Autor: Serasa S.A.

Edição: março 2016
Versão: 6.0

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos mínimos, obrigatoriamente observados pela AC Serasa Autoridade Certificadora Principal (ACP), AC integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação - DPC. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução de seus serviços.

1.1.2. Toda DPC elaborada no âmbito da ICP-Brasil obrigatoriamente adota a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10].

1.1.3. A Autoridade Certificadora Principal (ACP), está no nível imediatamente subsequente ao da AC Raiz.

1.2. Identificação

Esta Declaração de Práticas de Certificação, referida a seguir simplesmente como "DPC-Serasa ACP", descreve as práticas e os procedimentos empregados pela AC Serasa ACP no âmbito da ICP-Brasil. O OID desta DPC-Serasa ACP é 2.16.76.1.1.3.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridade Certificadora (AC)

Esta DPC-Serasa ACP se refere à AC Serasa ACP (SERASA S.A., com sede na Alameda dos Quinimuras, 187, São Paulo, SP, CEP: 04068-900, CNPJ no 62.173.620/0001-80).

1.3.2. Autoridade de Registro (AR)

1.3.2.1. Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, podem ser executados nas Autoridades de Registros vinculadas a AC Serasa ACP, cujos endereços estão disponíveis na página https://serasa.certificadodigital.com.br/ajuda/repositorio/.Nesta página estão relacionadas as seguintes informações:

a) relação de todas as ARS credenciadas, com informações sobre as PCs que implementam;
b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
d) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;
e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
f) acordos operacionais celebrados pelas ARs vinculadas com outras ARs da ICPBrasil, se for o caso.

1.3.2.2. A AC Serasa ACP manterá as informações acima sempre atualizadas.

1.3.3. Prestador de Serviços de Suporte

1.3.3.1. Os Prestadores de Serviços de Suporte vinculados à AC Serasa ACP estão relacionados na página https://serasa.certificadodigital.com.br/ajuda/repositorio/.

1.3.3.2. PSS são entidades utilizados pela AC Serasa ACP ou pela Serasa AR para desempenhar atividade descrita nesta DPC ou na PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infraestrutura física e lógica;
b) disponibilização de recursos humanos especializados; ou
c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC Serasa ACP manterá as informações acima sempre atualizadas.

1.3.4. Titulares de Certificado

A AC Serasa ACP emite certificados para Autoridades Certificadoras de nível imediatamente subsequente ao seu. Estas Autoridades Certificadoras atendem aos requisitos do Comitê Gestor da ICP-Brasil quanto ao credenciamento e funcionamento. Podem ser Titulares de Certificado Digital Serasa as pessoas jurídicas de direito público ou privado, nacionais ou internacionais, que atendam aos requisitos desta DPC-Serasa ACP.

1.3.5. Aplicabilidade

Os certificados emitidos pela AC Serasa ACP para suas ACs subsequentes têm sua utilização exclusiva para assinatura de certificados digitais e de Lista de Certificados Revogados (LCR).

1.4. Dados de Contato

Dúvidas decorrentes da leitura desta DPC-Serasa ACP e que não sejam respondidas mediante a leitura da página https://serasa.certificadodigital.com.br/ajuda/repositorio/ podem ser esclarecidas contatando:

Serasa S.A.
Alameda dos Quinimuras, 187
CEP: 04068-900
São Paulo, SP
Telefones: 11 2608-5033 e 11 2847-9201
Contato: Andreia Fernandez
Área: Governança e Compliance e-ID
E-mail: ar_compliance@br.experian.com

2. DISPOSIÇÕES GERAIS

2.1. Obrigações e Direitos

2.1.1. Obrigações da AC Serasa ACP

As obrigações da AC Serasa ACP são as abaixo relacionadas:

a) operar de acordo com esta DPC-Serasa ACP;
b) gerar e gerenciar o seu par de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado, ou o encerramento de suas atividades;
f) distribuir o seu próprio certificado;
g) emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu ou os certificados de AR vinculadas;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR) e, quando aplicável, disponibilizar consulta *on-line* de situação do certificado (OCSP - *On-line Certificate Status Protocol*);
k) publicar em sua página web sua DPC-Serasa ACP;
l) publicar, em sua página web, as informações definidas no item 2.6.1 deste documento;
m) publicar, em página web, informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;
n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;

o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
p) adotar as medidas de segurança e controle previstas na DPC-Serasa ACP e Política de Segurança da AC Serasa ACP, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
s) manter e testar regularmente seu Plano de Continuidade do Negócio;
t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas AC de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do Comitê Gestor da ICP-Brasil;
u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC Serasa ACP;
v) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos; e
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2. Obrigações da Serasa AR

As obrigações da Serasa AR são as abaixo relacionadas:

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de certificado à AC Serasa ACP utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) disponibilizar os certificados emitidos pela AC Serasa ACP aos seus respectivos solicitantes;
f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC Serasa ACP e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];
h) manter e garantir a segurança da informação por ela tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil;
i) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
j) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9 e 3.1.10; e
k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas.

2.1.3. Obrigações do Titular do Certificado

Constituem-se obrigações do titular de certificado emitido pela AC Serasa ACP:

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

2.1.4. Direitos da Terceira Parte (Relying Party)

2.1.4.1. Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital.

2.1.4.2. Constituem direitos da terceira parte:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;
b) verificar, a qualquer tempo, a validade do certificado. Um certificado emitido por AC integrante da ICPBrasil é considerado válido quando:

i) não constar da LCR da AC emitente;
ii) não estiver expirado; e
iii) puder ser verificado com o uso de certificado válido da AC emitente.

2.1.4.3. O não exercício desses direitos não afasta a responsabilidade da AC Serasa ACP e do titular do certificado.

2.1.5. Obrigações do Repositório da AC Serasa ACP

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

2.2. Responsabilidades

2.2.1. Responsabilidades da AC Serasa ACP

2.2.1.1. A AC Serasa ACP responde pelos danos a que der causa.

2.2.1.2. A AC Serasa ACP responde solidariamente pelos atos das entidades de sua cadeia de certificação: AC subordinadas, AR e PSS.

2.2.1.3. Não se aplica.

2.2.2. Responsabilidade da AR

As ARs vinculadas à AC Serasa ACP serão responsáveis pelos danos a que derem causa.

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (Relying Parties)

A terceira parte (Relying Party) não é responsável perante a AC Serasa ACP e as AC e AR a ela vinculadas, exceto na hipótese de prática de ato ilícito. Essa terceira parte deverá indenizar a AC Serasa ACP e/ou os titulares de seus certificados pelos danos a que der causa em decorrência de omissão ou ação não conforme com a legislação aplicável.

2.3.2. Relações Fiduciárias

2.3.2.1. A AC Serasa ACP ou Serasa AR indenizará integralmente os danos a que comprovadamente der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.2.2. A AC Serasa ACP dispõe de uma Política de Garantia que se estende a todos titulares de certificados digitais por ela emitidos e que prevê o pagamento de uma indenização no valor de R$ 40.000,00 (quarenta mil reais) por certificado pelos danos a que a Serasa ACP comprovadamente der causa. A Política de Garantia cobre perdas e danos decorrentes de comprometimento da chave privada da AC Serasa ACP, de erro na identificação do titular, de emissão defeituosa do certificado ou de erros ou omissões da AC Serasa ACP e da Serasa AR na prestação de seus serviços aos beneficiários. Os detalhes das condições de aplicação da Política de Garantia estão disponíveis na página web https://serasa.certificadodigital.com.br/ajuda/repositorio/politica-de-garantia/

2.3.3. Processos Administrativos

O titular do certificado que sofrer perdas e danos decorrentes do uso do Certificado Digital Serasa terá o direito comunicar à AC Serasa ACP que deseja a indenização prevista no documento Política de Garantia (https://serasa.certificadodigital.com.br/ajuda/repositorio/politica-de-garantia/) para tais casos, observadas as seguintes condições:

a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC Serasa ACP, tal comprometimento deverá ter sido comprovado por perícia realizada por perito especializado e independente;
b) nos casos de erro na identificação, o titular do certificado não poderá requerer qualquer indenização quando os dados constantes no certificado corresponderem aos dados fornecidos por esse titular à AC Serasa ACP;
c) nos casos de erro na transcrição, o titular do certificado não poderá requerer qualquer indenização quando houver aceito o certificado.

2.4. Interpretação e Execução
2.4.1. Legislação

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

2.4.2. Forma de interpretação e notificação

2.4.2.1. Caso esta DPC-Serasa ACP ou alguma de suas disposições venha a ser considerada ou declarada inválida, ilegal ou não aplicável por lei, a AC Serasa ACP tomará de imediato as medidas necessárias para adequar esta DPC-Serasa ACP ou a disposição em questão às exigências legais, sem prejuízo para o titular do certificado.

2.4.2.2. As notificações, solicitações ou quaisquer outras comunicações necessárias, sujeitas às práticas descritas nesta DPC-Serasa ACP, serão realizadas pela AC Serasa ACP, pela Serasa AR e pelas ACs e ARs vinculadas por e-mail a ser enviado ao endereço eletrônico fornecido pelo solicitante no formulário de solicitação. O e-mail será considerado como recebido quando enviado a esse endereço.

2.4.2.3. A DPC-Serasa ACP não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3. Procedimentos de solução de disputa

2.4.3.1. Em caso de conflito entre esta DPC-Serasa ACP e outras declarações, políticas, planos, acordos, contratos ou documentos que a AC Serasa ACP adotar, esta DPC-Serasa ACP prevalecerá.

2.4.3.2. Esta DPC-Serasa ACP não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3.3. Os casos omissos deverão ser encaminhados para apreciação da AC Raiz.

2.5. Tarifas de Serviço

Pelo certificado emitido a AC Serasa ACP cobrará o valor estabelecido contratualmente.

2.5.1. Tarifas de emissão e renovação de certificados

Pela emissão e renovação do certificado a AC Serasa ACP cobrará o valor estabelecido contratualmente.

2.5.2. Tarifas de acesso ao certificado

Pelo acesso ao certificado a AC Serasa ACP cobrará o valor estabelecido contratualmente.

2.5.3. Tarifas de revogação ou de acesso a informação de status

Pela revogação ou acesso a informação de status a AC Serasa ACP cobrará o valor estabelecido contratualmente.

2.5.4. Tarifas para outros serviços

Pelos demais serviços a AC Serasa ACP cobrará o valor estabelecido contratualmente.

2.5.5. Política de reembolso

Caso o certificado deva ser revogado por motivo de comprometimento da chave privada da AC Serasa ACP ou da mídia armazenadora da chave privada da AC Serasa ACP, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC Serasa ACP, esta reembolsará ao solicitante o preço pago pelo certificado, exceto em caso de emissão de outro certificado em substituição, sem cobrar pelo mesmo.

2.6. Publicação e Repositório

2.6.1. Publicação de informação da AC Serasa ACP

2.6.1.1. A AC Serasa ACP publica e mantém disponível em seu site (https://serasa.certificadodigital.com.br/ajuda/repositorio/) um repositório com disponibilidade de no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2. As seguintes informações são publicadas em seu repositório:

a) seu próprio certificado;
b) suas LCR;
c) sua DPC-Serasa ACP;
d) não se aplica;
e) uma relação, regularmente atualizada, contendo as AR vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;
f) uma relação, regularmente atualizada, das AR vinculadas que tenham celebrado acordos operacionais com outras AR da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado; e

g) uma relação, regularmente atualizada, dos PSS vinculados.

2.6.2. Frequência de publicação

A AC Serasa ACP manterá as informações de que trata o item anterior sempre atualizadas.

2.6.3. Controles de acesso

2.6.3.1. Não há qualquer restrição ao acesso para consulta às informações citadas nos itens acima.

2.6.3.2. São utilizados controles de acesso apropriados para restringir a possibilidade de escrita ou modificação dessas informações a pessoal autorizado.

2.6.4. Repositórios

Os repositórios da AC Serasa ACP podem ser acessados através da página https://serasa.certificadodigital.com.br/ajuda/repositorio/ utilizando o protocolo de acesso http.

2.7. Fiscalização e Auditoria de Conformidade

2.7.1. As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

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

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

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

2.7.5. A AC Serasa ACP e as entidades da ICP-Brasil a ela diretamente vinculadas – AC Subordinadas, AR Vinculadas e PSS, receberam auditoria prévia, para fins de credenciamento. E também será responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

2.8. Sigilo
2.8.1. Disposições Gerais

2.8.1.1. A chave privada de assinatura digital da AC Serasa ACP foi gerada e é mantida pela própria AC Serasa ACP, que é responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC Serasa ACP é de sua inteira responsabilidade.

2.8.1.2.Os responsáveis pelo uso de certificados da Autoridade Certificadora subsequente têm as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas.
Além disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.2. Tipos de informações sigilosas

Como princípio geral, nenhum documento, informação ou registro fornecido à AC Serasa ACP ou à Serasa AR deve ser divulgado.

2.8.3. Tipos de informações não sigilosas

2.8.3.1. Não são considerados como informações sigilosas pela AC Serasa ACP e pela Serasa AR:

a) os certificados e as LCR emitidos pela AC Serasa ACP,
b) as informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
c) as PCs implementadas pela AC – Não se aplica;
d) esta DPC-Serasa ACP;
e) as versões públicas de Políticas de Segurança;
f) a conclusão dos relatórios de auditoria.

2.8.3.2. Os dados fornecidos pelo solicitante não são considerados confidenciais quando:

a) estejam na posse legítima da AC Serasa ACP ou da Serasa AR antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;

b) posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro(s) com direitos legítimos para divulgação sua sem quaisquer restrições para tal;
c) sejam requisitados por determinação judicial ou governamental, desde que a AC Serasa ACP ou a Serasa AR comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação;

2.8.3.3. Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pela AC Serasa ACP e pela Serasa AR, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

2.8.4. Divulgação de informação de revogação/suspensão de certificado

2.8.4.1.A AC Serasa ACP disponibiliza permanentemente em seu site https://serasa.certificadodigital.com.br/ajuda/repositorio/, relação de certificados por ela emitidos que foram revogados.

2.8.4.2.Os motivos que justificaram a revogação são sempre informados para o titular ou responsável pelo certificado e mantidos confidenciais pela AC Serasa ACP e pela Serasa AR, exceto quando tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC Serasa ACP ou a Serasa AR, se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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

2.8.5. Quebra de sigilo por motivos legais

As informações fornecidas pelo solicitante ou titular do certificado, bem como os documentos e registros relativos ao solicitante, ao titular do certificado, à solicitação ou ao certificado emitido não são mantidas sob sigilo pela AC Serasa ACP ou pela Serasa AR quando a lei prevê a sua publicidade ou divulgação ou por ordem judicial.

2.8.6. Informações a terceiros

A AC Serasa ACP não fornece nem fornecerá a terceiros nenhum documento, informação ou registro sob sua guarda, exceto nas hipóteses mencionadas nesta DPC-Serasa ACP.

2.8.7. Divulgação por solicitação do titular

O titular do certificado, ou seu representante legal devidamente identificado, qualificado e autorizado, tem e terá sempre acesso às informações que lhe dizem respeito que estejam sob a guarda da AC Serasa ACP e da Serasa AR em razão da solicitação e da emissão do certificado digital. O titular do certificado pode autorizar a AC Serasa ACP

ou a Serasa AR a divulgar tais informações a terceiros ou unicamente às pessoas que indique nessa autorização.

Essa autorização pode ser feita no ato da solicitação do certificado, no próprio formulário de solicitação, ou posteriormente, por e-mail ou outro documento legalmente aceito.

2.8.8. Outras circunstâncias de divulgação de informação

A AC Serasa ACP e a Serasa AR podem divulgar informações que não sejam consideradas sigilosas pelo fato de:

a) estarem na posse legítima da AC Serasa ACP ou da Serasa AR antes de seu fornecimento pelo solicitante ou titular do certificado ou o solicitante ou titular do certificado haver autorizado a sua divulgação;
b) posteriormente ao seu fornecimento pelo solicitante ou titular do certificado, terem sido obtidas ou puderem ter sido obtidas legalmente de um terceiro com direitos legítimos para sua divulgação sem quaisquer restrições;
c) terem sido requisitadas por determinação judicial ou governamental, obrigando-se a AC Serasa ACP, nesse caso, a comunicar previamente, se possível, e de imediato o solicitante ou titular do certificado a existência de tal determinação.

2.9. Direitos de Propriedade Intelectual

A emissão do certificado não implica a transferência, cessão ou licença de direitos de propriedade intelectual de softwares, certificados, políticas, especificações de práticas e procedimentos, nomes, chaves criptográficas e outros da AC Serasa ACP ou da Serasa AR para o solicitante, exceto em relação ao próprio certificado emitido, o qual é objeto de licença de uso por prazo determinado nas condições estabelecidas nesta DPC e nos demais documentos aplicáveis.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Registro Inicial

3.1.1. Considerações Gerais

3.1.1.1. A Serasa AR efetua as atividades inerentes à função de autoridade de registro por meio de, no mínimo, dois agentes de registro, com base nos dados fornecidos no formulário de solicitação e nos documentos exigidos.

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

3.1.2. Tipos de nomes

3.1.2.1. A AC Serasa ACP emite certificados com nomes que permitam a identificação unívoca. Para isso utiliza o "distinguished name" do padrão ITU X.500, endereços de correio eletrônico ou endereços de página Web (URL).

3.1.2.2. O certificado emitido pela AC Serasa ACP não inclui o nome da pessoa responsável.

3.1.3. Necessidade de nomes significativos

A AC Serasa ACP faz uso de nomes significativos que possibilitam determinar a identidade da organização a que se referem, para a identificação dos titulares dos certificados emitidos pela AC Serasa ACP.

3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.5. Unicidade de nomes

Os identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC Serasa ACP. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6. Procedimento para resolver disputa de nomes

A AC Serasa ACP se reserva o direito de tomar todas as decisões referentes a disputas de nomes das entidades solicitantes de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.8. Método para comprovar a posse de chave privada

A confirmação de 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, relativos a POP (*Proof of Possession*).

3.1.9. Autenticação da identidade de um indivíduo

A confirmação da identidade é realizada mediante a presença física do representante legal da AC, com base em documentos de identificação legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil. Solicitações de certificados para AC subsequente são realizadas pela pessoa física legalmente responsável. Cabe à Serasa AR

verificar a autorização atribuída ao solicitante, bem como a presença dos documentos exigidos.

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

Deverá ser apresentada a seguinte documentação, em sua versão original, e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado, sendo que a AC Serasa ACP, ao seu critério, poderá solicitar documentos adicionais de identificação:

a) Cédula de Identidade ou Passaporte, se brasileiro;
b) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
c) Passaporte, se estrangeiro não domiciliado no Brasil;
d) caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data da validação presencial;
e) comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial;
f) mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4.
g) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11];
h) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11].

NOTA 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

NOTA 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

NOTA 3: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observa o disposto na lei vigente.

Nota 4: Para a identificação de indivíduo na emissão de certificado que integra o Documento RIC, deverá ser observado o disposto no item 3.1.1.6.

NOTA 5: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a CNH - Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

NOTA 6: Deverão ser consultadas as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL [1].

NOTA 7: Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

3.1.9.2. Não se aplica.

3.1.10. Autenticação da identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.1.1. Neste item define-se os procedimentos empregados pelas ARs vinculadas a AC Serasa ACP para a confirmação da identidade de uma pessoa jurídica.

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

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

a) apresentação do rol de documentos elencados no item 3.1.10.2;
b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
c) presença física dos representantes legais e do responsável pelo uso do certificado, e assinatura do termo de titularidade de que trata o item 4.1.1.

3.1.10.2. Documentos para efeitos de identificação de uma organização

3.1.10.2.1. A confirmação da identidade de uma AC subordinada é feita com base nos CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

3.1.10.2.2. A confirmação da identidade de uma pessoa jurídica é feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos a sua habilitação jurídica:
   i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;
   ii. se entidade privada:
      1. ato constitutivo, devidamente registrado no órgão competente; e
      2. documentos da eleição de seus administradores, quando aplicável;

b) Relativos a sua habilitação fiscal:
   i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
   ii. prova de inscrição no Cadastro Específico do INSS – CEI.

3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.10.3.1. Não se aplica.

3.1.10.3.2. Não se aplica.

3.1.11. Autenticação da identidade de equipamento ou aplicação

3.1.11.1. Não se aplica.

3.1.11.1.1. Não se aplica.

3.1.11.1.3. Não se aplica.

3.1.11.2. Não se aplica.

3.1.11.2.1. Não se aplica.

3.1.11.2.2. Não se aplica.

3.1.11.3.1. Não se aplica.

3.1.11.3.2. Não se aplica.

3.1.12. Não se aplica.

3.1.12.2. Não se aplica.

3.1.12.2.1. Não se aplica.

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

Antes da expiração do certificado o solicitante pode solicitar um novo certificado devendo ser observados os mesmos requisitos e procedimentos exigidos para a solicitação inicial do certificado, na forma e no prazo estabelecidos nesta DPC.

3.3. Geração de novo par de chaves após revogação

Após a revogação do certificado de AC de nível imediatamente subsequente ao da AC Serasa ACP, a AC subordinada deve executar os processos regulares de geração de seu novo par de chaves.

3.4. Solicitação de Revogação

A solicitação de revogação de certificado deve ser feita através de formulário específico, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita com base na confrontação de dados entre a solicitação

de revogação e a solicitação de emissão.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado

4.1.1. A solicitação de emissão de um Certificado Digital Serasa é feita mediante o formulário colocado à disposição do solicitante pela Serasa AR. Toda referência a formulário deverá ser entendida também como referência a outras formas que a Serasa ACP ou Serasa AR possa vir a adotar. Os procedimentos de solicitação incluem a assinatura de um contrato que estabelece os termos e condições de uso do certificado, bem como o fornecimento de todos os dados obrigatórios que permitam a comprovação dos atributos de identificação.

4.1.2. Uma solicitação de certificado para AC de nível imediatamente subseqüente ao da Serasa ACP somente é possível após o processo de credenciamento e a autorização de funcionamento da AC em questão no âmbito da ICP-Brasil conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.3. Nesse caso, aquela AC deve encaminhar a solicitação de seu certificado à Serasa ACP por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

4.2. Emissão de Certificado

4.2.1. Somente após e na hipótese de validação conclusiva pela Serasa AR dos dados fornecidos pelo solicitante no formulário de solicitação de Certificado Digital Serasa a AC Serasa ACP procederá à emissão e assinatura do certificado. O certificado emitido é inserido na relação de certificados emitidos pela AC Serasa ACP e cópia do certificado é entregue ao representante da AC.

4.2.2. Um certificado é considerado válido a partir do momento de sua emissão.

4.3. Aceitação de Certificado

O uso do certificado pelo seu titular caracteriza sua aceitação. A aceitação implica que o responsável pelo certificado reconhece a veracidade dos dados contidos nele. (No caso do certificado ser emitido para pessoas jurídicas, equipamentos ou aplicações, a declaração deverá ser feita pela pessoa física responsável pelo certificado).

4.4. Suspensão e Revogação de Certificado

4.4.1. Circunstâncias para revogação

4.4.1.1. Este item caracteriza as circunstâncias nas quais um certificado poderá ser revogado.

4.4.1.2. Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

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

4.4.1.3. Deve-se observar ainda que:

a) a AC Serasa ACP revogará, no prazo definido no item 4.4.3 o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil;
b) o CG da ICP-Brasil determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.4.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser solicitada:

a) pelo titular do certificado;
b) pela Serasa ACP;
c) pela Serasa AR; ou
d) por determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3. Procedimento para solicitação de revogação

4.4.3.1. A solicitação de revogação de certificado deverá ser feita através de formulário específico permitindo a identificação inequívoca do solicitante. Os agentes habilitados, conforme o item 4.4.2, podem facilmente e a qualquer tempo solicitar a revogação de certificados.

4.4.3.2. Como diretrizes gerais, esta DPC estabelece que:

a) o solicitante da revogação de um certificado é identificado;
b) as solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas;
c) as justificativas para a revogação de um certificado são documentadas;
d) o processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado, e no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC.

4.4.3.3. O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC vinculada à AC Serasa ACP após o recebimento da respectiva solicitação é de 12 (doze) horas.

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

4.4.3.5 A DPC deve garantir que a AC responsável responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR;

4.4.3.6. Não se aplica.

4.4.4. Prazo para solicitação de revogação

4.4.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1.

4.4.4.2. A AC Serasa ACP estabelece como 3 (três) dias o prazo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa pela AC Serasa ACP.

4.4.5. Circunstâncias para suspensão

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

4.4.6. Quem pode solicitar suspensão

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

4.4.7. Procedimento para solicitação de suspensão

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

4.4.8. Limites no período de suspensão

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

4.4.9. Frequência de emissão de LCR

4.4.9.1. Não se aplica.

4.4.9.2. Não se aplica.

4.4.9.3. O prazo máximo admitido para a emissão de LCR referente a certificados de AC é de 45 (quarenta e cinco) dias. Na revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC Serasa ACP deverá emitir nova LCR no prazo previsto no item 4.4.3 e notificar todas as AC de nível imediatamente subsequente ao seu.

4.4.9.4. Não se aplica.

4.4.10. Requisitos para verificação de LCR

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

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

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

Não se aplica.

4.4.12. Requisitos para verificação de revogação on-line

Não se aplica.

4.4.13. Outras formas disponíveis para divulgação de revogação

Não se aplica.

4.4.14. Requisitos para verificação de outras formas de divulgação de revogação

Não se aplica.

4.4.15. Requisitos especiais para o caso de comprometimento de chave

Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deverá notificar imediatamente a AC Serasa ACP, solicitando a revogação de seu certificado, através do formulário específico para tal fim.

4.5. Procedimentos de Auditoria de Segurança

4.5.1. Tipos de evento registrados

4.5.1.1. A AC Serasa ACP registra em arquivos de auditoria os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são incluídos em arquivos de auditoria:

a) iniciação e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC Serasa ACP;
c) mudanças na configuração da AC Serasa ACP ou nas suas chaves;
d) mudanças nas políticas de criação de certificados;
e) tentativas de acesso (login) e de saída do sistema (logoff);

f) tentativas não-autorizadas de acesso aos arquivos de sistema;
g) geração de chaves próprias da AC Serasa ACP ou de chaves de AC de nível imediatamente subsequente ao seu;
h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
l) operações de escrita nesse repositório, quando aplicável.

4.5.1.2. A AC Serasa ACP registra, eletrônica ou manualmente, as seguintes informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

a) registros de acessos físicos;
b) manutenção e mudanças na configuração de seus sistemas;
c) mudanças de pessoal e de perfis qualificados;
d) relatórios de discrepância e comprometimento; e
e) registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

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

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

4.5.1.5. Todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados são registrados eletronicamente em arquivos de auditoria. Os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

a) Os agentes de registro que realizaram as operações;
b) Data e hora das operações;
c) A associação entre os agentes que realizaram a validação e aprovação e o certificado gerado;
d) A assinatura digital do executante.

4.5.1.6. A AC Serasa ACP define em documento a estar disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados, e dos termos de titularidade.

4.5.2. Frequência de auditoria de registros (logs)

Os integrantes do operacional da AC Serasa ACP coletam e analisam os registros de auditoria a cada 45 dias quando da emissão da LCR. Todo evento estranho é destacado e analisado em profundidade, gerando relatório de ação para eventual correção. Essa análise envolve também uma inspeção breve de todos os registros, com a verificação de que não foram alterados, e é seguida de 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 AC Serasa ACP mantém localmente seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena os seus registros de auditoria da maneira descrita no item 4.6.

4.5.4. Proteção de registro (log) de auditoria

4.5.4.1. O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção, através das funcionalidades nativas dos sistemas operacionais.

4.5.4.2. Os acessos lógicos são liberados através da ferramenta nativa do sistema operacional de modo a assegurar o uso apenas a usuários ou processos autorizados.

4.5.4.3. Os acessos lógicos aos registros de eventos de auditoria são registrados em logs do próprio sistema operacional.

4.5.4.4. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

4.5.4.5. Os mecanismos de proteção descritos neste item obedecem à Política de Segurança da AC Serasa ACP, de conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

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

A AC Serasa ACP gera a cada 45 dias cópia de backup de seus registros de auditoria.

4.5.6. Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é interno à AC Serasa ACP e utiliza processos automatizados e manuais.

4.5.7. Notificação de agentes causadores de eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC Serasa ACP, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8. Avaliações de vulnerabilidade

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

4.6. Arquivamento de Registros

4.6.1. Tipos de eventos registrados

Os tipos de eventos arquivados pela AC Serasa ACP, são:

a) solicitações de certificados;
b) solicitações de revogação de certificados;
c) notificações de comprometimento de chaves privadas;
d) emissões e revogações de certificados;
e) emissões de LCR;
f) trocas de chaves criptográficas da AC Serasa ACP;
g) informações de auditoria previstas no item 4.5.1.

4.6.2. Período de retenção para arquivo

Os períodos de retenção para cada evento arquivado, são:

a) as LCR e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado. Para certificados expirados ou revogados antes de 31/03/2010, o prazo de retenção se reinicia em 31/03/2010; e
c) as demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 6 (seis) anos.

4.6.3. Proteção de arquivo

Os registros arquivados da AC Serasa ACP são classificados e armazenados com requisitos de segurança compatíveis com essa classificação e com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

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

4.6.4.1. Uma segunda cópia de todo o material arquivado será armazenada no site disaster recovery, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

4.6.4.3. A AC Serasa ACP verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

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

4.6.5.1. Os servidores estão sincronizados com a Fonte Confiável de Tempo da AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário da Fonte Confiável de Tempo da AC Raiz, inclusive os certificados emitidos por esses equipamentos.

4.6.5.2. No caso dos registros feitos manualmente e formulários de requisição de certificados, estes contêm a Hora Oficial do Brasil.

4.6.6. Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Serasa ACP em seus procedimentos operacionais são automatizados e manuais e internos.

4.6.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC Serasa ACP ou à Serasa AR, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado.

4.7. Troca de chave

4.7.1. Trinta dias antes da data de expiração do certificado digital, a Serasa AR comunica ao seu titular, através do e-mail cadastrado no formulário de solicitação de certificado, a data de expiração do mesmo.

4.7.2. A AC Serasa ACP mantém os certificados expirados de seus titulares armazenados permanentemente, para efeito de consulta histórica.

4.8. Comprometimento e Recuperação de Desastre

A AC Serasa ACP possui um Plano de Continuidade de Negócio (PCN), estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e testado pelo menos

uma vez por ano, para garantir a continuidade dos seus serviços críticos. Esse Plano administra as situações de crise mediante: identificação do motivo da crise, acionamento dos principais responsáveis pelo processo de certificação digital, acionamento das equipes envolvidas na solução do incidente, ação para impedir a continuidade do problema, avaliação da extensão da crise, acionamento da situação de recuperação, ações de recuperação propriamente ditas, notificações à AC Raiz da evolução corretiva e solução, registro da crise e análise para melhoria.

4.8.1. Recursos computacionais, software e dados corrompidos

4.8.1.1. Procedimentos descritos no Plano de Continuidade do Negócio da AC Serasa ACP, que incluem a identificação da crise, acionamento dos principais gestores, acionamento das equipes, contenção da crise, avaliação da extensão da crise, declaração do início das atividades de acionamento da situação de recuperação, notificação da crise, registro da crise, análise para melhoria.

4.8.1.2. Nas situações de crise relacionadas aos recursos computacionais, software e dados corrompidos ou quando houver suspeita de corrupção dos mesmos, após a identificação da crise ou confirmação da suspeita de corrupção, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de corrupção.

4.8.1.3. Os procedimentos de recuperação dos recursos computacionais, softwares e dados corrompidos envolvem, identificação da necessidade de recurso computacional alternativo e, em caso de necessidade, disponibilização de outro recurso computacional equivalente, instalação dos softwares necessários e recuperação dos dados através do arquivo de back-up, conforme detalhado no Manual de Procedimentos de Acionamento de Situação de Recuperação dos Negócios de Certificação Digital.

4.8.2. Certificado de entidade é revogado

Em caso de revogação do certificado da AC Serasa ACP, 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 subsequente, é gerado um novo par de chaves da AC Serasa ACP, emitido certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para as AC de nível imediatamente subsequente.

4.8.3. Chave de entidade é comprometida

Em caso de comprometimento da chave da AC Serasa ACP, 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 AC Serasa ACP e das AC de nível imediatamente subsequente, é gerado um novo par

de chaves, emitido certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para as AC de nível imediatamente subsequente.

4.8.4. Segurança dos recursos após desastre natural ou de outra natureza

Em caso de desastre natural ou de outra natureza, após a identificação da crise são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de exposição e comprometimento do ambiente. Na confirmação do desastre e constatado impossibilidade de operação no site, as atividades são transferidas para o site de recuperação de desastre.

4.8.5. Atividades das Autoridades de Registro

Procedimentos descritos no Plano de Continuidade do Negócio da Serasa da Serasa AR contemplam a recuperação, total ou parcial das atividades das AR, contendo, no mínimo as seguintes informações:

a) identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios;
b) identificação e concordância de todas as responsabilidades e procedimentos de emergência;
c) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial deve ser dada à avaliação da recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;
d) documentação dos processos e procedimentos acordados;
e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;
f) teste e atualização dos planos.

4.9. Extinção dos serviços de AC, AR ou PSS

Em caso de extinção da AC Serasa ACP, AR Serasa ou PSS serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], que incluem a divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, transferência da guarda de bases de dados e registros de arquivo.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os controles descritos a seguir são implementados pela AC Serasa ACP e pela Serasa AR para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1. Controles Físicos

Nos itens seguintes estão descritos os controles físicos referentes às instalações que abrigam os sistemas da AC Serasa ACP.

5.1.1. Construção e localização das instalações de AC

5.1.1.1. A localização e o sistema de certificação da AC Serasa ACP não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não são admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Na construção das instalações da AC Serasa ACP foram considerados, entre outros, os seguintes aspectos relevantes para os controles de segurança física:

a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, nobreaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;
b) Instalações para sistemas de telecomunicações;
c) Sistemas de aterramento e de proteção contra descargas atmosféricas;
d) Iluminação de emergência.

5.1.2. Acesso físico nas instalações de AC

A AC Serasa ACP implantou um sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a Política de Segurança da AC Serasa ACP e os requisitos que seguem.

5.1.2.1. Níveis de acesso

5.1.2.1. A AC Serasa ACP definiu 4 (quatro) níveis de acesso físico aos diversos ambientes, e 2 (dois) níveis relativos à proteção da chave privada da AC Serasa ACP.

5.1.2.1.2. O primeiro nível - ou nível 1 - situa-se após a primeira barreira de acesso às instalações da AC Serasa ACP. Para entrar em uma área de nível 1, cada indivíduo deve ser identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação da AC Serasa ACP devem transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC Serasa ACP ou da Serasa AR é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC Serasa ACP, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

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

5.1.2.1.5. O terceiro nível - ou nível 3 - situa-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC Serasa ACP. As atividades relativas ao ciclo de vida dos certificados digitais estão localizadas a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não podem permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

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

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

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC Serasa ACP 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 no mínimo de duas pessoas autorizadas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9. No quarto nível todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. No quarto nível, 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 possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10. A salas-cofre foi construída segundo as normas brasileiras aplicáveis.

5.1.2.1.11. Na AC Serasa ACP há 1 (um) ambiente de quarto nível para abrigar e segregar, respectivamente:

a) Equipamentos de produção on-line;
b) Equipamentos de produção off-line e cofre de armazenamento.

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um gabinete reforçado trancado. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos estão armazenados em ambiente de nível 5 ou superior.

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

a) É feito em aço ou material de resistência equivalente;
b) Possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de duas fechaduras, sendo uma comum a todos os depósitos e uma individual. Os dados de ativação da chave privada da AC Serasa ACP são armazenados nesses depósitos.

5.1.2.2. Sistemas físicos de detecção

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

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 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.

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

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

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

5.1.2.2.6. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes 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 câmeras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

5.1.2.3. Sistema de controle de acesso

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

5.1.2.4. Mecanismos de emergência

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

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

5.1.3. Energia e ar condicionado nas instalações de AC

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

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

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

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

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

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

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

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

5.1.3.9. O sistema de ar condicionado é interno, com troca de ar realizada apenas por abertura de porta.

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

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

5.1.4. Exposição à água nas instalações de AC

O ambiente de nível 4 encontra-se fisicamente protegido contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5. Prevenção e proteção contra incêndio nas instalações de AC

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

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

5.1.5.3. O ambiente de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso ao ambiente de nível 4 constituem eclusas, onde uma porta só se abre quando a anterior estiver fechada.

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

5.1.6. Armazenamento de mídia nas instalações de AC

São observados os critérios estabelecidos na norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7. Destruição de lixo nas instalações de AC

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

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

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

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

5.1.9. Instalações técnicas de AR

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

5.2. Controles Procedimentais
5.2.1. Perfis qualificados

5.2.1.1. A AC Serasa ACP efetua separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize o seu sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.2.1.2. A AC Serasa ACP estabelece perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

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

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

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. A AC Serasa ACP utiliza o requisito de controle multiusuário para a geração e a utilização da sua chave privada, na forma definida no item 6.2.2.

5.2.3. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Serasa ACP requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC Serasa ACP podem ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC Serasa ACP tem sua identidade e perfil verificados antes de:

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

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

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

5.2.3.3. A AC Serasa ACP implementa um padrão de utilização de "senhas fortes", definido na correspondente Política de Segurança e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Todos os empregados da AC Serasa ACP, da Serasa AR e dos PSS encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:
a) os termos e as condições do perfil que ocuparão;
b) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
c) o compromisso de não divulgar informações sigilosas a que tenham acesso.

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

Todo o pessoal da AC Serasa ACP e da Serasa AR 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 ICP-BRASIL[8] e na Política de Segurança da AC Serasa ACP.

5.3.2. Procedimentos de verificação de antecedentes

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

a) verificação de antecedentes criminais;

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

5.3.3. Requisitos de treinamento

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

a) princípios e mecanismos de segurança da AC Serasa ACP e da Serasa AR;
b) sistema de certificação em uso na AC Serasa ACP;
c) procedimentos de recuperação de desastres e de continuidade do negócio;
d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9 e 3.1.10; e
e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC Serasa ACP e da Serasa AR envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC Serasa ACP e da Serasa AR.

5.3.5. Frequência e sequência de rodízio de cargos

A AC Serasa ACP e a Serasa AR possuem pessoal e efetivo de contingência devidamente treinado, não fazendo uso de rodízio de pessoal.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC Serasa ACP e da Serasa AR, a AC Serasa ACP suspenderá, de imediato, o acesso dessa pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima contém os seguintes itens:

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

5.3.6.3. Concluído o processo administrativo, a AC Serasa ACP encaminha suas conclusões à AC Raiz.

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

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

5.3.7. Requisitos para contratação de pessoal

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

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC Serasa ACP torna disponível para todo o seu pessoal:

a) Sua DPC-Serasa ACP;
b) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e a sua Política de Segurança da AC Serasa ACP;
c) Documentação operacional relativa a suas atividades;
d) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação fornecida ao pessoal é classificada segundo a política de classificação de informação definida pela AC Serasa ACP e é mantida atualizada.

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficos da AC Serasa ACP é gerado pela própria AC Serasa ACP, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil ou do pedido de Revalidação dos dados cadastrais e solicitação de novo certificado da Autoridade Certificadora – AC no âmbito da infraestrutura de chaves públicas brasileira.

6.1.1.2. Pares de chaves são gerados somente pelo titular do certificado correspondente.
O par de chaves da AC Serasa ACP é gerado em módulo criptográfico homologado conforme o padrão ICP-Brasil NSH-2, utilizando algoritmo RSA para geração do par de chaves.

6.1.1.3. Não se aplica.

6.1.2. Entrega da chave privada à entidade titular

A geração e a guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3. Entrega da chave pública para emissor de certificado

Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, a AC Serasa ACP fará uso do padrão PKCS#10.

6.1.4. Disponibilização de chave pública da AC Serasa ACP para usuários

As formas para a disponibilização do certificado da Serasa ACP, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

a) formato PKCS#7, formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
b) diretório;
c) página Web da Serasa ACP (http://www.certificadodigital.com.br/repositorio);

d) outros meios seguros a serem aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Para certificados emitidos sob a cadeia Autoridade Certificadora Raiz Brasileira V2 e V5 o tamanho das chaves criptográficas associadas a certificados de AC será de 4096 (quatro mil e noventa e seis) bits, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.5.2. Para certificados emitidos sob a cadeia da AC Serasa ACP o tamanho das chaves criptográficas associadas a certificados de AC será de 4096 (quatro mil e noventa e seis) bits, com base nos requisitos aplicáveis estabelecidos pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.6. Geração de parâmetros de chaves assimétricas

A AC Serasa ACP adota o padrão ICP-Brasil NSH-2 para a geração de suas chaves assimétricas, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7. Verificação da qualidade dos parâmetros

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

6.1.8. Geração de chave por hardware ou software

O processo de geração do par de chaves da AC Serasa ACP é feito por hardware padrão ICP-Brasil NSH-2, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

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

6.2. Proteção da Chave Privada

As chaves privadas da AC Serasa ACP trafegam cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento.

6.2.1. Padrões para módulo criptográfico

O módulo criptográfico de geração de chaves assimétricas da AC Serasa ACP adota o padrão ICP-Brasil NSH-2, padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.2. Controle "n de m" para chave privada

A AC Serasa ACP estabelece como exigência de controle múltiplo para a utilização das suas chaves privadas:

a) Número mínimo de 2 ("n") (duas) pessoas de um grupo de 5 ("m")(cinco) pessoas para utilização das suas chaves privadas criadas em 18/04/2002;
b) Número mínimo de 2 (“n”) (duas) pessoas de um grupo de 20 (“m”) (vinte) pessoas para utilização das suas chaves privadas criadas a partir de 22/04/2004;
c) Número mínimo de 2 (“n”) (duas) pessoas de um grupo de 5 (“m”) (vinte) pessoas para utilização das suas chaves privadas criadas a partir da cadeia V5.

6.2.3. Recuperação (escrow) de chave privada

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

6.2.4. Cópia de segurança (backup) de chave privada

6.2.4.1. A AC Serasa ACP mantém cópias de segurança de suas próprias chaves privadas.

Estas cópias são armazenadas cifradas e protegidas com um nível de segurança não inferior àquele definido para a versão original da chave, e mantida pelo prazo de validade do certificado correspondente.

6.2.4.2. A AC Serasa ACP não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subsequente ao seu.

6.2.4.3. A AC não poderá manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido. Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido.

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

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas de sigilo são arquivadas com um nível de segurança não inferior àquele definido para a chave original. Não são arquivadas chaves privadas de assinatura digital.

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

6.2.6. Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7. Método de ativação de chave privada

Para a ativação das chaves privadas exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

6.2.8. Método de desativação de chave privada

Para a desativação das chaves privadas exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

6.2.9. Método de destruição de chave privada

Para a destruição das chaves privadas exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. As mídias de armazenamento das chaves privadas são 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 AC Serasa ACP e dos titulares de certificados de assinatura digital por ela emitidos permanecem armazenadas permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas da AC Serasa ACP e dos titulares de certificados de assinatura digital por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. Não se aplica.

6.3.2.4. O período máximo de validade admitido para certificados da AC SERASA ACP cadeia V2 e de certificados de AC subordinadas a ela é de 10 (dez) anos. A validade admitida para certificados da AC Serasa ACP cadeia V5 é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de ativação

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

6.4.2. Proteção dos dados de ativação

Os dados de ativação da chave privada da AC Serasa ACP são protegidos contra uso não autorizado, por meio de mecanismos de criptografia e de controle de acesso físico.

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos Técnicos Específicos de Segurança Computacional

6.5.1.1. A geração do par de chaves da AC Serasa ACP é realizada off-line, para impedir o acesso remoto não autorizado.

6.5.1.2. Não se aplica.

6.5.1.3. Cada computador servidor da AC Serasa ACP, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes características:

a) controle de acesso aos serviços e perfis da AC Serasa ACP;
b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC Serasa ACP;
c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
d) geração e armazenamento de registros de auditoria da AC Serasa ACP;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) mecanismos para cópias de segurança (backup).

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

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

6.5.1.6. Qualquer equipamento incorporado à AC Serasa ACP é preparado e configurado como previsto na Política de Segurança implementada, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A segurança computacional da AC Serasa ACP segue as recomendações do Trusted System Evaluation Criteria (TCSEC).

6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.

6.5.3.2. Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC Serasa ACP adota tecnologias de certificação digital e efetua as devidas customizações para adequar as necessidades do ambiente da AC, os quais são desenvolvidos por Analistas de Suporte, todos empregados de confiança. Estas customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluído é colocado em um ambiente de homologação. Finalizado o processo de homologação é encaminhado um pedido para a "Gerência de Mudança" que é coordenada pelo Gestor do Processo de Certificação Digital e é composto de outras áreas da Serasa, como por exemplo Segurança de Sistemas de Informação, Produção, etc., que avaliam e decidem quanto a sua implementação.

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

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC Serasa ACP utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação da AC Serasa ACP.

6.6.2.2. A AC Serasa ACP verifica os níveis configurados de segurança através de ferramentas do próprio sistema operacional.

6.6.2.3. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

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

6.7. Controles de Segurança de Rede

Não se aplica.

6.8. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico de geração de chaves assimétricas da AC Serasa ACP adota o padrão ICP-Brasil NSH-2.

7. PERFIS DE CERTIFICADO E LCR

7.1. Diretrizes Gerais

Nos seguintes itens desta DPC são descritos os aspectos dos certificados e LCR emitidos pela AC Serasa ACP.

7.2. Perfil do Certificado

Todos os certificados emitidos pela AC Serasa ACP estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.2.1. Número(s) de versão

Todos os certificados emitidos pela AC Serasa ACP implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de certificado

7.2.2.1. Os certificados emitidos pela AC Serasa ACP obedecem a ICP - Brasil, que define como obrigatórias as seguintes extensões:

7.2.2.2. Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V5:

a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Serasa ACP;
b) "Subject Key Identifier", não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado;
c) "Key Usage", crítica: somente os bits keyCertSign e CRLSign são ativados;
d) "Certificate Policies", não crítica: o campo policyQualifiers contém o endereço Web da DPC da AC Serasa ACP (http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-acp.pdf)

e) "Basic Constraints", crítica: contém o campo cA=True. O campo pathLenConstraint não é utilizado;
f) "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente ao certificado http://www.certificadodigital.com.br/repositorio/lcr/serasaacpv5.crl http://lcr.certificados.com.br/repositorio/lcr/serasaacpv5.crl

7.2.2.3. Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V2:

a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Serasa ACP;
b) "Subject Key Identifier", não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado;
c) "Key Usage", crítica: somente os bits keyCertSign e CRLSign são ativados;
d) "Certificate Policies", não crítica: o campo policyQualifiers contém o endereço Web da DPC da AC Serasa ACP (http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-acp.pdf);

e) "Basic Constraints", crítica: contém o campo cA=True. O campo pathLenConstraint não é utilizado;
f) "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente ao certificado http://www.certificadodigital.com.br/repositorio/lcr/serasaacpv2.crl http://lcr.certificados.com.br/repositorio/lcr/serasaacpv2.crl http://repositorio.icpbrasil.gov.br/lcr/Serasa/repositorio/lcr/serasaacpv2.crl

7.2.2.4. Para os certificados emitidos sob as cadeias V0 e V1 da Autoridade Certificadora Raiz Brasileira:

a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Serasa ACP;
b) "Subject Key Identifier", não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado;
c) "Key Usage", crítica: somente os bits keyCertSign e CRLSign são ativados;
d) "Certificate Policies", não crítica: o campo policyQualifiers contém o endereço Web da DPC da AC Serasa ACP (http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-acp.pdf);
e) "Basic Constraints", crítica: contém o campo cA=True. O campo pathLenConstraint não é utilizado;
f) "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente ao certificado:

i. http://www.certificadodigital.com.br/repositorio/crl/SerasaACP.crl para certificados emitidos até 22/04/2004;
ii. http://www.certificadodigital.com.br/repositorio/lcr/SerasaACP.crl para certificados emitidos de 23/04/2004 a 03/08/2006;

iii. http://www.certificadodigital.com.br/repositorio/lcr/serasaacp2006.crl para certificados emitidos de 04/08/2006 a 30/07/2008;
iv. http://www.certificadodigital.com.br/repositorio/lcr/serasaacpv1.crl, http://lcr.certificados.com.br/repositorio/lcr/Serasaacpv1.crl, http://repositorio.icpbrasil.gov.br/lcr/Serasa/repositorio/lcr/serasaacpv1.crl para certificados emitidos a partir de 31/07/2008.

7.2.3. Identificadores de algoritmo

Os certificados emitidos pela AC Serasa ACP são assinados com o uso do algoritmo RSA com SHA-1 como função de hash (OID = 1.2.840.113549.1.1.5) nas hierarquias V0 e V1, e algoritmo RSA com SHA-512 como função de hash (OID = 1.2.840.113549.1.1.13) nas hierarquias V2 e V5, conforme o padrão PKCS#1.

7.2.4. Formatos de nome

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

a) Para Certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V5:
C = BR
O = ICP-Brasil
CN = nome da AC v5

b)Para Certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V2:
C = BR
O = ICP-Brasil
CN = nome da AC v2

c) Para os certificados emitidos sob as cadeias V0 e V1 da Autoridade Certificadora Raiz Brasileira:

c1) para certificados emitidos até 30/07/2008:
C = BR
O = ICP-Brasil
CN = nome da AC

c2) para certificados emitidos a partir de 31/07/2008:
C = BR
O = ICP-Brasil
CN = nome da AC v1

7.2.5. Restrições de nome

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

a) os acentos não devem ser utilizados e devem ser substituídos pelo caractere não acentuado;
b) o cedilha deve ser substituído pelo caractere ‘c’;
c) 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

7.2.6. OID (Object Identifier) de DPC

O OID desta DPC-Serasa ACP é 2.16.76.1.1.3.

7.2.7. Uso da extensão "Policy Constraints"

Não se aplica.

7.2.8. Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço Web da DPC-Serasa ACP https://serasa.certificadodigital.com.br/ajuda/repositorio/

7.2.9. Semântica de processamento para extensões críticas

Não se aplica.

7.3. Perfil de LCR

7.3.1. Número(s) de versão

As LCR geradas pela AC Serasa ACP implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.3.2. Extensões de LCR e de suas entradas

As LCR da AC Serasa ACP obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões para certificados de AC:

a) "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC Serasa ACP que assina a LCR.
b) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC Serasa ACP.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

Qualquer alteração nesta DPC- Serasa ACP será submetida à aprovação do CG da ICP-Brasil.

8.2. Políticas de publicação e notificação

Esta DPC-Serasa ACP está disponível para a comunidade no endereço web https://serasa.certificadodigital.com.br/ajuda/repositorio/.

8.3. Procedimentos de aprovação

Esta DPC-Serasa ACP foi submetida à aprovação do CG da ICP-Brasil, durante o processo de credenciamento da AC Serasa ACP, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

9. DOCUMENTOS REFERENCIADOS

9.1. Resoluções do Comitê-Gestor da ICP-Brasil

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

Ref	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[11]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05

9.2. Instruções Normativas da AC Raiz

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

Ref	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

10. LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
AR - Autoridades de Registro
CEI - Cadastro Específico do INSS
CG - Comitê Gestor

CMM-SEI - Capability Maturity Model do Software Engineering Institute
CMVP - Cryptographic Module Validation Program
CN - Common Name
CNE - Carteira Nacional de Estrangeiro
CNPJ - Cadastro Nacional de Pessoas Jurídicas -
COBIT - Control Objectives for Information and related Technology
COSO - Comitee of Sponsoring Organizations
CPF - Cadastro de Pessoas Físicas
DMZ - Zona Desmilitarizada
DN - Distinguished Name
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira
IDS - Sistemas de Detecção de Intrusão
IEC - International Electrotechnical Commission
ISO – International Organization for Standardization
ITSEC - European Information Technology Security Evaluation Criteria
ITU - International Telecommunications Union
LCR - Lista de Certificados Revogados
NBR - Norma Brasileira
NIS - Número de Identificação Social
NIST - National Institute of Standards and Technology
OCSP - On-line Certificate Status Protocol
OID - Object Identifier
OU - Organization Unit
PASEP - Programa de Formação do Patrimônio do Servidor Público
PC - Políticas de Certificado
PCN - Plano de Continuidade de Negócio
PIS - P rograma de Integração Social
POP - Proof of Possession
PS - Política de Segurança
PSS - Prestadores de Serviço de Suporte
RFC – Request For Comments
RG - Registro Geral
SNMP - Simple Network Management Protocol
TCSEC - Trusted System Evaluation Criteria
TSDM - Trusted Software Development Methodology
UF - Unidade de Federação
URL - Uniform Resource Location