Autor: Serasa S.A.
Edição: Fevereiro 2018
Versão: 1.1

1. INTRODUÇÃO

1.1 Visão Geral

1.1.1 O documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras - AC integrantes da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PC.

1.1.2 Esta Política de Certificado de Assinatura Digital Servidor tipo A4 da Serasa Certificadora Digital (a seguir designada simplesmente por "PC SERASA CD SSL V5 A4") adota a mesma estrutura empregada naquele documento.

1.1.3. O tipo de certificado emitido sob esta PC é o Tipo A4 Servidor.

1.1.4. Não se aplica.

1.1.5. Esta PC refere-se exclusivamente a Certificados de Servidor Tipo A4 emitidos pela Serasa Certificadora Digital (a seguir designada simplesmente por "SERASA CD SSL V5").

1.1.6. Não se aplica.

1.1.7. Não se aplica.

1.1.8. Não se aplica.

1.2 Identificação

1.2.1. A PC SERASA CD SSL V5 A4 descreve os procedimentos e práticas da SERASA CD SSL V5 e os usos relacionados ao Certificado de Assinatura Digital Servidor tipo A4.

1.2.2. O OID (Object Identifier) da PC SERASA CD SSL V5 A4 é 2.16.76.1.2.4.31.

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridade Certificadora (AC)

1.3.1.1. Dados da Autoridade Certificadora

Esta PC se refere à SERASA CD SSL V5 (Serasa S.A., com sede na Alameda dos Quinimuras, 187, São Paulo, SP, CEP: 04068-900, CNPJ nº 62.173.620/0001-80).

1.3.2.1. As práticas e procedimentos de certificação da SERASA CD SSL V5 estão descritos na Declaração de Práticas de Certificação da SERASA CD SSL V5 (a seguir designada simplesmente por "DPC-SERASA CD SSL V5"). A SERASA CD SSL V5 mantém as informações acima sempre atualizadas.

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, são de competência das Autoridades de Registro vinculadas à AC SERASA-CD (AR Vinculadas) relacionadas na página https://serasa.certificadodigital.com.br/ajuda/repositorio/. Essa página contém:

a) Relação de todas as AR credenciadas, com informações sobre as PC 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 respectivas datas de encerramento das atividades;
f) Acordos operacionais celebrados pelas AR vinculada com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A SERASA CD SSL V5 mantém 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 SERASA CD SSL V5 estão relacionados na página https://serasa.certificadodigital.com.br/ajuda/repositorio/

1.3.3.2 PSS são entidades utilizados pela SERASA CD SSL V5 ou pelas ARs vinculadas 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 SERASA CD SSL V5 mantém as informações acima sempre atualizadas.

1.3.4 Titulares de Certificado

Os Titulares de Certificado de Assinatura Digital Servidor tipo A4 da SERASA CD SSL V5 podem ser pessoas físicas ou jurídicas, observados os itens 1.3.4, 3.1.9, 3.1.10 e 3.1.11 da DPC-SERASA CD SSL V5.

1.3.5 Aplicabilidade

1.3.5.1. Os certificados definidos por esta PC têm sua utilização vinculada a aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.2. As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.3.5.3. Na definição das aplicações para o certificado definido pela PC, a SERASA CD SSL V5 leva em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados - LCR e extensão do período de validade do certificado.

1.3.5.4. Os certificados emitidos pela AC SERASA CD SSL V5 podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.5. Os certificados emitidos sob esta PC são apropriados ao uso, por exemplo, nas aplicações apresentadas abaixo:

- Assinatura digital em correio eletrônico;
- Acesso a aplicações disponibilizadas pela Receita Federal do Brasil, ou por qualquer outro órgão da Administração Pública Direta ou Indireta, que aceitem este certificado;
- Software de assinatura elaborado em parceria com outros órgãos, entidades ou empresas;
- Confirmação de identidade na Web;
- Transações eletrônicas e transações on-line;
- Redes privadas virtuais (VPN);
- Cifração de chaves de sessão.

1.3.5.6. Não se aplica.

1.3.5.7. Não se aplica.

1.4 Dados de Contato

Dúvidas decorrentes da leitura desta PC 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: Luana Capelletti
Área: Governança e Compliance e-ID
E-mail: arcompliance@br.experian.com

2. DISPOSIÇÕES GERAIS

Os itens seguintes estão referidos nos correspondentes itens DPC-SERASA CD SSL V5.

2.1. Obrigações e direitos

2.1.1. Obrigações da AC
2.1.2. Obrigações das AR
2.1.3. Obrigações do Titular do Certificado
2.1.4. Direitos da terceira parte (*Relying Party*)
2.1.5. Obrigações do Repositório

2.2. Responsabilidades

2.2.1. Responsabilidades da AC
2.2.2. Responsabilidades das AR vinculadas

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (Relying Party)
2.3.2. Relações Fiduciárias
2.3.3. Processos Administrativos

2.4. Interpretação e Execução

2.4.1. Legislação
2.4.2. Forma de interpretação e notificação
2.4.3. Procedimentos de solução de disputa

2.5. Tarifas de Serviço

2.5.1. Tarifas de emissão e renovação de certificados
2.5.2. Tarifas de acesso a certificados
2.5.3. Tarifas de revogação ou de acesso à informação de status
2.5.4. Tarifas para outros serviços

2.5.5. Política de reembolso

2.6. Publicação e Repositório

2.6.1. Publicação de informação da AC
2.6.2. Frequência de publicação
2.6.3. Controles de acesso
2.6.4. Repositórios

2.7. Fiscalização e Auditoria de Conformidade

2.8. Sigilo

2.8.1. Tipos de informações sigilosas
2.8.2. Tipos de informações não sigilosas
2.8.3. Divulgação de informação de revogação e de suspensão de certificado
2.8.4. Quebra de sigilo por motivos legais
2.8.5. Informações a terceiros
2.8.6. Divulgação por solicitação do titular
2.8.7. Outras circunstâncias de divulgação de informação

2.9. Direitos de Propriedade Intelectual

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão referidos nos correspondentes itens da DPC-SERASA CD SSL V5.

3.1. Registro Inicial

3.1.1. Disposições Gerais
3.1.2. Tipos de nomes
3.1.3. Necessidade de nomes significativos
3.1.4. Regras para interpretação de vários tipos de nomes
3.1.5. Unicidade de nomes
3.1.6. Procedimento para resolver disputa de nomes
3.1.7. Reconhecimento, autenticação e papel de marcas registradas
3.1.8. Método para comprovar a posse de chave privada
3.1.9. Autenticação da identidade de um indivíduo
3.1.9.1. Documentos para efeitos de identificação de um indivíduo
3.1.9.2. Informações contidas no certificado emitido para um indivíduo
3.1.10. Autenticação da identidade de uma organização
3.1.10.1. Disposições Gerais
3.1.10.2. Documentos para efeitos de identificação de uma organização
3.1.10.3. Informações contidas no certificado emitido para uma organização
3.1.11. Autenticação da identidade de equipamento
3.1.11.1. Disposições Gerais
3.1.11.2. Procedimentos para efeitos de identificação de um equipamento

3.1.11.3 - Informações contidas no certificado emitido para um equipamento

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

3.3. Geração de novo par de chaves após expiração ou revogação

3.4. Solicitação de Revogação

4. REQUISITOS OPERACIONAIS

Os itens seguintes estão referidos nos correspondentes itens da DPC-SERASA CD SSL V5

4.1. Solicitação de Certificado

4.2. Emissão de Certificado

4.3. Aceitação de Certificado

4.4. Suspensão e Revogação de Certificado

4.4.1. Circunstâncias para revogação
4.4.2. Quem pode solicitar revogação
4.4.3. Procedimento para solicitação de revogação
4.4.4. Prazo para solicitação de revogação
4.4.5. Circunstâncias para suspensão
4.4.6. Quem pode solicitar suspensão
4.4.7. Procedimento para solicitação de suspensão
4.4.8. Limites no período de suspensão
4.4.9. Frequência de emissão de LCR
4.4.10. Requisitos para verificação de LCR
4.4.11. Disponibilidade para revogação ou verificação de status on-line
4.4.12. Requisitos para verificação de revogação on-line
4.4.13. Outras formas disponíveis para divulgação de revogação
4.4.14. Requisitos para verificação de outras formas de divulgação de revogação
4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.5. Procedimentos de Auditoria de Segurança

4.5.1. Tipos de eventos registrados
4.5.2. Frequência de auditoria de registros (*logs*)
4.5.3. Período de retenção para registros (*logs*) de auditoria
4.5.4. Proteção de registro (*log*) de auditoria
4.5.5. Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria

4.5.6. Sistema de coleta de dados de auditoria
4.5.7. Notificação de agentes causadores de eventos

4.5.8. Avaliações de vulnerabilidade

4.6. Arquivamento de Registros

4.6.1. Tipos de registros arquivados
4.6.2. Período de retenção para arquivo
4.6.3. Proteção de arquivo
4.6.4. Procedimentos para cópia de segurança (*backup*) de arquivo
4.6.5. Requisitos para datação (*time-stamping*) de registros
4.6.6. Sistema de coleta de dados de arquivo
4.6.7. Procedimentos para obter e verificar informação de arquivo

4.7. Troca de chave

4.8. Comprometimento e Recuperação de Desastre

4.8.1. Recursos computacionais, software ou dados são corrompidos
4.8.2. Certificado de entidade é revogado
4.8.3. Chave de entidade é comprometida
4.8.4. Segurança dos recursos após desastre natural ou de outra natureza
4.8.5. Atividades das Autoridades de Registro

4.9. Extinção dos serviços de AC, AR ou PSS

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os itens seguintes estão referidos nos correspondentes itens da DPC-SERASA CD SSL V5.

5.1. Controles Físicos

5.1.1. Construção e localização das instalações
5.1.2. Acesso físico
5.1.3. Energia e ar condicionado
5.1.4. Exposição à água
5.1.5. Prevenção e proteção contra incêndio
5.1.6. Armazenamento de mídia
5.1.7. Destruição de lixo
5.1.8. Instalações de segurança (backup) externas (off-site)

5.2. Controles Procedimentais

5.2.1. Perfis qualificados
5.2.2. Número de pessoas necessário por tarefa
5.2.3. Identificação e autenticação para cada perfil

5.3. Controles de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade
5.3.2. Procedimentos de verificação de antecedentes
5.3.3. Requisitos de treinamento
5.3.4. Frequência e requisitos para reciclagem técnica
5.3.5. Frequência e sequência de rodízio de cargos
5.3.6. Sanções para ações não autorizadas
5.3.7. Requisitos para contratação de pessoal
5.3.8. Documentação fornecida ao pessoal

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC. São também definidos outros controles técnicos de segurança utilizados pela AC e pela AR vinculada na execução de suas funções operacionais.

6.1. Geração e Instalação do Par de Chaves

Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, publicando nova versão do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

6.1.1. Geração do par de chaves

6.1.1.1. Quando o titular de certificado é uma pessoa física, esta é a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado é uma pessoa jurídica, esta indica por seu(s) representante(s) legal(s), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1. Não se aplica.

6.1.1.2. O processo de geração de chaves do tipo A, contemplada nesta PC, exige:

a) a instalação de hardware e software relacionados à mídia armazenadora do certificado selecionada pelo cliente;
b) o par de chaves será gerado em repositório protegido por senha e/ou identificação biométrica e cifrado por software;
c) o responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado deve executar pessoalmente a geração dos pares de chaves criptográficas.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

6.1.1.4. Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3],

em repositório protegido por senha e/ou identificação biométrica, cifrado por software.

6.1.1.5. A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

6.1.1.6. A mídia de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada é única e seu sigilo é suficientemente assegurado;
b) a chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
c) a chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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

Mídias Armazenadoras de Chaves Criptográficas

Tipo de Certificado	***Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)***
A4	Hardware criptográfico homologado junto à ICP-Brasil

6.1.1.8. A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do titular do certificado, conforme especificado no Termo de Titularidade, no caso de certificados de pessoa física. No caso de certificados de pessoa jurídica, equipamentos e aplicações, é da pessoa responsável indicada por seus(s) representante(s) legal(s), conforme especificado no Termo de Responsabilidade.

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável.

6.1.3. Entrega da chave pública para emissor de certificado

A entidade titular do certificado, através de seu software de acionamento, disponibiliza para a entrega de sua chave pública à AC SERASA CD SSL V5, à solicitante ou a correspondente AR vinculada, a chave pública em formato PKCS#10, através de uma sessão segura SSL - Secure Socket Layer.

6.1.4. Disponibilização de chave pública da SERASA CD SSL V5 para usuários

As formas para a disponibilização do certificado da SERASA CD SSL V5, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

a) No momento da disponibilização de um certificado para seu titular, usando formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [1];

b) Diretório;

c) Página Web da SERASA CD SSL V5 (https://serasa.certificadodigital.com.br/ajuda/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 da Autoridade Certificadora Raiz Brasileira V2 e V5 o tamanho mínimo admitido para chaves criptográficas de titular final é de 4096 bits. Para certificados emitidos sob as demais cadeias da Autoridade Certificadora Raiz Brasileira o tamanho mínimo admitido para chaves criptográficas de titular final é de 2048 bits.

6.1.5.2. Os algoritmos e o tamanhos de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3].

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas das entidades titulares de certificados adotarão o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros serão verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.8. Geração de chave por hardware ou software

O processo de geração do par de chaves das entidades titulares de certificados é feito em software.

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

Os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

6.2. Proteção da Chave Privada

A mídia de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:
a) A chave privada é única e seu sigilo é suficientemente assegurado;
b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.2.1. Padrões para módulo criptográfico

Não se aplica.

6.2.2. Controle "n de m" para chave privada

Não se aplica.

6.2.3. Custódia (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a custódia (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. Como diretriz geral, qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. A SERASA CD SSL V5 não pode manter cópia de segurança de chave privada de titular de certificado por ela emitido, segundo esta PC.

6.2.4.3. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3], como 3-DES, IDEA, SAFER+ e protegida com um nível de segurança não inferior àquele definido para a chave principal.

6.2.4.4. Através das tecnologias atualmente disponíveis, a entidade titular de certificado deve realizar a geração de cópia de segurança da chave privada.

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas das entidades titulares de certificados emitidos por esta PC não são arquivadas.

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

6.2.6. Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7. Método de ativação de chave privada

Cada entidade titular de certificado deve definir procedimentos necessários para a ativação da sua chave privada.

6.2.8. Método de desativação de chave privada

Cada entidade titular de certificado deve definir procedimentos necessários para a desativação da sua chave privada.

6.2.9. Método de destruição de chave privada

Cada entidade titular de certificado deve definir procedimentos necessários para a destruição da sua chave privada.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da SERASA CD SSL V5, dos titulares de certificados de assinatura digital e as LCR por ela emitidas permanecem armazenadas após a expiração dos certificados correspondentes permanentemente para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas dos respectivos titulares 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. O período máximo de uso das chaves privadas correspondentes aos certificados emitidos pela AC SERASA CD SSL V5 segundo esta PC é de 6 (seis) anos.

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de ativação

Os certificados de tipo A4 Servidor se utilizam, para geração e armazenamento do par de chaves e certificado, de repositório protegido por senha e/ou identificação biométrica, cifrado por software. No caso de ativação por senha, recomenda-se que as mesmas sejam criadas de forma aleatória, respeitando-se procedimentos básicos de segurança, tais como:

a) Nunca fornecer senha a terceiros;
b) Escolher senhas de 8 ou mais caracteres;
c) Definir senhas com caracteres numéricos e alfanuméricos;
d) Memorizar a senha e
e) Não escrevê-la.

6.4.2. Proteção dos dados de ativação

Para a proteção dos dados de ativação da chave privada da entidade titular do certificado, no caso de ativação por senha, recomenda-se:

a) Nunca fornecer senha a terceiros;
b) Escolher senhas de 8 ou mais caracteres;
c) Definir senhas com caracteres numéricos e alfanuméricos;

d) Memorizar a senha e não escrevê-la.

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

Nos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela SERASA CD SSL V5, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, tais como:

a) Senha de bios ativada;
b) Controle de acesso lógico ao sistema operacional;
c) Exigência de uso de senhas fortes;
d) Diretivas de senha e de bloqueio de conta;
e) Antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;
f) Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
h) Proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2. Classificação da segurança computacional

Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

Os itens abaixo não se aplicam a esta PC.

6.6.1. Controles de desenvolvimento de sistema

6.6.2. Controles de gerenciamento de segurança

6.6.3. Classificações de segurança de ciclo de vida

6.7. Controles de Segurança de Rede

Não se aplica.

6.8. Controles de Engenharia do Módulo Criptográfico

Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado devem obedecer aos padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3].

7. PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das LCR gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1. Perfil do Certificado

Os certificados emitidos pela SERASA CD SSL V5 estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1. Número(s) de versão

Os certificados emitidos pela SERASA CD SSL V5 implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2. Extensões de certificado

7.1.2.1. Neste item, a PC descreve todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2. Extensões Obrigatórias

Os certificados emitidos pela SERASA CD SSL V5 obedecem a ICP - Brasil, que define como obrigatórias as seguintes extensões:

a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da SERASA CD SSL V5;

b) "Key Usage", crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;

c) "Certificate Policies", não crítica: contém o OID desta PC e o endereço Web da DPC-SERASA CD SSL V5 http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-servidor-cd.pdf;

d) "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente.

d.1) Para certificados da cadeia V5: http://www.certificadodigital.com.br/repositorio/lcr/serasacdv5.crl e http://lcr.certificados.com.br/repositorio/lcr/serasacdv5.crl,

d.2) Para certificados da cadeia V2
http://www.certificadodigital.com.br/repositorio/lcr/serasacdv2.crl,
http://lcr.certificados.com.br/repositorio/lcr/serasacdv2.crl,
http://repositorio.icpbrasil.gov.br/lcr/Serasa/repositorio/lcr/serasacdv2.crl.

d.3) Para certificados da cadeia V1, emitidos a partir de 09/08/2008:
http://www.certificadodigital.com.br/repositorio/lcr/serasacdv1.crl,
http://lcr.certificados.com.br/repositorio/lcr/serasacdv1.crl,
http://repositorio.icpbrasil.gov.br/lcr/Serasa/repositorio/lcr/serasacdv1.crl

d.4) Para certificados emitidos de 05/08/2006 até 08/08/2008:
http://www.certificadodigital.com.br/repositorio/lcr/serasacd2006.crl

d.5) Para certificados emitidos de 23/04/2004 até 04/08/2006:
http://www.certificadodigital.com.br/repositorio/lcr/SerasaCD.crl

d.6) para certificados emitidos até 22/04/2004:
http://www.certificadodigital.com.br/repositorio/crl/SerasaCD.crl

e) "Authority Information Access", não crítica:

e.1) a primeira entrada contém o endereço na Web onde se obtêm o arquivo p7b com os certificados da cadeia:

i) Para certificados da cadeia V5:
http://www.certificadodigital.com.br/cadeias/serasaservidorcdv5.p7b

ii) Para certificados da cadeia V2
http://www.certificadodigital.com.br/cadeias/serasacdv2.p7b.

iii. para certificados emitidos a partir de 09/08/2008
http://www.certificadodigital.com.br/cadeias/serasacdv1.p7b

iv. para certificados emitidos até 08/08/2008;
http://www.certificadodigital.com.br/cadeias/SerasaCD2006.p7b

e.2) a segunda entrada contém o endereço na Web onde se acessa o serviço OCSP correspondente:

i) Para certificados da cadeia V5:
http://ocsp.certificadodigital.com.br/serasaservidorcdv5

ii) Para certificados da cadeia V2

http://ocsp.certificadodigital.com.br/serasacdv2

iii. para certificados emitidos a partir de 09/08/2008
http://ocsp.certificadodigital.com.br/serasacdv1

iv. para certificados emitidos de 05/08/2006 até 08/08/2008;
http://ocsp.certificadodigital.com.br/serasa_cd2006

v. para certificados emitidos de 25/07/2005 até 04/08/2006;
http://ocsp.certificadodigital.com.br/Serasa_CD

7.1.2.3. Subject Alternative Name

A ICP-Brasil define como obrigatória a extensão "Subject Alternative Name", não crítica, e com os seguintes formatos:

a) Para Certificados de Pessoa Física

a.1) 3 (três) campos otherName, obrigatórios, contendo, nesta ordem:

i OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o número de Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG do titular; nas 6 (seis) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

ii OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa física titular do certificado.

iii OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

a.2) não se aplica;

a.3) não se aplica;

b) Para Certificados de Pessoa Jurídica 4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:

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

ii OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado.

iii OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

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

c) Não se aplica.

d) Não se aplica.

7.1.2.4. Os campos otherName definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;
b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";
c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;
d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;
e) Todas as informações de tamanho variável referentes a números tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;
f) As 6 (seis) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;
g) Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

7.1.2.5. Campos otherName adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela SERASA CD SSL V5, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz. Para o preenchimento do campo PrincipalName serão permitidos os caracteres de “A“ a ”Z”, de “0” a “9” além dos caracteres “.” (ponto), “-” (hífen) e “@” (arroba), necessários à formação do endereço de e-mail do responsável pelo uso do certificado. Outros caracteres especiais, símbolos, espaços ou acentuação não são permitidos.

7.1.2.6. Os outros campos que compõem a extensão "Subject Alternative Name" poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

Extensões Não-Obrigatórias pela ICP-Brasil

a) Para Certificados de Pessoa Física - Sub-extensão "rfc822Name", parte da extensão "Subject Alternative Name", contendo o endereço e-mail do titular.

b) Para Certificados de Pessoa Jurídica - Sub-extensão "rfc822Name" parte da extensão "Subject Alternative Name", contendo o endereço e-mail do titular do certificado de pessoa jurídica.

7.1.2.7. Não se aplica.

7.1.2.8. Não se aplica.

7.1.2.9. A SERASA CD SSL V5 implementa a extensão "Extended Key Usage", não critica:

i. "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2) e
ii. "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4).

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela SERASA CD SSL V5 são assinados com o uso dos seguintes algoritmos, conforme o padrão PKCS#1.

a) RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11) ou RSA com SHA-512 como função de hash (OID = 1.2.840.113549.1.1.13) nas cadeias V2 e V5 da ICP-Brasil;

b) RSA com SHA-1 como função de hash (OID = 1.2.840.113549.1.1.5) nas demais cadeias da ICP-Brasil.

7.1.4. Formatos de nome

7.1.4.1. O nome do titular do certificado, constante do campo “Subject”, adota o “Distinguished Name” (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:
CN = em um certificado de equipamento ou aplicação, o identificador CN contém o URL correspondente. No caso do certificado de pessoa jurídica para o sistema COMPE, o formato será CCCC-XXX, onde CCCC=quatro posições numéricas contendo o código da instituição financeira e XXX=Nome da Instituição Financeira
OU = empresa associada ao emissor do certificado, intermediando o fornecimento de certificados
OU = nome fantasia (nome que associa uma entidade ao certificado)
OU = unidade (identifica grupo, área, divisão, seção ou qualquer outra identificação semelhante)
OU = referência (indica parâmetro adicional, que pode ser um nome, número, combinação de nome e número ou sequência alfanumérica)
OU = código (número, nome ou sequência alfanumérica)
OU = identificador (sequência alfanumérica)

OU = escopo (finalidade do certificado ou seu domínio de aplicação no contexto de um uso específico) O = ICP-Brasil
C = BR

NOTA1: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

NOTA2: Caso qualquer um dos campos OU acima não seja utilizado, será grafado com o texto "(EM BRANCO)".

7.1.4.2. Não se aplica.

7.1.5. Restrições de nome

7.1.5.1. Neste item estão descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela SERASA CD SSL V5 são as seguintes:

a) Os acentos não devem ser utilizados e devem ser substituídos pelo caractere não acentuado. A cedilha deve ser substituída pelo caractere ‘c’;
b) 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

Tabela 1 - Caracteres especiais admitidos em nomes

7.1.6. OID (Object Identifier) de Política de Certificado

O OID (Object Identifier) desta PC é 2.16.76.1.2.4.31.

7.1.7. Uso da extensão "Policy Constraints"

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo policyQualifiers da extensão “Certificate Policies” contém o endereço Web da DPC-SERASA CD SSL V5: (http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf) **Erro! A referência de hiperlink não é válida.**

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela SERASA CD SSL V5 implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela SERASA CD SSL V5 e sua criticalidade.

7.2.2.2. As LCR da SERASA CD SSL V5 obedecem a ICP-Brasil e possuem as seguintes extensões obrigatórias:

a) Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V5:
a.1) "Authority Key Identifier": contém o hash SHA-1 da chave pública da SERASA CD SSL V5 que assina a LCR;
a.2) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela SERASA CD SSL V5;

b) Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V2:
b.1) "Authority Key Identifier": contém o hash SHA-1 da chave pública da SERASA CD SSL V5 que assina a LCR;
b.2) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela SERASA CD SSL V5;
b.3) "Authority Information Access", não crítica, contendo endereço na Web onde se obtêm o

arquivo p7b com os certificados da cadeia: http://www.certificadodigital.com.br/cadeias/serasacdv2.p7b.

b.4) Para certificados emitidos sob as demais cadeias da Autoridade Certificadora Raiz Brasileira:
b.5) "Authority Key Identifier": contém o hash SHA-1 da chave pública da SERASA CD SSL V5 que assina a LCR;
b.6) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela SERASA CD SSL V5;
b.7) "Authority Information Access", não crítica, contendo endereço na Web onde se obtêm o arquivo p7b com os certificados da cadeia: http://www.certificadodigital.com.br/cadeias/serasacdv1.p7b a partir de 11/09/2010.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

Qualquer alteração nesta PC é submetida à aprovação do CG da ICP-Brasil.

8.2. Políticas de publicação e notificação

Esta PC está disponível para a comunidade no endereço web https://serasa.certificadodigital.com.br/ajuda/repositorio/

8.3. Procedimentos de aprovação

Esta PC foi submetida à aprovação, durante o processo de credenciamento da SERASA CD SSL V5, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

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
[1]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICPBRASIL	DOC-ICP-04
[2]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09

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
[3]	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 - Programa 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