DIGITALSIGN CERTIFICAÇÃO DIGITAL LTDA.
(PSC DIGITALSIGN)

DECLARAÇÃO DE PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL

VERSÃO 1.0 – 29/03/2022

CONTEÚDO

CONTROLE DE ALTERAÇÕES

Data	*Versão*	*Observações*
29/03/2022	1.0	Redação Inicial

AVISO LEGAL

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Este documento está baseado em 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 DIGITALSIGN é uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de armazenamento de chaves privadas para usuários finais, nos termos do DOC-ICP-04 [1].

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. Esta Declaração de Práticas de Prestador de Serviço de Confiança (DPPSC) estabelece os requisitos mínimos a serem obrigatoriamente observados pelo PSC DIGITALSIGN, entidade integrante da ICP-Brasil. A DPPSC é o documento que descreve as práticas e os procedimentos operacionais e técnicos empregados pelo PSC DIGITALSIGN na execução de seus serviços.

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. Este documento segue obrigatoriamente a estrutura empregada no DOC-ICP-17.

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

1.1.8. Esta DPPSC está conforme a *Internet Engineering Task Force* (IETF) RFC 3647, podendo sofrer atualizações regulares.

1.2. IDENTIFICAÇÃO

Este documento é designado Declaração de Práticas doe Prestadores de Serviço de Confiança DigitalSign e referida a seguir como "DPPSC'' do PSC DIGITALSIGN.

Este documento é identificado pela seguinte informação:

INFORMAÇÃO DO DOCUMENTO	
Versão/Edição	1.0
Data de Aprovação	29/03/2022
Data de Validade	Não se aplica
OID	2.16.76.1.11.8
Localização	http://www.digitalsigncertificadora.com.br/repositorio/psc/

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. PRESTADORES DE SERVIÇO DE CONFIANÇA

Esta DPPSC refere-se ao Prestador de Serviço de Confiança "PSC DIGITALSIGN".

1.3.1.1. Os Serviços prestados pelo PSC DIGITALSIGN estão identificados no endereço de web (URL): http://www.digitalsigncertificadora.com.br/repositorio/psc/

1.3.1.2. O PSC DIGITALSIGN 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. As atividades prestadas é "armazenamento de chaves privadas dos subscritores".

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

1.3.2. SUBSCRITORES

1.3.2.1. Qualquer pessoa física ou jurídica que esteja com a sua situação fiscal regular junto a Receita Federal poderão solicitar os serviços descritos nesta DPPSC.

1.3.2.2. Os subscritores deverão manifestar plena aprovação aos serviços contratados pelo PSC DIGITALSIGN, assim como o nível de acompanhamento que o PSC DIGITALSIGN 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 DIGITALSIGN, 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 DIGITALSIGN 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 destes certificados, estão relacionadas nas Políticas de Certificados de cada uma das ACs correspondentes.

1.4. DADOS DE CONTATO

DigitalSign Certificação Digital LTDA.
Rua General Bertoldo Klinger, 111 – Paulicéia – São Bernardo do Campo/SP
Nome: Guilherme Salgueiro de Almeida
Email: suporte@digitalsigncertificadora.com.br
Telefone: (55 11) 2666 7292
Celular: (55 11) 97562 7417

1.5. Procedimentos de Mudança de Especificação

A atualização deste documento será realizada sempre que haja necessidade para adequação da operação e/ou legislação vigente, sendo a análise das alterações serão submetidas a AC-Raiz. Esta DPPSC é atualizada sempre que um novo serviço implementado pelo PSC o exigir.

1.5.1. Políticas de publicação e notificação

Esta DPPSC é publicada em repositório disponível em:

http://www.digitalsigncertificadora.com.br/repositorio/psc/

1.5.2. Procedimentos de aprovação

Esta DPPSC foi submetida à aprovação, durante o processo de credenciamento do PSC DIGITALSIGN, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

1.6. Definições e Acrônimos

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. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da PSC DIGITALSIGN responsável por esta DPPSC, e o modo pelo qual serão disponibilizadas e a sua disponibilidade.

2.1.1.2. As seguintes informações, no mínimo, são publicadas pelo PSC DIGITALSIGN em página web:

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

b) Declarações Práticas de Prestadores de Serviço de Confiança – DPPSC;

c) os serviços que implementam;

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.

2.1.2. FREQUÊNCIA DE PUBLICAÇÃO

As informações de que trata o item anterior são publicadas anualmente ou quando necessário, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

2.1.3. CONTROLES DE ACESSO

Não há qualquer restrição ao acesso para consulta às informações descritas no item 2.1.1 desta DPPSC.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não-autorizado.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. SERVIÇO DE ARMAZENAMENTO E ACESSO ÀS CHAVES PRIVADAS DO SUBSCRITOR

A utilização do serviço de armazenamento de chaves privadas dos subscritores, realiza a identificação e autenticação dos subscritores conforme se segue:

a) As chaves privadas dos usuários finais, para os tipos de certificados que obrigatoriamente devem ser gerados e armazenados em hardware criptográficos, estão armazenadas dentro dos espaços (slots), ou equivalente, da fronteira criptográfica e segurança física de um HSM com certificação Inmetro válida no âmbito da ICP-Brasil, endereçados por conta de usuário;

b) Esse acesso ou comando de exportação às chaves privadas dos usuários é de uso, conhecimento e controle exclusivo do titular, sem a possibilidade de ingresso por outros titulares no mesmo HSM, qualquer funcionário do PSC DIGITALSIGN ou dependentes de outras chaves criptográficas;

c) O PSC DIGITALSIGN provê mecanismos de duplo fator de autenticação ao titular para acesso à chave privada, sendo um fator dentro da fronteira criptográfica do HSM e outro dentro do ambiente seguro e primeira interface de comunicação com HSM ou ambos dentro da fronteira criptográfica do HSM. Cada fator possui uma classe diferente (conhecimento, posse ou biometria). Os mecanismos de autenticação empregam método ou protocolo de validação que realiza a proteção da transmissão e dos dados de autenticação por meio de criptografia. Essa funcionalidade é apensada aos requisitos técnicos na manutenção da homologação dos HSM e são:

   i. Senhas (PIN/PUK): segundo regras da ICP-Brasil;

   ii. OTP: segundo regras da RFC 6238 (TOTP), RFC 6287, RFC 4226 (HOTP);

   iii. Biometria: segundo regras da ICP-Brasil;

   iv. Certificado de atributo: segundo regras da ICP-Brasil;

   v. Push Notification: segundo regras do XMPP extension protocol ou semelhante;

   vi. Outras autenticações semânticas em acordo com o DOC-ICP-17.01 [12] e previamente aprovadas pela AC Raiz.

4. REQUISITOS OPERACIONAIS

4.1. ARMAZENAMENTO E ACESSO ÀS CHAVES PRIVADAS DO SUBSCRITOR

A comunicação entre a aplicação do subscritor e acesso ao certificado e suas chaves utiliza:

a) linguagem de programação utilizada para construção da plataforma de acesso: Java e C#;

b) meio de acesso disponibilizado ao subscritor: webservice, página web e aplicativos para dispositivos móveis e computadores pessoais;

c) canal de segurança em que trafegam as autenticações: HTTPS;

d) arquitetura de rede: 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 são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pelo PSC DIGITALSIGN com o objetivo de manter um ambiente seguro.

4.3.1. TIPOS DE EVENTOS REGISTRADOS

4.3.1.1. O PSC DIGITALSIGN registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos são obrigatoriamente 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 DIGITALSIGN também 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. São registradas pelo PSC DIGITALSIGN:

a) Criação/Remoção de slot

b) Criação/Remoção de chave

c) Geração de CSR

d) Importação de Certificado

e) Uso de Chave

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 contêm 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 DO PSC DIGITALSIGN.

4.3.2. FREQUÊNCIA DE AUDITORIA DE REGISTROS (LOGS)

Os registros de auditoria do PSC DIGITALSIGN são analisados semanalmente pelo pessoal operacional. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal 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 DIGITALSIGN mantém localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena-os da maneira descrita no item 4.4.

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 do PSC DIGITALSIGN.

4.3.4.2. Os registros de auditoria gerados manualmente 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 do PSC DIGITALSIGN.

4.3.4.3. Os mecanismos de proteção descritos neste item obedecem à POLÍTICA DE SEGURANÇA DO PSC DIGITALSIGN.

4.3.5. PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTRO (LOG) DE AUDITORIA

Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela AC DigitalSign têm cópias de segurança semanais, efetuadas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas.

4.3.6. SISTEMA DE COLETA DE DADOS DE AUDITORIA

O sistema de coleta de dados de auditoria interno ao PSC DIGITALSIGN é uma combinação de processos automatizados e manuais, executada pelo seu pessoal operacional e/ou pelos seus sistemas.

4.3.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

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

4.3.8. AVALIAÇÕES DE VULNERABILIDADE

Os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria do PSC DIGITALSIGN, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pelo PSC e registradas para fins de auditoria.

4.4. ARQUIVAMENTO DE REGISTROS

Nos itens seguintes a seguir é descrita a política geral de arquivamento de registros, para uso futuro, implementada pelo PSC DIGITALSIGN.

4.4.1. TIPOS DE REGISTROS ARQUIVADOS

4.4.1.1. Os tipos de registros arquivados pelo PSC DIGITALSIGN são:

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. O período de retenção para cada registro arquivado, observando que os registros de armazenamento dos certificados digitais, inclusive arquivos de auditoria, são retidos 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 DO PSC DIGITALSIGN.

4.4.3. PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE ARQUIVO

4.4.3.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente diferente às instalações principais do PSC DIGITALSIGN, recebendo o mesmo tipo de proteção utilizada por ele no arquivo principal.

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

4.4.3.3. O PSC DIGITALSIGN verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.4.4. REQUISITOS PARA DATAÇÃO DE REGISTROS

As informações de data e hora nos registros baseiam-se no horário Greenwich Mean Time.

Nos casos em que, por algum motivo, os documentos formalizem o uso de outro formato, ele será aceito.

4.4.5. SISTEMA DE COLETA DE DADOS DE ARQUIVOS

Todos os sistemas de coleta de dados de arquivo utilizados pela PSC DIGITALSIGN nos 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 à PSC DIGITALSIGN, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

4.5. LIBERAÇÃO DO ESPAÇO DO SUBSCRITOR

A liberação de um espaço (slot) destinado a um subscritor se dará quando da expiração do certificado ou sua revogação e não uso mais por parte do usuário.

4.6. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

4.6.1. DISPOSIÇÕES GERAIS

4.6.1.1. Nos itens seguintes são descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no Plano de Continuidade de Negócios (PCN) do PSC DIGITALSIGN, estabelecido conforme a POLÍTICA DE SEGURANÇA DO PSC DIGITALSIGN, para garantir a continuidade dos seus serviços críticos.

4.6.1.2. O PSC DIGITALSIGN 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 DIGITALSIGN 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 DIGITALSIGN 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 DIGITALSIGN possui o Plano de Continuidade de Negócios onde são descritos os procedimentos de recuperação utilizados quando recursos computacionais, software ou dados estiverem corrompidos ou houver suspeita de corrupção.

4.6.3. SINCRONISMO DO PSC

Os servidores e demais ativos de rede do PSC DIGITALSIGN estão sincronizados com a hora Greenwich Mean Time – GMT. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT. No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

4.6.4. SEGURANÇA DOS RECURSOS APÓS DESASTRE NATURAL OU DE OUTRA NATUREZA

O PSC DIGITALSIGN possui um Plano de Continuidade de Negócios onde são descritos os procedimentos de recuperação 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. Caso seja necessária extinção dos serviços do PSC DIGITALSIGN serão efetuados os procedimentos aplicáveis no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

4.7.2. Possíveis rompimentos com os subscritores e terceiras partes, em consequência da cessação dos serviços de armazenamento dos certificados digitais serão minimizados e, em particular, será assegurada a manutenção continuada da informação necessária para que não haja prejuízos aos subscritores e as terceiras partes.

4.7.3. Antes de o PSC DIGITALSIGN 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 DIGITALSIGN 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 DIGITALSIGN 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 são descritos os controles físicos referentes às instalações que abrigam os sistemas do PSC DIGITALSIGN.

5.1.1. CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES DO PSC

As instalações do PSC DIGITALSIGN, não são publicamente identificados, sendo que possui relevantes aspectos de construção das instalações para os controles de segurança física, compreendendo entre outros:

a) Todas as Instalações de 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

O acesso físico ao PSC DIGITALSIGN é gerenciado e controlado por um sistema de controle de acesso físico que garanta a segurança de suas instalações, conforme a POLÍTICA DE SEGURANÇA DO PSC DIGITALSIGN e os requisitos que seguem.

5.1.2.1. NÍVEIS DE ACESSO

São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos do PSC DIGITALSIGN.

5.1.2.1.1. O primeiro nível – ou nível 1 – situar-se após a primeira barreira de acesso às instalações do PSC. O ambiente de nível 1 do PSC DIGITALSIGN desempenha a função de interface com cliente ou fornecedores que necessita comparecer ao PSC.

5.1.2.1.2. O segundo nível – ou nível 2 – é interno ao primeiro e requer 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.

5.1.2.1.3. O terceiro nível – ou nível 3 – Situar-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação do PSC. Qualquer atividade relativa ao armazenamento de certificados digitais dos usuários é realizada nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível, sendo que pessoas não autorizadas só podem permanecer nesse nível se estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos uma pessoa que possua esta permissão. No terceiro nível são controladas tanto as entradas quanto as saídas de

cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: cartão eletrônico e identificação biométrica ou digitação de senha.

5.1.2.1.4. O quarto nível – ou nível 4 – especificamente para os PSC de armazenamento de chaves privadas, interior ao terceiro, é onde ocorrerem 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 possui 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 é exigida enquanto o ambiente estiver ocupado.

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

5.1.2.1.6. A sala-cofre é construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

5.1.2.2. SISTEMAS FÍSICOS DE DETECÇÃO

5.1.2.2.1. A segurança de todos os ambientes do PSC DIGITALSIGN é 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 adota, adicionalmente, de Circuito Interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não permitem a captura de senhas digitadas nos sistemas.

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

5.1.2.2.5. O PSC DIGITALSIGN possui mecanismos que permitem, 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 4.

5.1.3. ENERGIA E AR-CONDICIONADO DO AMBIENTE DE NÍVEL 4 DO PSC

5.1.3.1. A infraestrutura do ambiente de nível 4 do PSC DIGITALSIGN é 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 do PSC e seus respectivos serviços. O PSC DIGITALSIGN possui um sistema de aterramento implantado.

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

5.1.3.3. São 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. São 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 (seis) 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 DO PSC DIGITALSIGN. Qualquer modificação nessa rede é documentada e autorizada previamente.

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 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 é permanentemente monitorada.

5.1.3.9. A capacidade de redundância de toda a estrutura de energia e ar-condicionado do ambiente de nível 4 do PSC são garantidas por meio de nobreaks e geradores de porte compatível.

5.1.4. EXPOSIÇÃO À ÁGUA NAS INSTALAÇÕES DO PSC

O ambiente de Nível 4 do PSC DIGITALSIGN está 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 DIGITALSIGN não é permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do nível 2.

5.1.5.2. Existem 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. O ambiente de nível 4 do PSC não possui saídas de água, para evitar danos aos equipamentos causados pela existência de sistema de sprinklers.

5.1.5.3. O ambiente de nível 4 possui sistema de prevenção contra incêndios, que aciona alarmes preventivos uma vez detectada fumaça no ambiente.

5.1.5.4. Nos demais ambientes do PSC DIGITALSIGN existem 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 são implantados pelo PSC DIGITALSIGN para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.

5.1.6. ARMAZENAMENTO DE MÍDIA NAS INSTALAÇÕES DO PSC

O PSC DIGITALSIGN atende 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 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 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 é usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala está disponível ao pessoal autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e atende aos requisitos mínimos estabelecidos por este documento para um ambiente de nível 2.

5.2. CONTROLES PROCEDIMENTAIS

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

5.2.1. PERFIS QUALIFICADOS

5.2.1.1. O PSC DIGITALSIGN garante 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 estão limitadas de acordo com seu perfil.

5.2.1.2. O PSC DIGITALSIGN estabelece 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 recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4. Quando um empregado se desligar do PSC DIGITALSIGN, suas permissões de acesso são revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro do PSC, são revistas suas permissões de acesso. Existe 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 requererem 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 podem ser executadas por um único empregado.

5.2.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

5.2.3.1. A DPPSC garante que todo empregado do PSC DIGITALSIGN tem 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 são:

a) diretamente atribuídos a um único empregado;

b) não são compartilhados; e

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

5.2.3.3. O PSC DIGITALSIGN implementa um padrão de utilização de "senhas fortes", definido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DO PSC DIGITALSIGN, com procedimentos de validação dessas senhas.

5.3. CONTROLES DE PESSOAL

Nos itens seguintes são descritos requisitos e procedimentos, implementados pelo PSC DIGITALSIGN 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. O PSC DIGITALSIGN garante que todos os empregados, 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 DIGITALSIGN envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais são admitidos conforme o estabelecido na POLÍTICA DE SEGURANÇA DO PSC DIGITALSIGN. O PSC DIGITALSIGN 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 DIGITALSIGN envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais são 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. PSC DIGITALSIGN poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3. REQUISITOS DE TREINAMENTO

Todo o pessoal do PSC DIGITALSIGN envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais receberem 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 DIGITALSIGN envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais são mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas do PSC.

5.3.5. FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

O PSC DIGITALSIGN não implementa rodízio de cargos.

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, o PSC DIGITALSIGN, de imediato, suspenderá o acesso dessa pessoa aos sistemas, assim instaurando 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 conterá, 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 DIGITALSIGN encaminhará 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 DIGITALSIGN 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 DO PSC DIGITALSIGN. O PSC DIGITALSIGN poderá definir requisitos adicionais para a contratação.

5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL

5.3.8.1. O PSC DIGITALSIGN disponibiliza para todo o seu pessoal pelo menos:

a) sua DPPSC;

b) a POLÍTICA DE SEGURANÇA DO PSC DIGITALSIGN;

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 está devidamente classificada segundo a política de classificação de informação definida pelo PSC e é mantida atualizada.

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. CONTROLES DE SEGURANÇA COMPUTACIONAL

6.1.1. DISPOSIÇÕES GERAIS

Neste item são indicados 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 DO PSC DIGITALSIGN.

6.1.2. REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL

6.1.2.1. Os sistemas e os equipamentos do PSC DIGITALSIGN, usados nos processos de gerenciamento dos sistemas de armazenamento de chaves privadas implementam, 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 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 são 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, serão destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade do PSC. Todos esses eventos são registrados para fins de auditoria.

6.1.2.4. Qualquer equipamento incorporado ao PSC 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 a seguir são descritos, quando aplicáveis, os controles implementados pelo PSC DIGITALSIGN no desenvolvimento de sistemas e no gerenciamento de segurança.

6.2.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA

6.2.1.1. O PSC DIGITALSIGN utiliza preferencialmente sistemas e tecnologias certificadas. Quaisquer desenvolvimentos e/ou customizações são realizadas em ambiente de desenvolvimento/homologação antes da sua passagem a produção.

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

6.2.2. CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.2.2.1. O PSC DIGITALSIGN utiliza ferramentas e procedimentos formais 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 é ser usada para a instalação e a contínua manutenção do sistema do PSC.

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 da DPPSC são descritos os controles relativos à segurança da rede do PSC DIGITALSIGN, incluindo *firewall* e recursos similares, observado o disposto da POLÍTICA DE SEGURANÇA DO PSC DIGITALSIGN.

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 aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes 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 permitam 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 DIGITALSIGN é permitido somente para os seguintes serviços:

a) não se aplica;

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 registro de auditoria.

6.3.2.3. O Oficial 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 possui 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 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 provem 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 são, 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 implementa 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 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 DIGITALSIGN 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 DIGITALSIGN 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) Não se aplica.

8.1.4. O PSC DIGITALSIGN 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. 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.

9.1.1. OBRIGAÇÕES DO PSC

Estão incluídas nas obrigações da PSC DIGITALSIGN:

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 ICPBrasil;

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.

9.1.2. OBRIGAÇÕES DO SUBSCRITOR

Ao contratar um serviço do PSC DIGITALSIGN, 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 Não se aplica.

9.1.3.2 Não se aplica.

9.1.3.3 Não se aplica.

9.2. RESPONSABILIDADES

9.2.1. RESPONSABILIDADES DO PSC

O PSC DIGITALSIGN responde pelos danos a que der causa.

9.3. RESPONSABILIDADE FINANCEIRA

9.3.1. INDENIZAÇÕES DEVIDAS PELA TERCEIRA PARTE (RELYING PARTY)

Não se aplica.

9.3.2. RELAÇÕES FIDUCIÁRIAS

O PSC DIGITALSIGN 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

Os processos administrativos cabíveis, relativos às operações do PSC DIGITALSIGN seguirão a legislação especifica na qual os procedimentos questionados se enquadram.

9.4. INTERPRETAÇÃO E EXECUÇÃO

9.4.1. LEGISLAÇÃO

O PSC é regido pela Medida Provisória nº 2.200-02, pelas Resoluções do Comitê Gestor da ICP-Brasil e da Secretaria da Receita Federal do Brasil, bem como pelas demais leis em vigor no Brasil.

9.4.2. FORMA DE INTERPRETAÇÃO E NOTIFICAÇÃO

9.4.2.1. Caso uma ou mais disposições desta DPPSC venha a ser, por qualquer razão, considerada inválida, ilegal, ou não aplicável por lei, tal não afeta as demais disposições, sendo esta DPPSC interpretada como se não contivesse tal disposição e, na medida do possível, interpretada para manter a intenção original da DPPSC.

Nesse caso, serão tomadas de imediato as medidas necessárias para adequar esta DPPSC.

9.4.2.2. As notificações ou qualquer outra comunicação necessária, relativas às práticas descritas nesta DPPSC, são feitas através de mensagem eletrônica assinada digitalmente, com chave pública certificada pela ICP-Brasil, ou por escrito e entregue ao PSC DIGITALSIGN.

9.4.3. PROCEDIMENTOS DE SOLUÇÃO DE DISPUTA

9.4.3.1. Caso haja de conflito entre a DPPSC e outras declarações, políticas, planos, acordos, contratos ou documentos que o PSC adotar, prevalecerá o disposto nesta DPPSC.

9.4.3.2. Estabelece-se que a DPPSC do PSC DIGITALSIGN 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, são especificadas pelo PSC DIGITALSIGN 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

Pelo armazenamento de chaves privadas para usuários finais o será cobrado o valor estabelecido contratualmente.

9.5.2. TARIFAS DE SERVIÇO DE ASSINATURA DIGITAL

Não se aplica.

9.5.3. TARIFAS DE SERVIÇO DE VERIFICAÇÃO DA ASSINATURA DIGITAL

Não se aplica.

9.5.4. OUTRAS TARIFAS

Pelos demais serviços será cobrado o valor estabelecido contratualmente.

9.5.5. POLÍTICA DE REEMBOLSO

Em caso de revogação do certificado por motivo de comprometimento da chave privada provocada pelo PSC DIGITALSIGN, será emitido gratuitamente outro certificado em substituição.

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. Não se aplica.

9.6.1.3. Não se aplica.

9.6.2. TIPOS DE INFORMAÇÕES SIGILOSAS

9.6.2.1. Todas as informações coletadas, geradas, transmitidas e mantidas no PSC DIGITALSIGN são consideradas sigilosas, exceto aquelas informações citadas no item 9.6.3.

9.6.2.2. Como princípio geral, nenhum documento, informação ou registro fornecido ao PSC DIGITALSIGN deverá ser divulgado, exceto quando for estabelecido um acordo com o subscritor para a sua publicação mais ampla.

9.6.3. TIPOS DE INFORMAÇÕES NÃO-SIGILOSAS

Os seguintes documentos do PC DIGITALSIGN são considerados documentos não-sigilosas:

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

O PSC DIGITALSIGN fornecerá, mediante ordem judicial ou por determinação legal, todos os documentos, informações ou registros sob sua guarda.

9.6.5. INFORMAÇÕES A TERCEIROS

Nenhum documento, informação ou registro sob a guarda do PSC DIGITALSIGN é fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, através de instrumento devidamente constituído, estiver corretamente identificada e autorizada para o fazer.

9.6.6. OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO

Não se aplica.

9.7. DIREITOS DE PROPRIEDADE INTELECTUAL

Os serviços prestados pelo PSC DIGITALSIGN implica a transferência, cessão ou licença de direitos de propriedade intelectual de softwares, certificados, políticas, especificações de práticas e procedimentos, nomes, chaves criptográficas e outros.

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 ICPBRASIL 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.