Declaração de Práticas do Prestador de Serviço de Confiança da SyngularID (DPPSC SyngularID)

Versão 1.0

Janeiro de 2023

Classificação da informação – Pública

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item alterado	Descrição da alteração
1.0	Janeiro/2023	-	Não há	Versão inicial – Baseada no DOC-ICP-17 versão 2.0

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 SyngularID – PSC SyngularID 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].

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 do Prestador de Serviço de Confiança - DPPSC - estabelece os requisitos mínimos a serem obrigatoriamente observados pelo PSC SyngularID integrante da ICP-Brasil. A DPPSC descreve as práticas e os procedimentos operacionais e técnicos empregados pelo PSC SyngularID na execução dos serviços.

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. Este documento adota a estrutura disponibilizada no DOC-ICP-17 versão 2.0 [8].

1.1.7. Aplicam-se ainda ao PSC SyngularID, no que couber, 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

Esta é a Declaração de Práticas de Prestador de Serviço de Confiança SyngularID, integrante da ICP-Brasil e comumente referida como “DPPSC SyngularID”, cujo OID (object identifier) é 2.16.76.1.11.9.

1.3. Comunidade e Aplicabilidade

1.3.1 Prestadores de Serviço de Confiança

Esta DPPSC refere-se ao PSC SyngularID, no âmbito da ICP-Brasil.

1.3.1.1. Endereço da página web (URL) onde estão publicados os serviços prestados pelo PSC: https://syngularid.com.br/repositorio/psc/.

1.3.1.2. O PSC SyngularID desempenha as atividades descritas nesta DPPSC, no DOC-ICP-17.01 e adendos relacionados. O PSC SyngularID se classifica na categoria:

(a) armazenamento de chaves privadas dos subscritores.

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

1.3.2 Subscritores

1.3.2.1. Pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras, podem solicitar os serviços descritos nesta DPPSC.

1.3.2.2. Os subscritores manifestam plena aprovação aos serviços contratados pelo PSC SyngularID, assim como o nível de monitoramento que o PSC realizará, para fins exclusivos de proteção da chave privada do titular na prestação de armazenamento de chaves privadas.

1.3.2.3. Não se aplica.

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

1.3.3 Aplicabilidade

As aplicações para as quais são adequados os certificados e, quando cabíves, as aplicações para as quais existam restrições ou proibições para o uso destes certificados, estão relacionados na Política de Certificado correspondente.

1.4. Dados de Contato

Instituição

Nome: SyngularID Tecnologia.
Endereço: Rua Lauro Linhares 2010 9º andar - Trindade - CEP: 88036-002 - Florianópolis/SC.

Unidade para Suporte

Nome: SyngularID Tecnologia.
Endereço: Rua Lauro Linhares 2010 9º andar - Trindade - CEP: 88036-002 - Florianópolis/SC Telefone: 48-3234-6696.
E-mail: compliance@syngularid.com.br

Gestor do PSC

Nome: Carlos Francisco Tatara
Endereço: Rua Lauro Linhares 2010 9º andar - Trindade - CEP: 88036-002 - Florianópolis/SC Telefone: 48-3234-6696.
E-mail: carlostatara@syngularid.com.br

1.5. Procedimentos de mudança de especificação

Qualquer alteração na DPPSC é submetida à aprovação da AC-Raiz. Esta DPPSC é atualizada sempre que um novo serviço é implementado pelo PSC.

1.5.1 Políticas de publicação e notificação

O PSC SyngularID publica esta DPPSC em seu site https://syngularid.com.br/repositorio/psc/.

1.5.2 Procedimentos de aprovação

Esta DPPSC foi submetida à aprovação, durante o processo de credenciamento do PSC SyngularID, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

1.6. Definições e Acrônimos

A tabela abaixo contém as siglas e definições utilizadas no texto deste DPPSC.

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 Certificação
PCO	Plano de Capacidade Operacional
PCN	Plano de Continuidade de Negócio
PSC	Prestadores de Serviço de Certificação
RFC	*Request For Comments*
TDSM	*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 são definidas as informações a serem publicadas pelo PSC SyngularID responsável por esta DPPSC, bem como o modelo pelo qual são disponibilizadas e sua disponibilidade.

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

(a) capacidade de armazenamento dos certificados 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;

(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 restrições para a consulta e leitura desta DPPSC. Os acessos para escrita nos locais de armazenamento e publicações são permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

3. IDENTIFICAÇÃO E AUTORIZAÇÃO

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

4. REQUISITOS OPERACIONAIS

4.1. Armazenamento e acesso aos certificados do subscritor

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

(a) linguagens de programação utilizadas para construção da plataforma de acesso são: Java e C++;

(b) meio de acesso disponibilizado ao subscritor é utilizando web service e aplicativo móvel;

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

(d) arquitetura de rede segue o modelo TCP/IP.

4.2. Serviço de criação, validação e armazenamento de assinaturas digitais

Não se aplica.

4.3. Procedimentos de Auditoria de Segurança

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

4.3.1 Tipos de eventos registrados

4.3.1.1. O PSC SyngularID 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 dos 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) não se aplica;

(k) não se aplica;

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

4.3.1.2. O PSC SyngularID 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. Seguem abaixo todas as informações que são registradas pelo PSC SyngularID:

(a) criação/remoção de slot;

(b) criação/remoção de chave;

(c) geração de CSR;

(d) importação de certificado; e

(e) uso da chave.

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

4.3.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços do PSC SyngularID são armazenadas, eletrônica ou manualmente, em local único, conforme a PS do PSC SyngularID.

4.3.2 Frequência de auditoria de registros (*logs*)

A periodicidade de auditoria não será superior a uma semana e são analisados pelo pessoal operacional do PSC SyngularID. 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 SyngularID 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 protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo

os requisitos da PS do PSC SyngularID.

4.3.4.2. As informações de auditoria geradas manualmente são protegidas contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da PS do PSC SyngularID.

4.3.4.3. Os mecanismos de proteção descritos neste item obedecem à PS do PSC SyngularID.

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

Os registros de auditoria e sumários de auditoria dos equipamentos utilizados pelo PSC SyngularID têm cópias de segurança (*backup*) semanais, feitas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas. Estas cópias são enviadas a Gerência de Segurança.

(a) Diariamente: cópia de segurança;

(b) Semanalmente: cópia armazenada para processos de auditoria.

4.3.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria, interno à PSC SyngularID é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

4.3.7 Notificação de agentes causadores de eventos

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

4.3.8 Avaliações de vulnerabilidade

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

4.4. Arquivamento de Registros

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

4.4.1 Tipos de registros arquivados

4.4.1.1. As seguintes informações são registradas e arquivadas pelo PSC SyngularID:

(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 dos registros de armazenamento de chaves privadas e arquivos de auditoria é de 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 sua classificação, conforme a PS do PSC SyngularID.

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

4.4.3.1. Uma segunda cópia de todo o material arquivado é armazenado em ambiente diferente às instalações principais do PSC SyngularID, 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 SyngularID verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.4.4 Requisitos para datação de registros

Informações de data e hora nos registros baseia-se no horário *Greenwich Mean Time* (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos for zero. 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 arquivo

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

4.4.6 Procedimentos para obter e verificar informações de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente ao PSC SyngularID, 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 SyngularID, estabelecido conforme a PS do PSC SyngularID, para garantir a continuidade dos seus serviços críticos.

4.6.1.2. O PSC SyngularID 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 SyngularID irá 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 SyngularID não mais proverá 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 SyngularID possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos e, que podem ser resumidas da seguinte forma:

(a) Identifica-se todos os elementos corrompidos;

(b) O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante; e

(c) Uma análise do nível do comprometimento é realizada para determinar quais ações serão executadas.

4.6.3 Sincronismo do PSC

Não se aplica.

4.6.4 Segurança dos recursos após desastre natural ou de outra natureza

O PSC SyngularID possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza.

4.7. Extinção dos serviços de PSC

4.7.1. Caso seja necessária a extinção dos serviços do PSC SyngularID, serão realizados os procedimentos aplicáveis dispostos no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

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

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

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

(b) o PSC SyngularID 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 SyngularID manterá ou transferirá a outro PSC, após aprovação da AC-Raiz, suas obrigações relativas a disponibilizar seus sistemas e hardwares, por um período razoável; e

(d) o PSC SyngularID notificará todas as entidades afetadas.

4.7.4. O PSC SyngularID 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 estão descritos os controles de segurança implementados pelo PSC SyngularID para executar de modo seguro suas funções, de acordo com o REGULAMENTO OPERACIONAL DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL - DOC-ICP-17.01 [4].

5.1. Segurança Física

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

5.1.1 Construção e localização das instalaÇões do PSC

Todos os aspectos de construção das instalações do PSC SyngularID, relevantes para os controles de segurança física, foram executados por técnicos especializados, compreendendo entre outros:

(a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;

(b) Instalações para sistemas de telecomunicações;

(c) Sistemas de aterramento e de proteção contra descargas atmosféricas; e

(d) Iluminação de emergência.

5.1.2 Acesso físico nas instalações do PSC

O acesso físico às dependências do PSC SyngularID é gerenciado e controlado internamente conforme o previsto na PS do PSC SyngularID 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 utilizados na operação do PSC SyngularID.

O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações do PSC SyngularID. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação do PSC transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo do PSC SyngularID é executado nesse nível.

Excetuados os casos previstos em lei, o porte de armas não é admitido no ambiente onde estão instalados os equipamentos utilizados na operação do PSC SyngularID, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, pagers, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

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

O terceiro nível – ou nível 3 – é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação do PSC SyngularID. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não estejam envolvidas com essas atividades não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autor- izada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: a identificação individual, como cartão eletrônico, e a identificação biométrica.

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

O quarto nível - ou nível 4 – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação do PSC SyngularID. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso

do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

No quarto nível, todas as paredes, o piso e o 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 a chamada sala-cofre - possuem proteção contra interferência eletromagnética externa.

A sala-cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.

5.1.2.2. Sistemas físicos de detecção

5.1.2.2.1. A segurança de todos os ambiente do PSC SyngularID 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 é 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 é dotado 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 SyngularID possui 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 está baseado em um ambiente 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 SyngularID é 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. É implementado sistema de aterramento.

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 PS do PSC SyngularID. 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 SyngularID é garantida 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 SyngularID está instalado em local protegido contra a exposição à água, infiltracões e inundações.

5.1.5 Prevenção e proteção contra incêncio nas instalações do PSC

5.1.5.1. Nas instalações do PSC 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. Existe o sistema de sprinklers no prédio, porém o ambiente de nível 3 do PSC SyngularID não possui saídas de água, para evitar danos aos equipamentos.

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 SyngularID existem extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitam o seu acesso e manuseio.

5.1.5.5. Mecanismos específicos estão implantados pelo PSC SyngularID 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 SyngularID 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 fisicamente destruídos.

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

Uma sala de armazenamento externa à instalação técnica principal do PSC SyngularID 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 desta DPPSC são descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados no PSC SyngularID, com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

5.2.1 Perfis qualificados

5.2.1.1. O PSC SyngularID 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 SyngularID 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, 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 SyngularID recebem 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 SyngularID, 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 devolve 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 SyngularID requerem a presença de, no mínimo, 2 (dois) empregados com perfis qualificados. Para os casos de cópias das chaves dos usuários e portabilidade da mesma são necessários, no mínimo, 3 (três) empregados com perfis distintos e qualificados. As demais tarefas do PSC são executadas por um único empregado.

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado do PSC SyngularID que ocupa perfil designado 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:

(a) são 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 SyngularID implementa um padrão de utilização de ”senhas fortes”, definido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [2], com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pelo PSC SyngularID 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. Todos os empregados do PSC SyngularID, encarregados de tarefas operacionais, tem 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 SyngularID envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas é admitido conforme o estabelecido em sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [2]. O PSC SyngularID 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 SyngularID envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas é 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 SyngularID poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

Todo o pessoal do PSC SyngularID envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

(a) princípios e tecnologias dos sistemas e hardwares de armazenamento de chaves privadas em uso no PSC;

(b) ICP-Brasil;

(c) princípios e tecnologias de certificação digital;

(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 SyngularID envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas do PSC.

5.3.5 Frequência e sequência de rodízio de cargos

O PSC SyngularID 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 SyngularID, de imediato, suspenderá o acesso dessa pessoa aos sistemas, instaurará processo administrativo para apurar os fatos e, se for o caso, adotará 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 SyngularID 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 SyngularID envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas é contratado conforme estabelecido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [2]. O PSC SyngularID poderá definir requisitos adicionais para a contratação.

5.3.8 Documentação fornecida ao pessoal

5.3.8.1. O PSC SyngularID disponibiliza para todo o seu pessoal:

(a) esta DPPSC;

(b) a sua Política de Segurança;

(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, estão definidas as medidas de segurança implantadas pelo PSC SyngularID para proteger as chaves privadas dos subscritores. Também são definidos outros controles técnicos de segurança utilizados na execução das funções operacionais.

6.1. Controles de Segurança Computacional

6.1.1 Disposições Gerais

Neste item são indicados os mecanismos utilizados para prover a segurança das estações de trabalho, servidores e demais sistemas e equipamentos, observado o disposto conforme estabelecido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [2].

6.1.2 Requisitos técnicos específicos de segurança computacional

6.1.2.1. Os sistemas e os equipamentos do PSC SyngularID, 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 de chaves 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, são 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 SyngularID é preparado e configurado como previsto na PS implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.1.3 Classificação da segurança computacional

Não se aplica.

6.2. Controles Técnicos do Ciclo de Vida

Nos itens seguintes estão descritos, quando aplicáveis, os controles implementados pelo PSC SyngularID no desenvolvimento de sistemas e no gerenciamento de segurança.

6.2.1 Controles de desenvolvimento de sistema

6.2.1.1. O desenvolvimento do sistema utiliza ferramentas de versionamento de código, onde toda modificação pode ser rastreada ao seu devido responsável. O processo de fechamento de versão ocorre através de mecanismo de integração contínua, com processos de validação e aprovação automáticos e manuais, incluindo aprovação do gestor do projeto. As novas versões são testadas e homologadas em ambiente de homologação antes de serem enviadas para ambiente de produção.

6.2.1.2. Os processos de projeto e desenvolvimento conduzidos pelo PSC SyngularID provem

documentação suficiente para suportar avaliações externas de segurança dos componentes do PSC SyngularID.

6.2.2 Controles de gerenciamento de seguranca

6.2.2.1. O PSC SyngularID verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.2.2.2. Uma metodologia formal de gerenciamento de configuração é 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 estão descritos os controles relativos à segurança da rede do PSC SyngularID, incluindo firewall e recursos similares, observado o disposto conforme estabelecido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [2].

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 operam em ambiente de, no mínimo, nível 4.

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 permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

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

(a) Não aplicável.

(b) pelo PSC, para a administração dos sistemas de gestão a partir de equipamento conectado por rede interna;

(c) pelo subscritor, para a armazenamento e acesso à chave privada.

6.3.2 Firewall

6.3.2.1. Mecanismos de *firewall* são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Os firewalls são dispostos e configurados de forma a promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida ”zona desmilitarizada” (DMZ) – em relação aos equipamentos com acesso exclusivamente interno ao PSC.

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

6.3.2.3. O 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 tem capacidade de ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar *traps* SNMP, executar programas definidos pela administração da rede, enviar *e-mail* aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

6.3.3.2. O sistema de detecção de intrusão tem a capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

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

6.3.4 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – são registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro é, no mínimo, semanal e todas as ações tomadas em decorrência desse exame são documentadas.

6.3.5 Outros controles de segurança de rede

6.3.5.1. O PSC SyngularID 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 SyngularID.

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 SyngularID estão em conformidade com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [5].

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 nos PSC SyngularID têm por objetivo verificar se seus processos, procedimentos e atividades estão em conformidade com suas respectivas DPPSC, PCO e PS, demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust*.

8.1.2. As fiscalizações do PSC SyngularID 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 do PSC SyngularID 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 SyngularID 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].

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 estão descritas as obrigações gerais das entidades envolvidas.

9.1.1 Obrigações do PSC

Neste item estão incluídas as obrigações do PSC SyngularID abaixo relacionadas:

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

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

(c) não se aplica;

(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 armazenados.

9.1.2 Obrigações do Subscritor

Ao contratar um serviço do PSC SyngularID, 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. Responsabilidade

9.2.1 Responsabilidades do PSC

O PSC SyngularID responde pelos danos a que der causa.

9.3. Responsabilidade Financeira

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

Exceto na hipótese de prática de ato ilícito, não há responsabilidade da terceira parte (*relying party*) perante o PSC SyngularID.

9.3.2 Relações Fiduciárias

O PSC SyngularID 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 SyngularID seguirão a legislação específica na qual os procedimentos questionados se enquadrarem.

9.4. Interprestação e Execução

9.4.1 Legislação

Esta DPPSC é regida pela Medida Provisória nº 2.200-02, pelas Resoluções do Comitê Gestor da ICP-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, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento. Nesse caso, o corpo técnico, do PSC SyngularID, examinará a disposição inválida e proporá à Comissão Técnica, no prazo máximo de 30 dias, nova redação ou retirada da disposição afetada. As práticas descritas nesta DPPSC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.4.2.2. Todas solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas nessa DPPSC serão realizadas por iniciativa do PSC SyngularID por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil.

9.4.3 Procedimentos de solução de disputa

9.4.3.1. No caso de um conflito entre esta DPPSC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nesta situação esta DPPSC será alterada para a solução da disputa.

9.4.3.2. Em caso de conflito prevalecem as práticas e procedimentos da ICP-Brasil.

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

9.5. Tarifas do Serviços

Nos itens a seguir, está especificada pelo PSC SyngularID a política tarifária e de reembolso aplicáveis, se for o caso.

9.5.1 Tarifas de armazenamento de certificados digitais para usuários finais

Variável conforme definição interna Comercial.

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

Variável conforme definição interna Comercial.

9.5.5 Política de reembolso

Variável conforme definição interna Comercial.

9.6. Sigilo

9.6.1 Disposições Gerais

9.6.1.1. A chave privada dos subscritores é mantida pelo PSC SyngularID, 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 pelo PSC SyngularID 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 SyngularID deverá ser divulgado.

9.6.3 Tipos de informações não sigilosas

Os seguintes documentos do PSC SyngularID são considerados documentos não sigilosos:

(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 SyngularID fornecerá, mediante ordem judicial ou por determinação legal, documentos, informações ou registros sob sua guarda.

9.6.5 Informações a terceiros

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

9.6.6 Outras circunstâncias de divulgação de informação

Nenhuma outra liberação de informação, que não as expressamente descritas nesta DPPSC, é permitida.

9.7. Direitos de Propriedade Intelectual

A SyngularID Tecnologia detém todos os direitos de propriedade intelectual sobre as ideias, conceitos, técnicas e invenções, processos e/ou obras, políticas, especificações de práticas e procedimentos, incluídas ou utilizadas nos produtos e serviços fornecidos pelo PSC SyngularID nos termos dessa DPPSC. Os Direitos de Propriedade terão proteção conforme a legislação aplicável.

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	DOC-ICP-04
[2]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[4]	REGULAMENTO OPERACIONAL DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17.01
[5]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[6]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[8]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17

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), August* 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, November* 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, March* 2002.

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