www.serpro.gov.br

Declarações de Práticas
de
Prestador de Serviço de Confiança

SERPRO

(DPPSC SERPRO)

Versão 2.0 de Novembro 2020

SUMÁRIO

1. INTRODUÇÃO.....6

1.1. Visão Geral.....6
1.2. Identificação.....7
1.3. Comunidade e Aplicabilidade.....7
1.3.1. Prestadores de Serviço de Confiança.....7
1.3.2. Subscritores.....7
1.3.3. Aplicabilidade.....7
1.4. Dados de Contato.....8
1.5. Procedimentos de mudança de especificação.....8
1.5.1. Políticas de publicação e notificação.....8
1.5.2. Procedimentos de aprovação.....8
1.6. Definições e Acrônimos.....9

2. RESPONSABILIDADE DO REPOSITÓRIO E PUBLICAÇÃO.....10

2.1. Publicação.....10
2.1.1. Publicação de informação do PSC.....10
2.1.2. Freqüência de publicação.....10
2.1.3. Controles de acesso.....10

3. IDENTIFICAÇÃO E AUTORIZAÇÃO.....10

4. REQUISITOS OPERACIONAIS.....11

4.1. Armazenamento e acesso aos certificados do subscritor.....11
4.2. Serviço de criação, validação e armazenamento de assinaturas digitais.....11
4.3. Procedimentos de Auditoria de Segurança.....11
4.3.1. Tipos de eventos registrados.....11
4.3.2. Freqüência de auditoria de registros (logs).....12
4.3.3. Período de retenção para registros (logs) de auditoria.....12
4.3.4. Proteção de registro (log) de auditoria.....12
4.3.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria.....13
4.3.6. Sistema de coleta de dados de auditoria.....13
4.3.7. Notificação de agentes causadores de eventos.....13
4.3.8. Avaliações de vulnerabilidade.....13
4.4. Arquivamento de Registros.....14
4.4.1. Tipos de registros arquivados.....14
4.4.2. Proteção de arquivo.....14

4.4.3. Procedimentos para cópia de segurança (backup) de arquivo.....14
4.4.4. Requisitos para datação de registros.....14
4.4.5. Sistema de coleta de dados de arquivo.....15
4.4.6. Procedimentos para obter e verificar informação de arquivo.....15
4.5. Liberação do espaço do subscritor.....15
4.6. Comprometimento e Recuperação de Desastre.....15
4.6.1. Disposições Gerais.....15
4.6.2. Recursos computacionais, software, e dados corrompidos.....16
4.6.3. Sincronismo do PSC.....16
4.6.4. Segurança dos recursos após desastre natural ou de outra natureza.....16
4.7. Extinção dos serviços de PSC.....16

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL.....17

5.1. Segurança Física.....17
5.1.1. Construção e localização das instalações do PSC.....17
5.1.2. Acesso físico nas instalações do PSC.....18
5.1.3. Energia e ar-condicionado do ambiente de nível 3 do PSC.....19
5.1.4. Exposição à água nas instalações do PSC.....20
5.1.5. Prevenção e proteção contra incêndio nas instalações do PSC.....20
5.1.6. Armazenamento de mídia nas instalações do PSC.....21
5.1.7. Destruição de lixo nas instalações do PSC.....21
5.1.8. Sala externa de arquivos (off-site) para PSC.....21
5.2. Controles Procedimentais.....21
5.2.1. Perfis qualificados.....22
5.2.2. Número de pessoas necessário por tarefa.....22
5.2.3. Identificação e autenticação para cada perfil.....22
5.3. Controles de Pessoal.....23
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade.....23
5.3.2. Procedimentos de verificação de antecedentes.....23
5.3.3. Requisitos de treinamento.....23
5.3.4. Freqüência e requisitos para reciclagem técnica.....24
5.3.5. Freqüência e seqüência de rodízio de cargos.....24
5.3.6. Sanções para ações não autorizadas.....24
5.3.7. Requisitos para contratação de pessoal.....25
5.3.8. Documentação fornecida ao pessoal.....25

6. CONTROLES TÉCNICOS DE SEGURANÇA.....25

6.1. Controles de Segurança Computacional.....25
6.1.1. Disposições Gerais.....25
6.1.2. Requisitos técnicos específicos de segurança computacional.....25
6.1.3. Classificação da segurança computacional.....26
6.2. Controles Técnicos do Ciclo de Vida.....26
6.2.1. Controles de desenvolvimento de sistema.....26

6.2.2. Controles de gerenciamento de segurança....26
6.2.3. Classificações de segurança de ciclo de vida....27
6.3. Controles de Segurança de Rede....27
6.3.1. Diretrizes Gerais....27
6.3.2. Firewall....27
6.3.3. Sistema de detecção de intrusão (IDS)....28
6.3.4. Registro de acessos não autorizados à rede....28
6.3.5. Outros controles de segurança de rede....28
6.4. Controles de Engenharia do Módulo Criptográfico....28

7. POLÍTICAS DE ASSINATURA....29

8. AUDITORIAS E AVALIAÇÕES DE CONFORMIDADE....29

8.1. Fiscalização e Auditoria de Conformidade....29

9. OUTROS ASSUNTOS DE CARÁTER COMERCIAL E LEGAL....29

9.1. Obrigações e direitos....29
9.1.1. Obrigações do PSC....30
9.1.2. Obrigações do Subscritor....30
9.1.3 Direitos da terceira parte (Relying Party)....31
9.2. Responsabilidades....31
9.2.1. Responsabilidades do PSC....31
9.3. Responsabilidade Financeira....31
9.3.1. Indenizações devidas pela terceira parte (Relying Party)....31
9.3.2. Relações Fiduciárias....31
9.3.3. Processos Administrativos....31
9.4. Interpretação e Execução....31
9.4.1. Legislação....31
9.4.2. Forma de interpretação e notificação....32
9.4.3. Procedimentos de solução de disputa....32
9.5. Tarifas de Serviço....32
9.5.1. Tarifas de armazenamento de certificados digitais para usuários finais....32
9.5.2. Tarifas de serviço de assinatura digital....32
9.5.3. Tarifas de serviço de verificação da assinatura digital....32
9.5.4. Tarifas de serviço para armazenamento de documentos eletrônicos....33
9.5.5 Outras tarifas....33
9.5.6. Política de reembolso....33
9.6. Sigilo....33
9.6.1. Disposições Gerais....33
9.6.2. Tipos de informações sigilosas....33
9.6.3. Tipos de informações não sigilosas....33
9.6.4. Quebra de sigilo por motivos legais....33

9.6.5. INFORMAÇÕES A TERCEIROS.....34
9.6.6. OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO.....34
9.7. DIREITOS DE PROPRIEDADE INTELECTUAL.....34

10. DOCUMENTOS DA ICP-BRASIL.....34

11. REFERÊNCIAS.....35

Controle de Alterações

Versão	Data	Responsável	Motivo	Descrição
1.0	Outubro/2018	Ronaldo Ion	Versão Inicial	Documento criado conforme DOC-ICP-17
2.0	Novembro/2020	Lucia Castelli	Revisão	Implementação Resolução 180/Inclusão Controle de Alterações
2.0	Novembro/2020	Alice Vasconcellos	Aprovação	

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento tem por base um conjunto de normativos criado para regulamentar os Prestadores de Serviço de Confiança no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1.2. O Prestador de Serviço de Confiança do SERPRO – PSC SERPRO é uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de armazenamento de certificados digitais para usuários finais, nos termos do DOC-ICP-04 [2].

1.1.3. As chaves privadas dos usuários finais são armazenadas em dispositivos normatizados conforme estabelecido no DOC-ICP-04 [2] e as assinaturas digitais no padrão ICP-Brasil são feitas pela chave do usuário em outros sistemas conforme ditame legal da ICP-Brasil.

1.1.4. Esta Declaração de Práticas de Prestador de Serviço de Confiança – DPPSC - estabelece os requisitos mínimos que são obrigatoriamente observados pelo PSC SERPRO integrante da ICP-Brasil. A DPPSC é o documento que descreve as práticas e os procedimentos operacionais e técnicos de empregados pelo PSC SERPRO na execução de seus serviços. Os procedimentos para controle dos registros necessários à eficácia das operações estão documentados no Manual de Segurança do CCD-SERPRO.

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 versão 2.0 [12].

1.1.7. Aplicam-se ainda ao PSC SERPRO, 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 SERPRO”, integrante da ICP-BRASIL e comumente referida como “DPPSC SERPRO”.
O Identificador de Objeto (OID) desta DPPSC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é 2.16.76.1.11.1

1.3. Comunidade e Aplicabilidade

1.3.1. Prestadores de Serviço de Confiança

Esta DPPSC se refere ao Prestador de Serviço de Confiança do SERPRO - PSC SERPRO.

1.3.1.1. O endereço da página web (URL) onde estão publicados os serviços prestados pelo PSC SERPRO é https://servicos.serpro.gov.br/psc/.

1.3.1.2. O PSC SERPRO desempenha as atividades descritas nesta DPPSC e no DOC-ICP- 17.01, assim como nos ADE-ICP relacionados, bem como estabelece os demais requisitos da ABNT NBR ISO 27001:2013 no Manual do SGSI do CCD. O PSC SERPRO é classificado na categoria de **"armazenamento de chaves privadas dos subscritores".**

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

1.3.2. Subscritores

1.3.2.1. Qualquer pessoa física ou jurídica que esteja cadastrada na Receita Federal pode solicitar os serviços descritos nesta DPPSC.

1.3.2.2. Os subscritores deverão manifestar plena aprovação aos serviços contratados pelo PSC SERPRO, assim como o nível de acompanhamento que o PSC SERPRO para fins exclusivos de proteção da chave privada do titular.

1.3.2.3. Não se aplica.

Nota 1: Os subscritores poderão, ao seu critério e em conformidade com o DOC-ICP-17.01[1], solicitar a sua desvinculação das suas chaves ao PSC.

1.3.3. Aplicabilidade

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

1.4. Contatos

Administrativo:

Nome: Pedro Moacir Rigo Motta

Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

E-mail: certificados@serpro.gov.br

Telefone: (61) 2021-7957

Suporte / Fraudes

Nome: Central de Serviços SERPRO

Página Web: https://atendimento.serpro.gov.br/certificacaodigital

E-mail: css.serpro@serpro.gov.br

Telefone: 0800 7282323

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 o exigir.

1.5.1. Políticas de publicação e notificação

O PSC SERPRO publica esta DPPSC em seu site https://servicos.serpro.gov.br/psc/.

1.5.2. Procedimentos de aprovação

Esta DPPSC foi submetida à aprovação, durante o processo de credenciamento, conforme 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 **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. Na URL do PSC SERPRO - https://servicos.serpro.gov.br/psc/ - estão disponíveis as informações que são publicadas pelo PSC SERPRO responsável por esta DPPSC, bem como o modo pelo qual são disponibilizadas e seu nível de disponibilidade.

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

a) capacidade de armazenamento dos certificados dos subscritores que opera;
b) sua DPPSC;
c) os serviços implementados;
d) 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 restrição ao acesso para consulta a esta DPPSC. Acessos para escrita nos locais de armazenamento e publicação são permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controle de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

3. IDENTIFICAÇÃO E AUTORIZAÇÃO

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

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) linguagem de programação JAVA na construção da plataforma de acesso;
b) web service como meio de acesso disponibilizado ao subscritor;
c) HTTPS no canal de segurança em que trafegam as autenticações;
d) TCP/IP como arquitetura de rede.

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 SERPRO com o objetivo de manter um ambiente seguro.

4.3.1. Tipos de eventos registrados

4.3.1.1. O PSC SERPRO 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) registros de acesso aos documentos dos subscritores;
l) registros de acesso ou tentativas de acesso à chave privada do subscritor.

4.3.1.2. O PSC SERPRO 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 deverão ser registradas pelo PSC SERPRO:

a) Criação/Remoção de slot;
b) Criação/Remoção de chave;
c) Geração de CSR;
d) Importação de Certificado;
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 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 SERPRO são armazenadas, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

4.3.2. Frequência de auditoria de registros (logs)

A periodicidade de auditoria de registros não será superior a uma semana e são analisados pelo pessoal operacional do PSC SERPRO. 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 SERPRO mantém localmente seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, armazena-os da maneira descrita no item 4.5.

4.3.4. Proteção de registro (log) de auditoria

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

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

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

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

O PSC SERPRO executa procedimentos de backup, de toda a solução (SISTEMA OPERACIONAL + APLICAÇÃO + BANCO DE DADOS) de duas formas:

a) Diariamente: cópia de segurança; e

b) Semanalmente: cópia armazenada para processos de auditoria.

4.3.6. Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelo sistemas do PCS, pelo sistema de controle de acesso e pelo pessoal operacional. A localização dos recursos se encontra na tabela abaixo:

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

4.3.7. Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria do PSC SERPRO 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 SERPRO, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas 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 SERPRO.

4.4.1. Tipos de registros arquivados

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

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 sua classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

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

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

4.4.4. Requisitos para datação de registros

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

4.4.5. Sistema de coleta de dados de arquivo

O sistema de coleta de dados de arquivos é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de PSC e pelo pessoal operacional. A coleta de dados se dá de acordo com a tabela abaixo:

Tipo de evento	Sistema de coleção	Registrado por
Utilização de chave	Automático	*Software* de PSC
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Correspondências formais	Manual	Pessoal de operações

4.4.6. Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos é verificada:

a) Na ocasião em que o arquivo é preparado;

b) Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

4.5. Liberação do espaço do subscritor

A liberação do espaço do subscritor consiste na eliminação das chaves e do certificado digital infraestrutura de armazenamento do PSC SERPRO sem a possibilidade de recuperação. Os logs das operações realizadas são registrados conforme item 4.3.1.3 e armazenados pelo período definido no item 4.4.1.

A liberação do espaço se dará a qualquer tempo nas hipóteses abaixo:

a) por solicitação do subscritor utilizando o canal de contato técnico definido no item 1.4;

b) pelo PSC SERPRO mediante consulta do status de vencimento ou revogação do certificado.

O procedimento de liberação é realizado pela equipe do PSC SERPRO conforme controles procedimentais definidos em 5.2.

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 SERPRO, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], para garantir a continuidade dos seus serviços críticos.

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

4.6.2. Recursos computacionais, software, e dados corrompidos

O PSC SERPRO 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 no seguinte:

a) É feita a identificação de todos os elementos corrompidos;

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

c) É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas.

4.6.3. Sincronismo do PSC

Os servidores do PSC SERPRO são sincronizados com a hora fornecida pela AC RAIZ por meio de sua Fonte Confiável do Tempo – FCT conforme DOC-ICP 07 [13] e implementado conforme o Modelo Tecnológico NTP do CCD SERPRO.

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

O PSC SERPRO 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 extinção dos serviços do PSC SERPRO serão efetuados os procedimentos aplicáveis descritos 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 conseqüência 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 SERPRO 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 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 SERPRO 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 SERPRO para executar de modo seguro suas funções, de acordo com o REGULAMENTO OPERACIONAL DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL-17.01 [10].

5.1. Segurança Física

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

5.1.1. Construção e localização das instalações do PSC

5.1.1.1. A localização e o sistema de certificação utilizado para a operação do PSC SERPRO não são publicamente identificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Todos os aspectos de construção das instalações do PSC SERPRO, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos abaixo:

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, retificadores e estabilizadores e similares;
b) Instalações para sistemas de telecomunicações;
c) Sistema 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 SERPRO é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICPBRASIL [4] e os requisitos que seguem.

5.1.2.1. Níveis de acesso

5.1.2.1.1. São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação do PSC SERPRO.

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

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação do PSC, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

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

5.1.2.1.5. 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. 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 possuem permissão de acesso não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

5.1.2.1.6. 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: a identificação individual, como cartão eletrônico, e a identificação biométrica.

5.1.2.1.7. Telefones celulares, bem como outros equipamentos portáteis de comunicação,

exceto aqueles exigidos para a operação do PSC, não são admitidos a partir do nível 3.

5.1.2.1.8. O quarto nível - ou nível 4 – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação do PSC. 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.

5.1.2.1.9. No quarto nível todas as paredes, o piso e o teto são revestidos de aço e concreto. 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.

5.1.2.1.10. 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 ambientes do PSC SERPRO 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 permite 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 SERPRO 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 está baseado em um ambiente nível 4.

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

5.1.3.1. A infraestrutura do ambiente de nível 3 do PSC SERPRO 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. 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 POLÍTICA DE SEGURANÇA DA ICPBRASIL [4]. Qualquer modificação nessa rede deverá 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 3 do PSC SERPRO é ser garantida por meio de *nobreaks* e geradores de porte compatível.

5.1.4. Exposição à água nas instalações do PSC

O ambiente de Nível 3 do PSC SERPRO 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 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. Há sistema de sprinklers no prédio, porém o ambiente de nível 3 do PSC SERPRO não possui saídas de água, para evitar danos aos equipamentos.

5.1.5.3. O ambiente de nível 3 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 SERPRO existem extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitam seu acesso e manuseio.
5.1.5.5. Mecanismos específicos estão implantados pelo PSC SERPRO para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.6. Armazenamento de mídia nas instalações do PSC

O PSC SERPRO 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 SERPRO 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 estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados no PSC SERPRO, com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

5.2.1.1. O PSC SERPRO 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 SERPRO 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 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 SERPRO, suas permissões de acesso são revogadas imediatamente. Quando há 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 SERPRO requerem a presença de, no mínimo, 2 (dois) empregados com perfis 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 que ocupa perfil designado no PSC SERPRO 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 SERPRO implementa um padrão de utilização de "senhas fortes", definido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pelo PSC SERPRO 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 SERPRO, encarregados de tarefas operacionais tem registrado em contrato ou termo de responsabilidade:
a) os termos e as condições do perfil que ocupam;
b) o compromisso de observar as normas, políticas e regras aplicáveis da ICPBrasil; 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 SERPRO responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]. O PSC SERPRO é o responsável pode 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 SERPRO envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de certificados 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 SERPRO pode definir requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

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

a) princípios e tecnologias dos sistemas e hardwares de armazenamento de certificados 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 Administrador 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. Freqüência e requisitos para reciclagem técnica

Todo o pessoal do PSC SERPRO envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas do PSC.

5.3.5. Freqüência e seqüência de rodízio de cargos

O PSC SERPRO 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 SERPRO, de imediato, suspenderá o acesso dessa pessoa aos sistemas, instaurará 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 SERPRO 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 SERPRO envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

5.3.8. Documentação fornecida ao pessoal

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

a) esta DPPSC;
b) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4];
c) documentação operacional relativa às suas atividades; e
d) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação fornecida ao pessoal está 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 SERPRO para proteger as chaves privadas dos subscritores. Também são definidos outros controles técnicos de segurança utilizados na execução das funções operacionais.

O sincronismo de tempo dos sistemas do PSC SERPRO utiliza a ICP-Brasil como fonte confiável de tempo em conformidade com o DOC-ICP-07 [11] e é implementado conforme o Modelo Tecnológico NTP do CCD SERPRO.

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 na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.1.2. Requisitos técnicos específicos de segurança computacional

6.1.2.1. Os sistemas e os equipamentos do PSC SERPRO, usados nos processos de gerenciamento dos sistemas de armazenamento de certificados 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 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 é 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 SERPRO deverá 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 SERPRO no desenvolvimento de sistemas e no gerenciamento de segurança.

6.2.1. Controles de desenvolvimento de sistema

6.2.1.1. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluído os testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente do CCD avalia e decide quando será a implementação no ambiente de produção.

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

6.2.2. Controles de gerenciamento de segurança

6.2.2.1. A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

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 SERPRO, incluindo firewall e recursos similares, observado o disposto da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.3.1.2. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como: roteadores, hubs, switches, firewall e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda os sistemas do PSC, estão localizados e operam 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 permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

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

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

a) não aplicável;

b) pelo PSC, para a administração dos sistemas de gestão a partir de equipamento

conectado por rede interna;
c) pelo subscritor, para a armazenamento e acesso à chave privada.

6.3.2. Firewall

6.3.2.1. Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Os firewalls são dispostos e configurados de forma a promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno ao PSC.
6.3.2.2. O software de firewall, entre outras características, implementa registros de auditoria.

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

6.3.3. Sistema de detecção de intrusão (IDS)

6.3.3.1. O sistema de detecção de intrusão tem capacidade de ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: envio de traps SNMP, execução de programas definidos pela administração da rede, envio de e-mail aos administradores, envio de mensagens de alerta ao firewall ou ao terminal de gerenciamento, execução de 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 provê 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 pode ser automatizada. A freqüência 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 SERPRO implementa serviço de proxy, restringindo o acesso, a partir de todas suas estações de trabalho, a serviços que não possam comprometer a segurança do ambiente do PSC.

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

6.4. Controles de Engenharia do Módulo Criptográfico

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

7. POLÍTICAS DE ASSINATURA

Não aplicável.

8. AUDITORIAS E AVALIAÇÕES DE CONFORMIDADE

8.1. Fiscalização e Auditoria de Conformidade

8.1.1. As fiscalizações e auditorias realizadas no PSC SERPRO 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 SERPRO 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 SERPRO 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 SERPRO recebeu auditoria prévia da AC-Raiz para fins de credenciamento na ICP-Brasil e passa por auditoria anual, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]. 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 estão descritas as obrigações gerais das entidades envolvidas.

9.1.1. Obrigações do PSC

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

a) operar de acordo com a sua DPPSC e com a descrição dos serviços que realiza;
b) gerenciar e assegurar a proteção das chaves privadas dos subscritores;
c) 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 do 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 certificados digitais 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 certificados armazenados.

9.1.2. Obrigações do Subscritor

Ao contratar um serviço do PSC SERPRO, se for o caso, o subscritor deve assegurar, por meio das aplicações disponibilizadas ao contratar um PSC, que o seu certificado em conjunto com o seu par de chaves 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 SERPRO 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 SERPRO 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 SERPRO seguirão a legislação específica na qual os procedimentos questionados se enquadrarem.

9.4. Interpretação e Execução

9.4.1. Legislação

A DPPSC SERPRO obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2200-2, de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil. Além disto, é apoiada em uma estrutura contratual entre SERPRO e Titulares de Certificados.

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 SERPRO, 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 SERPRO 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 DPC 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 de Serviço

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

9.5.1. Tarifas de armazenamento de certificados digitais para usuários finais

Valor referente ao serviço de armazenamento de certificados pelo PSC SERPRO e/ou contrato estipulado entre o SERPRO e a entidade que utiliza os serviços do PSC SERPRO.

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

Não se aplica.

9.5.5 Política de reembolso.

Não há tarifas adicionais que incidam sobre este serviço.

9.6. Sigilo

9.6.1. Disposições Gerais

9.6.1.1. A chave privada dos subscritores são mantidas pelo PSC SERPRO, que será responsável pelo seu sigilo.

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 SERPRO 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 SERPRO deverá ser divulgado.

9.6.3. Tipos de informações não sigilosas

Os seguintes documentos do PSC SERPRO 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

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda do PSC SERPRO é divulgado a entidades legais ou seus funcionários, exceto quando:

a) exista uma ordem judicial corretamente constituída; e
b) esteja corretamente identificado o representante da lei.

9.6.5. Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro, sob a guarda do PSC SERPRO, será fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

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

Todos os direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, documentos gerados para o PSC SERPRO de acordo com a legislação vigente pertencem e continuarão sendo propriedade do Serviço Federal de Processamento de Dados – SERPRO.

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.

[1]	PROCEDIMENTOS OPERACIONAIS MÍNIMOS PARA OS PRESTADORES DE SERVIÇOS DE CONFIANÇA DA ICP-Brasil	DOC-ICP-17.01
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[4]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[5]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[6]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS	DOC-ICP-09

	ENTIDADES INTEGRANTES DA ICP-BRASIL	
[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL	DOC-ICP-10
[11]	DIRETRIZES PARA SINCRONIZAÇÃO DE FREQUÊNCIA E DE TEMPO NA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL	DOC-ICP-07
[12]	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 3447, IETF - Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, february 2003

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

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

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

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.