro.gov.br/ACSERPRO/.

4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

4.5.1 TIPOS DE EVENTO REGISTRADOS

Todas as ações executadas pelo pessoal da ACSERPRO, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou.

A ACSERPRO registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

- Iniciação e desligamento do sistema de certificação;
- Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACSERPRO;
- Mudanças na configuração da ACSERPRO ou nas suas chaves;
- Mudanças nas políticas de criação de certificados;
- Tentativas de acesso (*login*) e de saída do sistema (*logoff*);
- Tentativas não autorizadas de acesso aos arquivos de sistema;
- Geração de chaves próprias da ACSERPRO ou de chaves de Titulares de Certificados;
- Emissão e revogação de certificados;
- Geração de LCR;

- Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
- Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
- Operações de escrita nesse repositório, quando aplicável.

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

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

Os registros de auditoria mínimos a serem mantidos pela ACSERPRO incluem além dos acima:

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

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.
Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da ACSERPRO é armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-Brasil.

4.5.2 Freqüência de auditoria de registros (*logs*)

A auditoria de registro será realizada sempre que houver utilização do sistema de certificação.

Os registros de auditoria são analisados pelo pessoal operacional da ACSERPRO. 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.

4.5.3 Período de Retenção para registros (*logs*) de Auditoria

A ACSERPRO 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 4.6.

4.5.4 Proteção de registro (*log*) de Auditoria

Os equipamentos da ACSERPRO, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança.
A inspeção contínua dos diversos registros dos sistemas é feita por meio das ferramentas nativas do sistema operacional, do banco de dados e do aplicativo de AC, e estão disponíveis somente para leitura. Pode ser feita também por relatórios emitidos a partir destas ferramentas. Estes dados de

auditoria são coletados e armazenados toda a vez que existir utilização do equipamento em uma sala de arquivos de nível de segurança 3.
Os registros de auditoria gerados eletrônica ou manualmente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da Política de Segurança da ICP-Brasil.

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

A ACSERPRO executa procedimentos de backup de todo o sistema de certificação, sempre que houver utilização do mesmo, seguindo scripts previamente desenvolvidos para estas atividades.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da ACSERPRO é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de ACSERPRO, pelo sistema de controle de acesso e pelo pessoal operacional.

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	AC ou Software de AR
Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado	Automático	Software de AR
Logs de *Backup* e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de *software* e *hardware*	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	*Software* de controle de acesso e pessoal de operações

4.5.7 Notificação de agentes causadores de eventos

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

4.5.8 Avaliações de vulnerabilidade

Uma Avaliação de Riscos de Segurança foi realizada para a ACSERPRO. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação.
Eventos que indiquem possível vulnerabilidade, detectados na análise dos registros de auditoria da ACSERPRO, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

4.6 ARQUIVAMENTO DE REGISTROS

4.6.1 Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela ACSERPRO:

- solicitações de certificados;
- solicitações de revogação de certificados;
- notificações de comprometimento de chaves privadas;
- emissões e revogações de certificados;
- emissões de LCR;
- trocas de chaves criptográficas da ACSERPRO;
- informações de auditoria previstas no item 4.5.1;
- correspondências formais;
- Processos de credenciamento de AC de nível imediatamente subseqüente ao da ACSERPRO.

4.6.2 Período de retenção para arquivo

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

- as LCR referentes a certificados de assinatura digital são retidas por, no mínimo, período igual ao do arquivamento dos respectivos certificados;
- as demais informações são retidas por, no mínimo, 6 (seis) anos.

Períodos de retenção específicos são definidos nas PC implementadas pela ACSERPRO, quando necessário.

4.6.3 Proteção de arquivos

Mídias de arquivos são guardadas em local seguro, sendo que a proteção criptográfica das mídias é adotada quando a classificação da informação assim o exigir. Também são protegidas de fatores ambientais como temperatura, umidade e magnetismo.
Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a Política de Segurança da ICP-Brasil.

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

Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da ACSERPRO, protegido com nível 3 de segurança.
As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.
É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 seis) meses.

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

Os servidores da ACSERPRO são sincronizados com a hora GMT fornecida pelo Observatório Nacional. 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.

4.6.6 Sistema de coleta de dados de arquivo

O sistema de coleta de dados de arquivos da ACSERPRO 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/ARe 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

4.6.7 Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da ACSERPRO e da AR-SERPRO é verificada:

- Na ocasião em que o arquivo é preparado;
- Semestralmente no momento de uma auditoria de segurança programada;
- Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

Somente podem ter acesso às informações de arquivo da AR-SERPRO :

- Pessoas corretamente identificadas e devidamente autorizadas, por meio de instrumento devidamente constituído, conforme definido no item 2.8.5;
- Titulares de Certificados, ou seus representantes legais, mediante solicitação formal, conforme definido no item 2.8.6.

4.7 TROCA DE CHAVE

A ACSERPRO comunica através de oficio, com 90 dias de antecedência, à AC subseqüente o vencimento do seu certificado, junto com as informações necessárias para a solicitação de uma nova chave.

4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

A ACSERPRO:

Estabelece e mantém documentação detalhada composta por:

- Plano de Contingência, incluindo o comprometimento de chaves, *hardware*, *software,* falhas de comunicações, e desastres naturais como fogo e inundação;
- Padrões de configuração, incluindo sistema operacional, *software* de anti-vírus e programas aplicativos específicos;
- Procedimentos de *backup*, arquivamento e armazenamento externo de segurança;

Provê a documentação a pedido:

- do CG da ICP-Brasil, quando da auditoria de práticas de DPC;
- de pessoas que administram a segurança ou auditoria de conformidade;

Provê treinamento apropriado a todo pessoal pertinente em contingência e procedimentos de recuperação de desastre.

4.8.1 Recursos computacionais, *software* ou dados corrompidos

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que recursos computacionais, *software* e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

- É feita a identificação de todos os elementos corrompidos;
- O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
- 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 ACSERPRO.

4.8.2 Certificado de entidade revogado

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que o certificado da ACSERPRO é revogado, e que podem ser resumidas da seguinte forma:

- Em caso de revogação do certificado da ACSERPRO, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados das AC de nível imediatamente subseqüente, é gerado o novo par de chaves da ACSERPRO, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela ACSERPRO, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.3 Chave de entidade comprometida

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que a chave privada da ACSERPRO é comprometida, e que podem ser resumidas nas ações listadas a seguir:

- Em caso de comprometimento da chave da ACSERPRO, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da ACSERPRO e das AC de nível imediatamente subseqüente. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela ACSERPRO, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

A ACSERPRO possui um Plano de Continuidade de Negócio 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 ACSERPRO 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 ACSERPRO faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a ACSERPRO 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.

4.9 EXTINÇÃO DA ACSERPRO OU AR-SERPRO

Quando for necessário encerrar as atividades da ACSERPRO ou da AR-SERPRO , o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes. Isto inclui:

- Prover com maior antecedência possível notificação para:
  - a AC Raiz da ICP-Brasil;
  - todas as entidades subordinadas.
- A transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a ACSERPRO ou para a AR-SERPRO extinta;
- Preservar qualquer registro não transferido a um sucessor.

As chaves públicas dos certificados emitidos pela ACSERPRO, dissolvida, serão armazenadas por outra AC, após aprovação da AC Raiz.
Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela ACSERPRO.
A ACSERPRO, 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.
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.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAS

5.1 CONTROLE FÍSICO

5.1.1 Construção e localização das instalações

A operação da ACSERPRO é executada dentro de um ambiente físico seguro em área de instalação altamente protegida.
Os componentes do sistema de certificação utilizados para a operação da ACSERPRO estão situados nas instalações **do SERPRO Rio de Janeiro, Horto.**
A localização e o sistema de certificação utilizado para a operação da ACSERPRO 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. Nenhuma das linhas telefônicas dentro do ambiente de certificação da AC oferece suporte a modems
Alguns aspectos de construção das instalações da ACSERPRO relevantes para os controles de segurança física são descritos abaixo. Outros detalhes estão descritos no restante do item 5.1.

- 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, instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas, foram executadas por técnicos especializados para garantir a proteção física da ACSERPRO.

5.1.2 Acesso físico

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

5.1.2.1 Níveis de Acesso

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

O primeiro nível – ou nível 1 – Situa-se após a primeira barreira de acesso às instalações da ACSERPRO. 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 ACSERPRO transitam

devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da ACSERPRO é executado nesse nível.
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 ACSERPRO, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *pagers*, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

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

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 ACSERPRO. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não estejam envolvidas com essas atividades não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.
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.

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

O quarto nível - ou nível 4 – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação da ACSERPRO, 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.
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.
A sala cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.
São dois os ambientes de quarto nível abrigados pela sala cofre:

- Sala de equipamentos de produção *off-line* e cofre de armazenamento.

No quarto 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: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica.

O quinto nível – ou nível 5 – é interno aos ambientes de nível 4, e compreende cofres e gabinetes trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em nível 5 ou superior.
Para garantir a segurança do material armazenado, o cofre ou o gabinete obedecem às seguintes especificações mínimas:

- Ser feito em aço ou material de resistência equivalente;

- Possuir tranca com chave.

O sexto nível – ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível, ou hardware criptográfico. Cada um desses depósitos dispõe de fechadura individual. A chave privada da ACSERPRO esta armazenada em um desses depósitos quando não estiver em operação. Quando em operação, a chave privada da ACSERPRO é armazenada em cartões criptográfico, em gabinete de nível 5.

5.1.2.2 Sistema físico de detecção

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.

As mídias de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.
Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.
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.
O sistema de monitoramento das câmeras 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.

5.1.2.4Mecanismos de emergência

Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da ACSERPRO 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.
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

A ACSERPRO possui sistema de fornecimento de energia sobressalente. Em caso de falta de energia, a ACSERPRO funciona temporariamente utilizando no-breaks com autonomia suficiente para casos onde é necessário o acionamento do gerador de apoio, que funciona durante o tempo da falta de energia.

A área de operações segura da ACSERPRO, nível 3 em diante, é conectada a uma fonte de energia padrão. Todos os componentes críticos são conectados a provisão de energia ininterrupta (UPS), prevenindo paradas anormais no caso de uma deficiência de força, de forma a atender os requisitos de disponibilidade dos sistemas da ACSERPRO e seus respectivos serviços. Um sistema de aterramento está implantado.
A área de operações segura da ACSERPRO, nível 3 em diante, tem um sistema de ar condicionado para controlar o calor e umidade que é independente do sistema de ar condicionado de edifício.
Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados. 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.
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.
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. Qualquer modificação nessa rede é previamente documentada.
Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.
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.
A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.
O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.
A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC é garantida por meio de:

- Geradores de porte compatível;
- Geradores de reserva, do mesmo porte dos citados no nível 1;
- Sistemas de *no-breaks* redundantes;
- Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água

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

5.1.5 Prevenção e proteção contra incêndio

Todas as instalações da ACSERPRO possuem sistemas de prevenção contra incêndio.
Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobre-aquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

Nas instalações da ACSERPRO não é permitido fumar ou portar objetos que produzam fogo ou faísca.
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.
Em caso de incêndio nas instalações da ACSERPRO, 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 ACSERPRO atende a norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”).

5.1.7 Destruição de lixo

Documentos em papel e demais mídias não em papel que contêm elementos confidenciais da ACSERPRO, informações comercialmente sensíveis ou confidenciais são eliminadas seguramente:

- No caso de mídia magnéticas:
  - Por desmagnetização e destruição completa do recurso;
  - Pelo uso de uma utilidade aprovada para esfregar ou sobrescrever mídias magnéticas.
- No caso de documentos em papel: pela trituração antes de ir para o lixo.
- No caso de outras mídias: pela destruição completa do recurso.

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

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

5.2 CONTROLES PROCEDIMENTAIS

5.2.1 Perfis qualificados

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. Um exemplo desta prática é que as pessoas que executam atividades de examinar registros de sistema, ou examinar *logs* de auditoria não são as mesmas pessoas envolvidas na atividade que gerou estes registros e *logs*, assegurando que as pessoas que executam estão agindo dentro das responsabilidades e dentro da política de segurança declarada.
Isto é realizado criando perfis separados e contas na estação de trabalho de serviço. Cada perfil possui uma quantia limitada de capacidade operacional. Este método permite um sistema de “verificações e equilíbrio” a ocorrer entre os vários perfis. Os seguintes perfis foram estabelecidos pela ACSERPRO:

- Gerente da AC;
- Administrador de Segurança;
- Administrador de Banco de Dados;
- Administrador do Sistema de Gerenciamento de Certificados;
- Administrador do Servidor *web*;
- Administrador do Sistema Operacional;
- Administrador do Security Server;
- Administrador de AC;
- Operador;
- Segurança patrimonial;
- Apoio administrativo.

Todos os operadores do sistema de certificação 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.
Quando um funcionário se desliga da ACSERPRO, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o funcionário ocupa com relação à ACSERPRO, são revistas suas permissões de acesso. Os termos de responsabilidade assinados pelo funcionário contém a descrição de todos os recursos, antes disponibilizados, que o funcionário deverá devolver à ACSERPRO no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

Controle multiusuário é requerido para a geração e a utilização da chave privada da ACSERPRO, conforme o descrito em 6.2.2.

Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da ACSERPRO necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da ACSERPRO. As demais tarefas da ACSERPRO podem ser executadas por um único operador.

5.2.3 Identificação e autenticação para cada perfil

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

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

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

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

A ACSERPRO 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, juntamente com procedimentos de validação dessas senhas.

5.3 CONTROLES DE PESSOAL

Todos os funcionários da ACSERPRO e da AR-SERPRO , encarregados de tarefas operacionais, tem registrado em contrato ou termo de responsabilidade:

- Os termos e as condições do perfil que ocupam;
- O compromisso de observar as normas, políticas e regras aplicáveis da ACSERPRO;
- O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
- 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 ACSERPRO 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 ACSERPRO e na Política de Segurança da ICP-Brasil.

5.3.2 Procedimentos de Verificação de Antecedentes

Com o propósito de resguardar a segurança e a credibilidade da ACSERPRO, 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:

- Verificação de antecedentes criminais;
- Verificação de situação de crédito;
- Verificação de histórico de empregos anteriores;
- Comprovação de escolaridade e de residência;

5.3.3 Requisitos de treinamento

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

- Princípios e mecanismos de segurança da ACSERPRO e das AR vinculadas;
- Sistema de certificação em uso na ACSERPRO;
- Procedimentos de recuperação de desastres e de continuidade do negócio;
- Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Freqüência e requisitos para reciclagem técnica

Todo o pessoal da ACSERPRO e das ARs 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 ACSERPRO. Treinamentos de reciclagem são realizados pela ACSERPRO sempre que necessário.

5.3.5 Freqüência e seqüência de rodízios de cargos

A ACSERPRO não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

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

5.3.7 Requisitos para contratação de pessoal

O pessoal da ACSERPRO e das AC de nível imediatamente subseqüente, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, ser contratado conforme o estabelecido na Política de Segurança da ICP Brasil.

5.3.8 Documentação disponibilizada ao pessoal

A ACSERPRO disponibiliza para todo o seu pessoal, para o das AC de nível imediatamente subseqüente e para a AR vinculada:

- Esta DPC;
- A PC que implementa;
- A Política de Segurança da ICP-Brasil;
- A Política de Segurança da ACSERPRO;
- Documentação de hardware e software relativa à função desempenhada;
- Documentação operacional relativa às suas atividades;
- Contratos, normas e políticas relevantes para suas atividades.

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

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 Geração do Par de Chaves

O par de chaves da ACSERPRO é gerado pela própria ACSERPRO, em módulo criptográfico de hardware com padrão de segurança FIPS 140-1 level 3, utilizando algorítmo RSA para geração do

par de chaves e algorítmo 3-DES para sua proteção, após o deferimento do pedido de credenciamento da mesma e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil.
O par de chaves criptográficas de uma AC de nível imediatamente subseqüente ao da ACSERPRO é gerado pela própria AC, após o deferimento do pedido de credenciamento e habilitação da mesma, e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil. Os procedimentos específicos estão descritos na PC implementada.
As PC implementadas pela ACSERPRO e pelas AC subordinadas definem o meio utilizado para armazenamento das respectivas chaves privadas, com base nos requisitos aplicáveis estabelecidos pelo documento "Requisitos Mínimos para Políticas de Certificado na ICP-Brasil", aprovados pela Resolução no 7, de 12 de dezembro de 2001, do Comitê Gestor da ICP-Brasil.

6.1.2 Entrega da chave privada à entidade titular

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

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

Os procedimentos para a entrega da chave pública de um solicitante de certificado à ACSERPRO estão detalhados na PC implementada.

6.1.4 Disponibilização de chave pública da ACSERPRO para usuários

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

- Formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- Diretório;
- Página *web* da ACSERPRO (http://ccd.serpro.gov.br/acserpro/);
- Outros meios seguros aprovados pelo CG da ICP-Brasil.

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a mesma mantém página correspondente para publicação https://thor.serpro.gov.br/ACSERPRO/.

6.1.5 Tamanhos de chave

O tamanho das chaves criptográficas associadas a certificados emitidos pela ACSERPRO será de, no mínimo 2048 (dois mil e quarenta e oito) bits, conforme estabelecido pela ICP-Brasil para chaves criptográficas associadas a certificados de AC.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da ACSERPRO seguem o padrão FIPS (*Federal Information Processing Standards*) 140-1[1] *level* 3, uma vez que utilizam *hardware* criptográfico com esta certificação.

6.1.7 Verificação da qualidade dos parâmetros

A verificação dos parâmetros de geração de chave é feita de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program*) do NIST (*National Institute of Standards and Technology*), uma vez que o *hardware* utilizado é certificado pelo NIST como FIPS 140-1 *level* 3.

6.1.8 Geração de chave por *hardware ou software*

O processo de geração do par de chaves da ACSERPRO é feito por hardware padrão FIPS (Federal Information Processing Standards) 140-1, level 3.
A PC implementada pela ACSERPRO caracteriza o processo utilizado para a geração de chaves criptográficas das AC de nível imediatamente subseqüente ao seu, com base nos requisitos aplicáveis estabelecidos pelo documento "Requisitos Mínimos para Políticas de Certificado na ICP-Brasil", aprovados pela Resolução nº 7, de 12 de dezembro de 2001, do Comitê Gestor da ICP-Brasil.

6.1.9 Propósitos de uso de chave (conforme campo "Key usage" na X.509 v3)

A chave privada da ACSERPRO é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCR.
As chaves privadas dos titulares de certificados emitidos pela ACSERPRO são utilizadas apenas para a assinatura dos certificados por ela emitidos e de suas LCR.

6.2 PROTEÇÃO DA CHAVE PRIVADA

A chave privada da ACSERPRO é gerada, armazenada e utilizada apenas em hardware criptográfico específico, classificado como FIPS 140-1 level 3, não havendo portanto tráfego da mesma em nenhum momento.

6.2.1 Padrões para módulo criptográfico

Toda a geração e armazenamento da chave da ACSERPRO, e também operações de assinatura de certificados pela ACSERPRO, são realizadas em um módulo de *hardware* criptográfico classificado como FIPS 140-1 Nível 3.

[1] FIPS 140-1 – *Federal Information Processing Standards* 140-1. Esse padrão será substituído pelo FIPS 140-2, hoje em fase de implantação por parte do National Institute of Standards and Technology.

O padrão requerido para os módulos de geração de chaves criptográficas das AC de nível imediatamente subseqüente ao da ACSERPRO é o FIPS 140-1 Nível 2 ou superior.

6.2.2 Controle “n de m’ para chave privada

A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da ACSERPRO é dividida em “9” partes e distribuídas por “9” custodiantes designados pela ACSERPRO (m), É necessária a presença de no mínimo “2” custodiantes (n) para a ativação do componente e a consequente utilização da chave privada.

6.2.3 Recuperação (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, das AC de nível imediatamente subseqüente.

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

A ACSERPRO 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.
A ACSERPRO não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subseqüentes ao seu.
Qualquer entidade titular de certificado pode, a seu critério, manter cópia de sua própria chave privada.
A cópia de segurança deve 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

As chaves privadas dos titulares de certificados emitidos pela ACSERPRO não são arquivadas.
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 ACSERPRO é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7 Método de ativação de chave privada

A ativação da chave privada da ACSERPRO é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de “2” de “9” dos *custodiantes* da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da ACSERPRO. As senhas utilizadas obedecem à política de senhas estabelecida pela ACSERPRO.

6.2.8 Método de desativação de chave privada

A chave privada da ACSERPRO, 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" de "9" dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da ACSERPRO. As senhas utilizadas obedecem à política de senhas estabelecida pela ACSERPRO.
Quando a chave privada da ACSERPRO 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 estivesse armazenada, deve ser sobrescrito.

6.2.9 Método de destruição de chave privada

Além do estabelecido no item 6.2.8 desta DPC, todas as cópias de segurança da chave privada da ACSERPRO e os cartões criptográficos dos custodiantes serão destruídos pelos administradores da ACSERPRO.

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

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

As chaves públicas da ACSERPRO, e dos certificados por ela emitidos, são armazenadas, após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

A chave privada da ACSERPRO é utilizada apenas durante o período de validade do certificado correspondente, cujo prazo máximo é de 8 anos. A chave pública da ACSERPRO 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.
Os certificados emitidos pela ACSERPRO para as AC de nível imediatamente subseqüente ao seu terão validade de no máximo 8 anos.

6.4 DADOS DE ATIVAÇÃO

6.4.1 Geração e instalação dos dados de ativação

São necessários as presenças de no mínimo dois custodiantes, com os cartões criptográficos e senha de ativação do módulo criptográfico.

6.4.2 Proteção dos dados de ativação.

Os dados de ativação são protegidos por cartões criptográficos individuais com senha, e são armazenados em ambiente de nível 6 de segurança.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 CONTROLES DE SEGURANÇA DOS COMPUTADORES

6.5.1 Requisitos técnicos específicos de segurança computacional

A ACSERPRO garante que a geração de seu par de chaves é realizada em ambiente *off-line,* para impedir o acesso remoto não autorizado.
Os computadores servidores, utilizados pela ACSERPRO e pelas AC subordinadas, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

- Controle de acesso aos serviços e perfis da ACSERPRO;
- Separação das tarefas e atribuições relacionadas a cada perfil qualificado da ACSERPRO;
- Acesso restrito aos bancos de dados da ACSERPRO;
- Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- Geração e armazenamento de registros de auditoria da ACSERPRO;
- Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- Mecanismos para cópias de segurança (*backup*).

Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.
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 ACSERPRO ou da AC subordinada, 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 ACSERPRO ou AC subseqüente. Todos esses eventos são registrados para fins de auditoria.

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

6.5.2 Classificação da segurança computacional

A ACSERPRO aplica configurações de segurança definida como EAL3, baseada na Common Criteria e desenvolvida para o sistema operacional SUSE LINUX pela SUSE, que disponibiliza as atualizações deste sistema operacional utilizado nos servidores do Sistema de Certificação Digital do SERPRO.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 Controles de desenvolvimento de sistemas

A ACSERPRO adota o Sistema de Certificação Digital do SERPRO (Serviço Ferderal 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.
Os processos de projeto e desenvolvimento conduzidos pela ACSERPRO provêem documentação suficiente para suportar avaliações externas de segurança dos componentes da ACSERPRO.

6.6.2 Controle de gerenciamento de segurança

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.

O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela ACSERPRO, 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:

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

6.6.3 Classificação de segurança de ciclo de vida

Este item não se aplica.

6.7 CONTROLES DE SEGURANÇA DE REDE

Este item não se aplica.

6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

O módulo criptográfico utilizado pela ACSERPRO para o armazenamento de sua chave privada é certificado como FIPS (*Federal Information Processing Standards*) 140-1, *level* 3.

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico aprovado pelo CG da ICP - Brasil.
O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
- a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
- a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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.

7. PERFIS DE CERTIFICADO E LCR

7.1 PERFIL DO CERTIFICADO

Todos os certificados emitidos pela ACSERPRO estão em conformidade com o formato definido pelo padrão ITU X.509.

7.1.1 Número(s) de versão

Todos os certificados emitidos pela ACSERPRO implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.1.2 Extensões de certificados

Os certificados emitidos pela ACSERPRO, sob a PC ACSERPRO, obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

- "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o resumo SHA-1 da chave pública da ACSERPRO;
- "*Subject Key Identifier*", não crítica: contém o *hash* SHA-1 da chave pública da AC titular do

certificado;

- "*Key Usage*", crítica: somente os bits e keyCertSign e cRLSign são ativados;
- "*Certificate Policies*", não crítica:
  - o campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;
  - o campo policyQualifiers contém o endereço *URL* da página *web, http://ccd.serpro.gov.br/acserpro/docs/dpcacserpro.pdf,* onde se obtém a DPC da ACSERPRO;
- O "Basic Constraints", crítica: contém o campo CA=TRUE;
- "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *web, http://ccd.serpro.gov.br/lcr/acserpro.crl,* onde se obtém a LCR da ACSERPRO.

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, consultar a DPC correspondente publicada na página https://thor.serpro.gov.br/ACSERPRO/docs/DPCACSERPRO.pdf.

7.1.3 Identificadores de algoritmos

Os certificados emitidos pela ACSERPRO são assinados com o uso do algoritmo RSA com SHA-1 como função *hash* (OID = 1.2.840.113549.1.1.5), conforme o padrão PKCS#1 (RFC 2313).

7.1.4 Formatos de nome

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

C= BR
O= ICP-Brasil
OU= **Serviço Federal de Processamento de Dados – SERPRO**
CN= nome da AC

Para os certificados de AC, emitidos sob a PC ACSERPRO, que emitem certificados para o Sistema de Pagamentos Brasileiro – SPB o nome da AC titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C= BR
O= ICP-Brasil
OU= Serviço Federal de Processamento de Dados – SERPRO
OU=CSPB-X *onde* "X" identifica a AC perante o SPB
CN= nome da AC

7.1.5 Restrições de nome

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

- não serão utilizados sinais de acentuação, tremas ou cedilhas;
- além dos caracteres alfanuméricos, podem 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

7.1.6 OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a ACSERPRO após conclusão do processo de seu credenciamento, é **2.16.76.1.1.2**.

7.1.7 Uso da extensão “Policy Constraints”

Não se aplica

7.1.8 Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço *web* da DPC da ACSERPRO, http://ccd.serpro.gov.br/acserpro/docs/dpcacserpro*.pdf.*

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, consultar a DPC correspondente publicada na página https://thor.serpro.gov.br/ACSERPRO/docs/DPCACSERPRO.pdf.

7.1.9 Semântica de processamento para extensões criticas

Extensões críticas são interpretadas, no âmbito da ACSERPRO, conforme a RFC 2459.

7.2 PERFIL DE LCR

7.2.1 Número (s) de versão

As LCR geradas pela ACSERPRO implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2 Extensões de LCR e de suas entradas

A ACSERPRO adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

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

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Qualquer alteração nesta DPC da ACSERPRO será submetida previamente à aprovação do CG da ICP-Brasil. A DPC será alterada sempre que uma nova PC impelementada o exigir.

8.2 POLÍTICAS DE PUBLICAÇÃO E DE NOTIFICAÇÃO

A ACSERPRO publica esta DPC, em sua página *web* acessível pela URL http://ccd.serpro.gov.br/acserpro/docs/dpcacserpro.pdf. Sempre que esta DPC for atualizada será alterado o arquivo disponibilizado na *web*.

Para os certificados emitidos pela ACSERPRO até 18 de março de 2005, a DPC correspondente é publicada na página https://thor.serpro.gov.br/ACSERPRO/docs/DPCACSERPRO.pdf.

8.3 PROCEDIMENTOS DE APROVAÇÃO

Essa DPC foi submetida à aprovação da AC-RAIZ da ICP-Brasil, durante o processo de credenciamento da ACSERPRO, conforme o determinado pelo documento “Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil”.