



Declaração de Práticas de Certificação das Autoridades Certificadoras com Raiz Serasa



Índice

1	INTRODUÇÃO	6
1.1	VISÃO GERAL.....	6
1.2	IDENTIFICAÇÃO	6
1.3	COMUNIDADE E APLICABILIDADE	6
1.3.1	Autoridade Certificadora (AC).....	6
1.3.2	Autoridade de Registro (AR)	6
1.3.3	Titulares de Certificado.....	7
1.3.4	Aplicabilidade.....	7
1.4	DADOS DE CONTATO.....	7
2	DISPOSIÇÕES GERAIS.....	8
2.1	OBRIGAÇÕES	8
2.1.1	Obrigações da Serasa CA.....	8
2.1.2	Obrigações das AR vinculadas.....	8
2.1.3	Obrigações do Titular do Certificado	9
2.1.4	Direitos da Terceira Parte (Relying Party).....	9
2.1.5	Obrigações do Repositório das Serasa CA.....	9
2.2	RESPONSABILIDADES	10
2.2.1	Responsabilidades das Serasa CA.....	10
2.2.2	Responsabilidades das AR vinculadas.....	10
2.2.3	Responsabilidades do titular do certificado	10
2.3	RESPONSABILIDADE FINANCEIRA.....	10
2.3.1	Indenizações devidas pela terceira parte (Relying Party).....	10
2.3.2	Relações Fiduciárias.....	10
2.3.3	Processos Administrativos.....	11
2.4	INTERPRETAÇÃO E EXECUÇÃO	11
2.4.1	Legislação.....	11
2.4.2	Forma de interpretação e notificação	11
2.4.3	Procedimentos de solução de disputa.....	11
2.5	TARIFAS DE SERVIÇO	12
2.5.1	Tarifas de emissão e renovação de certificados	12
2.5.2	Tarifas de acesso ao certificado.....	12
2.5.3	Tarifas de revogação ou de acesso a informação de status	12
2.5.4	Tarifas para outros serviços.....	12
2.5.5	Política de reembolso.....	12
2.6	PUBLICAÇÃO E REPOSITÓRIO	12
2.6.1	Publicação de informação das Serasa CA	12
2.6.2	Frequência de publicação	13
2.6.3	Controles de acesso.....	13
2.6.4	Repositórios.....	13
2.7	AUDITORIA DE CONFORMIDADE.....	13
2.7.1	Frequência de auditoria de conformidade	13
2.7.2	Identidade e qualificações do auditor	14
2.7.3	Relação entre auditor e parte auditada.....	14
2.7.4	Tópicos cobertos pela auditoria	14
2.7.5	Medidas adotadas em caso de não conformidade.....	15
2.7.6	Comunicação de resultados.....	15
2.8	SIGILO	15
2.8.1	Tipos de informações sigilosas.....	15



2.8.2	<i>Tipos de informações não sigilosas</i>	15
2.8.3	<i>Divulgação de informação de revogação/suspensão de certificado</i>	16
2.8.4	<i>Quebra de sigilo por motivos legais</i>	16
2.8.5	<i>Informações a terceiros</i>	16
2.8.6	<i>Divulgação por solicitação do titular</i>	16
2.8.7	<i>Outras circunstâncias de divulgação de informação</i>	17
2.9	DIREITOS DE PROPRIEDADE INTELECTUAL	17
3	IDENTIFICAÇÃO E AUTENTICAÇÃO	17
3.1	REGISTRO INICIAL	17
3.1.1	<i>Tipos de nomes</i>	17
3.1.2	<i>Necessidade de nomes significativos</i>	17
3.1.3	<i>Regras para interpretação de vários tipos de nomes</i>	18
3.1.4	<i>Unicidade de nomes</i>	18
3.1.5	<i>Procedimento para resolver disputa de nomes</i>	18
3.1.6	<i>Reconhecimento, autenticação e papel de marcas registradas</i>	18
3.1.7	<i>Método para comprovar a posse de chave privada</i>	18
3.1.8	<i>Autenticação da identidade de uma organização</i>	18
3.1.9	<i>Autenticação da identidade de um indivíduo</i>	19
3.1.10	<i>Autenticação de um domínio</i>	19
3.2	GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL	19
3.3	GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO	19
3.4	SOLICITAÇÃO DE REVOGAÇÃO	19
4	REQUISITOS OPERACIONAIS	20
4.1	SOLICITAÇÃO DE CERTIFICADO	20
4.2	EMISSÃO DE CERTIFICADO	20
4.3	ACEITAÇÃO DE CERTIFICADO	20
4.4	SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	20
4.4.1	<i>Circunstâncias para revogação</i>	20
4.4.2	<i>Quem pode solicitar revogação</i>	21
4.4.3	<i>Procedimento para solicitação de revogação</i>	21
4.4.4	<i>Prazo para solicitação de revogação</i>	21
4.4.5	<i>Circunstâncias para suspensão</i>	22
4.4.6	<i>Quem pode solicitar suspensão</i>	22
4.4.7	<i>Procedimento para solicitação de suspensão</i>	22
4.4.8	<i>Limites no período de suspensão</i>	22
4.4.9	<i>Frequência de emissão de LCR</i>	22
4.4.10	<i>Requisitos para verificação de LCR</i>	22
4.4.11	<i>Disponibilidade para revogação/verificação de status on-line</i>	22
4.4.12	<i>Requisitos para verificação de revogação on-line</i>	22
4.4.13	<i>Outras formas disponíveis para divulgação de revogação</i>	23
4.4.14	<i>Requisitos para verificação de outras formas de divulgação de revogação</i>	23
4.4.15	<i>Requisitos especiais para o caso de comprometimento de chave</i>	23
4.5	PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA	23
4.5.1	<i>Tipos de evento registrados</i>	23
4.5.2	<i>Frequência de auditoria de registros (logs)</i>	24
4.5.3	<i>Período de retenção para registros (logs) de auditoria</i>	24
4.5.4	<i>Proteção de registro (log) de auditoria</i>	24
4.5.5	<i>Procedimentos para cópia de segurança (back-up) de registro (log) de auditoria</i>	24
4.5.6	<i>Sistema de coleta de dados de auditoria</i>	24
4.5.7	<i>Notificação de agentes causadores de eventos</i>	25



4.5.8	<i>Avaliações de vulnerabilidade</i>	25
4.6	ARQUIVAMENTO DE REGISTROS	25
4.6.1	<i>Tipos de eventos registrados</i>	25
4.6.2	<i>Período de retenção para arquivo</i>	25
4.6.3	<i>Proteção de arquivo</i>	25
4.6.4	<i>Procedimentos para cópia de segurança (back-up) de arquivo</i>	25
4.6.5	<i>Requisitos para datação (time-stamping) de registros</i>	26
4.6.6	<i>Sistema de coleta de dados de arquivo</i>	26
4.6.7	<i>Procedimentos para obter e verificar informação de arquivo</i>	26
4.7	TROCA DE CHAVE	26
4.8	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE	26
4.9	EXTINÇÃO DA AC	26
5	CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL	27
5.1	CONTROLES FÍSICOS	27
5.1.1	<i>Construção e localização das instalações</i>	27
5.1.2	<i>Acesso físico</i>	28
5.1.2.1	<i>Níveis de acesso</i>	28
5.1.2.2	<i>Sistemas físicos de detecção</i>	29
5.1.2.3	<i>Sistema de controle de acesso</i>	30
5.1.2.4	<i>Mecanismos de emergência</i>	30
5.1.3	<i>Energia e ar condicionado</i>	30
5.1.4	<i>Exposição à água</i>	31
5.1.5	<i>Prevenção e proteção contra incêndio</i>	31
5.1.6	<i>Armazenamento de mídia</i>	32
5.1.7	<i>Destruição de lixo</i>	32
5.1.8	<i>Instalações de segurança (back-up) externas (off-site)</i>	32
5.2	CONTROLES PROCEDIMENTAIS	32
5.2.1	<i>Perfis qualificados</i>	32
5.2.2	<i>Número de pessoas necessário por tarefa</i>	33
5.2.3	<i>Identificação e autenticação para cada perfil</i>	33
5.3	CONTROLES DE PESSOAL	34
5.3.1	<i>Antecedentes, qualificação, experiência e requisitos de idoneidade</i>	34
5.3.2	<i>Procedimentos de verificação de antecedentes</i>	34
5.3.3	<i>Requisitos de treinamento</i>	34
5.3.4	<i>Frequência e requisitos para reciclagem técnica</i>	35
5.3.5	<i>Frequência e seqüência de rodízio de cargos</i>	35
5.3.6	<i>Sanções para ações não autorizadas</i>	35
5.3.7	<i>Requisitos para contratação de pessoal</i>	35
5.3.8	<i>Documentação fornecida ao pessoal</i>	35
6	CONTROLES TÉCNICOS DE SEGURANÇA	35
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	35
6.1.1	<i>Geração do par de chaves</i>	35
6.1.2	<i>Entrega da chave privada à entidade titular</i>	36
6.1.3	<i>Entrega da chave pública para emissor de certificado</i>	36
6.1.4	<i>Disponibilização de chave pública das Serasa CA para usuários</i>	36
6.1.5	<i>Tamanhos de chave</i>	36
6.1.6	<i>Geração de parâmetros de chaves assimétricas</i>	36
6.1.7	<i>Verificação da qualidade dos parâmetros</i>	36
6.1.8	<i>Geração de chave por hardware ou software</i>	37
6.1.9	<i>Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3)</i>	37
6.2	PROTEÇÃO DA CHAVE PRIVADA	37

6.2.1	<i>Padrões para módulo criptográfico</i>	37
6.2.2	<i>Controle "n de m" para chave privada</i>	37
6.2.3	<i>Recuperação (escrow) de chave privada</i>	38
6.2.4	<i>Cópia de segurança (backup) de chave privada</i>	38
6.2.5	<i>Arquivamento de chave privada</i>	38
6.2.6	<i>Inserção de chave privada em módulo criptográfico</i>	38
6.2.7	<i>Método de ativação de chave privada</i>	38
6.2.8	<i>Método de desativação de chave privada</i>	39
6.2.9	<i>Método de destruição de chave privada</i>	39
6.3	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	39
6.3.1	<i>Arquivamento de chave pública</i>	39
6.3.2	<i>Períodos de uso para as chaves pública e privada</i>	39
6.4	DADOS DE ATIVAÇÃO	40
6.4.1	<i>Geração e instalação dos dados de ativação</i>	40
6.4.2	<i>Proteção dos dados de ativação</i>	40
6.4.3	<i>Outros aspectos dos dados de ativação</i>	40
6.5	CONTROLES DE SEGURANÇA COMPUTACIONAL	40
6.5.1	<i>Requisitos Técnicos Específicos de Segurança Computacional</i>	40
6.5.2	<i>Classificação da segurança computacional</i>	41
6.6	CONTROLES TÉCNICOS DO CICLO DE VIDA	41
6.6.1	<i>Controles de desenvolvimento de sistema</i>	41
6.6.2	<i>Controles de gerenciamento de segurança</i>	41
6.6.3	<i>Classificações de segurança de ciclo de vida</i>	42
6.7	CONTROLES DE SEGURANÇA DE REDE	42
6.7.1	<i>Firewall</i>	42
6.7.2	<i>Sistema de detecção de intrusão (IDS)</i>	42
6.7.3	<i>Registro de acessos não autorizados à rede</i>	43
6.8	CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO	43
7	PERFIS DE CERTIFICADO E LCR	43
7.1	PERFIL DO CERTIFICADO	43
7.1.1	<i>Número(s) de versão</i>	43
7.1.2	<i>Extensões de certificado</i>	43
7.1.2.1	<i>Serasa CA I</i>	43
7.1.2.2	<i>Serasa CA II</i>	44
7.1.2.3	<i>Serasa CA III</i>	44
7.1.2.4	<i>Serasa CA IV</i>	45
7.1.3	<i>Identificadores de algoritmo</i>	46
7.1.4	<i>Formatos de nome</i>	46
7.1.5	<i>Restrições de nome</i>	46
7.1.6	<i>OID (Object Identifier) de DPC</i>	46
7.1.7	<i>Uso da extensão "Policy Constraints"</i>	46
7.1.8	<i>Sintaxe e semântica dos qualificadores de política</i>	46
7.1.9	<i>Semântica de processamento para extensões críticas</i>	47
7.2	PERFIL DE LCR	47
7.2.1	<i>Número(s) de versão</i>	47
7.2.2	<i>Extensões de LCR e de suas entradas</i>	47
8	ADMINISTRAÇÃO DE ESPECIFICAÇÃO	47
8.1	PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO	47
8.2	POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO	47
8.3	PROCEDIMENTOS DE APROVAÇÃO	47



Declaração de Práticas de Certificação das Autoridades Certificadoras com Raiz Serasa

Autor: Serasa S.A.
Edição: 17/11/2004
Versão: 1

1 INTRODUÇÃO

1.1 Visão Geral

Esta Declaração de Práticas de Certificação descreve as práticas e os procedimentos empregados pelas Autoridades Certificadoras Raiz da Serasa e pelas Autoridades Certificadoras subsequentes na execução de seus serviços.

As Autoridades Certificadoras da Serasa, contempladas nessa DPC, são as Autoridades Raiz:

- Serasa Certificate Authority I
- Serasa Certificate Authority II
- Serasa Certificate Authority III
- Serasa Certificate Authority IV

Com relação aos tipos específicos de certificado emitidos pelas Autoridades Certificadoras, referidas a seguir como Serasa CA, devem ser consultadas as Políticas de Certificado da Serasa (<http://www.certificadodigital.com.br/repositorio/Serasaca>), que explicam como um tipo específico de certificado é gerado e administrado pela Serasa CA e utilizado pela comunidade.

1.2 Identificação

Esta Declaração de Práticas de Certificação, referida a seguir simplesmente como "DPC", descreve as práticas e os procedimentos empregados pelas Serasa CA.

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridade Certificadora (AC)

Esta DPC se refere às SERASA CA (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)

Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus titulares, são de competência da



Serasa Autoridade de Registrol (SERASA S.A., com sede na Alameda dos Quinimuras, 187, São Paulo, SP, CEP: 04068-900, CNPJ no 62.173.620/0001-80), a seguir referida simplesmente como Serasa AR. O solicitante de um certificado digital é identificado nesta DPC como titular do certificado, inclusive quando o certificado solicitado não é emitido.

1.3.3 Titulares de Certificado

Pessoa físicas ou jurídicas de direito público ou privado, nacionais ou internacionais, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis podem ser Titulares de Certificado, para uso por pessoas físicas, pessoas jurídicas, em equipamentos ou aplicações.

NOTA 1: Em sendo o titular do certificado pessoa jurídica, uma pessoa física é designada como responsável pelo certificado e detentora da chave privada.

NOTA 2: Em se tratando de certificado emitido para equipamento ou aplicação, o titular é a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

1.3.4 Aplicabilidade

As Serasa CA implementa a Política de Certificado Digital das Autoridades Certificadoras com Raiz Serasa.

Os certificados emitidos pela Serasa CA I tem 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.

Os certificados emitidos pela Serasa CA II tem sua utilização vinculada a identificação de Web Sites, criptografia de dados, assinatura de códigos e protocolização de tempo (datação).

Os certificados emitidos pela Serasa CA III tem sua utilização exclusiva para assinatura de certificados digitais de autoridades certificadoras.

Os certificados emitidos pela Serasa CA IV tem sua utilização vinculada a identificação de Web Sites, criptografia de dados, assinatura de códigos, protocolização de tempo (datação) e login de rede Microsoft.

1.4 Dados de Contato

Dúvidas decorrentes da leitura desta DPC podem ser esclarecidas contatando:

SERASA S.A.

Alameda dos Quinimuras, no 187

CEP: 04068-900

São Paulo, SP

Telefones: (5511) 6847-8681



Fax: (5511) 6847 - 9746

Pessoa para contato: Igor Ramos Rocha (e-mail: irr@serasa.com)

2 DISPOSIÇÕES GERAIS

2.1 Obrigações

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. Os requisitos específicos associados a essas obrigações estão detalhados nas PC implementadas pelas Serasa CA.

2.1.1 Obrigações da Serasa CA

As obrigações das Serasa CA são as abaixo relacionadas:

- operar de acordo com esta DPC CA e com as PC que implementa;
- gerar e gerenciar o seus pares de chaves criptográficas;
- assegurar a proteção de suas chaves privadas;
- notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- distribuir os seus próprios certificados;
- emitir, expedir e distribuir os certificados de usuários finais;
- emitir, expedir e distribuir os certificados de autoridades certificadoras de nível subsequente aos seus;
- informar a emissão do certificado ao respectivo solicitante;
- revogar os certificados por elas emitidos;
- emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR);
- publicar esta DPC e as PC que implementam;
- adotar as medidas de segurança e controle previstas nesta DPC e PC implementadas, envolvendo seus processos, procedimentos e atividades
- manter a conformidade dos seus processos, procedimentos e atividades com a legislação vigente;
- manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pelas Serasa CA;

2.1.2 Obrigações das AR vinculadas

As obrigações das AR vinculadas são as abaixo relacionadas:

- receber solicitações de emissão ou de revogação de certificados;
- confirmar a identidade do solicitante e a validade da solicitação;
- encaminhar a solicitação de emissão ou de revogação de certificado à respectiva Serasa CA;
- informar aos respectivos titulares a emissão ou a revogação de seus certificados;

- disponibilizar os certificados emitidos aos seus respectivos solicitantes;
- identificar e registrar todas as ações executadas;
- obedecer no que couber estritamente a esta DPC e às PC aplicáveis, bem como respeitar a legislação aplicável;
- manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela Serasa CA;
- manter e garantir a segurança da informação por elas tratada.

2.1.3 Obrigações do Titular do Certificado

Constituem-se obrigações do titular de certificado emitido pelas Serasa CA:

- fornecer, de forma completa e precisa, todas as informações necessárias para sua identificação e/ou a identificação do equipamento a ser certificado;
- garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- utilizar os seus certificados e chaves privadas de forma apropriada, conforme o previsto na PC correspondente;
- conhecer os seus direitos e obrigações, contemplados pela DPC, pela PC correspondente e por outros documentos aplicáveis;
- informar a respectiva Serasa CA qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
- obedecer no que couber estritamente a esta DPC e às PC aplicáveis, bem como respeitar a legislação aplicável e as obrigações contratuais assumidas perante a respectiva Serasa CA e à AR vinculada.

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

2.1.4 Direitos da Terceira Parte (Relying Party)

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

Constituem direitos e obrigações da terceira parte:

- recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;
- verificar, a qualquer tempo, a validade do certificado. Certificados emitidos pelas Serasa CA são considerados válidos quando:
 - § não constar da LCR da AC emitente;
 - § não estiver expirado; e
 - § puder ser verificado com o uso de certificado válido da AC emitente.

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

2.1.5 Obrigações do Repositório das Serasa CA



- Disponibilizar, logo após a sua emissão, os certificados emitidos pelas Serasa CA e as suas LCR;
- estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
- implementar os recursos necessários para a garantia da segurança dos dados nele armazenados.

2.2 Responsabilidades

2.2.1 Responsabilidades das Serasa CA

As Serasa CA respondem pelos danos a que derem causa.

2.2.2 Responsabilidades das AR vinculadas

A AR vinculada é responsável pelos danos a que der causa.

As Serasa CA, responsável por esta DPC, respondem solidariamente pelos atos das AR a ela vinculadas.

2.2.3 Responsabilidades do titular do certificado

O titular do certificado é responsável pelas informações constantes do certificado que forneceu para sua identificação e/ou do equipamento, bem como pela atualização das mesmas.

2.3 Responsabilidade Financeira

2.3.1 Indenizações devidas pela terceira parte (Relying Party)

A terceira parte deverá indenizar as Serasa CA 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

As Serasa CA dispõem de uma Política de Garantia que se estende a todos titulares de certificados digitais por elas 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 as Serasa CA comprovadamente derem causa. A Política de Garantia cobre perdas e danos decorrentes de comprometimento das chaves privadas das Serasa CA, de erro na identificação do titular, de emissão defeituosa do certificado ou de erros ou omissões das Serasa CA e das AR vinculadas na prestação de seus serviços aos beneficiários.



2.3.3 Processos Administrativos

O titular do certificado que sofrer perdas e danos decorrentes do uso do Certificado Digital Serasa terá o direito de comunicar à Serasa CA que deseja a indenização prevista no documento Política de Garantia para tais casos, observadas as seguintes condições:

- a) nos casos de perdas e danos decorrentes de comprometimento das chaves privadas das Serasa CA, 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 Serasa CA ou às AR vinculadas;
- 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 obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor.

2.4.2 Forma de interpretação e notificação

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

As notificações, solicitações ou quaisquer outras comunicações necessárias, sujeitas às práticas descritas nesta DPC, serão realizadas pelas Serasa CA e pelas AR 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.

2.4.3 Procedimentos de solução de disputa

Em caso de conflito entre esta DPC e outras declarações, políticas, planos, acordos, contratos ou documentos, esta DPC prevalecerá.



2.5 Tarifas de Serviço

Pelo certificado emitido será cobrado o valor estabelecido contratualmente.

2.5.1 Tarifas de emissão e renovação de certificados

Pela emissão e renovação do certificado será cobrado o valor estabelecido contratualmente.

2.5.2 Tarifas de acesso ao certificado

Pelo acesso ao certificado será cobrado 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 será cobrado o valor estabelecido contratualmente.

2.5.4 Tarifas para outros serviços

Pelos demais serviços será cobrado o valor estabelecido contratualmente.

2.5.5 Política de reembolso

Caso o certificado deva ser revogado por motivo de comprometimento da chave privada de uma Serasa CA ou da mídia armazenadora da chave privada de uma Serasa CA, ou ainda quando constatada a emissão imprópria ou defeituosa do certificado do titular, imputável à respectiva Serasa CA, será reembolsado ao titular do certificado, 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 das Serasa CA

As Serasa CA publicam e mantêm disponíveis em seu site (www.certificadodigital.com.br/repositorio/serasaca), em no mínimo 90,0% (noventa por cento do tempo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, as seguintes informações:

- seu próprio certificado;
- sua LCR;



- esta DPC;
- as PC que implementa.

2.6.2 Frequência de publicação

As informações de que trata o item anterior são mantidas atualizadas em conformidade com a respectiva Política de Certificado.

2.6.3 Controles de acesso

Somente as Serasa CA, por seus funcionários competentes e designados especialmente para esse fim, podem alterar as informações constantes nesta DPC e nas PC que implementa.

Somente a Serasa CA, por seus funcionários competentes e designados especialmente para esse fim, pode efetuar as necessárias atualizações de suas LCR.

Os certificados das Serasa CA e os certificados emitidos pelas Serasa CA não podem ser modificados. Caso se faça necessário modificar os dados contidos nos mesmos, será necessária a revogação dos certificados.

Não há restrições para o acesso para leitura desta DPC, da respectiva PC e das LCR.

Todas as informações disponibilizadas pelas Serasa CA, conforme o item 2.6.1 desta DPC, estão disponíveis para leitura sem restrições.

2.6.4 Repositórios

Os repositórios das Serasa CA podem ser acessados através da página <http://www.certificadodigital.com.br/repositorio/serasaca>, utilizando o protocolo de acesso http.

Os repositórios estão disponíveis em no mínimo 90,0% (noventa por cento) do tempo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

Somente as Serasa CA, por seus funcionários competentes e designados especialmente para esse fim, podem alterar as informações constantes nos repositórios. Os repositórios obedecem aos requisitos do item 5.

2.7 Auditoria de Conformidade

As Serasa CA atuam em conformidade com os procedimentos descritos nesta DPC.

2.7.1 Frequência de auditoria de conformidade



As Serasa CA realizam periodicamente auditorias de conformidade das entidades a ela diretamente vinculadas.

2.7.2 Identidade e qualificações do auditor

Os relatórios de auditoria das ACs subsequentes, das AR vinculadas e dos prestadores de serviço de suporte vinculados diretamente às Serasa CA são fornecidos pela Serasa CA ou por empresa de auditoria contratada pelas Serasa CA, pela AC subsequente, pela AR vinculada ou pelo prestador de serviço de suporte.

2.7.3 Relação entre auditor e parte auditada

O auditor de empresa independente das Serasa CA é impedido de realizar a auditoria quando:

- houver motivo íntimo declarado;
- for amigo íntimo ou inimigo capital de membros das Serasa CA;
- for credor ou devedor das Serasa CA;
- tiver interesse no resultado das auditorias das Serasa CA

O auditor do quadro de empregados das Serasa CA está impedido de realizar auditoria de AR vinculada ou prestador de serviço, exceto da Serasa AR, quando:

- houver motivo íntimo declarado;
- for amigo íntimo ou inimigo capital de membros da AR vinculada;
- for credor ou devedor da AR vinculada;
- tiver interesse no resultado da auditoria da AR vinculada.

O auditor é devidamente qualificado e firma previamente à realização da auditoria declaração sob as penas da lei de que não se enquadra em qualquer das causas de impedimento.

2.7.4 Tópicos cobertos pela auditoria

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.

Os tópicos cobertos pela auditoria de conformidade incluem, dentre outros:

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



2.7.5 Medidas adotadas em caso de não conformidade

As entidades vinculadas às Serasa CA cumprem, no prazo estipulado pelas Serasa CA, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas.

2.7.6 Comunicação de resultados

Os relatórios completos das auditorias são entregues à Serasa CA Raiz, bem como à entidade auditada.

2.8 Sigilo

As chaves privadas de assinatura digital das Serasa CA foram geradas e são mantidas pelas próprias Serasa CA, que asseguram os seus sigilos. A divulgação ou utilização indevida da chave privada de assinatura pelas Serasa CA é de sua inteira responsabilidade.

Os titulares de certificados emitidos pela Serasa CA são responsáveis pela geração, manutenção e pela garantia do sigilo de suas respectivas chaves privadas, bem pela divulgação ou utilização indevidas dessas mesmas chaves.

As PC correspondentes delimitam as responsabilidades pela manutenção e pela garantia do sigilo das respectivas chaves privadas.

2.8.1 Tipos de informações sigilosas

Como princípio geral, nenhum documento, informação ou registro fornecido às Serasa CA ou às AR vinculadas deve ser divulgado.

2.8.2 Tipos de informações não sigilosas

Não são consideradas como informações sigilosas pelas Serasa CA e pelas AR vinculadas:

- os certificados e as LCR emitidos pelas Serasa CA;
- as informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
- as PC implementadas pela Serasa CA;
- esta DPC;
- os resultados finais de auditorias.

As Serasa CA e as AR vinculadas tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:



- a) estejam na posse legítima das Serasa CA ou da AR vinculada antes de seu fornecimento pelo titular ou o titular autorize formalmente a sua divulgação;
- b) posteriormente ao seu fornecimento pelo titular, 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.

Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pelas Serasa CA e pelas AR vinculadas, exceto na hipótese da alínea "c" acima, ou quando o titular requerer ou autorizar expressamente a sua divulgação a terceiros.

2.8.3 Divulgação de informação de revogação/suspensão de certificado

As Serasa CA disponibilizam permanentemente em seu site <http://www.certificadodigital.com.br/repositorio/serasaca>, com atualização definida na correspondente PC, relação de certificados por ela emitidos que foram revogados.

Os motivos que justificaram a revogação são mantidos confidenciais pelas Serasa CA e pelas AR vinculadas, exceto quando o titular do certificado revogado solicitar ou autorizar expressamente a sua divulgação a terceiros ou quando esse motivos tenham sido ou venham a ser publicados, ou sejam ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida das Serasa CA ou das AR vinculadas, ou ainda quando tais motivos sejam requisitados por determinação judicial ou governamental.

A suspensão de certificados não é admitida pelas Serasa CA.

2.8.4 Quebra de sigilo por motivos legais

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

2.8.5 Informações a terceiros

As Serasa CA não fornecem nem fornecerão a terceiros nenhum documento, informação ou registro sob sua guarda, exceto nas hipóteses mencionadas nesta DPC.

2.8.6 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 das Serasa CA e das AR vinculadas em razão da solicitação e da emissão do certificado



digital. O titular do certificado pode autorizar as Serasa CA ou as AR vinculadas 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, ou posteriormente, por documento legalmente aceito.

2.8.7 Outras circunstâncias de divulgação de informação

As Serasa CA e as AR vinculadas podem divulgar informações que não sejam consideradas sigilosas pelo fato de:

- a) estarem na posse legítima das Serasa CA ou das AR vinculadas antes de seu fornecimento pelo solicitante ou titular do certificado, ou titular do certificado haver autorizado a sua divulgação;
- b) posteriormente ao seu fornecimento pelo 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.

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 das Serasa CA ou das AR vinculadas para o titular do certificado.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Registro Inicial

As AR vinculadas efetuam a identificação de uma organização (item 3.1.8) e autenticação da identidade de um indivíduo (item 3.1.9) por meio da verificação da validade dos documentos de identificação fornecidos e com base nos dados fornecidos no formulário de solicitação descritos nas respectivas PC.

3.1.1 Tipos de nomes

As Serasa CA emitem 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 Necessidade de nomes significativos



As Serasa CA fazem uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem, para a identificação dos titulares dos certificados emitidos pelas Serasa CA.

3.1.3 Regras para interpretação de vários tipos de nomes

Os requisitos e procedimentos específicos, quando aplicáveis, estão detalhados nas PC implementadas.

3.1.4 Unicidade de nomes

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

3.1.5 Procedimento para resolver disputa de nomes

As Serasa CA se reservam 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.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.7 Método para comprovar a posse de chave privada

A confirmação 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.

Os métodos estão detalhados nas PC implementadas pelas Serasa CA.

3.1.8 Autenticação da identidade de uma organização

A confirmação da identidade de uma pessoa jurídica é feita com base em, no mínimo, os seguintes documentos:

- registro comercial, no caso de empresa individual;
- ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;



- prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ).

A pessoa física responsável por um certificado que tenha como titular uma pessoa jurídica deverá ser também identificada, na forma descrita no item seguinte.

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade do responsável pelo certificado é realizada com base em, no mínimo apresentação da cédula de identidade e da confirmação de inscrição no Cadastro de Pessoa Física.

Solicitações de certificados são realizadas pela pessoa física legalmente responsável. Cabe à AR vinculada as Serasa CA verificar a autorização atribuída ao solicitante, bem como a presença dos documentos exigidos. Os procedimentos utilizados pela AR vinculada estão descritos nas PC implementadas.

3.1.10 Autenticação de um domínio

A confirmação de um domínio é feita mediante confirmação junto aos órgãos de registro de domínio nacionais e internacionais.

O domínio a ser certificado deverá estar registrado para o titular do certificado digital. Caso contrário, a Pessoa Jurídica ou Física detentora do endereço deverá apresentar uma declaração de cessão de uso da URL, a qual autoriza o titular a utilizar o domínio. Esta declaração deverá ser registrada em cartório e ter firma reconhecida ou assinada digitalmente com certificado emitido no âmbito da ICP-Brasil.

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

Devem ser observados os mesmos requisitos e procedimentos exigidos para a solicitação inicial do certificado, na forma e no prazo estabelecidos na correspondente PC. A emissão de um novo certificado obedece ao estabelecido na correspondente PC implementada.

3.3 Geração de novo par de chaves após revogação

Após a revogação do certificado, o solicitante pode solicitar um novo certificado, enviando à AR vinculada uma solicitação, na forma, condições e prazo estabelecidos para a solicitação inicial de um certificado.

3.4 Solicitação de Revogação



A revogação do certificado é feita com base em comunicação assinada pelo titular do certificado ou pessoa com poderes de representação do titular do certificado.

4 REQUISITOS OPERACIONAIS

4.1 Solicitação de Certificado

A solicitação de emissão de um certificado digital é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR vinculada. Toda referência a formulário deverá ser entendida também como referência a outras formas que as Serasa CA ou AR Vinculadas possam 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, e a indicação de endereço eletrônico para o qual a Serasa AR Global deve enviar o certificado digital.

4.2 Emissão de Certificado

Somente após e na hipótese de validação conclusiva, pelas AR vinculadas, dos dados fornecidos pelo solicitante no formulário de solicitação de certificado digital as Serasa CA procede à emissão e assinatura do certificado.

O processo de emissão é inicializado com a verificação da CSR (Certificate Signing Request - Solicitação de Assinatura de Certificado) e submissão da requisição no padrão PKCS # 10 ao software das Serasa CA. Em seguida o certificado emitido é inserido na relação de certificados emitidos pela respectiva Serasa CA.

A notificação de emissão é feita por diferentes meios (e-mail contendo o certificado ou e-mail solicitando download em url específico ou em mídia), conforme definido na correspondente PC.

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 do mesmo. A aceitação implica que o titular reconhece e se responsabiliza pela veracidade dos dados contidos no certificado.

4.4 Suspensão e Revogação de Certificado

4.4.1 Circunstâncias para revogação

Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

- quando constatada emissão imprópria ou defeituosa do mesmo;
- quando for necessária a alteração de qualquer informação constante no mesmo;



- no caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora; ou
- no caso de revogação do certificado da respectiva Serasa CA.

Deve-se observar ainda que as Serasa CA revogarão, no prazo definido no item 4.4.3 o certificado da entidade que deixar de cumprir as determinações desta DPC.

4.4.2 Quem pode solicitar revogação

A revogação de um certificado somente pode ser solicitada:

- pelo titular do certificado;
- pelo responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
- por empresa ou órgão, quando o titular do certificado ou seu representante legal, fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- pela respectiva Serasa CA;
- pela AR vinculada;

4.4.3 Procedimento para solicitação de revogação

Para solicitar a revogação é necessário o envio às Serasa CA ou à AR vinculada de uma comunicação assinada pelo titular do certificado por pessoa com poderes para representá-lo e para solicitar a revogação do certificado.

Nos casos de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente ou da sua mídia armazenadora, a solicitação de revogação poderá ser feita também mediante qualquer outro mecanismo que as Serasa CA indiquem ao titular e que permita identificá-lo.

Como diretrizes gerais:

- o solicitante da revogação de um certificado é identificado;
- as solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas;
- as justificativas para a revogação de um certificado são documentadas;
- o processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado.

Todos os agentes habilitados, conforme o item 4.4.2 podem, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados. Os procedimentos detalhados estão descritos nas PC implementadas.

4.4.4 Prazo para solicitação de revogação

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



Cada PC implementada pelas Serasa CA estabelece o prazo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa pelas Serasa CA.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida pelas Serasa CA.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida pelas Serasa CA.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida pelas Serasa CA.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida pela Serasa CA.

4.4.9 Frequência de emissão de LCR

Cada PC implementada pelas Serasa CA define a frequência de emissão da LCR associada.

4.4.10 Requisitos para verificação de LCR

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

A autenticidade da LCR deve também ser confirmada por meio das verificações da assinatura da Serasa CA 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 deve notificar imediatamente a Serasa CA emitente, solicitando a revogação de seu certificado, de conformidade com o procedimento previsto no item 4.4.3 desta DPC e no item correspondente da PC implementada.

4.5 Procedimentos de Auditoria de Segurança

4.5.1 Tipos de evento registrados

As Serasa CA registram em arquivos de auditoria os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são incluídos em arquivos de auditoria:

- iniciação e desligamento do sistema de certificação;
- tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores das Serasa CA;
- mudanças na configuração das Serasa CA ou nas suas chaves;
- mudanças nas políticas de criação de certificados;
- tentativas de acesso (login) e de saída do sistema (logoff);
- tentativas não autorizadas de acesso aos arquivos de sistema;
- geração de chaves próprias das Serasa CA ou de usuários finais;
- emissão e revogação de certificados;
- geração de LCR;
- tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
- operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
- operações de escrita nesse repositório, quando aplicável.

As Serasa CA registram, eletrônica ou manualmente, as seguintes informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

- registros de acessos físicos;
- manutenção e mudanças na configuração de seus sistemas;
- mudanças de pessoal e de perfis qualificados;
- relatórios de discrepância e comprometimento; e



- registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

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

4.5.2 Frequência de auditoria de registros (logs)

O pessoal operacional das Serasa CA analisam os registros de auditoria periodicamente. 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

As Serasa CA mantêm localmente seus registros de auditoria por pelo menos 2 (dois) meses.

4.5.4 Proteção de registro (log) de auditoria

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.

Mecanismos de proteção utilizados:

- Os acessos lógicos são liberados através da ferramenta nativa do sistema operacional de modo a assegurar o uso apenas a usuários ou processos autorizados;
- Os acessos lógicos aos registros de eventos de auditoria são registrados em logs do próprio sistema operacional.

4.5.5 Procedimentos para cópia de segurança (back-up) de registro (log) de auditoria

As Serasa CA geram a cada mês cópia de back-up de seus registros de auditoria, através de procedimentos utilizando conexão segura.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é interno às Serasa CA 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 das Serasa CA, 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 das Serasa CA são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pelas Serasa CA e registradas para fins de auditoria.

4.6 Arquivamento de Registros

4.6.1 Tipos de eventos registrados

Os tipos de eventos arquivados pelas Serasa CA são:

- solicitações de certificados;
- solicitações de revogação de certificados;
- notificações de comprometimento de chaves privadas;
- emissões e revogações de certificados;
- emissões de LCR;
- trocas de chaves criptográficas da Serasa AC Global;
- informações de auditoria previstas no item 4.5.1.

4.6.2 Período de retenção para arquivo

O período de retenção para cada evento arquivado é de 1 (um) ano.

4.6.3 Proteção de arquivo

Os registros arquivados das Serasa CA são classificados e armazenados com requisitos de segurança compatíveis com essa classificação e com a Política de Segurança da Serasa.

4.6.4 Procedimentos para cópia de segurança (back-up) de arquivo

A cópia de todo o material arquivado é armazenada em local físico isolado das Serasa CA.



4.6.5 Requisitos para datação (time-stamping) de registros

Os servidores estão sincronizados com a hora GMT. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.

No caso dos registros feitos manualmente 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 pelas Serasa CA 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 às Serasa CA ou às AR vinculadas, 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

Trinta dias antes da data de expiração do certificado digital, a AR vinculada comunica ao seu titular a data de expiração do mesmo.

Expirado o certificado do titular, a respectiva Serasa CA remove esse certificado de seu diretório, mantendo-o armazenado por 5 (cinco) anos, para efeito de consulta histórica.

4.8 Comprometimento e Recuperação de Desastre

As Serasa CA possuem Plano de Continuidade de Negócio, estabelecido conforme a Política de Segurança da Serasa e testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos.

As Serasa CA mantêm os backups em ambiente físico isolado, garantindo sua recuperação em caso de sinistro.

4.9 Extinção da AC

Em caso de extinção de alguma Serasa CA serão tomadas as providências mencionadas no Plano de Encerramento das Serasa CA disponível no site <http://www.certificadodigital.com.br/repositorio/serasaca>, que incluem a divulgação da



decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, aplicativos dedicados à certificação digital, guarda de bases de dados e recuperação de informações.

A divulgação do encerramento das atividades de uma Serasa CA é feita mediante comunicação, com 180 dias de antecedência, aos usuários finais, com 150 dias de antecedência, e à comunidade em geral, com 90 dias de antecedência, mediante jornal de circulação nacional e no seu site <http://www.certificadodigital.com.br>.

A respectiva Serasa CA deixa de emitir certificados 180 dias após a comunicação pública, comprometendo-se a manter suas atividades de autoridade certificadora em operação até que todos os certificados emitidos por ela tenham sido revogados.

As base de dados e aplicativos relacionados ao processo de certificação digital deixam de estar operacionais 180 dias após a comunicação pública

Os back-ups relativos à operação de certificação digital serão mantidos armazenados por 6 anos, após os quais serão destruídos.

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os controles descritos a seguir são implementados pelas Serasa CA e pelas AR vinculadas 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 das Serasa CA.

5.1.1 Construção e localização das instalações

A localização e o sistema de certificação das Serasa CA 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.

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

- instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;
- instalações para sistemas de telecomunicações;
- sistemas de aterramento e de proteção contra descargas atmosféricas;



- iluminação de emergência.

As instalações das AR vinculadas não possuem aspectos de construção relevantes para os controles de segurança física.

5.1.2 Acesso físico

As Serasa CA implantaram sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a Política de Segurança da Serasa e os requisitos que seguem.

5.1.2.1 Níveis de acesso

As Serasa CA definem 4 (quatro) níveis de acesso físico aos diversos ambientes, e 2 (dois) níveis relativos à proteção da chave privada das Serasa CA.

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

Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da Serasa CA, 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.

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 Serasa CA.

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 Serasa CA. 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.

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.



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

No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da Serasa CA 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.

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.

Na Serasa CA há 1 (um) ambiente de quarto nível para abrigar e segregar, respectivamente:

- equipamentos de produção on-line;
- equipamentos de produção off-line e cofre de armazenamento.

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.

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

- é feito em aço ou material de resistência equivalente;
- possui tranca com chave.

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 são armazenados nesses depósitos.

5.1.2.2 Sistemas físicos de detecção

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.



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.

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.

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.

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

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

Mecanismos específicos foram implantados pelas Serasa CA 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.

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

A infra-estrutura do ambiente de certificação das Serasa CA 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 das Serasa CA e seus respectivos serviços. Um sistema de aterramento foi implantado.

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

Foram utilizados 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.

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

São mantidos atualizados os registros sobre a topologia da rede de cabos. Qualquer modificação nessa rede é previamente documentada.

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

O sistema de climatização atende 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.

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

O sistema de ar condicionado será interno, com troca de ar realizada apenas por abertura da porta.

A capacidade de redundância de toda a estrutura de energia e ar condicionado das Serasa CA é garantida, por meio de:

- geradores de porte compatível;
- geradores de reserva;
- sistemas de no-breaks redundantes;
- sistemas redundantes de ar condicionado.

5.1.4 Exposição à água

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

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.

Nas instalações das Serasa CA não é permitido fumar ou portar objetos que produzam fogo ou faísca.

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.

Em caso de incêndio nas instalações das Serasa CA, a 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

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

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 (back-up) externas (off-site)

A Serasa AC Global mantém seus backups em ambiente físico isolado, garantindo sua recuperação em caso de sinistro.

5.2 Controles Procedimentais

5.2.1 Perfis qualificados

As Serasa CA efetuam 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.

As Serasa CA estabelecem 4 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. A definição de responsabilidades para os quatro perfis poderá estar baseada na seguinte divisão:



- Suporte à Configurações
 - configuração e manutenção do hardware e do software de apoio das Serasa CA.
- Gestão da Segurança:
 - gerenciamento dos operadores das Serasa CA;
 - implementação das políticas de segurança das Serasa CA;
- Auditoria
 - verificação dos registros de auditoria;
 - verificação do cumprimento da DPC e das PC implementadas;
- Administração do Sistema:
 - configuração e manutenção do software das Serasa CA;
 - início e término dos serviços das Serasa CA;
 - gerenciamento dos processos de iniciação dos usuários internos às Serasa CA;
 - emissão, expedição, distribuição, revogação e gerenciamento de certificados;
 - distribuição de cartões (tokens).

Somente os empregados responsáveis por tarefas descritas para a Suporte à Configurações e a Administração do Sistema devem ter acesso ao sistema de certificação das Serasa CA.

Quando um empregado se desligar das Serasa CA, suas permissões de acesso são revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro das Serasa CA, 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

As Serasa CA utilizam o requisito de controle multiusuário para a geração e a utilização da sua chave privada, na forma definida no item 6.2.2.

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

5.2.3 Identificação e autenticação para cada perfil

Todo empregado das Serasa CA têm sua identidade e perfil verificados antes de:

- ser incluído em uma lista de acesso às instalações das Serasa CA;
- ser incluído em uma lista para acesso físico ao sistema de certificação das Serasa CA;
- receber um certificado para executar suas atividades operacionais nas Serasa CA;
- receber uma conta no sistema de certificação das Serasa CA.

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

- são diretamente atribuídos a um único empregado;
- não são compartilhados;
- são restritos às ações associadas ao perfil para o qual foram criados.

As Serasa CA implementam um padrão de utilização de "senhas fortes", definido na Política de Segurança da Serasa juntamente com procedimentos de validação dessas senhas.

5.3 Controles de Pessoal

Todos os empregados das Serasa CA e das AR vinculadas encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

- os termos e as condições do perfil que ocuparão;
- o compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade.

Todo o pessoal das Serasa CA e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido pelas Serasa CA.

5.3.2 Procedimentos de verificação de antecedentes

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

- verificação de antecedentes criminais;
- verificação de situação de crédito;
- verificação de histórico de empregos anteriores;
- comprovação de escolaridade e de residência.

5.3.3 Requisitos de treinamento

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

- princípios e mecanismos de segurança das Serasa CA e das AR vinculadas;
- sistema de certificação em uso nas Serasa CA;
- procedimentos de recuperação de desastres e de continuidade do negócio;
- outros assuntos relativos a atividades sob sua responsabilidade.



5.3.4 Frequência e requisitos para reciclagem técnica

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

5.3.5 Frequência e seqüência de rodízio de cargos

As Serasa CA e as AR vinculadas possuem pessoal e efetivo de contingência devidamente treinado, não fazendo uso de rodízio de pessoal.

5.3.6 Sanções para ações não autorizadas

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

5.3.7 Requisitos para contratação de pessoal

Todo o pessoal das Serasa CA e das AR vinculadas 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 Serasa.

5.3.8 Documentação fornecida ao pessoal

As Serasa CA tornarão disponível para todo o seu pessoal:

- esta DPC;
- as PC que implementa;
- documentação operacional relativa a suas atividades;
- contratos, normas e políticas relevantes para suas atividades.

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

O par de chaves criptográficas de cada Serasa CA é gerado pela própria Serasa CA.



Pares de chaves são gerados somente pelo titular do certificado correspondente, sendo que os procedimentos específicos estão descritos em cada PC implementada pela Serasa CA.

Cada PC implementada pela Serasa CA define o meio utilizado para armazenamento da chave privada.

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 Autoridade Certificado Serasa Raiz, encarregada da emissão de seu certificado, as Serasa CA farão uso do padrão PKCS#10.

Os procedimentos para a entrega da chave pública de um solicitante de certificado às Serasa CA estão detalhados em cada PC implementada.

6.1.4 Disponibilização de chave pública das Serasa CA para usuários

As formas para a disponibilização dos certificados das Serasa CA, e de todos os certificados da cadeia de certificação, para os usuários, compreendem, entre outras:

- formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- diretório;
- página Web das Serasa CA (<http://www.certificadodigital.com.br/repositorio/serasaca>).

6.1.5 Tamanhos de chave

Cada PC implementada pelas Serasa CA define o tamanho das chaves criptográficas associadas aos certificados emitidos.

6.1.6 Geração de parâmetros de chaves assimétricas

Cada PC define a geração das chaves criptográficas associadas aos certificados emitidos.

6.1.7 Verificação da qualidade dos parâmetros



Os parâmetros são verificados de acordo com as normas estabelecidas pelo CMVP (Cryptographic Module Validation Program) do NIST (National Institute of Standards and Technology).

6.1.8 Geração de chave por hardware ou software

O processo de geração do par de chaves da Serasa CA é feito por hardware padrão FIPS (Federal Information Processing Standards) 140-1 , level 3. Cada PC implementada pelas Serasa CA caracteriza o processo utilizado para a geração de chaves criptográficas dos titulares de certificados.

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

Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pelas Serasa CA, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC implementada.

As chaves privadas das Serasa CA são utilizadas apenas para a assinatura dos certificados por elas emitidos e de suas LCR.

6.2 Proteção da Chave Privada

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

Cada PC implementada especifica os requisitos específicos aplicáveis para a proteção das chaves privadas das entidades titulares de certificados.

6.2.1 Padrões para módulo criptográfico

O módulo criptográfico de geração de chaves assimétricas da Serasa CA adota o padrão FIPS (Federal Information Processing Standards) 140-1, no level 3.

Cada PC implementada especifica os requisitos específicos aplicáveis para a geração de chaves criptográficas dos titulares de certificado.

6.2.2 Controle "n de m" para chave privada

As Serasa CA estabelecem como exigência de controle múltiplo para a utilização das suas chaves privadas o número mínimo de 2 ("n") (duas) pessoas de um grupo de 5 ("m")(cinco) pessoas.



6.2.3 Recuperação (escrow) de chave privada

Não é permitida 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

Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua própria chave privada.

As Serasa CA mantêm cópia de segurança de sua própria chave privada.

As Serasa CA não mantêm cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

Cada PC implementada define os requisitos específicos aplicáveis. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

Não são arquivadas chaves privadas de assinatura digital.

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

Cada PC implementada define, quando aplicável, os requisitos para inserção da chave privada dos titulares de certificado em módulo criptográfico.

6.2.7 Método de ativação de chave privada

Para a ativação das chaves privadas exige-se o número mínimo de 1 ("n") (uma) pessoa 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.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.



6.2.8 Método de desativação de chave privada

Para a desativação das chaves privadas exige-se o número mínimo de 1 ("n") (uma) pessoa 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.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.9 Método de destruição de chave privada

Para a destruição das chaves privadas exige-se o número mínimo de 1 ("n") (uma) 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.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

As chaves públicas das Serasa CA e dos titulares de certificados digitais por ela emitidos permanecem armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade. Cada PC de assinatura digital implementada descreve os períodos de arquivamento da chave pública de entidade titular de certificado.

6.3.2 Períodos de uso para as chaves pública e privada

As chaves privadas das Serasa CA e dos titulares de certificados digitais por elas emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas são utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

Cada PC implementada pelas Serasa CA define o período máximo de validade do certificado.



O período máximo de validade admitido para certificados das Serasa CA Raiz é de 20 (vinte) anos.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Os dados de ativação da chave privada das Serasa CA são únicos e aleatórios. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

6.4.2 Proteção dos dados de ativação

Os dados de ativação das chaves privadas das Serasa CA são protegidos contra uso não autorizado, por meio de mecanismos de criptografia e de controle de acesso físico.

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

6.4.3 Outros aspectos dos dados de ativação

Não aplicável.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos Técnicos Específicos de Segurança Computacional

A geração dos pares de chaves das Serasa CA é realizada off-line, para impedir o acesso remoto não autorizado.

Os requisitos específicos aplicáveis estão descritos em cada PC implementada. Cada computador servidor das Serasa CA, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes características:

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



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

Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações das Serasa CA, 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 às atividades das Serasa CA. Todos esses eventos são registrados para fins de auditoria.

Qualquer equipamento incorporado às Serasa CA 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 das Serasa CA segue as recomendações do Trusted System Evaluation Criteria (TCSEC).

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistema

As Serasa CA adotam a tecnologia da RSA e para customizações do ambiente da AC responsável, que são desenvolvidos por Analistas de Suporte. 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 Gerente de Produção e é composto de outras áreas da Serasa, como por exemplo Auditoria de Sistema, Segurança de Sistemas de Informação, Produção, etc., que avaliam e decidem quanto a sua implementação.

Os processos de projeto e desenvolvimento conduzidos pelas Serasa CA provêm documentação suficiente para suportar avaliações externas de segurança dos componentes das Serasa CA.

6.6.2 Controles de gerenciamento de segurança

As Serasa CA utilizam metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação das Serasa CA.

As Serasa CA verificam os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional.



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 aplicável.

6.7 Controles de Segurança de Rede

Nos servidores do sistema de certificação das Serasa CA, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.

Todos os servidores e elementos de infra-estrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação das Serasa CA, estão localizados e operam em ambiente de nível 4.

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

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

6.7.1 Firewall

Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Firewalls promovem o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo - a conhecida "zona desmilitarizada" (DMZ) - em relação aos equipamentos com acesso exclusivamente interno às Serasa CA.

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

6.7.2 Sistema de detecção de intrusão (IDS)

O sistema de detecção de intrusão tem capacidade de ser configurado para reconhecer ataques em tempo real e responde-los automaticamente, com medidas tais



como: enviar traps SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta aos firewalls ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração dos firewalls.

O sistema de detecção de intrusão tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento. O sistema de detecção de intrusão provê o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.3 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado - em roteadores, firewalls ou IDS - são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é, no mínimo, diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico de geração de chaves assimétricas da Serasa CA adota o padrão FIPS (Federal Information Processing Standards) 140-1, level 3.

7 PERFIS DE CERTIFICADO E LCR

Cada PC implementada pelas Serasa CA especifica os formatos dos certificados gerados e das correspondentes LCR. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1 Perfil do Certificado

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

7.1.1 Número(s) de versão

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

7.1.2 Extensões de certificado

7.1.2.1 Serasa CA I

Os certificados emitidos pela Serasa CA I têm como obrigatórias as seguintes extensões:



- "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da Serasa CA I;
- "Key Usage", crítica: somente os bits digitalSignature, dataEncipherment, nonRepudiation e keyEncipherment estão ativados;
 - "Certificate Policies", não crítica: contém o OID desta PC e o endereço Web da DPC-Serasa CA (www.certificadodigital.com.br/repositorio/serasaca/dpc);
- "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente:
(www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl).

A Serasa CA I implementa a extensão "Extended Key Usage", não crítica, contendo os valores "client authentication" (OID 1.3.6.1.5.5.7.3.2), "E-mail protection" (OID 1.3.6.1.5.5.7.3.4) e "timestamping" (OID 1.3.6.1.5.5.7.3.8).

A Serasa CA I também pode implementar a extensão "Subject Alternative Name".

A Serasa CA I implementa a sub-extensão "rfc822Name" parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do titular do certificado de pessoa jurídica e de pessoa física.

7.1.2.2 Serasa CA II

Os certificados emitidos pela Serasa CA II têm como obrigatórias as seguintes extensões:

- "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da Serasa CA II;
- "Key Usage", crítica: somente os bits digitalSignature, dataEncipherment, nonRepudiation e keyEncipherment estão ativados;
- "Certificate Policies", não crítica: contém o OID desta PC e o endereço Web da DPC-Serasa CA (www.certificadodigital.com.br/repositorio/serasaca/dpc);
- "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente:
(www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl).

A Serasa CA II implementa a extensão "Extended Key Usage", não crítica, contendo os valores "server authentication" (OID 1.3.6.1.5.5.7.3.1), "timestamping" (OID 1.3.6.1.5.5.7.3.8) ou "signing of downloadable executable code" (OID 1.3.6.1.5.5.7.3.3).

A Serasa CA II também pode implementar a extensão "Subject Alternative Name".

A Serasa CA II implementa a sub-extensão "rfc822Name" parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do titular do certificado de pessoa jurídica e de pessoa física.

7.1.2.3 Serasa CA III

Os certificados emitidos pela Serasa CA III têm como obrigatórias as seguintes extensões para certificados de AC:

- "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da Serasa CA III;
- "Subject Key Identifier", não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado;
- "Key Usage", crítica: somente os bits keyCertSign e CRLSign são ativados;
- "Certificate Policies", não crítica: o campo PolicyIdentifier contém o OID da PC que implementa;
- O campo PolicyQualifiers contém o endereço Web da DPC da Serasa CA (www.certificadodigital.com.br/repositorio/serasaca/dpc);
- "Basic Constraints", crítica: contém o campo cA=True;
- "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente ao certificado: (www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl).

A Serasa CA III implementa a extensão "Extended Key Usage", não crítica, contendo os valores "client authentication" (OID 1.3.6.1.5.5.7.3.2), "server authentication" (OID 1.3.6.1.5.5.7.3.1), "E-mail protection" (OID 1.3.6.1.5.5.7.3.4) e "timestamping" (OID 1.3.6.1.5.5.7.3.8).

A Serasa CA III implementa a sub-extensão "rfc822Name" parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do titular do certificado de pessoa jurídica e de pessoa física.

7.1.2.4 Serasa CA IV

Os certificados emitidos pela Serasa CA IV têm como obrigatórias as seguintes extensões para certificados de AC:

- "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da Serasa CA IV;
- "Subject Key Identifier", não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado;
- "Key Usage", crítica: somente os bits keyCertSign e CRLSign são ativados;
- "Certificate Policies", não crítica: o campo PolicyIdentifier contém o OID da PC que implementa;
- O campo PolicyQualifiers contém o endereço Web da DPC da Serasa CA (www.certificadodigital.com.br/repositorio/serasaca/dpc);
- "Basic Constraints", crítica: contém o campo cA=True;
- "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente ao certificado: (www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIV.crl).

A Serasa CA IV implementa a extensão "Extended Key Usage", não crítica, contendo os valores "client authentication" (OID 1.3.6.1.5.5.7.3.2), "server authentication" (OID 1.3.6.1.5.5.7.3.1), "E-mail protection" (OID 1.3.6.1.5.5.7.3.4) e "timestamping" (OID 1.3.6.1.5.5.7.3.8).



A Serasa CA IV implementa a sub-extensão "rfc822Name" parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do titular do certificado de pessoa jurídica e de pessoa física.

7.1.3 Identificadores de algoritmo

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

7.1.4 Formatos de nome

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

7.1.5 Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pelas Serasa CA são as seguintes:

- não são utilizados sinais de acentuação, tremas ou cedilhas;
- além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Caractere	Código NBR9611 (hexadecimal)
Branco		20
(28
)		29
-		2D
.		2E
/		2F

Tabela 1 - Caracteres especiais admitidos em nomes

7.1.6 OID (Object Identifier) de DPC

O OID desta DPC é xxxxxxxxxxxxxxxx

7.1.7 Uso da extensão "Policy Constraints"

Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política



O campo policyQualifiers da extensão "Certificate Policies" contém o endereço Web da DPC Serasa CA (www.certificadodigital.com.br/repositorio/serasaca/dpc).

7.1.9 Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 2459.

7.2 Perfil de LCR

7.2.1 Número(s) de versão

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

7.2.2 Extensões de LCR e de suas entradas

As LCR da Serasa CA contém as seguintes extensões para certificados de AC:

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

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 Procedimentos de mudança de especificação.

Esta DPC é atualizada sempre que uma nova PC for implementada pela Serasa CA o exigir.

8.2 Políticas de publicação e notificação

Esta DPC está disponível para a comunidade no endereço web <http://www.certificadodigital.com.br/repositorio/serasaca>

8.3 Procedimentos de aprovação

Esta DPC foi submetida à aprovação da Microsoft , durante o processo de criação da Serasa CA.