Infraestrutura de Chaves Públicas Brasileira

PROCEDIMENTOS OPERACIONAIS PARA OS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL

DOC-ICP-17.01

Versão 1.0

xx de setembro de 2017

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução 1xx, de xx.09.2017 (Versão 1.0)		Criação do DOC-ICP-17.01.

LISTA DE 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*
FGTS	Fundo de Garantia do Tempo de Serviço
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	Prestadores de Serviço de Certificação
PSS	Prestadores de Serviço de Suporte
SHA	*Secure Hash Algorithm*
SICAF	Sistema de Cadastramento Unificado de Fornecedores
TAR	Tribunal de Contas da União
TCU	Tribunal de Contas da União

1. DISPOSIÇÕES GERAIS

a) Este documento tem por finalidade regulamentar os requisitos mínimos de segurança e os procedimentos operacionais a serem adotados pelos Prestadores de Serviço de Confiança (PSC) da ICP-Brasil.

b) Suplementa, para essas entidades, os regulamentos contidos no documento DOC-ICP-03, DOC-ICP-04, DOC-ICP-08 e DOC-ICP-09, tomando como base também a Política de Segurança da ICP-Brasil – DOC-ICP-02.

c) Os requisitos contidos neste documento deverão ser apresentados quando do credenciamento do PSC para armazenamento de certificados digitais dos usuários finais ou serviços de assinaturas digitais, verificação de assinaturas digitais e armazenamento de documentos, se for o caso, ou ambos e mantidos atualizados durante seu funcionamento enquanto a entidade estiver credenciada na ICP-Brasil.

d) O PSC deverá ter uma Política de Segurança da Informação composta por diretrizes, normas e procedimentos que descrevem os controles de segurança que devem ser seguidos em suas dependências e atividades, em consonância com o DOC-ICP-02.

e) Deverá existir um exemplar da Política de Segurança da Informação, no formato impresso, disponível para consulta no Nível 1 (vide regulamento no item 3) de segurança do PSC.

f) A Política de Segurança da Informação deverá ser seguida por todo pessoal envolvido nas atividades realizadas pelo PSC, do seu próprio quadro ou contratado.

g) Este documento define normas de segurança que deverão ser aplicadas nas áreas internas ao PSC, assim como no trânsito de informações, armazenamento de certificados, serviços de assinatura digital e verificação de assinatura digital e materiais com entidades externas.

h) A seguir são informados os requisitos que devem ser observados quanto a segurança de pessoal, segurança física, segurança lógica, segurança de rede, requisitos mínimos para armazenamento de certificados digitais, serviços de assinatura digital e verificação de assinatura digital, classificação da informação, salvaguarda de ativos da informação, gerenciamento de riscos, plano de continuidade de negócios e análise de registros de eventos.

2. SEGURANÇA PESSOAL

a) O PSC deverá ter uma Política de Gestão de Pessoas que disponha sobre os processos de contratação, demissão, descrição de cargos, avaliação de desempenho e capacitação.

b) A comprovação da capacidade técnica do pessoal envolvido nos serviços prestados pelo PSC deverá estar à disposição para eventuais auditorias e fiscalizações.

c) Todo pessoal envolvido nas atividades realizadas pelo PSC, do próprio quadro ou contratado, deverá assinar um termo, com garantias jurídicas, que garanta o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato.

d) O termo de sigilo da informação deverá conter cláusula explícita de responsabilização nos casos de quebra de regras ou regulamentos da ICP-Brasil.

e) Aplicar-se-á o termo de sigilo de informações a quaisquer outras entidades que porventura tenham acesso as informações internas e de terceiros originárias dos projetos coordenados pelo PSC.

f) O PSC deverá ter procedimentos formais de apuração e responsabilização em caso de descumprimento das regras estabelecidas pelas suas políticas ou pelas normas da ICP-Brasil.

g) O quadro de pessoal do PSC e contratados deverão possuir um dossiê contendo os seguintes documentos:

i. Contrato de trabalho ou cópia das páginas da carteira de trabalho onde conste o registro da contratação, termo de posse de servidor ou comprovante de situação funcional;

ii. Comprovante da verificação de antecedentes criminais;

iii. Comprovante da verificação de situação de crédito;

iv. Comprovante da verificação de histórico de empregos anteriores;

v. Comprovação de residência;

vi. Comprovação de capacidade técnica;

vii. Resultado da entrevista inicial, com a assinatura do entrevistador;

viii. Declaração em que afirma conhecer as suas atribuições e em que assume o dever de cumprir as regras aplicáveis da ICP-Brasil;

ix. Termo de sigilo.

h) Não serão admitidos estagiários no exercício fim das atividades do PSC.

i) Quando da demissão, o referido dossiê deverá possuir os seguintes documentos:

i. Evidências de exclusão dos acessos físico e lógico nos ambientes do PSC;

ii. Declaração assinada pelo empregado ou servidor de que não possui pendências, conforme previsto no item 7.3.10 do DOC-ICP-02.

3. SEGURANÇA FÍSICA

3.1. Disposições Gerais de Segurança Física

3.1.1. Níveis de acesso

3.1.1.1. São definidos pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes do PSC.

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

3.1.1.1.2. O segundo nível – ou nível 2 – será interno ao primeiro e deverá requerer a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo do PSC. A passagem do primeiro para o segundo nível deverá exigir identificação por meio eletrônico e o uso de crachá.

a) O ambiente de nível 2 deverá ser separado do nível 1 por paredes divisórias de escritório, alvenaria ou pré-moldadas de gesso acartonado. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso;

b) O acesso a este nível deverá ser permitido apenas a pessoas que trabalhem diretamente com as atividades de serviços de armazenamento dos certificados para usuários finais e serviços de assinatura digital e verificação da assinatura digital ou ao pessoal responsável pela manutenção de sistemas e equipamentos do PSC, como administradores de rede e técnicos de suporte de informática. Demais funcionários do PSC ou do possível ambiente que esta compartilhe não deverão acessar este nível;

c) Preferentemente, *nobreaks*, geradores e outros componentes da infraestrutura física deverão estar abrigados neste nível, para evitar acessos ao ambiente de nível 3 por parte de prestadores de serviços de manutenção;

d) Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações do PSC, a partir do nível 2. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser utilizados mediante autorização formal e sob supervisão.

3.1.1.1.3. O terceiro nível – ou nível 3 – deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação do PSC. Qualquer atividade relativa ao armazenamento de certificados digitais dos usuários e serviços de assinatura digital e verificação da assinatura digital deverá ser realizada nesse nível. Somente pessoas autorizadas poderão permanecer nesse nível.

a) No terceiro nível deverão ser controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica ou digitação de senha;

b) As paredes que delimitam o ambiente de nível 3 deverão ser de alvenaria ou material de resistência equivalente ou superior. Não deverá haver janelas ou outro tipo qualquer de abertura para o exterior, exceto a porta de acesso;

c) Caso o ambiente de Nível 3 possua forro ou piso falsos, deverão ser adotados recursos para impedir o acesso ao ambiente por meio desses, tais como grades de ferro estendendo-se das paredes até as lajes de concreto superior e inferior;

d) Deve haver uma porta única de acesso ao ambiente de nível 3, que abra somente depois que o funcionário tenha se autenticado eletronicamente no sistema de controle de acesso. A porta deverá ser dotada de dobradiças que permitam a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário;

e) Poderão existir no PSC vários ambientes de nível 3 para abrigar e segregar, quando for o caso:

i. equipamentos de produção e cofre de armazenamento;

ii. equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

NOTA 1: Caso a PSC se situe dentro de um *data center*, com requisitos de segurança julgados adequados pela AC-Raiz, poderá ser dispensada a existência de um ambiente de Nível 3 específico para a PSC.

3.1.1.1.4. O terceiro nível avançado – ou nível 3.1 –, no interior ao ambiente de nível 3, deverá compreender pelo menos um gabinete reforçado trancado, que abrigará o *hardware* criptográfico com os certificados digitais dos usuários da ICP-Brasil:

a) Para garantir a segurança do material armazenado, os gabinetes deverão obedecer às seguintes especificações mínimas:
   i. ser feitos em aço ou material de resistência equivalente;
   ii. possuir tranca com chave.

3.1.1.2. Todos os servidores e elementos de infraestrutura e proteção do segmento de rede, tais como roteadores, *hubs*, *switches* e *firewalls* devem:

a) operar em ambiente com segurança equivalente, no mínimo, ao nível 3 citado neste documento;

b) possuir acesso lógico restrito por meio de sistema de autenticação e autorização de acesso;

3.1.1.3. Os PSC devem ainda atender aos seguintes requisitos:

a) O ambiente físico do PSC deverá conter dispositivos que autentiquem e registrem o acesso de pessoas informando data e hora desses acessos;

b) O PSC deverá conter imagens que garantam a identificação de pessoas quando do acesso físico em qualquer parte de seu ambiente;

c) É mandatório o sincronismo de data e hora entre os mecanismos de segurança física garantindo a trilha de auditoria entre dispositivos de controle de acesso físico e de imagem;

d) Todos que transitam no ambiente físico do PSC deverão portar crachás de identificação, inclusive os visitantes;

e) Só é permitido o trânsito de material de terceiros pelos ambientes físicos do PSC mediante registro, garantindo a trilha de auditoria com informações de onde o material passou, a data e hora que ocorreu o trânsito e quem foi o responsável por sua manipulação;

f) O PSC deverá conter dispositivos de prevenção e controle de incêndios, temperatura, umidade, iluminação e oscilação na corrente elétrica em todo seu ambiente físico;

g) Todo material crítico inservível, descartável ou não mais utilizável deverá ter tratamento especial de destruição, garantindo o sigilo das informações lá contidas. O equipamento enviado para manutenção deverá ter seus dados apagados, de forma irreversível, antes de ser retirado do ambiente físico do PSC;

h) Os computadores pessoais, servidores e dispositivos de rede, e seus respectivos softwares, deverão estar inventariados com informações que permitam a identificação inequívoca;

i) Em caso de inoperância dos sistemas automáticos, o controle de acesso físico deverá ser realizado provisoriamente por meio de um livro de registro onde constará quem acessou, a data, hora e o motivo do acesso;

j) Deverão ser providenciados mecanismos para garantir a continuidade do fornecimento de energia nas áreas críticas, mantendo os ativos críticos de informação em funcionamento até que todos os processos e dados sejam assegurados caso o fornecimento de emergência se esgote;

l) No caso de armazenamento de certificados para usuários finais, deve ter no mínimo dois ambientes, sendo obrigatoriamente um para operação e outro para contingência;

m) No caso do PSC ser uma AC da ICP-Brasil, pode ser utilizado o nível 4 para abrigo do *hardware* criptográfico que armazenará as chaves dos usuários finais, desde que em dispositivo e gabinete segregados dos que operam as chaves de AC.

4. SEGURANÇA LÓGICA

a) O acesso lógico ao ambiente computacional do PSC se dará no mínimo mediante usuário individual e senha, que deverá ser trocada periodicamente;

b) Todos os equipamentos do parque computacional deverão ter controle de forma a permitir somente o acesso lógico a pessoas autorizadas;

c) Os equipamentos deverão ter mecanismos de bloqueio de sessão inativa;

d) O PSC deverá ter explícita a política de cadastro, suspensão e remoção de usuários em seu ambiente computacional. Os usuários deverão estar cadastrados em perfis de acesso que permitam privilégio mínimo para realização de suas atividades;

e) Os usuários especiais (a exemplo do *root* e do administrador) de sistemas operacionais, do *hardware* criptográfico, do banco de dados e de aplicações em geral devem ter suas

senhas segregadas de forma que o acesso lógico a esses ambientes se dê por, pelo menos, duas pessoas autorizadas;

f) Todo equipamento do PSC deverá ter *log* ativo e seu horário sincronizado com uma fonte confiável de tempo da ICP-Brasil;

g) As informações como *log*, trilhas de auditoria (do armazenamento de certificados digitais ao serviço de assinatura), registros de acesso (físico e lógico) e imagens deverão ter cópia de segurança cujo armazenamento será de 6 anos;

h) Os *softwares* dos sistemas operacionais, os antivírus e aplicativos de segurança devem ser mantidos atualizados;

i) É vedado qualquer tipo de acesso remoto ao ambiente de nível 3.

5. SEGURANÇA DE REDE

a) O tráfego das informações no ambiente de rede deverá ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos;

b) Não poderão ser admitidos acessos externos a rede interna do PSC. As tentativas de acessos externos deverão ser inibidas e monitoradas por meio de aplicativos que criem barreiras e filtros de acesso, assim como mecanismos de detecção de intrusão;

c) Deverão ser aplicados testes de segurança na rede interna e externa com aplicativos especializados com periodicidade de, no mínimo, uma vez a cada mês. Os testes na rede deverão ser documentados e as vulnerabilidades detectadas corrigidas.

6. REQUISITOS PARA ARMAZENAMENTO DE CERTIFICADOS DIGITAIS

6.1 Armazenamento dos certificados digitais.

a) As chaves dos usuários finais e os respectivos certificados gerados, para os tipos de certificados que obrigatoriamente devem ser gerados e armazenados em hardware criptográficos, devem estar armazenados dentro dos espaços (*slots*), ou equivalente, da fronteira criptográfica e segura física de um HSM homologado na ICP-Brasil, endereçados por conta de usuário;

b) Esse acesso às chaves dos usuários deve ser de uso e controle exclusivo do titular da chave privada, sem a possibilidade de ingresso por outros titulares no mesmo HSM, qualquer funcionário e sistema do PSC ou dependentes de outras soluções e chaves criptográficas;

c) O HSM deve prover mecanismos de duplo fator de autenticação ao titular para acesso à chave privada. Cada fator deve ser de uma classe diferente (conhecimento, posse, *push notifications* ou biometria). Os mecanismos de autenticação devem empregar método ou protocolo de validação que proteja os dados por meio de criptografia. Esta funcionalidade será apensada aos requisitos técnicos na renovação de homologação dos HSM;

d) Deverá ser feita, em outro ambiente, a cópia das chaves dos usuários finais, observados os mesmos requisitos de armazenamento do ambiente principal.

e) Esses espaços para armazenamento das chaves privadas dos usuários finais poderão ser liberados desde que não haja renovação por parte do mesmo ou a revogação da chave, entretanto deve-se manter o registro de armazenamento das chaves conforme Declaração de Prática do Prestador de Serviço de Confiança – DPPSC.

6.2 Protocolo e Rede

6.2.1 Os HSMs devem suportar o protocolo *Key Management Interoperability Protocol* – KMIP, versão 1.3 ou superior, devendo seguir, além dos relatados nesse documento, os seguintes requisitos:

6.2.1.1 Os PSC devem definir um conjunto de operações que se aplicam aos objetos gerenciados que por sua vez consistem em atributos, como mostrado na tabela a seguir.

Operações do Protocolo	Objetos Gerenciados	Atributos dos Objetos
Create	Certificate	Unique Identifier
Create Key Pair	Symmetric Key	Name
Register	Public Key	Object Type
Re-key	Private Key	Cryptographic Algorithm
Derive Key	Split Key	Cryptographic Length
Certify	Template	Cryptographic Parameters
Re-certify	Policy Template	Certificate Type
Locate	Secret Data	Certificate Issuer
Check	Opaque Object	Certificate Subject
Get	Key Block (para chaves) ou Value (para certificados)	Digest
Get Attributes		Operation Policy Name
Get Attribute List		Cryptographic Usage Mask
Add Attribute		Lease Time
Modify Attribute		Usage Limits
Delete Attribute		State
Obtain Lease		Initial Date
Get Usage Allocation		Activation Date
Activate		Process Start Date
Revoke		Protect Stop Date

Destroy		Deactivation Date
Archive		Destroy Date
Recover		Compromise Occurrence Date
Validate		Compromise Date
Query		Revocation Reason
Cancel		Archive Date
Poll		Object Group
Notify		Link
Put		Application Specific ID
		Contact Information
		Last Change Date
		Custom Attribute

6.2.1.2 Os objetos base são:

a) Os componentes dos objetos gerenciados.

i. Atributo: identificado pelo seu nome;

ii. *Key Block*, contém o valor da chave;

b) Os elementos do protocolo de mensagens;

c) Os parâmetros das operações.

6.2.1.3 Os objetos criptográficos gerenciáveis são:

a) Certificado, com o tipo e valor;

b) Chave simétrica, com o *Key Block*;

c) Chave Pública, com o *Key Block*;

d) Chave Privada, com o *Key Block*;

e) Chave Dividida, com o par e o *Key Block*;

f) Dados Reservados, com o tipo e o *Key Block*.

6.2.1.4 Os objetos gerenciáveis são:

a) *Template* e a Política de *Template*;
i. um *template* possui um subconjunto de atributos que indicam o que é um objeto criado a partir desse modelo;
ii. a política de um *template* tem um subconjunto de atributos que indica como um objeto criado a partir desse modelo pode ser usado;
iii. os *templates* (ou a política de *template*) devem possuir somente atributos.

b) Objeto opaco, sem *Key Block*.

6.2.1.5 Os atributos contêm os metadados de um objeto gerenciável, nos quais:

a) Número identificador único, estado, entre outros;

b) Os atributos devem ser pesquisados com a operação “locate”.

6.2.1.6 Os atributos podem ser configurados, modificados e apagados.

6.2.1.7 Os valores das estruturas de codificações (TTLV, definição dos valores, *Text String*, *Structure*, *Byte String*, *Integer*, *Big Integer*, *Long Integer*, *Boolean*, *Date-Time* e *Enumerations*), dos campos dos objetos, dos atributos, dos formatos e conteúdos das mensagens, da manipulação de

erros e dos parâmetros (solicitação e resposta) das operações cliente/servidor devem seguir integralmente o estabelecido neste documento e no *Key Management Interoperability Protocol Specification Version 1.3, OASIS Standard, 27 December 2016*, ou versionamento superior.

NOTA XX: O ITI poderá requisitar aos fabricantes de HSM testes no modelo descrito no sítio https://www.snia.org/forums/ssif/kmip ou equivalente.

6.2.2 Para a operação duplo fator de autenticação do titular da chave privada, deve ser criada uma nova extensão ao tipo de credencial, conforme relatado a seguir:

6.2.2.1 Para o novo tipo de credencial deve ser configurado o seguinte:

a) Credential Type: TOKEN

Object	Encoding	Required	Description
Credential Value	Structure		
Token	Text String	Yes	Valor atual do “TOKEN”

b) Fluxo de uso

i. durante o credenciamento, o PSC deve requisitar a criação de um novo usuário (via KMIP), indicando que o mesmo necessita de um segundo fator de autenticação para utilizar seus objetos e cadastrando seu nome de usuário e senha. O PSC indica ao usuário como instalar seu aplicativo de Token.

ii. o “TOKEN” do usuário deve ser inicializado para sincronizar seus dados. Esse processo pode ser feito pelo próprio usuário através do aplicativo de “TOKEN” via KMIP no momento da primeira conexão utilizando seu usuário e senha. O HSM gera então a chave que será utilizada no “TOKEN”.

iii. na posse de seu token “TOKEN” sincronizado e de seu usuário e senha, o usuário pode então criar sua chave no HSM utilizando a aplicação do PSC diretamente via comando KMIP.

iv. o usuário já pode utilizar sua chave criada anteriormente utilizando o aplicativo do PSC, de posse de sua Senha + Token.

6.2.2.2 Este mecanismo de “TOKEN” deve ser configurado na área de execução segura do HSM.

NOTA XX: Pode ser encontrada mais referências sobre o protocolo KMIP no sítio https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip.

6.2.3 Poderá ser arquitetado um *pool* de HSM para operação, replicação e gerenciamento das chaves dos usuários finais, devendo seguir, além dos relatados nesse documento, os seguintes requisitos.

a) Especificação e estabelecimento de uma comunicação segura (sessão SSL/TLS) entre os HSM;

b) Os HSM poderão estar em ambientes distintos desde que os mecanismos de acesso e segurança se mantenham os descritos neste documento.

6.2.4 Os PSC no âmbito da ICP-Brasil devem atender aos critérios mínimos de 99,9% de “nível de tempo de atividade” (*uptime*) e 99,5% de “solicitações atendidas com sucesso”, ambos a serem verificados por mês.

7. SERVIÇO DE ASSINATURA DIGITAL, VERIFICAÇÃO DE ASSINATURA DIGITAL E ARMAZENAMENTO DE DOCUMENTOS ASSINADOS.

7.1. Introdução

7.1.1. Os requisitos a seguir foram baseadas nos padrões para criação e validação de assinaturas definidas nas especificações do ETSI.

7.2. Criação de Assinaturas

7.2.1. O objetivo da criação de assinaturas é para gerar uma assinatura cobrindo um documento eletrônico (texto, som, imagem, entre outros) do assinante, o certificado de assinatura ou uma referência a esse certificado, bem como os atributos da assinatura que suportam essa assinatura.

7.2.2. Um modelo funcional básico de um ambiente para a criação de assinaturas se constitui por:

- signatário que quer criar uma assinatura em um documento eletrônico;
- um aplicativo condutor que representa um ambiente de usuário (por exemplo, um aplicativo de negócios) que o assinante usa para acessar a funcionalidade de assinatura; e
- um sistema de criação de assinatura, que implementa a funcionalidade de assinatura.

7.2.3. Antes de iniciar o procedimento de assinatura o sistema deve verificar a validade do certificado. Ao receber o retorno da assinatura o sistema deve bater a resposta com a chave publica.

NOTA: O envolvimento humano de um signatário nem sempre é necessário. A assinatura pode ser um processo automatizado e implementado na aplicação no ambiente do usuário.

7.3. Dispositivos para criação de assinaturas

7.3.1. São sistemas ou equipamentos configurados para implementar códigos e/ou outros mecanismos que possibilitem ativação da chave privada do signatário para a criação das assinaturas digitais.

7.3.2. Os dispositivos para criação de assinatura devem conter os certificados de assinatura ou possuírem uma referência inequívoca a eles. Devem ainda, poder verificar os dados de autenticação do assinante.

7.3.3. Todos os equipamentos para criação de assinaturas devem ser homologados no âmbito da ICP-Brasil conforme definido no conjunto de documentos DOC-ICP-10 e seus complementares.

7.4. Interface da aplicação com o dispositivo de criação de assinaturas

7.4.1. A interface entre a aplicação de assinatura e o dispositivo ou equipamento de criação devem garantir 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.

7.4.2. O uso do dispositivo de criação pode exigir que o usuário insira dados específicos de autenticação do assinante. Toda informação trocada entre a aplicação e o dispositivo deve trafegar de forma criptografada.

7.4.3. Mais de um mecanismo de autenticação pode ser usado para fornecer uma garantia de autenticação suficiente.

7.4.4. Um mecanismo de autenticação do signatário pode ser de uma forma que evite ataques de representação.

NOTA 1: A natureza dos mecanismos de autenticação e os dados de autenticação do assinante são determinados pelo dispositivo de criação de assinaturas. Existem padrões para diferentes interfaces, tipos dispositivos ou equipamentos e mecanismos de autenticação.

NOTA 2: Em alguns casos, o uso de dados de autenticação do signatário será obrigatório e outros requisitos sobre a natureza dos mecanismos de autenticação e as interfaces podem ser impostas.

7.5. Suítes de Assinatura

7.5.1. Todos os algoritmos envolvidos no cálculo de qualquer elemento da assinatura sejam baseados em algoritmos e comprimentos de chaves apropriados estão definidos no documento DOC-ICP-01.01.

7.6. Formatos de Assinaturas

7.6.1. A ICP-Brasil padroniza as assinaturas digitais baseadas em políticas explícitas de assinatura. As políticas de assinatura preveem os formatos CAdES, XAdES e PAdES.

7.6.2. Todos os formatos e perfis de assinatura digital no âmbito da ICP-Brasil estão definidos no conjunto de documentos DOC-ICP-15 e seus complementares.

7.7. Assinatura com Carimbo do Tempo

7.7.1. Uma assinatura com carimbo do tempo é uma assinatura que prova que a assinatura já existia em um determinado momento. Os carimbos do tempo são emitidos pelas Autoridades de Carimbo do Tempo (ACT) credenciadas na ICP-Brasil e fornece data/hora na assinatura como uma propriedade não assinada adicionada à uma assinatura digital.

7.7.2. A ICP-Brasil define no documento DOC-ICP-11 o modelo de carimbo do tempo adotado em sua infraestrutura.

7.7.3. As políticas de assinatura regulamentadas no âmbito da ICP-Brasil definem o uso de carimbo do tempo.

7.8. Validação de Assinaturas

7.8.1. O processo de validação de uma assinatura deve validar a assinatura contra uma política de validação de assinatura, que consiste de um conjunto de restrições de validação, e deve gerar um relatório com indicação da situação de validação, fornecendo os detalhes da validação técnica de cada uma das restrições aplicáveis, que podem ser relevantes para a aplicação demandante na interpretação dos resultados.

7.8.2. Na ICP-Brasil, conforme disposto no documento DOC-ICP-15, uma assinatura digital é criada pelo signatário de acordo com uma política de assinatura. A validade de uma assinatura digital é avaliada pelo verificador utilizando a mesma política de assinatura usada na criação dessa assinatura digital. O item 6.6.2, acima, define os todos os formatos e perfis regulamentados no âmbito da ICP-Brasil.

7.8.3. Os requisitos para geração e verificação de assinaturas digitais no ãmbito da ICP-Brasil estão descritos no documento DOC-ICP-15.01.

7.9. Acordo de Nível de Serviço

7.9.1. O acordo de nível de serviço para todos os serviços credenciados do PSC deverá ser de no mínimo 99,5%.

8. CLASSIFICAÇÃO DA INFORMAÇÃO

a) Toda informação gerada e custodiada pelo PSC deverá ser classificada segundo o seu teor crítico e grau de confidencialidade, de acordo com sua própria Política de Classificação de Informação;

b) A classificação da informação no PSC deverá ser realizada independente da mídia onde se encontra armazenada ou o meio pelo qual é trafegada;

c) A informação poderá ser classificada em:

i. Público: Qualquer ativo de informação, de propriedade do PSC ou não, que poderá vir ao público sem maiores consequências danosas ao funcionamento normal do PSC. Poderá ser acessado por qualquer pessoa, seja interna ou externa ao PSC. Integridade da informação não é vital;

ii. Pessoal: Qualquer ativo de informação relacionado à informação pessoal. Por exemplo: mensagem pessoal de correio eletrônico, arquivo pessoal, dados pessoais, etc;

iii. Interna: Qualquer ativo de informação, de propriedade do PSC ou não, que não seja considerada pública. Ativo de informação relacionado às atividades do PSBio que é direcionada estritamente para uso interno. A divulgação não autorizada do ativo de informação poderia causar impacto à imagem do PSC. Por exemplo: código fonte de programa, cronograma de atividades, atas de reuniões, etc;

iv. Confidencial: Qualquer ativo de informação que seja crítico para as atividades do PSC em relação ao sigilo e integridade. Qualquer material e informação recebida

para ensaio, assim como qualquer resultado do ensaio (como relatório) deverá ser considerado confidencial.

NOTA 2: Caso o PSC seja entidade da Administração Pública Federal – APF, aplicar-se-á as disposições do Decreto nº 7.845/2012 e demais normas aplicáveis à APF, no que couber.

9. SALVAGUARDA DE ATIVOS DA INFORMAÇÃO

a) O PSC deverá, em sua Política de Segurança da Informação, definir como será realizada a salvaguarda de ativos de informação no formato eletrônico, também denominado backup.

b) A salvaguarda de ativos da informação deverá ter descrita as formas de execução dos seguintes processos:

i. Procedimentos de *backup*;

ii. Indicações de uso dos métodos de *backup*;

iii. Tabela de temporalidade;

iv. Local e restrições de armazenamento e salvaguarda em função da fase de uso;

v. Tipos de mídia;

vi. Controles ambientais do armazenamento;

vii. Controles de segurança;

viii. Teste de restauração de *backup*.

c) O PSC deverá ter política de recebimento, manipulação, depósito e descarte de materiais de terceiros.

10. GERENCIAMENTO DE RISCOS

O PSC deverá ter um processo de gerenciamento de riscos, atualizado, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados atualizado, no mínimo, anualmente.

11. PLANO DE CONTINUIDADE DE NEGÓCIOS

Um Plano de Continuidade do Negócio – PCN deverá ser implementado e testado no PSC, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio em caso de inoperância total ou parcial de seu ambiente.

12. ANÁLISES DE REGISTRO DE EVENTOS

Todos os registros de eventos (*logs*, trilhas de auditorias e imagens) deverão ser analisados, no mínimo, mensalmente e um relatório deverá ser gerado com assinatura do responsável pelo PSC. Todos os registros da transação biométrica por parte do PSC deverão ser guardados por um período de 6 anos.