RESOLUÇÃO CG ICP-BRASIL Nº 180 DE 20 DE OUTUBRO DE 2020

Aprova a versão revisada e consolidada do documento Requisitos Mínimos para as Declarações de Práticas dos Prestadores de Serviço de Confiança da ICP-Brasil – DOC-ICP-17.

O COORDENADOR DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no uso das atribuições que lhe confere o art. 6º, §1º, inc. IV, do Regimento Interno, torna público que o COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no exercício das competências previstas no art. 4º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, em plenária por videoconferência realizada em 20 de outubro de 2020,

CONSIDERANDO a determinação estabelecida pelo Decreto nº 10.139, de 28 de novembro de 2019, para revisão e consolidação dos atos normativos inferiores a decreto, editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional,

RESOLVEU:

Art. 1º Esta Resolução aprova a versão revisada e consolidada do documento Requisitos Mínimos para as Declarações de Práticas dos Prestadores de Serviço de Confiança da ICP-Brasil.

Art. 2º Fica aprovada a versão 2.0 do documento DOC-ICP-17 – Requisitos Mínimos para as Declarações de Práticas dos Prestadores de Serviço de Confiança da ICP-Brasil, anexa a esta Resolução.

Art. 3º Fica revogada a Resolução nº 132, de 10 de novembro de 2017.

Art. 4º Esta Resolução entra em vigor em 03 de novembro de 2020.

THIAGO MEIRELLES FERNANDES PEREIRA

Assinado de forma digital por THIAGO MEIRELLES FERNANDES PEREIRA
Dados: 2020.10.21 09:18:57 -03'00'

THIAGO MEIRELLES FERNANDES PEREIRA

ANEXO

Infraestrutura de Chaves Públicas Brasileira

REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL

DOC-ICP-17

Versão 2.0

20 de outubro de 2020

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução 180, de 20.10.2020 Versão 2.0		Revisão e consolidação do DOC-ICP-17, conforme Decreto nº 10.139, de 28 de novembro de 2019.
Resolução 132, de 10.11.2017 Versão 1.0		Criação do DOC-ICP-17.

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 – PSC 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 [1], ou serviços de assinaturas e verificações de assinaturas digitais padrão ICP-Brasil nos documentos e transações eletrônicas ou ambos.

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 [1] 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 pelos PSCs integrantes 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 na execução de seus serviços. Não obstante, as ACs devem observar a mudança na respectiva DPC e PC caso utilizem para armazenamento de chaves dos seus usuários finais o modelo PSC (ciclo de vida do certificado – descrição dos procedimentos de armazenamento).

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

1.1.6. Toda DPPSC elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.

1.1.7. Aplicam-se ainda aos PSCs 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

Neste item deve ser identificada a DPPSC.

1.3. Comunidade e Aplicabilidade

1.3.1. Prestadores de Serviço de Confiança

Neste item deve ser identificado o PSC integrante da ICP-Brasil a que se refere esta DPPSC.

1.3.1.1. Neste item deve ser identificado o endereço da página web (URL) onde estão publicados os serviços prestados pelo PSC.

1.3.1.2. PSC são entidades utilizadas 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; ou
b) serviço de assinatura digital, verificação da assinatura digital; ou
c) ambos.

1.3.1.3. O PSC deverá manter as informações acima sempre atualizadas.

1.3.2. Subscritores

1.3.2.1 Neste item devem ser caracterizadas as pessoas físicas ou jurídicas que poderão solicitar os serviços descritos nesta DPPSC.

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, serviços de assinaturas digitais e verificação das assinaturas digitais e, por ventura, no armazenamento de documentos assinados, neste último caso conforme legislação vigente.

1.3.2.3 Os subscritores deverão ter 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

Este item da DPPSC deve relacionar e identificar os serviços prestados pelo PSC que definem como cada um desses autorizados devem ser utilizados pela comunidade. Nas descrições estarão relacionadas as aplicações para as quais a comunidade fará uso dos serviços.

1.4. Dados de Contato

Neste item devem ser incluídos o nome, o endereço e outras informações da PSC responsável pela DPPSC. Devem ser também informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5. Procedimentos de mudança de especificação

Neste item devem ser descritos a política e os procedimentos utilizados para realizar alterações na DPPSC. Qualquer alteração na DPPSC deverá ser submetida à aprovação da AC Raiz.

A DPPSC deverá ser atualizada sempre que um novo serviço for implementado pelo PSC responsável.

1.5.1. Políticas de publicação e notificação

Neste item devem ser descritos os mecanismos empregados para a distribuição da DPPSC à comunidade envolvida.

1.5.2. Procedimentos de aprovação

Toda DPPSC deverá ser submetida à aprovação, durante o processo de credenciamento do PSC responsável, 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 contidas 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

2.1.1.1. Neste item devem ser definidas as informações a serem publicadas pelo PSC responsável pela DPPSC, o modo pelo qual serão disponibilizadas e a sua disponibilidade.

2.1.1.2. As seguintes informações, no mínimo, deverão ser publicadas pelo PSC em página web:

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

b) sua DPPSC;

c) os serviços que implementam;

d) as condições gerais mediante as quais são prestados os serviços de armazenamento de chaves privadas, assinatura digital e verificação da assinatura digital;

e) se pretende continuar a prestar o serviço ou se está mediante a qualquer fiscalização dos serviços.

2.1.2. Frequência de publicação

Neste item deve ser informada a frequência de publicação das informações de que trata o item anterior, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

2.1.3. Controles de acesso

Neste item devem ser descritos os controles e as eventuais restrições para acesso, leitura e escrita das informações publicadas pelo PSC, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil.

3. IDENTIFICAÇÃO E AUTORIZAÇÃO

Neste item o PSC responsável deve descrever a forma utilizada para identificar e autorizar os subscritores, caso necessária a realização de tais procedimentos.

4. REQUISITOS OPERACIONAIS

4.1. Armazenamento e acesso às chaves privadas do subscritor

Neste item da DPPSC o PSC deve, além do descrito 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, relatar como os componentes de software farão comunicação entre a aplicação do subscritor e acesso ao certificado e suas chaves, descrevendo:

a) a linguagem de programação utilizada para construção da plataforma de acesso;

b) os meios de acesso disponibilizados ao subscritor (aplicativos para dispositivos móveis, para PC, páginas web, entre outros);

c) o canal de segurança em que trafegam as autenticações;

d) a arquitetura de rede da aplicação de acesso.

4.2. Serviço de criação e validação de assinaturas digitais

Neste item da DPPSC o PSC deve, além do descrito 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, relatar como as plataformas de assinatura digital e verificação da assinatura digital funcionarão.

4.3. Procedimentos de Auditoria de Segurança

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

4.3.1. Tipos de eventos registrados

4.3.1.1. O PSC responsável pela DPPSC deverá registrar em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

a) iniciação e desligamento dos sistemas de PSC;

b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores do PSC;

c) mudanças na configuração dos sistemas de PSC;

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 das assinaturas digitais criadas e verificações realizadas;

k) registros de acesso aos documentos dos subscritores;

l) registros de acesso ou tentativas de acesso a chave privada do subscritor.

4.3.1.2. O PSC responsável pela DPPSC deverá também registrar, 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. Neste item, a DPPSC deve especificar todas as informações que deverão ser registradas pelo PSC responsável.

4.3.1.4. A DPPSC deve prever que todos os registros de auditoria deverão conter a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos deverão conter o horário UTC. Registros manuais em papel poderão conter a hora local desde que especificado o local.

4.3.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços do PSC deverá ser 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*)

A DPPSC deve estabelecer a periodicidade, não superior a uma semana, com que os registros de auditoria do PSC responsável serão analisados pelo seu pessoal operacional. Todos os eventos significativos deverão ser explicados em relatório de auditoria de registros. Tal análise deverá envolver 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 deverão ser documentadas.

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

Neste item, a DPPSC deve estabelecer que o PSC responsável mantenha localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, deverá armazená-los da maneira descrita no item 4.4.

4.3.4. Proteção de registro (*log*) de auditoria

4.3.4.1. Neste item, a DPPSC deve descrever os mecanismos obrigatórios incluídos no sistema de registro de eventos do PSC responsável para proteger os seus registros de auditoria contra leitura não autorizada, modificação e remoção.

4.3.4.2. Também devem ser descritos os mecanismos obrigatórios de proteção de informações manuais de auditoria contra a leitura não autorizada, modificação e remoção.

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

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

Neste item da DPPSC devem ser descritos os procedimentos adotados pelo PSC responsável para gerar cópias de segurança (*backup*) de seus registros de auditoria e a sua periodicidade, que não deve ser superior a uma semana.

4.3.6. Sistema de coleta de dados de auditoria

Neste item da DPPSC devem ser descritos e localizados os recursos utilizados pelo PSC responsável para a coleta de dados de auditoria.

4.3.7. Notificação de agentes causadores de eventos

A DPPSC deve observar que quando um evento for registrado pelo conjunto de sistemas de auditoria do PSC responsável, nenhuma notificação deverá ser enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.3.8. Avaliações de vulnerabilidade

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

4.4. Arquivamento de Registros

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

4.4.1. Tipos de registros arquivados

4.4.1.1 Neste item da DPPSC devem ser especificados os tipos de registros arquivados, que deverão compreender, 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 no item 4.3.1.1.

4.4.1.2 Neste item, a DPPSC deve estabelecer os períodos de retenção para cada registro arquivado, observando que os registros de armazenamento de chaves privadas e/ou certificados digitais, de assinaturas digitais criadas, de verificações das assinaturas digitais e, por ventura, dos documentos armazenados, inclusive arquivos de auditoria, deverão ser retidos por, no mínimo, 7 (sete) anos.

4.4.2. Proteção de arquivo

A DPPSC deve estabelecer que todos os registros arquivados devem ser 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 deve estabelecer que uma segunda cópia de todo o material arquivado deverá ser armazenada em ambiente diferente às instalações principais do PSC responsável, 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 responsável pela DPPSC deverá verificar a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.4.4. Requisitos para datação de registros

Neste item, a DPPSC deve estabelecer os formatos e padrões de data e hora contidos em cada tipo de registro.

4.4.5. Sistema de coleta de dados de arquivo

Neste item da DPPSC devem ser descritos e localizados os recursos de coleta de dados de arquivo utilizados pelo PSC responsável.

4.4.6. Procedimentos para obter e verificar informação de arquivo

Neste item da DPPSC devem ser detalhadamente descritos os procedimentos definidos pelo PSC responsável para a obtenção ou a verificação de suas informações de arquivo.

4.5. Liberação do espaço do subscritor

Neste item, a DPPSC deve descrever os procedimentos técnicos e operacionais que serão usados pelo PSC responsável para liberação de um espaço (*slot*) destinado a um subscritor onde estavam armazenadas as chaves privadas do mesmo, no caso de expiração e não uso mais por parte do usuário ou revogação do certificado.

4.6. Comprometimento e Recuperação de Desastre

4.6.1. Disposições Gerais

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

4.6.1.2. O PSC deve assegurar, 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 deve disponibilizar 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 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. Em caso de comprometimento de uma operação de serviço de assinatura digital ou verificação da assinatura digital dos documentos assinados, sempre que possível, o PSC deve disponibilizar a todos os subscritores e terceiras partes informações que possam ser utilizadas para identificar quais documentos que podem ter sido afetados, a não ser que isso viole a privacidade dos subscritores ou comprometa a segurança dos serviços do PSC.

4.6.2. Recursos computacionais, *software*, e dados corrompidos

Neste item da DPPSC devem ser descritos os procedimentos de recuperação utilizados pelo PSC responsável quando recursos computacionais, *software* ou dados estiverem corrompidos ou houver suspeita de corrupção.

4.6.3. Sincronismo do PSC

Neste item a DPPSC deve descrever os procedimentos de recuperação previstos pelo PSC para utilização nas hipóteses de sincronismo com a fonte confiável de tempo da ICP-Brasil ou, se for o caso, com o pool de HSM para operação.

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

Neste item da DPPSC devem ser descritos os procedimentos de recuperação utilizados pelo PSC responsável após a ocorrência de um desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro.

4.7. Extinção dos serviços de PSC

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 deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços do PSC responsável.

4.7.2. O PSC deve assegurar que possíveis rompimentos com os subscritores e terceiras partes, em consequência da cessação dos serviços de armazenamento das chaves privadas, assinaturas digitais e verificações de assinaturas digitais 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 cessar seus serviços os seguintes procedimentos serão executados, no mínimo:

a) o PSC disponibilizará a todos os subscritores e partes receptoras informações a respeito de sua extinção;

b) o PSC 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, por um período razoável;

c) o PSC 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 notificará todas as entidades afetadas.

4.7.4. O PSC 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 devem ser descritos os controles de segurança implementados pelo PSC responsável pela DPPSC para executar de modo seguro suas funções, de acordo com regulamento editado por instrução normativa da AC Raiz que defina os procedimentos operacionais mínimos para os prestadores de serviço de confiança da ICP-Brasil.

5.1. Segurança Física

Nos itens seguintes da DPPSC devem ser descritos os controles físicos referentes às instalações que abrigam os sistemas do PSC responsável.

5.1.1. Construção e localização das instalações do PSC

Neste item a DPPSC deve descrever aspectos de construção das instalações do PSC responsável, relevantes para os controles de segurança física, 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

Todo PSC integrante da ICP-Brasil deverá implantar um sistema de controle de acesso físico que garanta 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

O PSC deve descrever minuciosamente cada nível de acesso e o seu conjunto de sistemas, *softwares* e *hardwares* implantados, em conformidade com as descrições dos níveis de acesso 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..

5.1.2.2. Sistemas físicos de detecção

5.1.2.2.1. A segurança de todos os ambientes do PSC deverá ser feita em regime de vigilância 24 x 7 (vinte e quatro horas por dia, sete dias por semana).

5.1.2.2.2. A segurança poderá ser realizada por:

a) guarda armado, uniformizado, devidamente treinado e apto para a tarefa de vigilância; ou

b) circuito interno de TV, sensores de intrusão instalados em todas as portas e janelas e sensores de movimento, monitorados local ou remotamente por empresa de segurança especializada.

5.1.2.2.3. O ambiente de nível 3 deverá ser dotado, adicionalmente, de Circuito Interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não deverão permitir a captura de senhas digitadas nos sistemas.

5.1.2.2.4. As mídias resultantes dessa gravação deverão ser armazenadas por, no mínimo, 1 (um) ano, em ambiente de nível 2.

5.1.2.2.5. O PSC deverá possuir mecanismos que permitam, em caso de falta de energia:

a) iluminação de emergência em todos os ambientes, acionada automaticamente;

b) continuidade de funcionamento dos sistemas de alarme e do circuito interno de TV.

5.1.2.3. Sistema de controle de acesso

O sistema de controle de acesso deverá estar baseado em um ambiente de nível 3.

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

5.1.3.1. A infraestrutura do ambiente de nível 3 do PSC deverá ser dimensionada com sistemas e dispositivos que garantam o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia devem ser mantidas de forma a atender os requisitos de disponibilidade dos sistemas do PSC e seus respectivos serviços. Um sistema de aterramento deverá ser implantado.

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

5.1.3.3. Deverão ser 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. Deverão ser utilizados dutos separados para os cabos de energia, de telefonia e de dados.

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

5.1.3.5. Deverão ser mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL **[4]**. Qualquer modificação nessa rede deverá ser documentada e autorizada previamente.

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

5.1.3.7. O sistema de climatização deverá atender aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente.

5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização deverá ser permanentemente monitorada.

5.1.3.9. A capacidade de redundância de toda a estrutura de energia e ar-condicionado do ambiente de nível 3 do PSC deverá ser garantida por meio de *nobreaks* e geradores de porte compatível.

5.1.4. Exposição à água nas instalações do PSC

O ambiente de Nível 3 do PSC deve estar instalado em local protegido contra a exposição à água, infiltrações e inundações.

5.1.5. Prevenção e proteção contra incêndio nas instalações do PSC

5.1.5.1. Nas instalações do PSC não será permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do nível 2.

5.1.5.2. Deverão existir no interior do ambiente nível 3 extintores de incêndio das classes B e C, para apagar incêndios em combustíveis e equipamentos elétricos, dispostos no ambiente de forma a facilitar o seu acesso e manuseio. Em caso da existência de sistema de *sprinklers* no prédio, o ambiente de nível 3 do PSC não deverá possuir saídas de água, para evitar danos aos equipamentos.

5.1.5.3. O ambiente de nível 3 deve possuir sistema de prevenção contra incêndios, que acione alarmes preventivos uma vez detectada fumaça no ambiente.

5.1.5.4. Nos demais ambientes do PSC deverão existir extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitem o seu acesso e manuseio

5.1.5.5. Mecanismos específicos deverão ser implantados pelo PSC para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir 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 deve acionar imediatamente os alarmes de abertura de portas.

5.1.6. Armazenamento de mídia nas instalações do PSC

O PSC responsável deverá atender à 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

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis deverão ser 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, deverão ser fisicamente destruídos.

5.1.8. Sala externa de arquivos (*off-site*) para PSC

Uma sala de armazenamento externa à instalação técnica principal do PSC deve ser usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala deverá estar disponível a pessoal autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e deverá atender aos requisitos mínimos estabelecidos por este documento para um ambiente de nível 2.

5.2. Controles Procedimentais

Nos itens seguintes da DPPSC devem ser descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados no PSC responsável, 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 responsável pela DPPSC deverá garantir a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente os serviços do ambiente sem ser detectado. As ações de cada empregado deverão estar limitadas de acordo com seu perfil.

5.2.1.2. O PSC deverá estabelecer um mínimo de 3 (três) perfis distintos para sua operação, a saber:

a) Administrador do sistema – autorizado a instalar, configurar e manter os sistemas confiáveis para gerenciamento do carimbo do tempo, bem como administrar a implementação das práticas de segurança do PSC;

b) Operador de sistema – responsável pela operação diária dos sistemas confiáveis do PSC. Autorizado a realizar *backup* e recuperação do sistema.

c) Auditor de Sistema – autorizado a ver arquivos e auditar os *logs* dos sistemas confiáveis do PSC.

5.2.1.3. Todos os empregados do PSC deverão receber treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso serão determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4. Quando um empregado se desligar do PSC, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro do PSC, deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver ao PSC no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

Todas as tarefas executadas no cofre ou gabinete onde se localizam os serviços do PSC deverão requerer a presença de, no mínimo, 2 (dois) empregados com perfis qualificados. Para os casos de cópias das chaves dos usuários e portabilidade da mesma serão necessários, no mínimo, 3 (três) empregados com perfis distintos e qualificados. As demais tarefas do PSC poderão ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. A DPPSC deve garantir que todo empregado do PSC responsável terá sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso físico às instalações do PSC;

b) ser incluído em uma lista para acesso lógico aos sistemas confiáveis do PSC;

c) ser incluído em uma lista para acesso lógico aos sistemas do PSC.

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

a) ser diretamente atribuídos a um único empregado;

b) não ser compartilhados; e

c) ser restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. O PSC deverá implementar um padrão de utilização de "senhas fortes", definido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL **[4]**, com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Nos itens seguintes da DPPSC devem ser descritos requisitos e procedimentos, implementados pelo PSC responsável em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. A DPPSC deve garantir que todos os empregados do PSC responsável, encarregados de tarefas operacionais terão 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; e

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 responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverá ser admitido conforme o estabelecido na **POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]**. O PSC responsável poderá definir requisitos adicionais para a admissão.

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 responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverá ser submetido a:

a) verificação de antecedentes criminais;

b) verificação de situação de crédito;

c) verificação de histórico de empregos anteriores; e

d) comprovação de escolaridade e de residência.

5.3.2.2. O PSC responsável poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

Todo o pessoal do PSC responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas

digitais, verificações de assinaturas digitais deverão receber 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 responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverá ser mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas do PSC.

5.3.5. Frequência e sequência de rodízio de cargos

Neste item, a DPPSC pode definir uma política a ser adotada pelo PSC responsável para o rodízio de pessoal entre os diversos cargos e perfis por elas estabelecidos. Essa política não deverá contrariar os propósitos estabelecidos no item 5.2.1 para a definição de perfis qualificados.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. A DPPSC deve prever que na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional, o PSC deverá, de imediato, suspender o acesso dessa pessoa aos sistemas, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.

5.3.6.2. O processo administrativo referido acima deverá conter, no mínimo, os seguintes itens:

a) relato da ocorrência com *modus operandis*;

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 responsável deverá encaminhar 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 responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverá ser contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL **[4]**. O PSC responsável poderá definir requisitos adicionais para a contratação.

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A DPPSC deve garantir que o PSC responsável tornará disponível para todo o seu pessoal pelo menos:

a) sua DPPSC;

b) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4];

c) documentação operacional relativa às suas atividades; e

d) contratos, normas e políticas relevantes para suas atividades.

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

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPPSC deve definir as medidas de segurança implantadas pelo PSC responsável para proteger as chaves privadas dos subscritores, manter os serviços relativos a assinaturas digitais, assim como o sincronismo de seus sistemas com a fonte confiável de tempo da

ICP-Brasil. Devem também ser definidos outros controles técnicos de segurança utilizados pelo PSC na execução de suas funções operacionais.

6.1. Controles de Segurança Computacional

6.1.1. Disposições Gerais

Neste item, a DPPSC deve indicar 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 deve prever que os sistemas e os equipamentos do PSC responsável, 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;

b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado do PSC;

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;

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 deverão ser 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 deverá ter 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, 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. Todos esses eventos deverão ser registrados para fins de auditoria.

6.1.2.4. Qualquer equipamento incorporado ao PSC deverá ser 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

Neste item da DPPSC deve ser informada, quando disponível, a classificação atribuída à segurança computacional do PSC responsável, segundo critérios como: *Trusted System Evaluation Criteria* (TCSEC), *Canadian Trusted Products Evaluation Criteria*, *European Information Technology Security Evaluation Criteria* (ITSEC), *Common Criteria* e eIDAS.

6.2. Controles Técnicos do Ciclo de Vida

Nos itens seguintes da DPPSC devem ser descritos, quando aplicáveis, os controles implementados pelo PSC responsável no desenvolvimento de sistemas e no gerenciamento de segurança.

6.2.1. Controles de desenvolvimento de sistema

6.2.1.1. Neste item da DPPSC devem ser abordados aspectos tais como: segurança do ambiente e do pessoal de desenvolvimento, práticas de engenharia de *software* adotadas, metodologia de desenvolvimento de *software*, entre outros, aplicados ao *software* do sistema do PSC ou a qualquer outro *software* desenvolvido ou utilizado pelo PSC responsável.

6.2.1.2. Os processos de projeto e desenvolvimento conduzidos pelo PSC deverão prover documentação suficiente para suportar avaliações externas de segurança dos componentes do PSC.

6.2.2. Controles de gerenciamento de segurança

6.2.2.1. Neste item da DPPSC devem ser descritas as ferramentas e os procedimentos empregados pelo PSC responsável 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.

6.2.3. Classificações de segurança de ciclo de vida

Neste item da DPPSC deve ser informado, quando disponível, o nível de maturidade atribuído ao ciclo de vida de cada sistema, com base em critérios como: *Trusted Software Development Methodology* (TSDM), *Capability Maturity Model do Software Engineering Institute* (CMM-SEI) e o Plano de Capacidade Operacional – PCO.

6.3. Controles de Segurança de Rede

6.3.1. Diretrizes Gerais

6.3.1.1. Neste item da DPPSC devem ser descritos os controles relativos à segurança da rede do PSC responsável, 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, deverão estar localizados e operar em ambiente de, no mínimo, nível 3.

6.3.1.3. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes deverão ser 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 deverá ser restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas deverão implementar filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.3.1.5. O acesso à Internet deverá ser 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 deverá ser permitido somente para os seguintes serviços:

a) pela EAT da ICP-Brasil, para o sincronismo e auditoria dos sistemas de assinaturas;

b) pelo PSC, para a administração dos sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;

c) pelo subscritor, para a armazenamento e acesso à chave privada e aos serviços de assinatura digital, verificação da assinatura digital.

6.3.2. Firewall

6.3.2.1. Mecanismos de *firewall* deverão ser implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Os *firewalls* deverão ser 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, deverá implementar registros de auditoria.

6.3.2.3. O Oficial de Segurança deve verificar 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 deverá ter 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 automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

6.3.3.2. O sistema de detecção de intrusão deverá ter 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 deverá prover 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 – deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro deverá ser, no mínimo, semanal e todas as ações tomadas em decorrência desse exame deverão ser documentadas.

6.3.5. Outros controles de segurança de rede

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

6.3.5.2. As estações de trabalho e servidores devem estar 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

Este item da DPPSC deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada dos subscritores do PSC responsável. Poderão ser indicados padrões de referência, como aqueles definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil **.**

7. POLÍTICAS DE ASSINATURA

Neste item da DPPSC, o PSC de Assinatura Digital deve informar as Políticas de Assinatura Digital que pratica, seguindo o disposto em regulamento editado por instrução normativa da AC Raiz que defina os requisitos das políticas de assinatura digital na ICP-Brasil. . Esse documento trata das Políticas e dos Padrões de Assinatura adotados no âmbito da ICP-Brasil.

8. AUDITORIAS E AVALIAÇÕES DE CONFORMIDADE

8.1. Fiscalização e Auditoria de Conformidade

8.1.1. As fiscalizações e auditorias realizadas nos PSC da ICP-Brasil 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 dos PSC da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL **[7]**.

8.1.3. As auditorias dos PSC da ICP-Brasil 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) quanto a autenticação e ao sincronismo de tempo pela Entidade de Auditoria do Tempo (EAT) observado o disposto no documento PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS DO TEMPO NA ICP-BRASIL **[3].**

8.1.4. Neste item da DPPSC, o PSC responsável deve informar que recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e que é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL **[6]**. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.1.5. Neste item da DPPSC, o PSC responsável deve informar que recebeu auditoria prévia da EAT quanto aos aspectos de autenticação e sincronismo, sendo regularmente auditada, para fins de continuidade de operação, com base no disposto no documento PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS DO TEMPO NA ICP-BRASIL **[3].**

8.1.6. Neste item da DPPSC, o PSC responsável deve informar que as entidades da ICP-Brasil, se for o caso, a ela diretamente vinculadas também receberam auditoria prévia, para fins de credenciamento, e que o PSC é responsável pela realização de auditorias anuais, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo 8.1.3.

9. OUTROS ASSUNTOS DE CARÁTER COMERCIAL E LEGAL

9.1. Obrigações e direitos

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

9.1.1. Obrigações do PSC

Neste item devem ser incluídas as obrigações da PSC responsável pela DPPSC, contendo, no mínimo, as abaixo relacionadas:

a) operar de acordo com a sua DPPSC e com a descrição dos serviços que realiza;

b) gerenciar e assegurar a proteção das chaves privadas dos subscritores;

c) manter os PSC sincronizados e auditados pela Entidade de Auditoria do Tempo da ICP-Brasil;

d) tomar as medidas cabíveis para assegurar que subscritores e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;

e) monitorar e controlar a operação dos serviços fornecidos;

f) 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;

g) publicar em sua página web sua DPPSC e as Políticas de Segurança (PS) aprovadas que implementa;

h) publicar, em sua página web, as informações definidas no item 2.1.1.2 deste documento;

i) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

j) adotar as medidas de segurança e controle previstas na DPPSC, 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;

k) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

l) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

m) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);

n) 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;

o) 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

p) 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, se for o caso, o subscritor deve assegurar, por meio das aplicações disponibilizadas ao contratar um PSC, que o seu par de chaves e/ou certificados digitais foram corretamente armazenados e se a chave privada usada para assinar está funcional.

9.1.3 Direitos da terceira parte (*Relying Party*)

9.1.3.1 Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do serviço de assinatura digital, verificação da assinatura digital.

9.1.3.2 Constituem direitos da terceira parte:

a) recusar a utilização do serviço de assinatura digital, verificação da assinatura digital e guarda de documentos eletrônicos do PSC para fins diversos do seu propósito de uso na ICP-Brasil.

b) verificar, a qualquer tempo, a validade da assinatura digital. Uma assinatura digital ICP-Brasil é considerada válida quando:

i. o certificado digital não constar da LCR da AC emitente;

ii. a chave privada utilizada para assinar digitalmente não tiver sido comprometida até o momento da verificação;

iii. puder ser verificada com o uso da cadeia de certificados que a gerou;

iv. o propósito de uso esteja em conformidade com o definido na política do certificado digital do(s) signatário(s).

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

9.2. Responsabilidades

9.2.1. Responsabilidades do PSC

O PSC responsável responde pelos danos a que der causa.

9.3. Responsabilidade Financeira

9.3.1. Indenizações devidas pela terceira parte (*Relying Party*)

Neste item deve ser estabelecida a inexistência de responsabilidade da terceira parte (*relying party*) perante o PSC, exceto na hipótese de prática de ato ilícito.

9.3.2. Relações Fiduciárias

Neste item deve constar que o PSC responsável 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

Neste item devem ser relacionados os processos administrativos cabíveis, relativos às operações do PSC responsável pela DPPSC.

9.4. Interpretação e Execução

9.4.1. Legislação

Neste item deve ser indicada a legislação que ampara a DPPSC.

9.4.2. Forma de interpretação e notificação

9.4.2.1. Neste item devem ser relacionadas as providências a serem tomadas na hipótese de uma ou mais das disposições da DPPSC ser, por qualquer razão, considerada inválida, ilegal ou não aplicável.

9.4.2.2. Deve também ser definida a forma pela qual serão realizadas as notificações, as solicitações ou quaisquer outras comunicações necessárias, relativas às práticas descritas na DPPSC.

9.4.3. Procedimentos de solução de disputa

9.4.3.1. Neste item devem ser definidos os procedimentos a serem adotados em caso de conflito entre a DPPSC e outras declarações, políticas, planos, acordos, contratos ou documentos que o PSC adotar.

9.4.3.2. Deve também ser estabelecido que a DPPSC do PSC responsável não prevaleça sobre as normas, critérios, práticas e procedimentos da 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, deve ser especificada pelo PSC responsável pela DPPSC a política tarifária e de reembolso aplicáveis, se for o caso.

9.5.1. Tarifas de armazenamento de chaves privadas para usuários finais;

9.5.2. Tarifas de serviço de assinatura digital;

9.5.3. Tarifas de serviço de verificação da assinatura digital;

9.5.4. Outras tarifas;

9.5.5. Política de reembolso.

9.6. Sigilo

9.6.1. Disposições gerais

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

9.6.1.2 As assinaturas digitais e verificações das assinaturas digitais que poderão ser realizadas pelo PSC, que será responsável pelo seu sigilo, mantendo as trilhas de auditoria com horário e data sincronizados com a EAT, inclusive podendo identificar qual documento, IP ou URL, entre outros, que devem ser previamente autorizados pelo subscritor, foram assinados com a chave privada do mesmo.

9.6.1.3 Os documentos assinados digitalmente pelos subscritores poderão ser mantidos pelo PSC, desde que expressamente acordado com o subscritor e de acordo com a legislação vigente, que será responsável pelo seu sigilo.

9.6.2. Tipos de informações sigilosas

9.6.2.1. Neste item devem ser identificados os tipos de informações consideradas sigilosas pelo PSC responsável pela DPPSC, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.6.2.2. A DPPSC deve estabelecer, como princípio geral, que nenhum documento, informação ou registro fornecido pelo subscritor ao PSC deverá ser divulgado, exceto quando for estabelecido um acordo com o subscritor para sua publicação mais ampla.

9.6.3. Tipos de informações não sigilosas

Neste item devem ser indicados os tipos de informações consideradas não sigilosas pelo PSC responsável pela DPPSC, os quais deverão compreender, entre outros:

a) os certificados dos subscritores;

b) a DPPSC do PSC;

c) versões públicas de PS; e

d) a conclusão dos relatórios de auditoria.

9.6.4. Quebra de sigilo por motivos legais

Este item deve estabelecer o dever do PSC responsável pela DPPSC de fornecer documentos, informações ou registros sob sua guarda, mediante ordem judicial.

9.6.5. Informações a terceiros

Este item da DPPSC deve estabelecer como diretriz geral que nenhum documento, informação ou registro sob a guarda do PSC responsável pela DPPSC deverá ser fornecido a qualquer pessoa,

exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

9.6.6. Outras circunstâncias de divulgação de informação

Neste item da DPPSC devem ser descritas, quando cabíveis, quaisquer outras circunstâncias em que poderão ser divulgadas informações sigilosas.

9.7. Direitos de Propriedade Intelectual

Neste item da DPPSC devem ser tratadas as questões referentes aos direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, documentos assinados digitalmente de acordo com a legislação vigente.

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]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001	**DOC-ICP-04**
[2]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL Aprovado pela Resolução nº 36, de 21 de outubro de 2004	**DOC-ICP-10**
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL Aprovado pela Resolução nº 61, de 28 de novembro de 2008	**DOC-ICP-14**
[4]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pela Resolução nº 02, de 25 de setembro de 2001	**DOC-ICP-02**
[5]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	**DOC-ICP-03**
[6]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 29 de agosto de 2003	**DOC-ICP-08**
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 25, de 24 de outubro de 2003	**DOC-ICP-09**

11. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 11.515/NB 1334: Critérios de segurança física relativos ao armazenamento de dados. 2007.

RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.

RFC 3447, IETF - Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, february 2003.

RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, November 2003.

RFC 3647, IETF - Internet X-509 Public Key Infrastructure Certificate Policy and Certifications Practices Framework, novembro de 2003.

RFC 4210, IETF - Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP), september 2005.

RFC 4211, IETF - Internet X.509 Public Key Infrastructure. Certificate Request Message Format (CRMF), september 2005.

ETSI TS 101.861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.

Regulation (EU) 910/2014 - relativo à identificação eletrônica e aos serviços de confiança para as transações eletrônicas no mercado interno Europeu.