Declaração de Práticas de Prestador de Serviço de Confiança Safeweb

DPPSC - SAFEWEB

Versão 1.0
Fevereiro 2019

PSC SAFEWEB
DECLARAÇÃO DE PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado
1.0	04/02/2019	N/A	Versão inicial

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1. Este documento tem por base um conjunto de normativos criados para regulamentar os Prestadores de Serviço de Confiança - PSC no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Tal conjunto se compõe dos seguintes documentos:

a) REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DOS PRESTADORES DE SERVIÇO DE CONFIANÇA – PSC DA ICP-BRASIL (DOC-ICP-17);
b) REGULAMENTO OPERACIONAL DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL [DOC-ICP-17.01];

1.1.2. O Prestador de Serviço de Confiança da ICP-Brasil é uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de armazenamento de certificados digitais e/ou chaves privadas para usuários finais, nos termos do DOC-ICP-04 [11], ou serviços de assinaturas e verificações de assinaturas digitais padrão ICP-Brasil nos documentos e transações eletrônicas ou ambos.

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

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

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

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

1.1.7. Aplicam-se ainda ao PSC SAFEWEB, no que couber, os regulamentos dispostos nos demais documentos da ICP-Brasil, entre os quais destacamos:

a) POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4];
b) CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5];
c) CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6];
d) CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7];

e) REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [9].

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 Safeweb", integrante da ICP-BRASIL e comumente referida como "DPPSC SAFEWEB".

O Object Identifier – OID desta DPPSC é **2.16.76.1.11.5.**

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. PRESTADORES DE SERVIÇO DE CONFIANÇA

Esta DPPSC se refere ao PSC SAFEWEB.

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

1.3.1.2. O PSC SAFEWEB desempenha as atividades descritas nesta DPPSC e no DOC-ICP-17.01:

a) armazenamento de certificados digitais e/ou chaves privadas dos subscritores; e
b) serviço de assinatura digital, verificação da assinatura digital.

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

1.3.2. SUBSCRITORES

Qualquer pessoa física ou jurídica que possua certificado digital emitido na ICP-Brasil válido poderá solicitar os serviços de PSC Safeweb.

Os subscritores deverão manifestar plena aprovação aos serviços contratados pelo PSC SAFEWEB, assim como o nível de acompanhamento, que o PSC SAFEWEB deverá informar e será utilizado para fins exclusivos de proteção da chave privada do titular, seja na prestação de armazenamento de certificados digitais e/ou das chaves privadas, serviços de assinaturas digitais e verificação das assinaturas digitais e, por ventura, no armazenamento de documentos assinados, neste último caso conforme legislação vigente.

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

Nota 1: Os subscritores poderão solicitar a desvinculação das suas chaves ao PSC de armazenamento de certificados digitais e/ou chaves criptográficas ao seu critério, em conformidade com os procedimentos de portabilidade dispostos no documento DOC-ICP-17.01.

1.3.3. APLICABILIDADE

As aplicações para as quais são adequados os certificados e, quando cabíveis, as aplicações para as quais existem restrições ou proibições para o uso destes certificados, estão relacionadas nas Políticas de Certificados de cada uma das ACs correspondentes.

1.4. DADOS DE CONTATO

Dúvidas decorrentes da leitura desta DPPSC e que não sejam respondidas mediante a leitura da página https://www.safeweb.com.br/repositorio podem ser esclarecidas contatando:

Contato: Setor de Compliance
Telefone: + 55 4007.2410
E-mail compliance@safeweb.com.br
Safeweb Segurança da Informação Ltda.

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 implementado pelo PSC o exigir.

1.5.1. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

O PSC SAFEWEB publica esta DPPSC em seu site https://www.safeweb.com.br/repositorio

1.5.2. PROCEDIMENTOS DE APROVAÇÃO

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

1.6. DEFINIÇÕES E ACRÔNIMOS

AC - Autoridade Certificadora
AC RAIZ - Autoridade Certificadora Raiz da ICP-Brasil

AS - Sistemas Autônomos
CG - Comitê Gestor da ICP-Brasil
CNPJ - Cadastro Nacional de Pessoa Jurídica
CPF - Cadastro de Pessoa Física
CSR - *Certificate Signing Request*
DMZ - Zona Desmilitarizada
DPPSC - Declaração de Práticas de Prestador de Serviço de Confiança
EAT - Entidade de Auditoria do Tempo
HTTP - HyperText Transfer Protocol ou Protocolo de Transferência de Hipertexto
ICP-BRASIL - Infraestrutura de Chaves Públicas Brasileira
IP - *Internet Protocol* ou Protocolo de Internet
IDS - Sistemas de Detecção de Intrusão
ISO - *International Organization for Standardization*
OID - *Object Identifier*
PSC - Prestadores de Serviço de Certificação
PSS - Prestadores de Serviço de Suporte
TCP - *Transmission Control Protocol* ou Protocolo de Controle de Transmissão
VPN - *Virtual Private Network* ou Rede Privada Virtual

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 SAFEWEB responsável por esta DPPSC, e o modo pelo qual é informado a sua disponibilidade.

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

a) capacidade de armazenamento dos certificados e das chaves privadas dos subscritores que opera;
b) sua DPPSC;
c) os serviços implementados;
d) as condições gerais mediante as quais são prestados os serviços de armazenamento de certificados digitais e/ou chaves privadas, assinatura digital e verificação da assinatura digital;
e) se pretende continuar a prestar o serviço ou se está mediante a qualquer fiscalização dos serviços.

2.1.2. FREQUÊNCIA DE PUBLICAÇÃO

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

2.1.3. CONTROLES DE ACESSO

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

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 pela SAFEWEB.

4. REQUISITOS OPERACIONAIS

4.1. ARMAZENAMENTO E ACESSO ÀS CHAVES PRIVADAS E/OU CERTIFICADOS DIGITAIS DO SUBSCRITOR

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

a) linguagem de programação utilizada para construção da plataforma de acesso é C# e .NET;
b) meio de acesso disponibilizado ao subscritor através de aplicativos para dispositivos móveis e computadores pessoais, página web e *web services*;
c) HTTPS como canal de segurança em que trafegam as autenticações;
d) o modelo TCP/IP como arquitetura de rede da aplicação.

4.2. SERVIÇO DE CRIAÇÃO, VALIDAÇÃO E ARMAZENAMENTO DE ASSINATURAS DIGITAIS

O assinador do PSC Safeweb possibilita assinar qualquer tipo de arquivo. Ao assinar um arquivo, um segundo arquivo com a extensão ".p7s" será gerado contendo a assinatura digital nos padrões definidos conforme DOC-ICP-15.03.

É possível realizar uma assinatura nova e gerar um novo arquivo ".p7s" ou realizar coassinaturas e

manter várias assinaturas em um único arquivo ".p7s".

A aplicação também oferece a opção de validação de assinaturas no padrão ICP-Brasil, sendo possível validar apenas assinaturas desanexadas de arquivos em geral ou anexadas em um arquivo do tipo ".pdf".

Para validar assinaturas em arquivos em geral, são necessários o arquivo original e o arquivo da assinatura digital com a extensão ".p7s". O arquivo de assinatura pode ser simples (um único assinante) ou coassinaturas.

Para arquivos em formato ".pdf" basta informar o arquivo assinado, sem que seja necessário informar o arquivo ".p7s".

O acesso à aplicação, para criação e validação de assinatura digital, ocorre através de uma página web com autenticação através de certificado digital padrão ICP-Brasil.

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 SAFEWEB com o objetivo de manter um ambiente seguro.

4.3.1. TIPOS DE EVENTOS REGISTRADOS

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

a) iniciação e desligamento dos sistemas de PSC;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores do PSC;
c) mudanças na configuração dos sistemas de PSC;
d) tentativas de acesso (*login*) e de saída do sistema (*logoff*);
e) tentativas não-autorizadas de acesso aos arquivos de sistema;
f) registros de armazenamentos das chaves privadas e/ou certificados digitais;
g) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas;
h) operações falhas de escrita ou leitura, quando aplicável;
i) todos os eventos relacionados à sincronização com a fonte confiável de tempo;
j) registros das assinaturas digitais criadas e verificações realizadas;
k) registros de acesso aos documentos dos subscritores;
l) registros de acesso ou tentativas de acesso à chave privada do subscritor.

4.3.1.2. O PSC SAFEWEB 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 SAFEWEB:

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 SAFEWEB é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

4.3.2. FREQUÊNCIA DE AUDITORIA DE REGISTROS (LOGS)

A periodicidade de auditoria de registros não será superior a uma semana e são analisados pela equipe da Segurança da Informação do PSC SAFEWEB. 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 SAFEWEB mantém localmente seus registros de auditoria por pelo menos 02 (dois) meses e, subsequentemente, 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 SAFEWEB gera cópias de segurança (backup) de seus registros de auditoria, de toda a solução (sistema operacional, aplicação e 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 sistema do PSC, pelo sistema de controle de acesso e pelo pessoal operacional.

A localização dos recursos se encontra na tabela abaixo:

Tipo de evento	Método de coleta	Registrado por
Sucesso e fracasso de tentativas de 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 login e logout	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 responsável 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
Atualização 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 SAFEWEB 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 SAFEWEB, 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 SAFEWEB.

4.4.1. TIPOS DE REGISTROS ARQUIVADOS

As seguintes informações são registradas e arquivadas pelo PSC SAFEWEB:

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.

O período de retenção para cada registro arquivado deverá ser observado, incluindo os registros de armazenamento de chaves privadas e/ou certificados digitais, de assinaturas digitais criadas, de verificações das assinaturas digitais e, por ventura, dos documentos armazenados, inclusive arquivos de auditoria, que deverão ser retidos por, no mínimo, 6 (seis) 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

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

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

4.5.1.3. O PSC SAFEWEB 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 SAFEWEB 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 dará de acordo com a tabela abaixo:

Tipo de evento	Método de coleta	Registrado por
Utilização da chave privada	Automático	Software de PSC
Notificação 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 obtida ou 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 de um (slot) destinado a um subscritor se dará de duas formas:

a) Quando solicitado pelo subscritor ao PSC Safeweb, mediante confirmação da identidade do subscritor.

b) Quando da expiração do certificado ou sua revogação, sem a intervenção do subscritor.

Em ambas as formas, será realizada a eliminação completa do slot do subscritor.

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

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

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

O PSC SAFEWEB 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 SAFEWEB 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 consequência da cessação dos serviços de armazenamento de certificados digitais e/ou das chaves privadas, assinaturas digitais e verificações de assinaturas 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 SAFEWEB cessar seus serviços os seguintes procedimentos serão executados, no mínimo:

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

4.7.4. O PSC SAFEWEB 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 SAFEWEB 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 SAFEWEB.

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 SAFEWEB 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 SAFEWEB, 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, nobreaks, baterias, quadros de distribuição de energia e de telefonia, subestações, 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 SAFEWEB é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [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 SAFEWEB.

5.1.2.1.2. O primeiro nível (nível 1) situa-se após a primeira barreira de acesso às instalações da AC. Para entrar em uma área de nível 1, cada indivíduo deve ser identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação do PSC devem transitar 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, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4 O segundo nível (nível 2) é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. A passagem do primeiro para o segundo nível exige identificação 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.

5.1.2.1.5. O terceiro nível (nível 3) situa-se dentro do segundo 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 possuam permissão de acesso não podem permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6. No nível 3 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: senha individual e 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. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da 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 no mínimo de duas pessoas autorizadas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9. No quarto nível todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo

uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 possuem proteção contra interferência eletromagnética externa.

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

5.1.2.1.11. No PSC há 1 (um) ambiente de quarto nível para abrigar e segregar, respectivamente:

a) Equipamentos de produção on-line;

b) Equipamentos de produção off-line e cofre de armazenamento.

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre ou gabinete reforçado trancado. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos estão armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre ou o gabinete obedecem às seguintes especificações mínimas:

a) É feito em aço ou material de resistência equivalente;

b) Possui tranca com chave e segredo.

5.1.2.1.14. O sexto nível (nível 6), consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de uma fechadura comum, com duas cópias de chave. Os dados de ativação da chave privada do PSC SAFEWEB são armazenados nesses depósitos.

5.1.2.2. SISTEMAS FÍSICOS DE DETECÇÃO

5.1.2.2.1. A segurança de todos os ambientes do PSC SAFEWEB 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; e

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 4.

5.1.2.2.5. O PSC SAFEWEB 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 4 DO PSC

5.1.3.1. A infraestrutura do ambiente de nível 4 do PSC SAFEWEB 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 ICP-BRASIL [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 4 do PSC SAFEWEB é ser garantida por meio de nobreaks e geradores de porte compatível.

5.1.4. EXPOSIÇÃO A ÁGUA NAS INSTALAÇÕES DO PSC

O ambiente de nível 4 do PSC SAFEWEB 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 SAFEWEB 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 4 do PSC SAFEWEB 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 SAFEWEB 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 SAFEWEB 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 SAFEWEB 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 SAFEWEB 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 SAFEWEB, 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 SAFEWEB 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 SAFEWEB 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 SAFEWEB, 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 na sala cofre onde se localizam os serviços do PSC SAFEWEB 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 serão necessários, no mínimo, 3 (três) empregados com perfis distintos e qualificados. As demais tarefas do PSC poderão ser executadas por um único empregado.

5.2.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

5.2.3.1. Todo empregado que ocupa perfil designado no PSC SAFEWEB 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 SAFEWEB 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 SAFEWEB 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 SAFEWEB, 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 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 SAFEWEB responsável envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de certificados digitais e/ou de chaves privadas, assinaturas digitais, verificações de assinaturas digitais é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4]. O PSC SAFEWEB responsável poderá definir requisitos adicionais para a admissão.

5.3.2. PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal do PSC SAFEWEB 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 SAFEWEB poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3. REQUISITOS DE TREINAMENTO

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

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

5.3.4. FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA

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

5.3.5. FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

O PSC SAFEWEB 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 SAFEWEB, 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 SAFEWEB 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 SAFEWEB envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de certificados e/ou chaves privadas, assinaturas digitais, verificações de assinaturas digitais 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 SAFEWEB 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 SAFEWEB para proteger as chaves privadas dos subscritores, manter os serviços relativos a assinaturas digitais, assim como o sincronismo de seus sistemas com a fonte confiável de tempo da ICP-Brasil. 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 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 SAFEWEB, usados nos processos de gerenciamento dos sistemas de armazenamento de certificados e/ou chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverão implementar, implementam, entre outras, as seguintes características:

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

críticos; e

f) mecanismos para cópias de segurança (backup).

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

6.1.2.3. Qualquer equipamento, ou parte desse, ao ser enviado para manutenção são apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações do PSC, o equipamento que passou por manutenção 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 SAFEWEB 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 SAFEWEB no desenvolvimento de sistemas e no gerenciamento de segurança.

6.2.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA

6.2.1.1. O ciclo de desenvolvimento de software do PSC Safeweb consiste nas seguintes etapas principais:

a) análise de sistema, onde os requisitos de software são identificados, juntamente com as regras de negócio;

b) desenvolvimento de software, onde os requisitos são desenvolvidos em um ambiente específico para este fim;

c) teste de software, onde as novas funcionalidades são homologadas em um ambiente de homologação;

d) implantação de software, onde as mudanças homologadas realizadas no sistema, são publicadas no ambiente de produção. Esta última é previamente agendada e aprovada

através de processo de Gestão de Mudanças.

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

6.2.2. CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.6.2.1 O PSC SAFEWEB utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção dos seus sistemas.

6.6.2.2. O PSC SAFEWEB verifica os níveis configurados de segurança através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando os resultados com as configurações aprovadas.

6.6.2.3. 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.

6.2.3. 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 SAFEWEB, 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 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 às 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) pela EAT da ICP-Brasil, para o sincronismo e auditoria dos sistemas de assinaturas;
b) pelo PSC, para a administração dos sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;
c) pelo subscritor, para a armazenamento e acesso à chave privada, e aos serviços de assinatura digital, verificação da assinatura digital.

6.3.2. FIREWALL

6.3.2.1. Mecanismos de firewall 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:

a) enviar traps SNMP;
b) executar programas definidos pela administração da rede;
c) enviar e-mail aos administradores;
d) enviar mensagens de alerta ao firewall ou ao terminal de gerenciamento;
e) promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do firewall.

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

6.3.3.3. O sistema de detecção de intrusão 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

6.3.4.1 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 SAFEWEB 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 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 SAFEWEB adotam o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

7. POLÍTICAS DE ASSINATURA

O PSC Safeweb utiliza as Políticas de Assinatura conforme disposto no documento DOC-ICP-15.03 - REQUISITOS DAS POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL [12].

8. AUDITORIAS E AVALIAÇÕES DE CONFORMIDADE

8.1. FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE

8.1.1. As fiscalizações e auditorias realizadas no PSC SAFEWEB 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 SAFEWEB 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. DAS AUDITORIAS DO PSC SAFEWEB

8.1.3.1. 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].

8.1.3.2. Quanto a autenticação e ao sincronismo de tempo: pela Entidade de Auditoria do Tempo (EAT) observado o disposto no documento PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS DO TEMPO NA ICP-BRASIL [3].

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

8.1.5. O PSC SAFEWEB recebeu auditoria prévia da Entidade de Auditoria do Tempo (EAT) quanto aos aspectos de autenticação e sincronismo, sendo regularmente auditada, para fins de continuidade de operação, com base no disposto no documento PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS DO TEMPO NA ICP-BRASIL [3].

8.1.6. As entidades da ICP-Brasil diretamente vinculadas ao PSC SAFEWEB, também receberam auditoria prévia, para fins de credenciamento, e o PSC é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme citado no parágrafo 8.1.3.

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 SAFEWEB abaixo relacionadas:

a) operar de acordo com a sua DPPSC e com a descrição dos serviços que realiza;
b) gerenciar e assegurar a proteção das chaves privadas dos subscritores;
c) manter os PSC sincronizados e auditados pela Entidade de Auditoria do Tempo da ICP-Brasil;

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

e) monitorar e controlar a operação dos serviços fornecidos;

f) notificar ao subscritor titular 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 e/ou chaves privadas para usuários finais, com cobertura suficiente (definir valor mínimo) 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 digitais correspondentes armazenados e assinaturas realizadas e verificadas.

9.1.2. OBRIGAÇÕES DO SUBSCRITOR

Ao contratar um serviço do PSC SAFEWEB, se for o caso, o subscritor deve assegurar, por meio das aplicações disponibilizadas, que o seu certificado digital foi corretamente armazenado e se a chave privada usada para assinar está funcional.

9.1.3 DIREITOS DA TERCEIRA PARTE (RELYING PARTY)

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

9.1.3.2. Constituem direitos da terceira parte:

a) recusar a utilização do serviço de assinatura digital, verificação da assinatura digital e guarda de documentos eletrônicos do PSC para fins diversos do seu propósito de uso na ICP-Brasil.
b) verificar, a qualquer tempo, a validade da assinatura digital.
c) uma assinatura digital ICP-Brasil é considerada válida quando:
i. o certificado digital não constar da LCR da AC emitente;
ii. a chave privada utilizada para assinar digitalmente não tiver sido comprometida até o momento da verificação;
iii. puder ser verificada com o uso da cadeia de certificados que a gerou;
iv. o propósito de uso esteja em conformidade com o definido na política do certificado digital do(s) signatário(s).

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

9.2. RESPONSABILIDADES

9.2.1. RESPONSABILIDADES DO PSC

O PSC SAFEWEB responde pelos danos a que der causa.

9.3. RESPONSABILIDADE FINANCEIRA

9.3.1. INDENIZAÇÕES DEVIDAS PELA TERCEIRA PARTE (RELYING PARTY).

9.3.1.1. A terceira parte - *Relying Party* - não é responsável perante o PSC SAFEWEB, exceto na hipótese de prática de ato ilícito. Nesse caso, essa terceira parte responderá em quaisquer esferas de direito, e deverá indenizar o PSC e/ou, os titulares de seus certificados, pelos danos a que derem causa, em decorrência de omissão ou ação não conforme com a legislação aplicável.

9.3.2. RELAÇÕES FIDUCIÁRIAS

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

Os detalhes das condições de aplicação da Política de Garantia estão disponíveis na página web www.safeweb.com.br.

9.3.3. PROCESSOS ADMINISTRATIVOS

Os processos administrativos cabíveis, relativos às operações do PSC SAFEWEB seguirão a legislação específica na qual os procedimentos questionados se enquadrarem.

9.4. INTERPRETAÇÃO E EXECUÇÃO

9.4.1. LEGISLAÇÃO

A DPPSC SAFEWEB atende aos requisitos da legislação em vigor, incluindo a Medida Provisória n o 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 SAFEWEB 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 SAFEWEB, 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 SAFEWEB 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, a 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

Pelos serviços disponibilizados será cobrado o valor estabelecido contratualmente.

9.5.1. TARIFAS DE ARMAZENAMENTO DE CERTIFICADOS DIGITAIS E/OU CHAVES PRIVADAS

PARA USUÁRIOS FINAIS

Pelos serviços de armazenamento de certificados e/ou chaves privadas de usuários finais pelo PSC SAFEWEB e/ou contrato estipulado entre a SAFEWEB e a entidade que utiliza os serviços do PSC SAFEWEB, será cobrado o valor estabelecido contratualmente.

9.5.2. TARIFAS DE SERVIÇO DE ASSINATURA DIGITAL

Pelos serviços de assinatura digital será cobrado o valor estabelecido contratualmente.

9.5.3. TARIFAS DE SERVIÇO DE VERIFICAÇÃO DA ASSINATURA DIGITAL

Pelos serviços de verificação da assinatura digital será cobrado o valor estabelecido contratualmente.

9.5.4. TARIFAS DE SERVIÇO PARA ARMAZENAMENTO DE DOCUMENTOS ELETRÔNICOS

Pelos serviços de armazenamento de documentos eletrônicos será cobrado o valor estabelecido contratualmente.

9.5.5. OUTRAS TARIFAS

Não há tarifas adicionais que incidam sobre este serviço.

9.5.6. POLÍTICA DE REEMBOLSO

Não se aplica.

9.6. SIGILO

9.6.1. DISPOSIÇÕES GERAIS

9.6.1.1. As chaves privadas dos subscritores são mantidas pelo PSC SAFEWEB, que será responsável pelo seu sigilo.

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

9.6.1.3. Os documentos assinados digitalmente pelos subscritores poderão ser mantidos pelo PSC,

desde que expressamente acordado com o subscritor e de acordo com a legislação vigente, que será responsável pelo seu sigilo.

9.6.2. TIPOS DE INFORMAÇÕES SIGILOSAS

9.6.2.1. Todas as informações coletadas, geradas, transmitidas e mantidas pelo PSC SAFEWEB 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 SAFEWEB deverá ser divulgado, exceto quando for estabelecido um acordo com o subscritor para sua publicação mais ampla.

9.6.3. TIPOS DE INFORMAÇÕES NÃO SIGILOSAS

Os seguintes documentos do PSC SAFEWEB 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

9.6.4.1 Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda do PSC SAFEWEB e suas AR vinculadas 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

9.6.5.1 Como diretriz geral, nenhum documento, informação ou registro, sob a guarda do PSC SAFEWEB, 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

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

9.7. DIREITOS DE PROPRIEDADE INTELECTUAL

9.7.1 Todos os direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, documentos assinados digitalmente e gerados para o PSC SAFEWEB, de acordo com a legislação vigente, pertencem e continuarão sendo propriedade da Safeweb.

10. DOCUMENTOS DA ICP-BRASIL

Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal.

O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

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

BRASIL, **Decreto nº 4.264, de 10 de junho de 2002** - Restabelece e Modifica o Regulamento anterior.

BRASIL, **Lei nº 9.933, de 20 de dezembro de 1999.** Dispõe sobre o Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (CONMETRO) e sobre o Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO).

RFC 1305, IETF. **Network Time Protocol version 3.0.**

RFC 2030, IETF. **Simple Network Time Protocol (SNTP) version 4.**0.

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

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

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

ETSI TS 101.861 - v 1.2.1. **Technical Specification /Time Stamping Profile**. Março de 2002.

ETSI TS 102.023 - v 1.1.1. **Technical Specification/Policy Requirements for Time Stamping Authorities**. Abril de 2002.

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