Declaração de Práticas de Prestador de Serviço de Confiança da ICP-BRASIL –

PSC CERTISIGN

DPPSC do PSC Certisign

Versão 1.0- 15/05/2018

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
1.0	15/05/2018	Resolução n. 132 Instrução Normativa nº07	Não se aplica	Criação da DPPSC do PSC Certisign

Declaração de Práticas de Prestador de Serviço de Confiança da ICP-BRASIL do PSC CERTISIGN

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Esta Declaração de Práticas de Prestador de Serviço de Confiança (DPPSC) descreve as práticas e os procedimentos empregados pelo Prestador de Serviço de Confiança Certisign (PSC Certisign), integrante na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na execução dos seus serviços de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas.

A estrutura desta DPPSC está baseada nos DOC-ICP-17[12] e DOC-ICP-17.01[10]. As referências a formulários presentes nesta DPPSC deverão ser entendidas também como referências a outras formas que o PSC Certisign ou entidades a ela vinculadas possa vir a adotar.

1.1.2. O Prestador de Serviço de Confiança – PSC da ICP-Brasil é uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de armazenamento de chaves privadas para usuários finais, nos termos do DOC-ICP-04[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. O DOC-ICP-17[12] estabelece os requisitos mínimos a serem obrigatoriamente observados pelos PSC integrantes da ICP-Brasil na elaboração de suas Declarações de Práticas de Prestador de Serviço de Confiança – DPPSC. A DPPSC é o documento que descreve as práticas e os procedimentos operacionais e técnicos empregados pelo PSC na execução de seus serviços. Não obstante, as ACs devem observar a mudança na respectiva DPPSC e PC caso utilizem para armazenamento de chaves dos seus usuários finais o modelo PSC (ciclo de vida do certificado – descrição dos procedimentos de armazenamento).

1.1.5. O DOC-ICP-17[12] 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. Esta DPPSC foi elaborada no âmbito da ICP-Brasil e adota a mesma estrutura empregada no O DOC-ICP-17[12].

1.1.7. Aplicam-se ainda aos PSC da ICP-Brasil, no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil, entre os quais destacamos:
a) DOC-ICP-02 - POLÍTICA DE SEGURANÇA DA ICP-BRASIL[4];
b) DOC-ICP-03 - CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[5];
c) DOC-ICP-08 - CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6];
d) DOC-ICP-09 - CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[7];
e) DOC-ICP-10 - 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 DPPSC é chamada Declaração de Práticas de Prestador de Serviço de Confiança e referida como "DPPSC do PSC Certisign", cujo OID (*object identifier*) é 2.16.76.1.11.2, conforme definido no DOC-ICP-04.01.

1.3. Comunidade e Aplicabilidade

1.3.1. Prestadores de Serviço de Confiança

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

1.3.1.1. Os serviços prestados pelo PSC Certisign estão publicados no endereço da página web (URL) http://icp-brasil.certisign.com.br/repositorio/psc-certisign/index.htm.

1.3.1.2. PSC são entidades utilizadas para desempenhar as atividades descritas nesta DPPSC e no DOC-ICP-17.01[10], assim como nos adendos de documentos normativos (ADE-ICP) relacionados, e se classificam em três categorias, conforme o tipo de atividade prestada:
a) armazenamento de chaves privadas dos subscritores; ou
b) serviço de assinatura digital, verificação da assinatura digital; ou
c) ambos.

O PSC Certisign presta os serviços de:
a) armazenamento de chaves privadas dos subscritores; e
b) serviço de assinatura digital e verificação da assinatura digital.

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

1.3.2. Subscritores

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

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

Os subscritores tem acesso, quando do uso do serviço de assinatura do PSC Certisign, 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 o PSC Certisign de armazenamento de chaves criptográficas ao seu critério, em conformidade com os procedimentos de portabilidade dispostos no documento DOC-ICP-17.01[10].

1.3.3. Aplicabilidade

O PSC Certisign presta os serviços de:
a) armazenamento de chaves privadas dos subscritores; e
b) serviço de assinatura digital e verificação da assinatura digital.

1.4. Dados de Contato

Empresa: Certisign Certificadora Digital S.A.

Endereço: Rua Bela Cintra, 904 – 11. Andar – São Paulo

CEP: 01415-000

Área: Normas e Compliance

Contato: Patricia T O Leite

Telefone: (11) 4501-2417

E-mail: icpbrasil@certisign.com.br
normas@certisign.com.br

1.5. Procedimentos de mudança de especificação

Alterações nesta DPPSC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas do PSC Certisign. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da ICP-Brasil.

Esta DPPSC é atualizada sempre que um novo serviço implementado pelo PSC Certisign o exigir.

1.5.1. Políticas de publicação e notificação

O PSC Certisign mantém página específica com a versão corrente desta DPPSC para consulta pública, a qual está disponibilizada no endereço Web: http://icp-brasil.certisign.com.br/repositorio/dpc/psc-certisign/psc-dppsc-certisign.pdf.

1.5.2. Procedimentos de aprovação

Alterações nesta DPPSC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas do PSC Certisign.

Esta DPPSC foi submetida à aprovação, durante o processo de credenciamento do PSC Certisign, conforme o determinado pelo DOC-ICP-03[5].

1.6. Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo de Tempo
AR	Autoridade de Registro
AUDIBRA	Instituto dos Auditores Internos do Brasil
CD	Compact Disc
CG	Comitê Gestor da ICP-Brasil
CFC	Conselho Federal de Contabilidade
CGU	Controladoria Geral da União
CGAF	Coordenação Geral de Auditoria e Fiscalização
CMMI	Capability Maturity Model Integration
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations
CVM	Comissão de Valores Mobiliários
DAFN	Diretoria de Auditoria, Fiscalização e Normalização
DOU	Diário Oficial da União

DVD	Digital Versatile Disc
EAT	Entidade de Auditoria do Tempo – ICP-Brasil
IBRACON	Instituto dos Auditores Independentes do Brasil
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IIA	Information Systems Audit and Control Association
ISACA	Information Systems Audit and Control Association
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
MPS-BR	Melhoria de Processo do Software Brasileiro
PDF	Portable Document Format
PLAAO	Plano Anual de Auditoria Operacional
PSC	Prestador de Serviço de Confiança
PSCert	Prestadores de Serviço de Certificação
PSS	Prestadores de Serviço de Suporte
SHA	Secure Hash Algorithm

2. RESPONSABILIDADE DO REPOSITÓRIO E PUBLICAÇÃO

2.1. Publicação

2.1.1. Publicação de informação do PSC

2.1.1.1. As informações descritas abaixo são publicadas em página web do PSC Certisign (http://icp-brasil.certisign.com.br/repositorio/psc-certisign/index.htm), obedecendo as regras e os critérios estabelecidos nesta DPPSC.

A disponibilidade das informações publicadas pelo PSC Certisign em página web é de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.1.2. As seguintes informações estão publicadas pelo PSC Certisign em sua página web:
a) capacidade de armazenamento das chaves privadas dos subscritores que opera: 1 milhão de certificados
b) esta DPPSC;
c) os serviços que implementa:
- serviço de armazenamento e acesso às chaves privadas do subscritor
- serviço de criação, validação e armazenamento de assinaturas digitais

d) as condições gerais mediante as quais são prestados os serviços de armazenamento de chaves privadas, assinatura digital e verificação da assinatura digital:
- Chaves armazenadas em dispositivos de segurança em hardware (HSMs) e hospedados em um data center credenciado pelo órgão regulador

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

2.1.2. Frequência de publicação

O PSC Certisign atualiza a página web http://icp-brasil.certisign.com.br/repositorio/psc-certisign/index.htm após aprovação da AC Raiz da ICP-Brasil 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 e demais informações citadas em 2.1.1.2.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado. A máquina que armazena as informações acima se encontra em nível 4 de segurança física e requer uma senha de acesso.

3. IDENTIFICAÇÃO E AUTORIZAÇÃO

3.1. Serviço de Armazenamento e acesso às chaves privadas do subscritor

O PSC Certisign, ao realizar o Serviço de Armazenamento e acesso às chaves privadas do subscritor, realiza a identificação e autorização dos subscritores como se segue:

a) Cada subscritor terá uma conta e fará, acesso a ela a partir de seu logon e senha
    a. Neste serviço, o cliente verificará aspectos dos certificados, como quantidade de certificados em seu nome, sua validade, proximidade de expiração etc.
b) O subscritor, para acesso à sua chave privada, deverá apresentar
    a. Senhas (PIN/PUK): segundo regras da ICP-Brasil;
    b. OTP: segundo regras da RFC 6238 (TOTP), RFC 6287, RFC 4226 (HOTP).

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

O PSC Certisign, ao realizar o Serviço criação, validação e armazenamento de assinaturas digitais, realiza a identificação e autorização dos subscritores como se segue:

a) Cada subscritor terá uma conta e fará, acesso a ela a partir de seu logon e senha
    a. Neste serviço, o cliente verificará aspectos do serviço de assinatura digital, como volume de assinaturas contratadas e utilizadas, etc.
b) O subscritor, para acesso à sua chave privada, como o objetivo de realizar uma assinatura digital, deverá apresentar:
    a. Senhas (PIN/PUK): segundo regras da ICP-Brasil;
    b. OTP: segundo regras da RFC 6238 (TOTP), RFC 6287, RFC 4226 (HOTP).
c) O serviço de validação de assinaturas é gratuito e pode ser acesso de duas formas:
    a. via código de verificação: exclusiva para assinaturas providas pelo próprio PSC Certisign, não necessita de autenticação
    b. via análise do arquivo assinado: para tal, é necessário que o demandante da verificação esteja logado e disponibilize o arquivo assinado (p7s, pdf ou xml) para validação . As assinaturas, nesta segunda forma de validação, podem ter sido geradas por qualquer PSC.
d) O serviço de armazenamento de assinaturas mantém as assinaturas, assim como seus documentos, armazenados por 5 anos a contar da data de upload do documento no PSC Certisign.

4. REQUISITOS OPERACIONAIS

4.1. Armazenamento e acesso às chaves privadas do subscritor

A comunicação entre a aplicação do subscritor e acesso ao certificado e suas chaves, no PSC Certisign, possui os seguintes componentes:

a) a linguagem de programação utilizada para construção da plataforma de acesso: JAVA e C++;

b) os meios de acesso disponibilizados ao subscritor:

- aplicativos para dispositivos móveis Android e iOS,
- aplicativo Desktop para Windows e MacOS,
- páginas web para gestão da carteira de certificados;

c) o canal de segurança em que trafegam as autenticações: canal TLS com autenticação por chaves RSA

d) a arquitetura de rede da aplicação de acesso: a aplicação está localizada dentro uma infraestrutura de TI redundante (servidores, estrutura de redes e segurança lógica) e hospedados em um data center que atende aos mais exigentes níveis de segurança física e lógica.

Os demais detalhes operacionais estão descritos no documento "Procedimentos operacionais do PSC Certisign como prestador de serviço de confiança da ICP-BRASIL" disponível em http://icp-brasil.certisign.com.br/repositorio/pc/psc-certisign/psc-po-certisign.pdf.

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

Abaixo o PSC Certisign descreve sua plataforma de assinatura digital e verificação da assinatura digital de forma ampla. Maiores detalhes de como as plataformas de assinatura digital e verificação da assinatura digital funcionam no PSC Certisign estão descritos no documento "Procedimentos operacionais do PSC Certisign como prestador de serviço de confiança da ICP-BRASIL" disponível em http://icp-brasil.certisign.com.br/repositorio/pc/psc-certisign/psc-po-certisign.pdf.

4.2.1. Serviço de criação de assinaturas digitais

O PSC Certisign desenvolveu sistemas que possibilitam a ativação da chave privada do signatário para a criação das assinaturas digitais.

A interface entre a aplicação de assinatura e o dispositivo de criação do PSC Certisign garante que somente com a autenticação do titular do certificado, que deve ter controle exclusivo da chave privada, seja possível requerer a criação dos dados de uma assinatura digital.

Toda informação trocada entre a aplicação e o dispositivo trafega de forma criptografada e todos os algoritmos e tamanho de chaves envolvidos no cálculo de qualquer elemento da assinatura digital encontram-se definidos no documento DOC-ICP-01.01[13].

O PSC Certisign implementou assinaturas digitais baseadas nas políticas de assinatura padronizadas e aprovadas na ICP-Brasil como descrito no item 7.

4.2.2. Serviço de validação de assinaturas digitais

O processo de validação de uma assinatura digital pelo PSC Certisign é realizada contra uma Política de Assinatura ICP-Brasil, e gera um relatório com indicação da situação de validação (Válida, Inválida ou Indeterminada), fornecendo os detalhes da validação técnica de cada uma das restrições aplicáveis, que podem ser relevantes para a aplicação demandante na interpretação dos resultados.

Os requisitos para verificação de assinaturas digitais no âmbito da ICP-Brasil estão descritos no documento DOC-ICP-15.01[15].

4.2.3. Serviço de armazenamento de assinaturas digitais

O PSC Certisign desenvolveu sistemas que possibilitam o armazenamento e guarda dos arquivos contendo as assinaturas digitais pertinentes aos documentos assinados.

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

4.3. Procedimentos de Auditoria de Segurança

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

4.3.1. Tipos de eventos registrados

4.3.1.1. O PSC Certisign 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 armazenamento 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 Certisign 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. O PSC Certisign registra as seguintes informações adicionais:
a) Serviço de Armazenamento e acesso às chaves privadas do subscritor
- Criação, edição e exclusão de usuários
- Definição/modificação de fator de autenticação
- Geração de chave
- Emissão de certificado
- Uso da chave (autenticação/assinatura)
- Consulta a certificados
- Exclusão de chave
- Renovação de certificado
- Exportação de chave
- Importação de chave

b) Serviço de criação, validação e armazenamento de assinaturas digitais:
- Acesso à plataforma
- Quem criou o fluxo
- Registro do fluxo da assinatura
- Assinatura realizada
- Tipo da assinatura realizada
- Verificação do documento
- Extrato de consumo no mês

4.3.1.4. Todos os registros de auditoria contem a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos contem o horário UTC.
Registros manuais em papel contem 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 Certisign é armazenada, eletrônica ou manualmente, em local único, conforme o DOC-ICP-02 [4].

4.3.2. Frequência de auditoria de registros (logs)

Os registros de auditoria do PSC Certisign são analisados pelo seu pessoal operacional em periodicidade não superior a uma semana. 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 Certisign mantém localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, os armazena da maneira descrita no item 4.4.

4.3.4. Proteção de registro (log) de auditoria

4.3.4.1. O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção através das funcionalidades nativas dos sistemas operacionais. As ferramentas disponíveis no sistema operacional liberam os acessos lógicos aos registros de auditoria somente a usuários ou aplicações autorizadas, através de permissões dadas pelo administrador do sistema de acordo com a função dos usuários ou aplicações e orientação do departamento de segurança.

O próprio sistema operacional também registra os acessos aos arquivos onde estão armazenados os registros de auditoria.

4.3.4.2. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção através de controles de acesso aos ambientes físicos onde são armazenados estes registros.

4.3.4.3. Os mecanismos de proteção descritos obedecem à Política de Segurança do PSC Certisign, em conformidade com a DOC-ICP-02[4].

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

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

4.3.6. Sistema de coleta de dados de auditoria

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

4.3.7. Notificação de agentes causadores de eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria do PSC Certisign, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.3.8. Avaliações de vulnerabilidade

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

4.4. Arquivamento de Registros

Nos itens seguintes desta DPPSC está descrita a política geral de arquivamento de registros implementada pelo PSC Certisign.

4.4.1. Tipos de registros arquivados

Os tipos de registros arquivados pelo PSC CERTISIGN compreendem, entre outros:
a) notificações de comprometimento de chaves privadas dos subscritores por qualquer motivo;
b) notificações de comprometimento de arquivos armazenados dos subscritores por qualquer motivo;
c) informações de auditoria previstas no item 4.3.1.1.

O período de retenção (i) dos registros de armazenamento de chaves privadas e/ou certificados digitais, (ii) de assinaturas digitais criadas, (iii) de verificações das assinaturas digitais e (iv) dos documentos armazenados, inclusive arquivos de auditoria é de 6 (seis) anos.

4.4.2. Proteção de arquivo

Todos os registros são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a DOC-ICP-02[4].

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

4.4.3.1. O PSC Certisign estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à PSC Certisign, recebendo o mesmo tipo de proteção utilizada por ela 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 Certisign verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.4.4. Requisitos para datação de registros

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

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

4.4.5. Sistema de coleta de dados de arquivo

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

4.4.6. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente ao PSC Certisign, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

4.5. Liberação do espaço do subscritor

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

4.6. Comprometimento e Recuperação de Desastre

4.6.1. Disposições Gerais

4.6.1.1. Nos itens seguintes desta DPPSC estão descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no Plano de Continuidade de Negócios (PCN) do PSC Certisign, estabelecido conforme o DOC-ICP-02[4], para garantir a continuidade dos seus serviços críticos.

4.6.1.2. O PSC Certisign 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. Neste caso, o PSC Certisign disponibilizará 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 Certisign não 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, verificação da assinatura digital ou armazenamento dos documentos assinados, sempre que possível, o PSC Certisign disponibilizará 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

Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança do PSC Certisign, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação. Caso haja necessidade, o Gerente de Segurança decretará a contingência.

4.6.3. Sincronismo do PSC

O processo de sincronização do relógio interno dos equipamentos do PSC Certisign é realizado por meio do protocolo DS/NTP, que exige um TAC (Time Attribute Certificate) válido, enviado pelo ITI. Caso não exista um TAC ou o TAC esteja expirado, o serviço de SCT não realiza nenhuma assinatura de tempo até que um novo processo de sincronia seja realizado e um TAC válido seja recebido.

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

Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, a Gerência de Infraestrutura notifica o Gerente de Segurança, responsável pela contingência, e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:
a) garantir a integridade física das pessoas que se encontram nas instalações do PSC Certisign;
b) monitorar e controlar o foco da contingência;
c) minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

4.7. Extinção dos serviços de PSC

4.7.1. Observado o disposto no item 4 do DOC-ICP-03[5], este item da DPPSC descreve os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços do PSC Certisign.

4.7.2. O PSC Certisign assegura que possíveis rompimentos com os subscritores e terceiras partes, em consequência da cessação dos serviços de armazenamento das chaves privadas, assinaturas digitais, verificações de assinaturas digitais e, por ventura, armazenamento dos documentos assinados sejam minimizados e, em particular, assegura a manutenção continuada da informação necessária para que não haja prejuízos aos subscritores e as terceiras partes.

4.7.3. Antes do PSC Certisign cessar seus serviços os seguintes procedimentos, no mínimo, serão executados:
a) o PSC Certisign disponibilizará a todos os subscritores e partes receptoras informações a respeito de sua extinção;
b) o PSC Certisign 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 Certisign 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 Certisign notificará todas as entidades afetadas.

4.7.4. O PSC Certisign providenciará os meios para cobrir os custos de cumprimento destes requisitos mínimos no caso de falência ou se por outros motivos for incapaz de arcar com os seus custos.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes são descritos os controles de segurança implementados pelo PSC Certisign para executar de modo seguro suas funções, de acordo com o DOC-ICP-17.01[10].

5.1. Segurança Física

Nos itens seguintes da DPPSC são descritos os controles físicos referentes às instalações que abrigam os sistemas do PSC Certisign.

5.1.1. Construção e localização das instalações do PSC

A construção das instalações do PSC Certisign implementam os seguintes controles de segurança física:
a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares ficam em ambiente seguro;
b) Instalações para sistemas de telecomunicações, subestações e retificadores ficam em ambiente seguro com entrada e saída controlada;
c) Sistemas de aterramento e de proteção contra descargas atmosféricas foram implementados; e
d) Iluminação de emergência em todos os ambientes de nível 4, além das áreas cobertas por câmeras de monitoramento.

5.1.2. Acesso físico nas instalações do PSC

O PSC Certisign possui sistema de controle de acesso físico que garante a segurança de suas instalações, conforme o DOC-ICP-02 [4] e os requisitos que seguem.

5.1.2.1. Níveis de acesso

5.1.2.1.1. O PSC Certisign possui 4 (quatro) níveis de acesso físico aos seus ambientes.

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações do PSC Certisign. 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 Certisign transitam devidamente identificadas e acompanhadas.

Nenhum tipo de processo operacional ou administrativo do PSC Certisign 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 PSC Certisign 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 são utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro 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 Certisign. 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 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação do PSC Certisign.

Pessoas não envolvidas com as atividades do PSC Certisign não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa 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: identificação individual, por meio de cartão eletrônico, 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 Certisign, 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 Certisign. 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, é exigido, 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 sendo 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 – que constituem as chamadas salas-cofre - 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 foram sanadas por normas internacionais pertinentes.

5.1.2.1.11. No PSC Certisign, existem ambientes de quarto nível para abrigar e segregar:
a) equipamentos de produção on-line, gabinete reforçado de armazenamento e equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores - (Data Center);
b) equipamentos de produção off-line e cofre de armazenamento (Sala de cerimônia).

5.1.2.1.12. Para garantir a segurança do material armazenado, o cofre e o gabinete obedecem às seguintes especificações:
a) confeccionado em aço;
b) possui tranca com chave.

5.1.2.2 Sistemas físicos de detecção

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

5.1.2.2.2. A segurança 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 localmente.

5.1.2.2.3. Os ambientes de nível 3 e 4 são dotados de Circuito Interno de TV ligado a um sistema local de gravação 24x7. O posicionamento e a capacidade dessas câmeras não permitem a recuperação de senhas digitadas nos sistemas.

5.1.2.2.4. As mídias resultantes dessa gravação deverão ser armazenadas por, no mínimo, 1 (um) ano, em ambiente de nível 3.

5.1.2.2.5. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados ininterruptamente.

5.1.2.2.6. Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que o critério mínimo de ocupação deixa de ser satisfeito, devido à saída de um ou mais empregados, ocorre a reativação automática dos sensores de presença.

5.1.2.2.7. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

5.1.2.2.8. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes estão localizados em ambiente de nível 3 e são permanentemente monitorados por guarda armado. As instalações do sistema de monitoramento estão sendo monitoradas, por sua vez, por câmera de vídeo que permite acompanhar as ações do guarda.

5.1.2.2.9. O PSC 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 de nível 4.

5.1.3. Energia e ar-condicionado do ambiente de nível 4 do PSC

5.1.3.1. A infraestrutura do ambiente de nível 4 do PSC 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 Certisign e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente do PSC Certisign.

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

5.1.3.3. Existem 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, telefonia e dados.

5.1.3.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, a cada 6 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 DOC-ICP-02[4]. Qualquer modificação nessa rede é documentada e autorizada previamente.

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

5.1.3.7. O sistema de climatização atende os requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante à falhas.

5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9. O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado do PSC Certisign é garantida, por meio de:
a) gerador de porte compatível;
b) gerador de reserva;
c) sistemas de no-breaks redundantes;
d) sistemas redundantes de ar condicionado.

5.1.4. Exposição à água nas instalações do PSC

A estrutura inteiriça do ambiente de nível 4 construído na forma de célula estanque, provê proteção física contra exposição à água, infiltrações e inundações provenientes de qualquer fonte externa.

5.1.5. Prevenção e proteção contra incêndio nas instalações do PSC

5.1.5.1. Nas instalações do PSC Certisign 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. Os ambientes de nível 3 do PSC não possuem saídas de água advindos do sistema de sprinklers do prédio, para evitar danos aos equipamentos.

5.1.5.3. Os ambientes de nível 3 e 4 possuem sistema de prevenção contra incêndios, que aciona alarmes preventivos uma vez detectada fumaça no ambiente.

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

5.1.5.5. Mecanismos específicos foram implantados pelo PSC 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 Certisign atender à norma brasileira NBR 11.515/NB 1334 *("Critérios de Segurança Física Relativos ao Armazenamento de Dados"*).

5.1.7. Destruição de lixo nas instalações do PSC

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis 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) paro PSC

Uma sala de armazenamento externa à instalação técnica principal do PSC é usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala está disponível a 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 Certisign, com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, também é estabelecido o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

5.2.1.1. O PSC Certisign pratica uma política de segregação de funções, controlando e registrando o acesso físico e lógico funções críticas, com o intuito de evitar que um empregado utilize indevidamente os serviços do ambiente sem ser detectado. As ações de cada empregado são limitadas de acordo com seu perfil.

5.2.1.2. O PSC estabelece um mínimo de 3 (três) perfis distintos para sua operação, a saber:
a) Administrador do sistema – autorizado a instalar, configurar e manter os sistemas confiáveis para gerenciamento do carimbo do tempo, bem como administrar a implementação das práticas de segurança do PSC;
b) Operador de sistema – responsável pela operação diária dos sistemas confiáveis do PSC. Autorizado a realizar backup e recuperação do sistema.
c) Auditor de Sistema – autorizado a ver arquivos e auditar os logs dos sistemas confiáveis do PSC.

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

5.2.1.4. O PSC Certisign possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos empregados. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o empregado devolve à PSC Certisign 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 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 é necessário, no mínimo, 3 (três) empregados com perfis distintos e qualificados. As demais tarefas do PSC são executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Esta DPPSC garante que todo empregado do PSC Certisign 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 Certisign adota padrão de utilização de "senhas fortes", definido na sua Política de Segurança e em conformidade com o DOC-ICP-02[4], juntamente com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Nos itens seguintes desta DPPSC são descritos requisitos e procedimentos, implementados pelo PSC Certisign em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida.

O PSC Certisign garante que todos os seus empregados, 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;
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 Certisign envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverá ser admitido conforme o estabelecido no DOC-ICP-02[4].

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 Certisign envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais 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. Não se aplica.

5.3.3. Requisitos de treinamento

Todo o pessoal do PSC Certisign envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais deverão receber treinamento documentado, suficiente para o domínio dos seguintes temas:
a) princípios e tecnologias dos sistemas e hardwares de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais em uso no PSC;
b) ICP-Brasil;
c) princípios e tecnologias de certificação digital e de assinaturas digitais;
d) princípios e mecanismos de segurança de redes e segurança do PSC;
e) procedimentos de recuperação de desastres e de continuidade do negócio;
f) familiaridade com procedimentos de segurança, para pessoas com responsabilidade de Oficial de Segurança;
g) familiaridade com procedimentos de auditorias em sistemas de informática, para pessoas com responsabilidade de Auditores de Sistema;
h) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

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

5.3.5. Frequência e sequência de rodízio de cargos

Não se aplica.

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 do PSC Certisign, o acesso dessa pessoa ao sistema de certificação é suspenso, é instaurado processo administrativo para apurar os fatos e, se for o caso, serão tomadas as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima contém, 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 Certisign encaminha 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 Certisign envolvido em atividades diretamente relacionadas com os processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais foi contratado conforme o estabelecido no DOC-ICP-02[4].

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. O PSC Certisign disponibiliza para todo o seu pessoal:
a) esta DPPSC;
b) sua Política de Segurança;

c) documentação operacional relativa às suas atividades; e
d) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. A documentação fornecida é classificada segundo a política de classificação de informação definida pelo PSC Certisign e é mantida atualizada.

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, esta DPPSC define as medidas de segurança implantadas pelo PSC Certisign 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 pelo PSC na execução de suas funções operacionais.

6.1. Controles de Segurança Computacional

6.1.1. Disposições Gerais

Neste item, esta DPPSC indica os mecanismos utilizados para prover a segurança de suas estações de trabalho, servidores e demais sistemas e equipamentos, observado o disposto no DOC-ICP-02[4].

6.1.2. Requisitos técnicos específicos de segurança computacional

6.1.2.1. A DPPSC garante que os sistemas e os equipamentos do PSC Certisign, usados nos processos de gerenciamento dos sistemas de armazenamento de chaves privadas, assinaturas digitais, verificações de assinaturas digitais implementam, entre outras, as seguintes características:

a) controle de acesso aos serviços e perfis do PSC Certisign;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado do PSC Certisign;
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 Certisign;
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 certificação e mecanismos de segurança física.

6.1.2.3. As informações sensíveis contidas nos equipamentos são retiradas dos equipamentos para manutenção. Os números de série dos equipamentos e as datas de envio e de recebimento da manutenção são controlados. Ao retornar às instalações do PSC Certisign, o equipamento que passou por manutenção é inspecionado. As informações sensíveis armazenadas, relativas à atividade do PSC Certisign, são destruídas de maneira definitiva nos equipamentos que deixam de ser utilizados em caráter permanente. Todos esses eventos são registrados para fins de auditoria.

6.1.2.4. Equipamentos utilizados pelo PSC Certisign são preparados e configurados como previsto na Política de Segurança do PSC Certisign ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade.

6.1.3. Classificação da segurança computacional

A segurança computacional do PSC Certisign segue as recomendações do Common Criteria.

6.2. Controles Técnicos do Ciclo de Vida

6.2.1. Controles de desenvolvimento de sistema

6.2.1.1. O PSC Certisign utiliza os modelos clássico espiral e SCRUM no desenvolvimento dos sistemas, de acordo com a melhor adequação destes modelos ao projeto em desenvolvimento. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, o PSC Certisign utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos.

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

6.2.2. Controles de gerenciamento de segurança

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

6.2.2.2. O PSC Certisign utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

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 são descritos os controles relativos à segurança da rede do PSC Certisign, incluindo firewalls 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, firewalls, e sistemas de detecção de intrusos (IDS), localizados no segmento de rede que hospeda o sistema de certificação estão localizados e operam em ambiente de nível 4.

6.3.1.3. As versões mais recentes, dos sistemas operacionais,dos aplicativos servidores e das eventuais correções (patches), são disponibilizadas pelos respectivos fabricantes e 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 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 o armazenamento e acesso à chave privada e aos serviços de assinatura digital e 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. O firewall promove 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 à PSC Certisign.

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

6.3.3.2. O sistema de detecção de intrusão reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com 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. A frequência de exame dos arquivos de registro é diária 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 Certisign implementa serviço de proxy, restringindo o acesso, a partir de todas suas estações de trabalho, a serviços que possam comprometer a segurança do ambiente do PSC.

6.3.5.2. As estações de trabalho e servidores são 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

O módulo criptográfico utilizado para armazenamento da chave privada dos subscritores do PSC Certisign está em conformidade com o padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO), conforme definido no documento DOC-ICP-01.01[13].

7. POLÍTICAS DE ASSINATURA

O PSC Certisign implementa as seguintes políticas de assinatura, seguindo o disposto no documento DOC-ICP-15.03[16]:

- POLÍTICA PADRÃO AD-RB BASEADA EM CADES
- POLÍTICA PADRÃO AD-RT BASEADA EM CADES
- POLÍTICA PADRÃO AD-RV BASEADA EM CADES
- POLÍTICA PADRÃO AD-RC BASEADA EM CADES
- POLÍTICA PADRÃO AD-RA BASEADA EM CADES
- POLÍTICA PADRÃO AD-RB BASEADA EM XADES
- POLÍTICA PADRÃO AD-RT BASEADA EM XADES
- POLÍTICA PADRÃO AD-RV BASEADA EM XADES
- POLÍTICA PADRÃO AD-RC BASEADA EM XADES
- POLÍTICA PADRÃO AD-RA BASEADA EM XADES
- POLÍTICA PADRÃO AD-RB BASEADA EM PADES
- POLÍTICA PADRÃO AD-RT BASEADA EM PADES
- POLÍTICA PADRÃO AD-RC BASEADA EM PADES
- POLÍTICA PADRÃO AD-RA BASEADA EM PADES

O PSC Certisign está em conformidade com as LPA registradas em: https://www.iti.gov.br/repositorio/84-repositorio/133-artefatos-de-assinatura-digital.

8. AUDITORIAS E AVALIAÇÕES DE CONFORMIDADE

8.1. Fiscalização e Auditoria de Conformidade

8.1.1 As fiscalizações e auditorias realizadas nos PSC da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPPSC, PCO e OS, demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pela WebTrust.

8.1.2. As fiscalizações dos PSC da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no DOC-ICP-09[7].

8.1.3. As auditorias dos PSC da ICP-Brasil são realizadas:
a) quanto aos procedimentos operacionais, pela AC-Raiz, por meio de pessoal de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no DOC-ICP-08[6];
b) quanto a autenticação e ao sincronismo de tempo pela Entidade de Auditoria do Tempo (EAT) observado o disposto no DOC-ICP-14[3].

8.1.4. O PSC Certisign recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no DOC-ICP-08[6]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.1.5. O PSC Certisign recebeu auditoria prévia da EAT quanto aos aspectos de autenticação e sincronismo, sendo regularmente auditada, para fins de continuidade de operação, com base no disposto no DOC-ICP-14[3].

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

9. OUTROS ASSUNTOS DE CARÁTER COMERCIAL E LEGAL

9.1. Obrigações e direitos

Nos itens a seguir são descritas as obrigações gerais das entidades envolvidas.

9.1.1. Obrigações do PSC

a) operar de acordo com a sua DPPSC e com a descrição dos serviços que realiza;
b) gerenciar e assegurar a proteção das chaves privadas dos subscritores;
c) manter os PSC sincronizados e auditados pela Entidade de Auditoria do Tempo da ICP-Brasil;
d) tomar as medidas cabíveis para assegurar que subscritores e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
e) monitorar e controlar a operação dos serviços fornecidos;
f) notificar ao subscritor titular da chave e certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado ou o encerramento de suas atividades;
g) publicar em sua página web sua DPPSC e a Políticas de Segurança (PS) aprovadas que implementa;
h) publicar, em sua página web, as informações definidas no item 2.1.1.2 deste documento;
i) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

j) adotar as medidas de segurança e controle previstas na DPPSC, no Plano de Capacidade Operacional (PCO) e PS que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
k) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
l) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
m)manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);
n) manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de armazenamento de chaves privadas para usuários finais, com cobertura suficiente e compatível com o risco dessas atividades;
o) informar aos subscritores que contratam os seus serviços sobre coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima; e
p) informar à AC-Raiz, mensalmente, a quantidade de chaves privadas ou certificados digitais correspondentes armazenados e assinaturas realizadas e verificadas.

9.1.2. Obrigações do Subscritor

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

9.1.3. Direitos da terceira parte (Relying Party)

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

9.1.3.2. Constituem direitos da terceira parte:
a) recusar a utilização do serviço de assinatura digital, verificação da assinatura digital e guarda de documentos eletrônicos do PSC para fins diversos do seu propósito de uso na ICP-Brasil;
b) verificar, a qualquer tempo, a validade da assinatura digital.

Uma assinatura digital ICP-Brasil é considerada válida quando:
i. o certificado digital não constar da LCR da AC emitente;
ii. a chave privada utilizada para assinar digitalmente não tiver sido comprometida até o momento da verificação;
iii. puder ser verificada com o uso da cadeia de certificados que a gerou;
iv. o propósito de uso esteja em conformidade com o definido na política do certificado digital do(s) signatário(s).

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

9.2. Responsabilidades

9.2.1. Responsabilidades do PSC

O PSC Certisign responde pelos danos a que der causa.

9.3. Responsabilidade Financeira

9.3.1. Indenizações devidas pela terceira parte (Relying Party)

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

9.3.2. Relações Fiduciárias

O PSC Certisign indeniza integralmente os prejuízos que, comprovadamente, der causa, quando o subscritor for pessoa física.
Em situações justificáveis, pode ocorrer limitação da indenização, quando o subscritor for pessoa jurídica.

9.3.3. Processos Administrativos

O subscritor que sofrer perdas e danos decorrentes às operações do PSC Certisign tem o direito de comunicar ao PSC Certisign que deseja a indenização prevista no item 9.3.2 acima que tenha sido comprovado por perícia realizada por perito especializado e independente.

9.4. Interpretação e Execução

9.4.1. Legislação

Esta DPPSC é regida pela Medida Provisória nº 2.200-02, pelas Resoluções do Comitê Gestor da ICP-Brasil, bem como pelas demais leis em vigor no Brasil.

9.4.2. Forma de interpretação e notificação

9.4.2.1. Na hipótese de uma ou mais disposições desta DPPSC ser, por qualquer razão, considerada inválida, ilegal, ou conflituosa com norma da ICP-Brasil, a inaplicabilidade não afeta as demais disposições, sendo esta interpretada, então, como se não contivesse tal disposição e, na medida do possível, interpretada para manter a intenção original da DPPSC. Nesse caso, o Grupo de Práticas e Políticas do PSC Certisign examinará a disposição inválida e proporá à nova redação ou retirada da disposição afetada.

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

9.4.3. Procedimentos de solução de disputa

9.4.3.1. Em caso de conflito entre esta DPPSC, outras declarações, políticas, planos, acordos, contratos ou outros documentos que o PSC Certisign adotar, prevalece o disposto nesta DPPSC.

9.4.3.2. Esta DPPSC do PSC Certisign não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.4.3.3. Casos omissos deverão ser encaminhados para apreciação da AC Raiz.

9.5. Tarifas de Serviço

9.5.1. Tarifas de armazenamento de chaves privadas para usuários finais

Variável conforme definição interna Comercial.

9.5.2. Tarifas de serviço de assinatura digital

Variável conforme definição interna Comercial.

9.5.3. Tarifas de serviço de verificação da assinatura digital

Variável conforme definição interna Comercial.

9.5.4. Outras tarifas

Variável conforme definição interna Comercial.

9.5.5. Política de reembolso

Em caso de revogação do certificado por motivo de comprometimento da chave privada ou da mídia armazenadora da chave privada dos subscritores do PSC Certisign, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável o PSC Certisign, será emitido gratuitamente outro certificado em substituição.

9.6. Sigilo

9.6.1. Disposições Gerais

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

9.6.1.2. As assinaturas digitais e verificações das assinaturas digitais que são realizadas pelo PSC Certisign, que será responsável pelo seu sigilo, mantendo as trilhas de auditoria com horário e data sincronizados com a EAT, inclusive identificando qual documento, IP ou URL, entre outros, que 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 Certisign, 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. Como princípio geral, todo documento, informação ou registro fornecido ao PSC Certisign pelos subscritores é sigiloso.

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

9.6.3. Tipos de informações não sigilosas

Os tipos de informações consideradas não sigilosas pelo PSC Certisign são:
a) os certificados dos subscritores;
b) esta DPPSC;
c) versões públicas da Política de Segurança; e
d) a conclusão dos relatórios de auditoria.

9.6.4. Quebra de sigilo por motivos legais

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

9.6.5. Informações a terceiros

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

9.6.6. Outras circunstâncias de divulgação de informação

Não se aplica.

9.7. Direitos de Propriedade Intelectual

A Certisign Certificadora Digital S.A. detém todos os direitos de propriedade intelectual sobre as ideias, conceitos, técnicas e invenções, processos e/ou obras, políticas, especificações de práticas e procedimentos, incluídas ou utilizadas nos produtos e serviços fornecidos pelo PSC Certisign nos termos dessa DPPSC.

Os Direitos de Propriedade terão proteção conforme a legislação aplicável.

10. DOCUMENTOS REFERENCIADOS

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]	PROCEDIMENTOS OPERACIONAIS MÍNIMOS PARA OS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17.01
[11]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[12]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[13]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[14]	VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL	DOC-ICP-15
[15]	REQUISITOS MÍNIMOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL	DOC-ICP-15.01
[16]	REQUISITOS DAS POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL	DOC-ICP-15.03

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.