Declaração de Práticas de Prestador de Serviço de Confiança - SERASA

Versão 2.0

28 de janeiro de 2021

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução 132, de 10.11.2017 (Versão 1.0)	-	Criação do DOC-ICP-17.
Resolução 180 de 22.10.2020.	4.4.1.	Tempo de armazenamento das informações do PSC;

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento faz parte de um conjunto de normativos criado para regulamentar os Prestadores de Serviço de Confiança de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas, referenciados neste documento como Prestadores de Serviço de Confiança - PSC, no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1.2. O Prestador de Serviço de Confiança Serasa – PSC SERASA da ICP-Brasil é uma entidade credenciada, auditada e fiscalizada pelo Instituto Nacional de Tecnologia da Informação - ITI que provê serviços de armazenamento de chaves privadas para usuários finais, nos termos do DOC-ICP-04 [11].

1.1.3. A utilização de Prestadores de Serviços de Confiança para estes serviços elencados é facultativa. Chaves privadas dos usuários finais armazenados em dispositivos normatizados conforme estabelecido no DOC-ICP-04 [11] e assinaturas digitais padrão ICP-Brasil feitas pela chave do usuário em outros sistemas são válidas conforme ditame legal da ICP-Brasil.

1.1.4. Este documento estabelece os requisitos mínimos a serem obrigatoriamente observados pelo PSC SERASA integrante da ICP-Brasil na elaboração de suas Declarações de Práticas de Prestador de Serviço de Confiança – DPPSC. A DPPSC é o documento que descreve as práticas e os procedimentos operacionais e técnicos empregados pelo PSC SERASA na execução de seus serviços. Não obstante, as ACs devem observar a mudança na respectiva DPPSC e DPC caso utilize para armazenamento de chaves dos seus usuários finais o modelo PSC SERASA (ciclo de vida do certificado – descrição dos procedimentos de armazenamento).

1.1.5. Este documento tem como base as normas da ICP-Brasil, as RFC 4210, 4211, 3628, 3447 3161 do IETF, Regulation (EU) 910/2014 e o documento TS 101 861 do ETSI.

1.1.6. A DPPSC SERASA, elaborada no âmbito da ICP-Brasil, adota a mesma estrutura empregada no DOC-ICP-17. Versão 2.0 [12]

1.1.7. Aplicam-se ainda à PSC SERASA da ICP-Brasil, no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil.

1.1.8. Esta DPPSC está baseada na Internet Engineering Task Force (IETF) RFC 3647, podendo sofrer atualizações regulares.

1.2. Identificação

Esta é a “Declaração de Práticas de Prestador de Serviço de Confiança SERASA”, integrante da ICP-BRASIL e comumente referida como “DPPSC SERASA”. – **OID 2.16.76.1.11.4.**

1.3. Comunidade e Aplicabilidade

1.3.1. Prestadores de Serviço de Confiança

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

1.3.1.1. Os serviços prestados pelo PSC SERASA estão publicados e disponíveis em: https://serasa.certificadodigital.com.br/repositorio/psc-serasa/

1.3.1.2. O PSC SERASA é uma entidade utilizada para desempenhar atividade descrita nesta DPPSC e em regulamento editado por instrução normativa da AC Raiz que defina os procedimentos operacionais mínimos para os prestadores de serviço de confiança da ICP-Brasil, assim como nos adendos - ADE-ICP relacionados, e se classificam em três categorias, conforme o tipo de atividade prestada:

a) armazenamento de chaves privadas dos subscritores;

b) serviço de assinatura digital, verificação da assinatura digital; ou

c) ambos.

1.3.1.3. O PSC SERASA mantém as informações acima sempre atualizadas.

1.3.2. Subscritores

1.3.2.1. Podem utilizar os serviços descritos nesta DPPSC as pessoas físicas e jurídicas de direito público ou privado, nacionais ou internacionais, que atendam aos requisitos deste documento.

1.3.2.2. Os subscritores deverão manifestar plena aprovação aos serviços contratados pelo PSC, assim como o nível de acompanhamento que o PSC deverá informar, para fins exclusivos de proteção da chave privada do titular, seja na prestação de armazenamento das chaves privadas.

1.3.2.3. Os subscritores terão acesso, quando do uso do serviço de assinatura do PSC, por meio do ambiente do usuário, no mínimo, das 10 (dez) últimas assinaturas digitais realizadas.

Nota 1: Os subscritores poderão solicitar a desvinculação das suas chaves ao PSC de armazenamento de chaves criptográficas ao seu critério, em conformidade com os procedimentos de portabilidade dispostos em regulamento editado por instrução normativa da AC Raiz que defina os procedimentos operacionais mínimos para os prestadores de serviço de confiança da ICP-Brasil.

1.3.3. Aplicabilidade

As aplicações para as quais são adequados os certificados e, quando cabíveis as aplicações para as quais existem restrições ou proibições para o uso deste certificado, estão relacionadas na Política de Certificado Correspondente.

1.4. Dados de Contato

A DPPSC SERASA é administrada pela Unidade de Negócio de Certificação Digital da Serasa S/A, situada à Alameda dos Quinimuras, nº 187, Planalto Paulista, São Paulo, SP, CEP 04068-900.
Pessoa para Contato: Giseli Mioti
(11) 2608-5023
arcompliance@br.experian.com

1.5. Procedimentos de mudança de especificação

Qualquer alteração realizada na DPPSC SERASA será submetida à aprovação da AC-Raiz.
A DPPSC SERASA será atualizada sempre que um novo serviço implementado pelo PSC SERASA o exigir.

1.5.1. Políticas de publicação e notificação

Esta DPPSC está publicada no repositório do PSC SERASA, no seguinte endereço:
https://serasa.certificadodigital.com.br/repositorio/psc-serasa/

1.5.2. Procedimentos de aprovação

A presente DPPSC foi aprovada pela AC Raiz durante o processo de credenciamento do PSC SERASA, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

1.6. Definições e Acrônimos

Neste item devem ser descritas todas as definições e acrônimos contidos no documento.

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
CG	Comitê Gestor da ICP-Brasil
CMM-SEI	Capability Maturity Model do Software Engineering Institute
DMZ	Zona Desmilitarizada
DPC	Declarações de Práticas de Certificação
DPPSC	Declarações de Práticas dos Prestadores de Serviço de Confiança
EAT	Entidade de Auditoria do Tempo
HSM	Hardware Security Module
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IETF	Internet Engineering Task Force
ITI	Instituto Nacional de Tecnologia da Informação
NBR	Norma Brasileira
PC	Política de certificado
PCO	Plano de Capacidade Operacional
PCN	Plano de Continuidade do Negócio
PSC	Prestador de Serviço de Confiança
RFC	Request For Comments
TSDM	Trusted Software Development Methodology
UTC	Universal Time Coordinated

2. RESPONSABILIDADE DO REPOSITÓRIO E PUBLICAÇÃO

2.1. Publicação

2.1.1. Publicação de informação do PSC SERASA

2.1.1.1. O PSC SERASA, responsável pela DPPSC SERASA, disponibiliza em site as informações referentes ao serviço de PSC.

2.1.1.2. As seguintes informações, no mínimo, estão publicadas pelo PSC SERASA em página web:

a) capacidade de armazenamento das chaves privadas dos subscritores que opera;
b) DPPSC SERASA;

c) os serviços implementados;
d) as condições gerais mediante as quais são prestados os serviços de armazenamento de chaves privadas;
e) se pretende continuar a prestar o serviço ou se está mediante a qualquer fiscalização dos serviços, se for o caso.

2.1.2. Frequência de publicação

Todos os itens citados no item 2.1.1. terão sua publicação atualizada no repositório do PSC SERASA sempre que houver alteração no conteúdo destes.

2.1.3. Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPPSC. Acessos para escrita nos locais de armazenamento e publicação são permitidos apenas às pessoas responsáveis designadas especificamente para este fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

3. IDENTIFICAÇÃO E AUTORIZAÇÃO

A identificação e a autorização para utilização do serviço deve seguir os critérios estabelecidos na Declaração de Práticas e na Política de Certificado da Autoridade Certificadora autorizada pelo PSC SERASA.

4. REQUISITOS OPERACIONAIS

4.1. Armazenamento e acesso às chaves privadas do subscritor

O armazenamento e acesso aos certificados digitais pelas aplicações do subscritor utiliza:

a) linguagem de programação utilizada para construção da plataforma de acesso: Java
b) meios de acesso disponibilizados ao subscritor:
   i. aplicativos para dispositivos móveis, para PC, páginas web, entre outros;
   ii. aplicativo Desktop;
   iii. páginas web para gestão de certificados.
c) as autenticações trafegam em canal seguro (túnel TLS) e as interações entre serviços do subscritor e O PSC SERASA ocorrem mediante autenticação;
d) arquitetura de rede da aplicação de acesso segue o modelo TCP/IP.

4.2. Serviço de criação e validação de assinaturas digitais

NÃO SE APLICA

4.3. Procedimentos de Auditoria de Segurança

Nos itens seguintes da DPPSC SERASA estão descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pelo PSC SERASA com o objetivo de manter um ambiente seguro.

4.3.1. Tipos de eventos registrados

4.3.1.1. O PSC SERASA pela DPPSC SERASA registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos estão obrigatoriamente incluídos em arquivos de auditoria:

a) Iniciação e desligamento dos sistemas de PSC SERASA;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores do PSC SERASA;
c) mudanças na configuração dos sistemas de PSC SERASA;
d) tentativas de acesso (login) e de saída do sistema (logoff);
e) tentativas não-autorizadas de acesso aos arquivos de sistema;
f) registros de armazenamentos das chaves privadas e/ou certificados digitais;
g) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas;

h) operações falhas de escrita ou leitura, quando aplicável;
i) todos os eventos relacionados à sincronização com a fonte confiável de tempo;
j) registros de acesso ou tentativas de acesso à chave privada do subscritor.

4.3.1.2. O PSC SERASA pela DPPSC SERASA registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema, tais como:

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

4.3.1.3. O PSC SERASA registra as seguintes informações:

a) Criação e remoção de slot;
b) Criação e remoção de chave;
c) Geração de CSR;
d) Uso da chave;
e) Inventário das chaves.

4.3.1.4. Todos os registros de auditoria contêm a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos contém o horário UTC. Registros manuais em papel podem conter a hora local desde que especificado o local.

4.3.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada está armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

4.3.2. Frequência de auditoria de registros (logs)

Os registros de auditoria do PSC SERASA são analisados em, no máximo, 1 (uma) semana pela área de operação do PSC SERASA. Todos os eventos significativos serão explicados em relatório de auditoria de registros. A análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.3.3. Período de retenção para registros (logs) de auditoria

O PSC SERASA mantém localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, esses registros serão armazenados conforme disposto no item 4.5

4.3.4. Proteção de registro (log) de auditoria

4.3.4.1. Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da Política de Segurança da ICP-Brasil.

4.3.4.2. As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da Política de Segurança da ICP-Brasil.

4.3.4.3. Os mecanismos de proteção descritos neste item obedecem à POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

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

O PSC SERASA executa procedimentos de backup, de toda a solução de duas formas (Sistema Operacional + Aplicação + Banco de Dados):

a) Diariamente – Cópia de segurança;
b) Semanalmente – Cópia Armazenada para processos de auditoria.

4.3.6. Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é uma combinação de processos automatizados e manuais executados pelo sistema operacional. Pelo sistema do PSC, pelo sistema de controle de acesso e pelo pessoal operacional. Segue abaixo a localização dos recursos:

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de *log-in* e *log-out*	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional
Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados	Automático	AC ou Software de PSC
Logs de *Backup* e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de *software* e *hardware*	Manual	Pessoal de operações
Manutenção de sistema	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	Software de controle de acesso e pessoal de operações

4.3.7. Notificação de agentes causadores de eventos

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

4.3.8. Avaliações de vulnerabilidade

Eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria do PSC SERASA, serão analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes deverão ser implementadas pelo PSC SERASA e registradas para fins de auditoria.

4.4. Arquivamento de Registros

Nos itens seguintes da DPPSC SERASA é descrita a política geral de arquivamento de registros, para uso futuro, implementada pelo PSC SERASA.

4.4.1. Tipos de registros arquivados

São arquivados pelo PSC SERASA os tipos de registros abaixo, que compreendem, entre outros:

a) notificações de comprometimento de chaves privadas dos subscritores por qualquer motivo;
b) notificações de comprometimento de arquivos armazenados dos subscritores por qualquer motivo;
c) informações de auditoria previstas neste item.

O período de retenção para cada registro arquivado, observando que os registros de armazenamento de chaves privadas e/ou certificados digitais, inclusive arquivos de auditoria, é retido por, no mínimo, 7 (sete) anos.

4.4.2. Proteção de arquivo

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

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

4.4.3.1. A DPPSC SERASA estabelece que uma segunda cópia de todo o material arquivado deverá ser armazenada em ambiente diferente às instalações principais do PSC SERASA, recebendo o mesmo tipo de proteção utilizada por ele no arquivo principal.

4.4.3.2. As cópias de segurança deverão seguir os períodos de retenção definidos para os registros dos quais são cópias.

4.4.3.3. O PSC SERASA pela DPPSC SERASA deverá verificar a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.4.4. Requisitos para datação de registros

Os servidores do PSC SERASA são sincronizados com hora fornecida pela AC RAIZ por meio de sua fonte confiável do Tempo – FCT conforme DOC-ICP-07[13]. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por estes equipamentos.
No caso dos registros feitos manualmente, estes contem a Hora Oficial do Brasil.

4.4.5. Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pelo PSC SERASA em seus procedimentos operacionais são automatizados e manuais e internos.

4.4.6. Procedimentos para obter e verificar informação de arquivo

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

4.5. Liberação do espaço do subscritor

A liberação do espaço do subscritor se dará mediante consulta ao status de validade ou revogação do certificado digital.

4.6. Comprometimento e Recuperação de Desastre

4.6.1. Disposições Gerais

4.6.1.1. Nos itens seguintes da DPPSC SERASA são descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no Plano de Continuidade de Negócios (PCN) do PSC SERASA, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], para garantir a continuidade dos seus serviços críticos.

4.6.1.2. O PSC SERASA assegura, no caso de comprometimento de sua operação por qualquer um dos

motivos relacionados nos itens abaixo, que as informações relevantes sejam disponibilizadas aos subscritores e às terceiras partes. O PSC SERASA disponibiliza a todos os subscritores e terceiras partes uma descrição do comprometimento ocorrido.

4.6.1.3. No caso de comprometimento de uma operação de armazenamento e acesso das chaves de um ou mais subscritores, o PSC SERASA não deverá mais prover esse serviço, até serem tomadas as medidas administrativas pela AC Raiz, informando aos subscritores sobre o problema e devidos encaminhamentos que estes deverão tomar.

4.6.1.4. Não se aplica.

4.6.2. Recursos computacionais, software, e dados corrompidos

O PSC SERASA possui um PCN que especifica as ações a serem tomadas no caso em que recursos computacionais, softwares ou dados são corrompidos, e que podem ser resumidas da seguinte forma:

a) É feita a identificação de todos os elementos corrompidos;
b) O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
c) É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas.

4.6.3. Sincronismo do PSC SERASA

Os servidores são sincronizados com a Fonte Confiável de Tempo da AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário da Fonte Confiável de Tempo da AC Raiz.

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

O PSC SERASA possui um Plano de Continuidade de Negócio que detalha todas as possíveis ações.

4.7. Extinção dos serviços de PSC SERASA

4.7.1. Observado o disposto no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5], este item da DPPSC SERASA descreve os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços do PSC SERASA.

4.7.2. O PSC SERASA assegura que possíveis rompimentos com os subscritores e terceiras partes, em consequência da cessação dos serviços de armazenamento das chaves privadas, sejam minimizados e, em particular, assegurar a manutenção continuada da informação necessária para que não haja prejuízos aos subscritores e as terceiras partes.

4.7.3. Antes de o PSC SERASA cessar seus serviços os seguintes procedimentos serão executados, no mínimo:

a) o PSC SERASA disponibilizará a todos os subscritores e partes receptoras informações a respeito de sua extinção;
b) o PSC SERASA transferirá a outro PSC, após aprovação da AC-Raiz, as obrigações relativas à manutenção do armazenamento das chaves, certificados e documentos assinados, se for o caso, e de auditoria necessários para demonstrar a operação correta do PSC SERASA, por um período razoável;
c) o PSC SERASA manterá ou transferirá a outro PSC, após aprovação da AC-Raiz, suas obrigações relativas a disponibilizar seus sistemas e hardwares, por um período razoável;
d) o PSC SERASA notificará todas as entidades afetadas.

4.7.4. O PSC SERASA providenciará os meios para cobrir os custos de cumprimento destes requisitos mínimos no caso de falência ou se por outros motivos se ver incapaz de arcar com os seus custos.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes são descritos os controles de segurança implementados pelo PSC SERASA pela DPPSC SERASA para executar de modo seguro suas funções, de acordo com o REGULAMENTO OPERACIONAL DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL - DOC-ICP-17.01 [10].

5.1. Segurança Física

Nos itens seguintes da DPPSC SERASA estão descritos os controles físicos referentes às instalações que abrigam os sistemas do PSC SERASA.

5.1.1. Construção e localização das instalações do PSC SERASA

A construção das instalações do PSC SERASA, relevantes para os controles de segurança física, foram executadas por técnicos especializados, compreendendo entre outros:

a) 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;
b) Instalações para sistemas de telecomunicações;
c) Sistemas de aterramento e de proteção contra descargas atmosféricas; e
d) Iluminação de emergência.

5.1.2. Acesso físico nas instalações do PSC SERASA

O PSC SERASA possui sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a POLÍTICA DE SEGURANÇA DA ICP- BRASIL [4] e os requisitos que seguem.

5.1.2.1. Níveis de acesso

5.1.2.1.1. O PSC SERASA definiu 4 (quatro) níveis de acesso físico aos diversos ambientes do PSC Serasa.

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações do PSC Serasa. O ambiente de nível 1 do PSC Serasa na ICP-Brasil desempenha a função de interface com cliente ou fornecedores que necessitam comparecer ao PSC Serasa.

5.1.2.1.3. O segundo nível – ou nível 2 – é interno ao primeiro e requerer a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo do PSC. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá.

a) O ambiente de nível 2 é separado do nível 1 por paredes divisórias de escritório, alvenaria ou pré-moldadas de gesso acartonado. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso;

b) O acesso à este nível será permitido apenas a pessoas que trabalhem diretamente com as atividades de serviços de armazenamento dos certificados para usuários finais e serviços de assinatura digital e verificação da assinatura digital ou ao pessoal responsável pela manutenção de sistemas e equipamentos do PSC, como administradores de rede e técnicos de suporte de informática. Demais funcionários do PSC ou do possível ambiente que esta compartilhe não deverão acessar este nível;

c) Preferentemente, nobreaks, geradores e outros componentes da infraestrutura física deverão estar abrigados neste nível, para evitar acessos ao ambiente de nível 3 por parte de prestadores de serviços

de manutenção;

d) Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações do PSC, a partir do nível 2. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e sob supervisão.

5.1.2.1.4. O terceiro nível – ou nível 3 – deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação do PSC. Qualquer atividade relativa ao armazenamento de certificados digitais dos usuários e serviços de assinatura digital e verificação da assinatura digital deverá ser realizada nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível.

a) No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. São utilizados dois tipos de mecanismos de controle para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica ou digitação de senha;

b) As paredes que delimitam o ambiente de nível são de alvenaria ou material de resistência equivalente ou superior. Não há janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso;
c) Caso o ambiente de Nível 3 possua forro ou piso falsos, deverão ser adotados recursos para impedir o acesso ao ambiente por meio desses, tais como grades de ferro estendendose das paredes até as lajes de concreto superior e inferior;

d) Há uma porta única de acesso ao ambiente de nível 3, que abre somente depois que o funcionário tenha se autenticado eletronicamente no sistema de controle de acesso. A porta deverá ser dotada de dobradiças que permitam a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário;

5.1.2.1.5. O terceiro nível avançado – ou nível 3.1 –, especificamente para os PSC de assinatura digital, no interior ao ambiente de nível 3, deverá compreender pelo menos um gabinete reforçado trancado, que abrigará todo o hardware e software utilizado pelo PSC de assinatura digital:

a) Para garantir a segurança do material armazenado, os gabinetes deverão obedecer às seguintes especificações mínimas: i. Ser feitos em aço ou material de resistência equivalente; ii.Possuir tranca com chave.

5.1.2.1.6. O quarto nível – ou nível 4 – especificamente para os PSC de armazenamento de chaves privadas, interior ao terceiro, é onde deverão ocorrer atividades especialmente sensíveis da operação do PSC de armazenamento de chaves privadas. Todos os sistemas e equipamentos necessários a essas atividades deverão estar localizados a partir desse nível. O nível 4 deverá possuir os mesmos controles de acesso do nível 3 e, adicionalmente, deverá exigir, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas deverá ser exigida enquanto o ambiente estiver ocupado.

5.1.2.1.7. No quarto nível, todas as paredes, piso e teto deverão ser revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto deverão ser inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não deverão permitir a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - deverão possuir proteção contra interferência eletromagnética externa.

5.1.2.1.8. As salas-cofre deverão ser construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

5.1.2.1.9. Poderão existir, no PSC, vários ambientes de terceiro nível avançado, no caso de PSC de assinatura digital, ou vários ambientes de quarto nível, no caso de PSC de armazenamento de chaves privadas, para abrigar e segregar, quando for o caso:

a) Equipamentos de produção on-line; e

b) Equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

5.1.2.1.10. Todos os servidores e elementos de infraestrutura e proteção do segmento de rede, tais como roteadores, hubs, switches e firewalls devem: a) Operar em ambiente com segurança equivalente, no mínimo, no terceiro nível avançado para o caso de PSC de assinatura digital, ou no quarto nível, no caso de PSC de armazenamento de chaves privadas citados neste documento; b) Possuir acesso lógico restrito por meio de sistema de autenticação e autorização de acesso.

5.1.2.1.11. Os PSC devem ainda atender aos seguintes requisitos:

a) O ambiente físico do PSC deverá conter dispositivos que autentiquem e registrem o acesso de pessoas informando data e hora desses acessos;
b) O PSC deverá conter imagens que garantam a identificação de pessoas quando do acesso físico em qualquer parte de seu ambiente;
c) É mandatório o sincronismo de data e hora entre os mecanismos de segurança física garantindo a trilha de auditoria entre dispositivos de controle de acesso físico e de imagem;
d) Todos que transitam no ambiente físico do PSC deverão portar crachás de identificação, inclusive os visitantes;
e) Só é permitido o trânsito de material de terceiros pelos ambientes físicos do PSC mediante registro, garantindo a trilha de auditoria com informações de onde o material passou, a data e hora que ocorreu o trânsito e quem foi o responsável por sua manipulação;
f) O PSC deverá conter dispositivos de prevenção e controle de incêndios, temperatura, umidade, iluminação e oscilação na corrente elétrica em todo seu ambiente físico;
g) Todo material crítico inservível, descartável ou não mais utilizável deverá ter tratamento especial de destruição, garantindo o sigilo das informações lá contidas. O equipamento enviado para manutenção deverá ter seus dados apagados, de forma irreversível, antes de ser retirado do ambiente físico do PSC;
h) Os computadores pessoais, servidores e dispositivos de rede, e seus respectivos softwares, deverão estar inventariados com informações que permitam a identificação inequívoca;
i) Em caso de inoperância dos sistemas automáticos, o controle de acesso físico deverá ser realizado provisoriamente por meio de um livro de registro onde constará quem acessou, a data, hora e o motivo do acesso;
j) Deverão ser providenciados mecanismos para garantir a continuidade do fornecimento de energia nas áreas críticas, mantendo os ativos críticos de informação em funcionamento até que todos os processos e dados sejam assegurados caso o fornecimento de emergência se esgote;
l) No caso de armazenamento de chaves privadas para usuários finais, deve ter no mínimo dois ambientes físicos, sendo obrigatoriamente um para operação e outro para contingência;
m) No caso do PSC ser uma AC da ICP-Brasil, pode ser utilizado o nível 4 para abrigo do hardware criptográfico que armazenará as chaves privadas dos usuários finais, assim como os serviços de autenticação, desde que em gabinete cadeado, cuja chave do cadeado deve estar em posse de funcionário distinto dos perfis lógicos do PSC, segregados dos que operam o ambiente de uma AC;
n) Todos os equipamentos e ambiente computacional que serão utilizados no PSC deverão ter sua data e horário sincronizados com a EAT.

5.1.2.2. Sistemas físicos de detecção

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

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

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

5.1.2.2.4. Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não é satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais

empregados, o critério mínimo de ocupação deixa de ser satisfeito, ocorre a reativação automática dos sensores de presença.

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

5.1.2.2.6. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados por guarda, armado, e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda

5.1.2.3. Sistema de controle de acesso

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

5.1.3. Energia e ar-condicionado do ambiente de nível 3 do PSC SERASA

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

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

5.1.3.3. Foram 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.

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

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

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

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

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

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

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

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

5.1.4. Exposição à água nas instalações do PSC SERASA

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

5.1.5. Prevenção e proteção contra incêndio nas instalações do PSC SERASA

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

5.1.5.2. Nas instalações DO PSC SERASA não é permitido fumar ou portar objetos que produzam fogo ou faísca.

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

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

5.1.6. Armazenamento de mídia nas instalações do PSC SERASA

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

5.1.7. Destruição de lixo nas instalações do PSC SERASA

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

5.1.7.2. 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. Sala externa de arquivos (off-site) para o PSC SERASA

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

5.2. Controles Procedimentais

Nos itens seguintes da DPPSC SERASA descreve os requisitos para a caracterização e o reconhecimento de perfis qualificados no PSC SERASA, com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

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

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

5.2.1.3. Todos os operadores do sistema de certificação DO PSC SERASA recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, assinado pelo operador no momento da contratação com base nas necessidades de cada perfil.

5.2.1.4. Quando um empregado se desligar da PSC SERASA, suas permissões de acesso são

revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da PSC SERASA, suas permissões de acesso são revistas. Há uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deve devolver ao PSC no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

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

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado DO PSC SERASA tem sua identidade e perfil verificados antes de:

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

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

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

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

5.3. Controles de Pessoal

Todos os empregados da PSC SERASA e dos PSS encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

a) os termos e as condições do perfil que ocuparão;
b) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
c) o compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

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

5.3.2. Procedimentos de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal DO PSC SERASA envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido a:

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

5.3.2.2. Não se aplica.

5.3.3. Requisitos de treinamento

Todo o pessoal DO PSC SERASA envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e tecnologias dos sistemas e hardwares de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais em uso no PSC;
b) ICP-Brasil;
c) Princípios e tecnologias de certificação digital e de assinaturas digitais;
d) Princípios e mecanismos de segurança de redes e segurança do PSC;
e) Procedimentos de recuperação de desastres e de continuidade do negócio;
f) Familiaridade com procedimentos de segurança, para pessoas com responsabilidade de Oficial de Segurança;
g) Familiaridade com procedimentos de auditorias em sistemas de informática, para pessoas com responsabilidade de Auditores de Sistema;
h) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal DO PSC SERASA 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 DO PSC SERASA.

5.3.5. Frequência e sequência de rodízio de cargos
O PSC SERASA possuem pessoal e efetivo de contingência devidamente treinado, não fazendo uso de rodízio de pessoal.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional DO PSC SERASA, O PSC SERASA suspenderá, de imediato, o acesso dessa pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis

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

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

5.3.6.3. Concluído o processo administrativo, O PSC SERASA encaminha suas conclusões à AC Raiz.

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

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

5.3.7. Requisitos para contratação de pessoal

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

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. O PSC SERASA torna disponível para todo o seu pessoal:

a) Sua DPPSC-Serasa;
b) A Política de Segurança da ICP-BRASIL [8]
c) Documentação operacional relativa a suas atividades;
d) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação fornecida ao pessoal é classificada segundo a política de classificação de informação definida pelo PSC SERASA e é mantida atualizada

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPPSC SERASA define as medidas de segurança implantadas pelo PSC SERASA para proteger as chaves privadas dos subscritores.

6.1. Controles de Segurança Computacional

6.1.1. Disposições Gerais

Neste item, a DPPSC SERASA indica os mecanismos utilizados para prover a segurança de suas estações de trabalho, servidores e demais sistemas e equipamentos, observado o disposto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.1.2. Requisitos técnicos específicos de segurança computacional

6.1.2.1. A DPPSC SERASA prevê que os sistemas e os equipamentos do PSC SERASA, usados nos processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverão implementar, entre outras, as seguintes características:

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

6.1.2.2. Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de gerenciamento do carimbo do tempo e com mecanismos de segurança física.

6.1.2.3. Qualquer equipamento, ou parte desse, ao ser enviado para manutenção terão apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações do PSC SERASA, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, observados os dispostos no ato de descredenciamento, deverão ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade do PSC SERASA. Todos esses eventos deverão ser registrados para fins de auditoria.

6.1.2.4. Qualquer equipamento incorporado ao PSC SERASA será preparado e configurado como previsto na PS implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.1.3. Classificação da segurança computacional

Não se aplica.

6.2. Controles Técnicos do Ciclo de Vida

Nos itens seguintes da DPPSC SERASA descreve s, quando aplicáveis, os controles implementados pelo PSC SERASA no desenvolvimento de sistemas e no gerenciamento de segurança.

6.2.1. Controles de desenvolvimento de sistema

6.2.1.1. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluídos os testes é colocado em um ambiente de homologação. Finalizado o processo de homologação das customizações, será avaliado e decidido quando ser a implementação no ambiente de produção.

6.2.1.2. Os processo de projeto e desenvolvimento conduzidos pelo PSC SERASA provem documentação suficiente para suportar avaliações externas de segurança dos componentes do PSC SERASA.

6.2.2. Controles de gerenciamento de segurança

6.2.2.1. Neste item da DPPSC SERASA são descritas as ferramentas e os procedimentos empregados pelo PSC SERASA para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

6.2.2.2. Uma metodologia formal de gerenciamento de configuração deverá ser usada para a instalação e a contínua manutenção do sistema do PSC SERASA.

6.2.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.3. Controles de Segurança de Rede

6.3.1. Diretrizes Gerais

6.3.1.1. Neste item estão descritos os controles relativos à segurança da rede do PSC SERASA, incluindo firewall e recursos similares, observado o disposto da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.3.1.2. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como: roteadores, hubs, switches, firewall e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda os sistemas do PSC, estão localizados e operar em ambiente de, no mínimo, nível 3.

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

6.3.1.4. O acesso lógico aos elementos de infraestrutura 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.

6.3.1.5. O acesso à Internet é provido por no mínimo duas linhas de comunicação de sistemas autônomos (AS) distintos.

6.3.1.6. O acesso via rede aos sistemas do PSC é permitido somente para os seguintes serviços:

a) Não aplicável;
b) Pelo PSC, para a administração dos sistemas de gestão a partir de equipamento conectado por rede interna.
c) pelo subscritor, para a armazenamento e acesso à chave privada.

6.3.2. Firewall

6.3.2.1. Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Os firewalls são dispostos e configurados de forma a promover 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 ao PSC.

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

6.3.2.3. O Administrador de Segurança verifica periodicamente as regras dos firewalls, para assegurar-se que apenas o acesso aos serviços realmente necessários é permitido e que está bloqueado o acesso a portas desnecessárias ou não utilizadas.

6.3.3. Sistema de detecção de intrusão (IDS)

6.3.3.1. O sistema de detecção de intrusão tem capacidade de ser configurado para reconhecer ataques em tempo real e respondê-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 ao firewall ou ao terminal de gerenciamento, promover a desconexão automá tica de conexões suspeitas, ou ainda a reconfiguração do firewall.

6.3.3.2. 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.

6.3.3.3. O sistema de detecção de intrusão prove o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.3.4. 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, que poderá ser automatizada. A frequência de exame dos arquivos de registro é, no mínimo, semanal e todas as ações tomadas em decorrência desse exame são documentadas.

6.3.5. Outros controles de segurança de rede

6.3.5.1. O PSC SERASA implementa serviço de proxy, restringindo o acesso, a partir de todas suas estações de trabalho, a serviços que não possam comprometer a segurança do ambiente do PSC.

6.3.5.2. As estações de trabalho e servidores estão dotadas de antivírus, antispyware e de outras ferramentas de proteção contra ameaças provindas da rede a que estão ligadas.

6.4. Controles de Engenharia do Módulo Criptográfico

Os módulos criptográficos utilizados pelo PSC SERASA adotam o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

7. POLÍTICAS DE ASSINATURA

Não se aplica.

8. AUDITORIAS E AVALIAÇÕES DE CONFORMIDADE

8.1. Fiscalização e Auditoria de Conformidade

8.1.1 As fiscalizações e auditorias realizadas no PSC SERASA têm por objetivo verificar se seus processos, procedimentos e atividades estão em conformidade com suas respectivas DPPSC, PCO e PS, demais normas e procedimentos estabelecidos pela ICP - Brasil e com os princípios e critérios definidos pelo WebTrust.

8.1.2 As fiscalizações do PSC SERASA são realizadas pela AC -Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7].

8.1.3 As auditorias dos PSC SERASA são realizadas:

a) Quanto aos procedimentos operacionais, pela AC -Raiz, por meio de pessoal de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].
b) Não se aplica.

8.1.4 O PSC SERASA recebeu auditoria prévia da AC-Raiz para fins de credenciamento na ICP-Brasil e passa por auditoria anual, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

8.1.5 Não se aplica.

8.1.6 Não se aplica.

9. OUTROS ASSUNTOS DE CARÁTER COMERCIAL E LEGAL

9.1. Obrigações e direitos

Nos itens a seguir são descritas as obrigações gerais das entidades envolvidas. Caso haja obrigações específicas implementadas, as mesmas devem ser descritas.

9.1.1. Obrigações do PSC SERASA

Neste item são descritas as obrigações do PSC SERASA pela DPPSC SERASA:

a) operar de acordo com a sua DPPSC SERASA e com a descrição dos serviços que realiza;
b) gerenciar e assegurar a proteção das chaves privadas dos subscritores;
c) tomar as medidas cabíveis para assegurar que subscritores e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
d) monitorar e controlar a operação dos serviços fornecidos;
e) notificar ao subscritor titular da chave e certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado ou o encerramento de suas atividades;
f) publicar em sua página web sua DPPSC SERASA e as Políticas de Segurança (PS) aprovadas que implementa;
g) publicar, em sua página web, as informações definidas no item 2.1.1.2 deste documento;
h) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
i) adotar as medidas de segurança e controle previstas na DPPSC SERASA, no Plano de Capacidade Operacional (PCO) e PS que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
j) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
k) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
l) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);

m) manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de armazenamento de chaves privadas para usuários finais, com cobertura suficiente e compatível com o risco dessas atividades;

n) informar aos subscritores que contratam os seus serviços sobre coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima; e

o) informar à AC-Raiz, mensalmente, a quantidade de chaves privadas ou certificados digitais correspondentes armazenados e assinaturas realizadas e verificadas.

9.1.2. Obrigações do Subscritor

Ao contratar um serviço do PSC SERASA, se for o caso, o subscritor deve assegurar, por meio das aplicações disponibilizadas ao contratar um PSC SERASA, que o seu par de chaves e/ou certificados digitais foram corretamente armazenados.

9.1.3. Direitos da terceira parte (Relying Party)

9.1.3.1. Não se aplica.

9.1.3.2. Não se aplica.

9.1.3.3. O não exercício desses direitos não afasta a responsabilidade do PSC SERASA e do titular do certificado.

9.2. Responsabilidades

9.2.1. Responsabilidades do PSC SERASA

O PSC SERASA responde pelos danos a que der causa.

9.3. Responsabilidade Financeira

9.3.1. Indenizações devidas pela terceira parte (Relying Party)

Inexiste a responsabilidade da terceira parte (relying party) perante o PSC SERASA, exceto na hipótese de prática de ato ilícito.

9.3.2. Relações Fiduciárias

O PSC SERASA indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o subscritor for pessoa jurídica.

9.3.3. Processos Administrativos

Quaisquer processos administrativos cabíveis, relativos às operações do PSC SERASA, regido pela DPPSC SERASA, deverão seguir as legislações e textos normativos regulatórios específicos de sua atividade.

9.4. Interpretação e Execução

9.4.1. Legislação

A DPPSC Serasa está sujeita às normas e procedimentos descritos na Medida Provisória nº 2.200/2 de 24 de agosto de 2001 e, ainda, a todas as resoluções, instruções normativas, portarias e documentos principais do Comitê Gestor da ICP-Brasil. Em relação aos titulares dos certificados, a relação é regida pelo contrato firmado entre as partes.

9.4.2. Forma de interpretação e notificação

9.4.2.1. Sendo identificada a invalidade ou inaplicabilidade de um ou mais itens deste documento, somente estes deixarão de produzir efeito, não sendo as demais condições afetadas. Imediatamente o PSC SERASA reavaliará o conteúdo de todo o documento, realizando os ajustes necessários, e submeterá, em

até 30 (trinta) dias, a nova versão da DPPSC para apreciação e aprovação do Instituto Nacional de Tecnologia da Informação – ITI.

9.4.2.2. Qualquer forma de comunicação, solicitação ou notificação no tocante às práticas dispostas nesta DPPSC deverá ser realizada pelo PSC SERASA junto ao Comitê Gestor da ICP-Brasil.

9.4.3. Procedimentos de solução de disputa

9.4.3.1. Havendo qualquer tipo de conflito entre as normas estabelecidas pelo Comitê Gestor da ICP-Brasil e as condições dispostas nesta DPPSC sempre prevalecerão as normas e procedimentos estabelecidos pela ICP-Brasil. E aplicar-se-á o disposto no item 9.4.2.1. acima.

9.4.3.2. Havendo conflito prevalecerão as normas e procedimentos estabelecidos pela ICP-Brasil.

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

9.5. Tarifas de Serviço

Nos itens a seguir, estão especificadas pelo PSC SERASA pela DPPSC SERASA a política tarifária e de reembolso aplicáveis, se for o caso.

9.5.1. Tarifas de armazenamento de chaves privadas para usuários finais
A tarifa é variável conforme determinação interna do setor Comercial do PSC SERASA.

9.5.2. Não se aplica.

9.5.3. Não se aplica.

9.5.4. Outras tarifas
A tarifa é variável conforme determinação interna do setor Comercial do PSC SERASA.

9.5.5. Política de reembolso.
A tarifa é variável conforme determinação interna do setor Comercial do PSC SERASA.

9.6. Sigilo

9.6.1. Disposições Gerais

9.6.1.1. A chave privada dos subscritores serão mantidas pelo PSC SERASA, que será responsável pelo seu sigilo, mantendo trilhas de auditoria com horário e data de seu acesso disponível ao subscritor.

9.6.1.2. Não se aplica.

9.6.1.3. Não se aplica.

9.6.2. Tipos de informações sigilosas

9.6.2.1. São consideradas sigilosas todas as informações, dados, documentos, biometrias ou correlatos que forem coletadas, tratadas e/ou armazenadas pelo PSC SERASA, com exceção do previsto no item 9.3.6. abaixo.

9.6.2.2. Como princípio geral, que nenhum documento, informação ou registro fornecido pelo subscritor ao PSC SERASA será divulgado, exceto quando for estabelecido um acordo com o subscritor para sua publicação mais ampla ou nos casos previstos no item 9.6.4. abaixo.

9.6.3. Tipos de informações não sigilosas

Abaixo estão descritas as informações consideradas não sigilosas pelo PSC SERASA:

a) os certificados dos subscritores;
b) a DPPSC SERASA do PSC SERASA;
c) versões públicas de PS; e
d) a conclusão dos relatórios de auditoria.

9.6.4. Quebra de sigilo por motivos legais

O PSC SERASA reserva-se no direito de disponibilizar às autoridades, mediante cumprimento de judicial, quaisquer informações requisitadas, sejam elas classificadas como sigilosas ou não.

9.6.5. Informações a terceiros

Nenhum documento, informação, ou registro, sob a guarda do PSC SERASA serão fornecidos a terceiros, exceto quando o requerente solicite por meio de instrumento devida demente constituído e corretamente identificado.

9.6.6. Outras circunstâncias de divulgação de informação

Nenhuma outra liberação de informação, que não as expressamente descritas neste documento, é permitida.

9.7. Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual de certificados, politicas, especificações de práticas e procedimentos, nomes e chaves criptográficas, documentos gerados para o PSC SERASA de acordo com a legislação vigente pertencem e continuarão sendo propriedade da SERASA S/A.

10. DOCUMENTOS 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]	VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-11
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-13
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[4]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[5]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[6]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[8]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL	DOC-ICP-10
[10]	REGULAMENTO OPERACIONAL DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17.01
[11]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

11. REFERÊNCIAS

BRASIL, Decreto nº 4.264, de 10 de junho de 2002 - Restabelece e Modifica o Regulamento anterior.
BRASIL, Lei nº 9.933, de 20 de dezembro de 1999 - Dispõe sobre o Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (CONMETRO) e sobre o Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO).
RFC 1305, IETF - Network Time Protocol version 3.0.
RFC 2030, IETF - Simple Network Time Protocol (SNTP) version 4.0.
RFC 3647, IETF - Internet X-509 Public Key Infrastructure Certificate Policy and Certifications Practices Framework, novembro de 2003.
RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001. RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, November 2003. ETSI TS 101.861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.
ETSI TS 102.023 - v 1.1.1 Technical Specification / Policy Requirements for Time Stamping Authorities, abril de 2002.
Regulation (EU) 910/2014 - relativo à identificação eletrônica e aos serviços de confiança para as transações eletrônicas no mercado interno Europeu.