Requisitos Operacionais – PSC Serasa

1. Requisitos Operacionais

1.1. Armazenamento e acesso aos certificados do subscritor

Os componentes de software que fazem a comunicação entre a aplicação do subscritor e acesso ao certificado possuem as seguintes características técnicas:

a) As linguagens de programação utilizadas para a plataforma são Java, C++ e C.
b) O subscritor tem acesso à plataforma através de interface web de gestão, webservices, aplicativos móveis e *plugins* (CSP, KSP e PKCS#11) para computadores *desktop*.
c) As autenticações são protegidas por TLS.
d) A arquitetura de rede segue o modelo TCP/IP.

1.2. Serviço de criação e validação de assinaturas digitais

Não se aplica.

1.3. Procedimentos de Auditoria de Segurança

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

1.3.1. Tipos de eventos registrados

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

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

1.3.1.2. O PSC 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.

1.3.1.3. O PSC registra os seguintes eventos, em específico:

a) Criação e remoção de compartimentos;
b) Criação e remoção de chaves;
c) Geração de CSR e solicitação de certificado em AC;
d) Importação de certificado associado à chave;
e) Importação de certificado com chave (A1);
f) Usos de chave (assinatura digital);
g) Alteração de credenciais de acesso (PIN e segundo fator de autenticação);
h) Tentativas de autenticação inválidas;

1.3.1.4. Todos os registros contêm as seguintes informações:

a) Data e horário do evento, em UTC;
b) Identificação única do agente causador do evento;

1.3.1.5. Toda a documentação relacionada aos serviços do PSC é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

1.3.2. Frequência de auditoria de registros (logs)

Os registros de auditoria são analisados pela equipe operacional do PSC com periodicidade não superior a uma semana. Os eventos significativos são explicados em relatório de auditoria de registros. A 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.

1.3.3. Período de retenção para registros (logs) de auditoria

O PSC mantém os registros de auditoria localmente por pelo menos 2 (dois) meses e, subsequentemente, armazena-os da maneira descrita no item 4.5.

1.3.4. Proteção de registro (log) de auditoria

1.3.4.1. Os registros de auditoria gerados eletronicamente são protegidos contra leitura não autorizada, modificação e remoção, através de políticas de controle de acesso aos arquivos e suas cópias de segurança.

1.3.4.2. As informações geradas manualmente são protegidas de leitura não autorizada, modificação e remoção.

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

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

O PSC executa procedimentos de backup de logs da solução das seguintes formas:

a) Diariamente: cópia de segurança;
b) Semanalmente: cópia de segurança para processos de auditoria;

1.3.6. Sistema de coleta de dados de auditoria

Os seguintes sistemas coletam dados de auditoria relacionados à operação do PSC.

Sistema operacional:

a) Alterações de segurança e configurações (sucesso e erro)
b) Início e parada da aplicação
c) Login e logout (sucesso e erro)
d) Criação, modificação e remoção de contas

Sistema PSC:

a) Alterações de segurança e configurações (sucesso e erro);
b) Início e parada da aplicação;
c) Login e logout (sucesso e erro);
d) Criação, modificação e remoção de contas;
e) Criação, modificação e remoção de compartimentos;
f) Criação e remoção de chaves e certificados;
g) Uso de chaves;

HSM:

a) Criação e remoção de compartimentos;
b) Criação e remoção de chaves e certificados;
c) Uso de chaves;

Registros manuais:

a) Acessos ao ambiente;
b) Manutenções do sistema;
c) Mudanças de pessoal;
d) Atualizações de software e hardware;
e) Alterações de configurações;

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

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

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

1.4.1. Tipos de registros arquivados

Os seguintes tipos de registro são arquivados:

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 neste item.

O período de retenção para cada registro arquivado é de no mínimo 6 (seis) anos.

1.4.2. Proteção de arquivo
Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

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

1.4.3.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente diferente das instalações principais do PSC, recebendo o mesmo tipo de proteção utilizada no arquivo principal.

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

1.4.3.3. O PSC verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

1.4.4. Requisitos para datação de registros

Os servidores do PSC são sincronizados com a hora fornecida pela AC Raiz por meio de sua Fonte Confiável do Tempo - FCT conforme DOC-ICP 07. Todas as informações geradas de auditoria recebem o horário em UTC com horário recebido desta fonte.

1.4.5. Sistema de coleta de dados de arquivo

O sistema de coletas de arquivos é uma combinação de processos automatizados executados pelo sistema operacional e sistema de PSC e manuais executados pela equipe operacional.

1.4.6. Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos é verificada:

a) Na ocasião em que o arquivo é obtido no respectivo sistema;
b) Em qualquer momento quando auditoria completa de segurança é requerida;

1.5. Liberação do espaço do subscritor

A remoção de compartimento (*slot*) destinado a um subscritor ocorrerá após a expiração e revogação do certificado, caso não haja interesse do usuário na continuidade dos serviços através da emissão de novo certificado no mesmo compartimento.

1.6. Comprometimento e Recuperação de Desastre

1.6.1. Disposições Gerais

1.6.1.1. Nos seguintes itens são descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no Plano de Continuidade de Negócios (PCN) do PSC, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], para garantir a continuidade dos seus serviços críticos.

1.6.1.2. O PSC assegura, no caso de comprometimento de sua operação por qualquer um dos motivos relacionados nos itens abaixo, que as informações relevantes serão disponibilizadas aos subscritores e às terceiras partes. O PSC irá disponibilizar a todos os subscritores e terceiras partes uma descrição do comprometimento ocorrido.

1.6.1.3. No caso de comprometimento de uma operação de armazenamento e acesso das chaves de um ou mais subscritores, o PSC não proverá mais esse serviço até serem tomadas as medidas administrativas pela AC Raiz, informando aos subscritores sobre o problema e devidos encaminhamentos que estes deverão tomar.

1.6.1.4. Não se aplica.

1.6.2. Recursos computacionais, software, e dados corrompidos

O PSC possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que os recursos computacionais, *software* e/ou dados são corrompidos, que inclui as seguintes ações:

a) Identificação de todos elementos corrompidos;
b) Identificação do instante inicial do comprometimento, para invalidação de transações posteriores àquele instante;
c) Análise do nível de comprometimento para determinação das ações a serem executadas.

1.6.3. Sincronismo do PSC

Não se aplica.

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

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

1.7. Extinção dos serviços de PSC

1.7.1. Caso seja necessária a extinção dos serviços do PSC serão efetuados os procedimentos aplicáveis descritos no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

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

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

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

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