imprensaoficial

Declaração de Práticas de Certificação da AUTORIDADE CERTIFICADORA RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO

DPC DA AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO

Versão 1.1 – abril de 2015

ÍNDICE

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora Raiz da Secretaria da Fazenda do Estado de São Paulo em hierarquia privada na execução dos seus serviços de certificação digital.

1.1.2. Apesar de estar sob hierarquia privada, a estrutura desta DPC está baseada no DOC-ICP-05 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Declarações de Prática de Certificação das Autoridades Certificadoras da ICP-Brasil. As referências a formulários presentes nesta DPC deverão ser entendidas também como referências a outras formas que a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO ou entidades a ela vinculadas possa vir a adotar.

1.1.3. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO está certificada em nível igual ao seu próprio nível, ou seja, caracterizando certificado auto-assinado. O seu certificado contém a chave pública correspondente à chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO utilizada para assinar os certificados de AC de nível imediatamente subsequente (AC Subsequente) ao seu e à sua LCR (Lista de Certificados Revogados).

1.1.4. O certificado da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é usado na emissão de certificados digitais de AC Subsequentes, com o objetivo de identificar as AC de nível imediatamente subsequente ao seu, referidas neste documento como AC Subsequentes. Para regulamentar usos específicos dos certificados emitidos pela a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são publicadas Políticas de Certificado disponíveis em página web (http://acsat.imprensaoficial.com.br/repositorio).

1.2. Identificação

Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da Secretaria da Fazenda do Estado de Sao Paulo e referida como "DPC da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO", cujo OID (*object identifier*) é 1.3.6.1.4.1.30253.2.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

Esta DPC refere-se à AC Raiz da Secretaria da Fazenda do Estado de São Paulo.

1.3.2. Prestador de Serviço de Suporte.

1.3.2.1. A relação de todos os Prestadores de Serviço de Suporte – PSS vinculados diretamente a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é publicada em serviço de diretório e/ou em página web da AC RAIZ SECRETARIA DA FAZENDA DO ESTADO DE SÃO PAULO SP (http://acsat.imprensaoficial.com.br/repositorio).

1.3.2.2. PSS são entidades utilizadas pela AC e/ou suas AR para desempenhar atividade descrita nesta DPC ou nas PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) Disponibilização de infra-estrutura física e lógica;

b) Disponibilização de recursos humanos especializados; ou

c) Disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.3. Titulares de Certificado

1.3.3.1. Apenas pessoas jurídicas podem ser titulares de certificados de AC Subsequente emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

1.3.4. Aplicabilidade

1.3.4.1. Os certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO tem sua utilização exclusiva para assinatura de certificados digitais de AC de nível imediatamente subsequente (AC Subsequente) ao seu e de sua Lista de Certificados Revogados (LCR).

1.4. Dados de Contato

Nome: Secretaria da Fazenda do Estado de São Paulo

Endereço: Av. Rangel Pestana, 300 - São Paulo / SP - 01017-911

Nome: Alexandre Palmeira Mendonça

Telefone: (11) 3243-3452

E-mail: diretordti@fazenda.sp.gov.br

2. DISPOSIÇÕES GERAIS

2.1. Obrigações e Direitos

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

2.1.1. Obrigações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO

a) Operar de acordo com esta DPC;

b) Gerar e gerenciar seus pares de chaves criptográficas;

c) Assegurar a proteção de suas chaves privadas;

d) Notificar os usuários quando ocorrer suspeita de comprometimento da chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

e) Distribuir seu próprio certificado;

f) Emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu;

g) Informar a emissão do certificado ao respectivo solicitante;

h) Revogar os certificados emitidos;

i) Emitir, gerenciar e publicar sua LCR;

j) Publicar em sua página web esta DPC da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

k) Publicar em sua página web as informações descritas no item 2.6.1.2 desta DPC;

l) Utilizar protocolo de comunicação seguro ao disponibilizar serviços de solicitação, geração e entrega de certificados digitais para os solicitantes ou usuários de certificados digitais via web;

m) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas por esta DPC;

n) Adotar as medidas de segurança e controle previstas nesta DPC da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

o) Manter a conformidade dos seus processos, procedimentos e atividades tendo como base as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

p) Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

q) Manter e testar regularmente seu Plano de Continuidade do Negócio;

r) Não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;

s) Tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações.

2.1.2. Obrigações do Titular do Certificado

a) Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;

b) Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

c) Utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto nesta DPC;

d) Conhecer os seus direitos e obrigações contemplados por esta DPC;

e) Informar à A SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO o comprometimento ou suspeita de comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;

f) Verificar, no momento da geração do certificado, a veracidade e exatidão das informações contidas no seu certificado e notificar a A SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, solicitando a imediata revogação do certificado que contiver inexatidões ou erros; e

g) Obedecer estritamente a esta DPC da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, bem como respeitar a legislação aplicável,

2.1.3. Direitos da Terceira Parte (Relying Party)

2.1.3.1. Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital.

2.1.3.2. Constitui direito da terceira parte:

a) Recusar a utilização do certificado para fins diversos dos previstos nesta DPC;

b) Verificar, a qualquer tempo, a validade do certificado.

Um certificado emitido pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é considerado válido quando:

a) Não constar da LCR da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

b) Não estiver expirado; e

c) Sua validade puder ser verificada através de certificado válido da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

2.1.3.3. O não exercício desse direito não afasta a responsabilidade da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e do titular do certificado.

2.1.4. Obrigações do Repositório

a) Disponibilizar, logo após a sua emissão, os certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e sua LCR;

b) Estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

c) Implementar os recursos necessários para a segurança dos dados nele armazenados; e

d) Disponibilizar verificação on-line do status do certificado ou outro mecanismo de atualização de status, quando aplicável;

2.2.

2.3. Responsabilidades

2.3.1. Responsabilidades da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO

2.2.1.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO responde pelos danos a que der causa.2.2.1.2. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO responde solidariamente pelos atos das entidades de sua cadeia de certificação: AC subordinadas e PSS.

2.4. Interpretação e Execução

2.4.1. Forma de interpretação e notificação

2.4.1.1. Na hipótese de uma ou mais disposições desta DPC ser, por qualquer razão, considerada inválida, ilegal ou conflituosa, a inaplicabilidade não afeta as demais disposições, sendo esta DPC interpretada, então, como se não contivesse tal disposição e, na medida do possível, interpretada para manter a intenção original da DPC. Nesse caso, a SECRETARIA DA FAZENDA DO ESTADO DE SÃO PAULO examinará a disposição inválida e proporá nova redação ou retirada da disposição afetada, na forma do item 8 desta DPC.

2.4.1.2. As notificações ou qualquer outra comunicação necessária, relativas às práticas descritas nesta DPC, são feitas através de mensagem eletrônica, ou por escrito e entregue à SECRETARIA DA FAZENDA DO ESTADO DE SÃO PAULO.

2.4.2. Procedimentos da solução de disputa

2.4.2.1. Em caso de conflito entre esta DPC da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO ou outros documentos que a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO adotar, prevalece o disposto nesta DPC.

2.4.2.2. Casos omissos deverão ser encaminhados para apreciação da SECRETARIA DA FAZENDA DO ESTADO DE SÃO PAULO.

2.5. Tarifas de Serviço

2.5.1. Tarifas de emissão e renovação de certificados

Não serão cobradas tarifas para emissão e renovação de certificados.

2.6. Publicação e Repositório

2.6.1. Publicação de informação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO

2.6.1.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO em http://acsat.imprensaoficial.com.br/repositorio, obedecendo as regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO em serviço de diretório e/ou página web é de 99,5% (noventa e nove virgulo cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2. As seguintes informações são publicadas em serviço de diretório e/ou em página web da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO (http://acsat.imprensaoficial.com.br/repositorio):

a) Seus próprios certificados;

b) Suas LCRs;

c) Esta DPC;

2.6.2. Frequência de publicação

Certificados são publicados imediatamente após sua emissão. A publicação da LCR se dá conforme o item 3.4.5 desta DPC. As versões ou alterações desta DPC são atualizadas no web site da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

2.6.3. Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos ou desta lista 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.

2.6.4. Repositórios

O repositório da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e pode ser encontrado na página Web (http://acsat.imprensaoficial.com.br/repositorio).

As publicações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO podem ser consultadas através do protocolo http.

Somente a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar a atualizações nas informações por ela publicadas no seu repositório.

2.7. Sigilo

2.7.1. Disposições gerais

2.7.1.1. AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO gera e mantém sua chave privada, sendo responsável pelo seu sigilo. A divulgação ou utilização indevida da sua chave privada é de sua inteira responsabilidade;

2.7.1.2. O responsável pelo uso do certificado de AC Subsequente, titular de certificado emitido pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é responsável pela geração, utilização, manutenção e sigilo da chave privada correspondente a chave pública contida no certificado;

2.7.1.3. O Titular do certificado emitido pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO responderá pelo uso que o responsável fizer de sua chave privada, bem como pela divulgação ou utilização indevida dessa chave;

2.7.2. Tipos de informações sigilosas

2.7.2.1. Como princípio geral, todo documento, informação ou registro fornecido à AC é sigiloso;

2.7.2.2. Nenhum documento, informação ou registro fornecido pelos titulares de certificado à AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO será divulgado.

2.7.3. Tipos de informações não-sigilosas

As informações consideradas não-sigilosas compreendem:

a) Os certificados e a LCR emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

b) Informações corporativas que constem nos certificados ou em diretórios públicos;

c) Esta DPC;

A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO trata como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

a) Estejam na posse legítima da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;

b) Posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro(s) com direitos legítimos para divulgação sua sem quaisquer restrições para tal;

c) Sejam requisitados por determinação judicial ou governamental, desde que a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

2.7.4. Divulgação de informação de revogação ou suspensão de certificado

2.7.4.1. Informações sobre revogação de certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são fornecidas em sua LCR;

2.7.4.2. A razão para a revogação de certificado é informada ao titular do certificado.

2.7.5. Quebra de sigilo por motivos legais

2.7.5.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO fornecerá, mediante ordem judicial ou por determinação legal, documentos, informações ou registros sob sua guarda.

2.7.6. Informações a terceiros

Nenhum documento, informação ou registro sob a guarda da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é fornecido a qualquer pessoa, exceto quando a pessoa que requerer, através de instrumento devidamente constituído, estiver corretamente identificada e autorizada para fazê-lo.

2.7.7. Divulgação por solicitação do Titular

2.7.7.1. O titular de certificado e seu representante legal têm acesso a quaisquer dos seus próprios dados relativos ao certificado digital e podem autorizar a divulgação de seus registros;

2.7.7.2. Autorizações podem ser apresentadas de duas formas:

a) Por meio eletrônico, contendo assinatura válida garantida por certificado emitido na ICP-Brasil;

b) Por solicitação escrita, com firma reconhecida.

2.7.8. Nenhuma liberação de informação é permitida sem autorização numa das formas acima, exceto nos casos do item 2.7.5.

2.8. Direitos de Propriedade Intelectual

2.8.1. A SECRETARIA DA FAZENDA DO ESTADO DE SÃO PAULO SP detém todos os direitos de propriedade intelectual sobre as ideias, conceitos, técnicas e invenções, processos e/ou obras, incluídas ou utilizadas nos produtos e serviços fornecidos por AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO nos termos dessa DPC;

2.8.2. Os Direitos de Propriedade terão proteção conforme a legislação aplicável.

2.9. Geração de novo par de chaves ou Renovação antes da expiração do atual

2.9.1. No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO para a geração de novo par de chaves e de seu correspondente certificado ou renovação do certificado, antes da expiração do certificado vigente;

2.9.2. O processo descrito acima é conduzido através da adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado.

2.10. Geração de novo par de chaves após expiração ou revogação

2.10.1. Após a revogação ou expiração do certificado, os procedimentos utilizados para confirmação da identidade do solicitante de novo certificado são os mesmos exigidos na solicitação inicial do certificado, na forma e prazo descritos nesta DPC;

2.10.2. Após a expiração ou revogação de certificado de AC de nível imediatamente subsequente ao da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, a AC Subsequente executa os processos regulares de geração de seu novo par de chaves.

2.11. Solicitação de Revogação

2.11.1. A solicitação de revogação de certificado é realizada através de declaração assinada pelo(s) representante(s) legal(is) com firma(s) reconhecida(s);

2.11.2. A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na solicitação. As solicitações de revogação de certificado são registradas.

3. REQUISITOS OPERACIONAIS

3.1. Solicitação de Certificado

3.1.1. A AC Subsequente encaminha a solicitação de seu certificado à AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO por meio de seu(s) representante(s) legal(is).

3.2. Emissão de Certificado

3.2.1. A emissão de certificado é realizada automaticamente através do Web Service.

3.2.2. O certificado da AC é considerado válido a partir do momento de sua emissão.

3.3. Aceitação de Certificado

3.3.1. A pessoa física responsável verifica as informações contidas no certificado quanto a integridade e autenticidade das informações. Caso estejam incorretas, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

a) Concorda com as responsabilidades, obrigações e deveres nesta DPC;

b) Garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

c) Afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

3.3.2. A aceitação do certificado de uma AC Subsequente é declarada por seu responsável através da assinatura do Termo de Aceite.

3.4. Suspensão e Revogação de Certificado

3.4.1. Circunstâncias para revogação

3.4.1.1. O titular do certificado e o responsável pelo certificado podem solicitar a revogação de seu certificado a qualquer tempo, independente de qualquer circunstância.

3.4.1.2. O certificado é obrigatoriamente revogado:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;

b) Quando for necessária a alteração de qualquer informação constante no mesmo;

c) No caso de extinção, dissolução ou transformação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

d) No caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou de seu módulo criptográfico armazenador; ou

e) No caso de extinção, dissolução ou transformação do titular do certificado.

3.4.1.3. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO revoga, no prazo definido no item 3.4.4, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas nesta DPC.

3.4.2. Quem pode solicitar revogação

A revogação do certificado de uma AC de nível imediatamente subsequente ao da AC Raiz somente pode ser feita:

a) Por determinação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

b) Por solicitação do responsável pelo certificado;

c) Por determinação da AC titular do certificado;

3.4.3. Procedimento para solicitação de revogação

3.4.3.1. Uma solicitação de revogação é necessária para que se inicie o processo de revogação. O solicitante da revogação habilitado pode solicitar facilmente e a qualquer tempo a revogação de certificado, evitando assim a utilização indevida do certificado;

Instruções para a solicitação de revogação do certificado são obtidas em página web disponibilizada pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

3.4.3.2. Como diretrizes gerais:

a) O Solicitante da revogação de um certificado é identificado;

b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

c) As justificativas para a revogação de um certificado são registradas;

d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado.

3.4.3.4. O prazo máximo admitido para a conclusão do processo de revogação dos certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, após o recebimento da respectiva solicitação é de 12 (doze) horas.

3.4.3.5. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido da solicitação de sua revogação e a emissão da LCR correspondente, na forma do item 2.3.2.

3.4.4. Prazo para solicitação de revogação

3.4.4.1. A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 3.4.1 desta DPC.

3.4.5. Frequência de emissão de LCR

3.4.5.1. Neste item é definida a frequência para a emissão de LCR referente a certificados de AC de nível imediatamente subsequente a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

3.4.5.2. A frequência máxima admitida para a emissão de LCR referente a certificados de AC Subsequente é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, é emitida nova LCR no prazo previsto no item 3.4.3 e notificada a todas as AC de nível imediatamente subsequente ao seu.

3.4.6. Requisitos para verificação de LCR

3.4.6.1. A verificação da validade do certificado na respectiva LCR é obrigatória, antes do mesmo ser utilizado.

3.4.6.2. Também é obrigatória a verificação da autenticidade da LCR, por meio das verificações da assinatura da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e do período de validade da LCR.

3.4.7. Requisitos especiais para o caso de comprometimento de chave

3.4.7.1. O titular de certificado deve notificar imediatamente, à AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 3.4.3;

3.4.7.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada, de acordo com o previsto na legislação vigente;

3.4.7.3. Todos os documentos e relatórios relativos são arquivados após a conclusão deste processo.

3.5. Procedimentos de Auditoria de Segurança

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO com o objetivo de manter um ambiente seguro.

3.5.1. Tipos de eventos registrados

3.5.1.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) Iniciação e desligamento do sistema de certificação;

b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

c) Mudanças na configuração dos sistemas AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO ou nas suas chaves;

d) Mudanças nas políticas de criação de certificados;

e) Tentativas de acesso (login) e de saída do sistema (logoff);

f) Tentativas não-autorizadas de acesso aos arquivos do sistema;

g) Geração de chaves próprias da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO ou de chaves das AC Subsequentes;

h) Emissão e revogação de certificados;

i) Geração de LCR;

j) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;

k) Operações de falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e

l) Operações de escrita nesse repositório, quando aplicável.

3.5.1.2. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO também registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

m) Registros de acessos físicos;

n) Manutenção e mudanças na configuração de seus sistemas;

o) Mudanças de pessoal e perfis qualificados;

p) Relatórios de discrepância e comprometimento; e

q) Registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

3.5.1.3. Os registros de auditoria, eletrônicos ou manuais, contêm a data e a hora do evento registrado e a identidade do agente que o causou;

3.5.1.4. A documentação relacionada aos serviços da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é armazenada, eletrônica ou manualmente, em local único, de forma estruturada para facilitar o acesso e consulta nos processos de auditoria;

3.5.1.5. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO define, em documento disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados e do termo de titularidade.

3.5.2. Frequência de auditoria de registros (logs)

3.5.2.1. A periodicidade com que os registros de auditoria da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são analisados pelo pessoal operacional é de uma semana;

3.5.2.2. 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.

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

3.5.3.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses e, subsequentemente, armazena-os da maneira descrita no item 3.6.

3.5.4. Proteção de registro (log) de auditoria

3.5.4.1. 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;

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

3.5.4.3. 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;

3.5.5. Sistema de coleta de dados de auditoria

3.5.5.1. O sistema de coleta de dados de auditoria interna à AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

3.5.6. Notificação de agentes causadores de eventos

3.5.6.1. Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

3.5.7. Avaliações de vulnerabilidade

3.5.7.1. Os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e registradas para fins de auditoria.

3.6. Arquivamento de Registros

3.6.1. Tipos de registros arquivados

a) Solicitações de certificados;

b) Solicitações e justificativas de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR;

f) Trocas de chaves criptográficas da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO; e

g) Informações de auditoria previstas no item 3.5.1.

3.6.2. Período de retenção para arquivo

a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;

b) As cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado. O prazo de retenção já em curso, quando da alteração desta alínea, será reiniciado; e

c) As demais informações, inclusive os arquivos de auditoria, deverão ser retidas por, no mínimo, 6 (seis) anos.

3.6.3. Proteção de arquivo

3.6.3.1. Todos os registros são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA.

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

3.6.4.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

3.6.4.3. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

3.6.5. Requisitos para datação (time-stamping) de registros

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

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

3.6.6. Sistema de coleta de dados de arquivo

3.6.6.1. Todos os sistemas de coleta de dados de arquivo utilizados pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO em seus procedimentos operacionais são automatizados, manuais e internos.

3.6.7. Procedimentos para obter e verificar informação de arquivo

3.6.7.1. A verificação de informação de arquivo deve ser solicitada formalmente à AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

3.7. Troca de chave

3.7.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO fornece novo certificado a AC Subsequente utilizando o mesmo procedimento utilizado para emissão do certificado inicial ou permite a renovação do certificado já existente, precisando este estar válido. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO publica em sua página web informações sobre a renovação do certificado.

3.8. Comprometimento e Recuperação de Desastre

3.8.2. Recursos computacionais, *software*, e dados corrompidos

3.8.2.1. Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, 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.

3.8.3. Certificado de entidade é revogado

3.8.3.1. Em caso de revogação do certificado da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, o Gerente de Segurança, juntamente com o Gerente de Criptografia da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

3.8.4. Chave da entidade é comprometida

3.8.4.1. Em caso de suspeita de comprometimento de chave da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com o Gerente de Criptografia da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, que decretam o início da fase de resposta e seguem um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

a) Todos os certificados afetados serão revogados e as partes serão notificadas através da página web da SEFAZ;

b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO estiver encerrando suas atividades.

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

3.8.5.1. Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, o Departamento de Infraestrutura, responsável pela contingência, notifica o Gerente de Segurança 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 da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

b) Monitorar e controlar o foco da contingência;

c) Minimizar os danos aos ativos de processamento do Órgão, de forma a evitar a descontinuidade dos serviços.

3.9. Extinção dos serviços de AC ou PSS

3.9.1. No caso de encerramento das atividades, a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO segue os requisitos e procedimentos descritos no documento Plano de Encerramento. Esse plano tem abordagem multidisciplinar envolvendo aspectos de varias áreas do Órgão, como jurídico, comercial, técnicos/tecnológicos, entre outros. De acordo com esse plano a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO:

a) Comunicará publicamente a extinção dos serviços da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, através do Diário Oficial;

b) Revogará todos os certificados gerados pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO nos prazos estipulados nesta DPC após a publicação e comunicará as partes afetadas através de mensagem eletrônica;

c) Extinguirá os serviços de emissão de certificados;

d) Extinguirá os serviços de revogação, como emissão da LCR e/ou conservação dos serviços de status on-line após a revogação completa de todos os certificados;

e) Destruirá a chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO extinta seguindo o procedimento descrito na DPC Item 5.2.8.

f) Poderá transferir os dados e gravações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO para a Autoridade Certificadora sucessora, aprovada pela AC Raiz. O período no qual os mesmos ficarão armazenados está descrito na DPC item 3.6.

g) Poderá transferir as chaves públicas dos certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO para serem armazenadas por outra AC aprovada pela AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO. Caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à Imprensa Oficial do Estado de São Paulo.

h) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

i) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

3.9.2. Em caso de falência ou extinção da AC, a documentação e registros relativos à emissão de certificados deverá ser entregue para guarda da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

3.9.3. No caso de encerramento das atividades como PSS vinculada a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, diretamente, deverá seguir os seguintes requisitos e procedimentos:

a) Publicará, em sua página web, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso;
b) Manterá a guarda de toda a documentação comprobatória em seu poder.

4. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

4.1. Controles Físicos

4.1.1. Construção e localização das instalações

4.1.1.1. A localização e o sistema de certificação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não existem ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos;

4.1.1.2. As 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;

4.1.1.3. As instalações para sistemas de telecomunicações, subestações e retificadores ficam em ambiente seguro com entrada e saída controlada;

4.1.1.4. Existem sistemas de aterramento e de proteção contra descargas atmosféricas;

4.1.1.5. Existe iluminação de emergência em todos os ambientes de nível 4, além das áreas cobertas por câmeras de monitoramento.

4.1.2. Acesso físico nas instalações de AC

A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO possui sistema de controle de acesso físico que garante a segurança de suas instalações;

4.1.2.1 Níveis de acesso

4.1.2.1.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO possui 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 2 (dois) níveis de proteção da chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

4.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO. 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 da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO transitam devidamente identificadas e acompanhadas;

Nenhum tipo de processo operacional ou administrativo da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é executado nesse nível.

4.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO 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;

4.1.2.1.4. 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 da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá;

4.1.2.1.5. O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

Qualquer atividade relativa ao ciclo de vida dos certificados digitais é executada a partir desse nível.

Pessoas não envolvidas com essas atividades 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;

4.1.2.1.6. 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;

4.1.2.1.7. Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, não são admitidos a partir do nível 3;

4.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO tais como emissão e revogação de certificados e emissão de LCR. 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;

4.1.2.1.9. No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto. As paredes, piso e o teto, são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gazes 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;

4.1.2.1.10. As salas-cofre foram construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas foram sanadas por normas internacionais pertinentes;

4.1.2.1.11. Na AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, existem ambientes de quarto nível para abrigar e segregar:

a) Equipamentos de produção on-line, gabinete reforçado de armazenamento e equipamentos de rede e infra-estrutura - firewall, roteadores, switches e servidores - (Datacenter);
b) Equipamentos de produção off-line e cofre de armazenamento (Sala de cerimônia);

4.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre interior à sala de cerimônia e um gabinete reforçado trancado no Datacenter. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior;

4.1.2.1.13. 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.

4.1.2.1.14. O sexto nível (nível 6) constitui-se de pequenos depósitos localizados no interior do cofre da sala de cerimônia (Nível 5). Cada um desses depósitos dispõe de 2 fechaduras, sendo uma individual e a outra comum a todos os depósitos. Os dados de ativação da chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são armazenados nesses depósitos.

4.1.2.2 Sistemas físicos de detecção

4.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7;

4.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) trimestralmente, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível;

4.1.2.2.3. 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;

4.1.2.2.4. 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;

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

4.1.2.2.6. 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.

4.1.2.3 Sistema de controle de acesso

O sistema de controle de acesso está baseado em um ambiente de nível 4.

4.1.2.4 Mecanismos de emergência

4.1.2.4.1. Mecanismos específicos são implantados pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO 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;

4.1.2.4.2. Todos os procedimentos referentes aos mecanismos de emergência são documentados. Os mecanismos e procedimentos de emergência são verificados, semestralmente, por meio de simulação de situações de emergência.

4.1.3. Energia e ar condicionado nas instalações de AC

4.1.3.1. A infra-estrutura do ambiente de certificação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO está 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 da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

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

4.1.3.3. 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;

4.1.3.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, a cada 6 meses, na busca de evidências de violação ou de outras anormalidades;

4.1.3.5. São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela Política de Segurança. Qualquer modificação nessa rede é previamente documentada;

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

4.1.3.7. 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;

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

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

4.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO 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.

4.1.4. Exposição à água nas instalações de AC

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

4.1.5. Prevenção e proteção contra incêndio nas instalações de AC

4.1.5.1. Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações;

4.1.5.2. Nas instalações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO não é permitido fumar ou portar objetos que produzam fogo ou faísca;

4.1.5.3. A sala-cofre de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre constituem eclusas, onde uma porta só abre quando a anterior estiver fechada;

4.1.5.4. Em caso de incêndio nas instalações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, a temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

4.1.6. Armazenamento de mídia nas instalações de AC

4.1.6.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO atende às normas NBR 11.515 e NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados “).

4.1.7. Destruição de lixo nas instalações de AC

4.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo;

4.1.7.2. Todos os dispositivos magnéticos não mais utilizáveis e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis são desmagnetizados com ferramentas específicas, e são fisicamente destruídos.

4.1.8. Instalações de segurança (*backup*) externas (*off-site*)

4.1.8.1. As instalações de backup atendem os requisitos mínimos estabelecidos por este documento. Sua localização é tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não serão atingidas e tornar-se-ão totalmente operacionais em, no máximo, 48 (quarenta e oito) horas.

4.2. Controles Procedimentais

4.2.1. Perfis qualificados

4.2.1.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO pratica uma política de segregação de funções, controlando e registrando o acesso físico e lógico às funções críticas do ciclo de vida dos certificados digitais, de forma a garantir a segurança da atividade de certificação e evitar a manipulação desautorizada do sistema. As ações permitidas são limitadas de acordo com o perfil de cada cargo.

4.2.1.2. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO estabelece 4 perfis distintos para sua operação, atribuídos às seguintes gerências:

- Gerência de Operações:

- Configuração e manutenção do hardware e do software da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
- Gerenciamento e controle da tecnologia empregada nos serviços de certificação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
- Controle de acesso dos funcionários à rede da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
- Gerenciamento dos operadores da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
- Controle de acesso ao sistema de certificação.

- Gerência de Segurança:

  - Implementação da Política de Segurança da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
  - Verificação dos registros de auditoria;
  - Supervisão do cumprimento das práticas e procedimentos determinados na Política de Segurança da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
  - Acompanhamento das auditorias de segurança realizadas por terceiros;
  - Verificação do cumprimento desta DPC;
  - Autorização e concessão de acesso às instalações físicas e autorização de acessos lógicos ao sistema de certificação;
  - Utilização de criptografia para a segurança da base de dados de registro de auditoria do sistema de certificação.

- Gerência de Criptografia:

  - Administração e controle dos componentes criptográficos da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
  - Verificação dos registros de acesso aos diferentes níveis de proteção das chaves privadas das AC (logs);
  - Elaboração das cerimônias de geração de chaves de AC;
  - Armazenamento dos registros de auditoria do sistema de certificação;
  - Utilização de criptografia para segurança de acesso ao aplicativo de certificação.

- Gerência de Validação:

  - Supervisão e controle dos processos de identificação dos solicitantes de certificados;
  - Gerenciamento dos certificados: emissão, expedição, distribuição, revogação de certificados.

4.2.1.3. Os operadores do sistema de certificação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO recebem treinamento específico antes de obter qualquer tipo de acesso ao sistema. O tipo e o nível de acesso estão

determinados, em documento formal (Política de Segurança da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO), com base nas necessidades de cada perfil;

4.2.1.4. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO 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 AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO no ato de seu desligamento.

4.2.2. Número de pessoas necessário por tarefa

4.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

4.2.2.2. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC podem ser executadas por um único empregado.

4.2.3. Identificação e autenticação para cada perfil

4.2.3.1. Todo empregado da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO tem sua identidade e perfil verificados antes de:

a) Ser incluído em uma lista de acesso às instalações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

b) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

c) Receber um certificado para executar suas atividades operacionais na AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO; e

d) Receber uma conta no sistema de certificação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

4.2.3.2. Os certificados, contas e senhas utilizados 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.

4.2.3.3. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO adota padrão de utilização de "senhas fortes", em conformidade com a Política de Segurança, juntamente com procedimentos de validação dessas senhas.

4.3. Controles de Pessoal

Todos os empregados da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e PSS vinculados encarregados de tarefas operacionais têm registrado em contrato ou termo de titularidade:

a) Os termos e as condições do perfil que ocupam;
b) O compromisso de observar as normas, políticas e regras aplicáveis;
c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

4.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme estabelecido na Política de Segurança.

4.3.2. Procedimentos de verificação de antecedentes

4.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido, pelo menos, 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.

4.3.3. Requisitos de treinamento

4.3.3.1. Todo o pessoal da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebem treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e mecanismos de segurança da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
b) Sistema de certificação em uso na AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

c) Procedimentos de recuperação de desastres e de continuidade do negócio;
d) Outros assuntos relativos a atividades sob sua responsabilidade.

4.3.4. Frequência e requisitos para reciclagem técnica

4.3.4.1. O pessoal da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre mudanças tecnológicas nos sistemas da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

4.3.5. Sanções para ações não autorizadas

4.3.5.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, o acesso dessa pessoa ao sistema de certificação é suspenso, é instaurado processo administrativo para apurar os fatos e, se for o caso, são tomadas as medidas administrativas legais cabíveis.

4.3.5.2. 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.

4.3.5.3. Concluído o processo administrativo, a AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO encaminha suas conclusões à SEFAZ.

4.3.5.4. 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 AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

4.3.6. Requisitos para contratação de pessoal

4.3.6.1. Todo o pessoal da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO envolvido em atividades diretamente relacionadas com os

processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na Política de Segurança.

4.3.7. Documentação fornecida ao pessoal

4.3.7.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO disponibiliza para todo o seu pessoal:

a) A DPC da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
b) Documentação operacional relativa a suas atividades; e
c) Contratos, normas e políticas relevantes para suas atividades.

4.3.7.2. A documentação fornecida é classificada segundo a política de classificação de informação definida pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e é mantida atualizada.

5. CONTROLES TÉCNICOS DE SEGURANÇA

5.1. Geração e Instalação do Par de Chaves

5.1.1. Geração do par de chaves

5.1.1.1. O par de chaves criptográficas da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é gerado pela própria AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

A geração do par de chaves de AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, treinados para a função.

A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é gerado em módulos criptográficos de hardware, com padrão de segurança FIPS 140-2 nível 3.

5.1.1.2. Pares de chaves das AC Subsequente são gerados somente pelas AC Subsequente, titulares do certificado correspondente, que indicarão, por seu(s) representante(s) legal(s), a pessoa responsável pela geração do par de chaves criptográficas.

A geração do par de chaves de AC Subsequente é realizada em processo verificável, obrigatoriamente na presença de funcionários de confiança da AC Subsequente treinados para a função. A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves das AC Subsequente é gerado e armazenado em módulo criptográfico de hardware, com padrão de segurança FIPS 140-2 nível 3.

5.1.2. Entrega da chave privada à entidade titular

5.1.2.1. A geração e a guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

5.1.3. Entrega da chave pública para emissor de certificado

5.1.3.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO entrega cópia de sua chave pública para a AC Raiz em formato PKCS #10. Essa entrega é feita por representante legal constituído da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, em cerimônia especifica, em data e hora previamente estabelecida;

5.1.3.2. A chave pública de uma AC Subsequente é entregue pelo representante legal da AC Subsequente, em cerimônia específica, em data e hora previamente estabelecidas pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

5.1.4. Disponibilização de chave pública da AC para usuários

5.1.4.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO disponibiliza o seu certificado e todos os certificados da cadeia de certificação para seus usuários, através de endereço Web: (http://acsat.imprensaoficial.com.br/repositorio).

5.1.5. Tamanhos de chave

5.1.5.1. O tamanho mínimo das chaves criptográficas associadas aos certificados de AC Subsequentes é de RSA 4096.

5.1.6. Geração de parâmetros de chaves assimétricas

5.1.6.1. Os parâmetros de geração de chaves assimétricas da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO adotam o padrão FIPS 140-2 nível 3.

5.1.7. Geração de chave por *hardware ou software*

5.1.7.1. As chaves da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão FIPS 140-2 nível 3;

5.1.7.2. As chaves criptográficas das AC Subsequentes são geradas, armazenadas e utilizadas dentro de hardware específico, compatível com os requisitos da norma FIPS 140-2 nível 3.

5.1.8. Propósitos de uso de chave (conforme o campo *"key usage"* na X.509 v3)

5.1.8.1. A chave privada das AC Subsequentes é utilizada apenas para a assinatura dos certificados por ela emitidos e para assinatura de sua LCR;

5.1.8.2. A chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

5.2. Proteção da Chave Privada

A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO implementa uma combinação de controles físicos, lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas.

A chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é armazenada de forma cifrada no mesmo componente seguro de *hardware* utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

Os titulares de certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado da suas chaves privadas.

5.2.1. Padrões para módulo criptográfico

5.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO adota o padrão FIPS (Federal Information Process ing Standards) 140-2, nível 3;

5.2.1.2. Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS 140-2 nível 3.

5.2.2. Controle “n de m” para chave privada

5.2.2.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO exige controle múltiplo para utilização da sua chave privada;

5.2.2.2. É necessária a presença de pelo menos 3 (três) de um grupo de 10 (dez) funcionários de confiança, com perfis qualificados para a utilização da chave privada da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

5.2.3. Recuperação (*escrow*) de chave privada

5.2.3.1. Não é permitida, a recuperação (escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

5.2.4. Cópia de segurança (*backup*) de chave privada

5.2.4.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO mantém cópia de segurança de sua chave privada;

5.2.4.2. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico e protegida com um nível de segurança não inferior àquele definido para a chave original.

5.2.5. Inserção de chave privada em módulo criptográfico

5.2.5.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

5.2.6. Método de ativação de chave privada

5.2.6.1. A ativação das chaves privadas das AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é coordenada pelo seu Gerente de Criptografia, onde 3 de um grupo de 10 funcionários com perfis qualificados da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, detentores de partição da chave de ativação do equipamento criptográfico (PIN), apresentam tais componentes em cerimônia específica;

5.2.6.2. Esses funcionários são identificados pelo crachá funcional emitido pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO contendo fotografia, nome, e departamento do funcionário.

5.2.7. Método de desativação de chave privada

A chave privativa da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, instalada em ambiente de produção dos sistemas de certificação, localiza-se em nível de segurança 4, onde só é permitido o acesso ao ambiente em duplas devidamente autorizadas pelo sistema de controle de acesso da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

Dentro deste ambiente, somente funcionários qualificados do departamento de operações têm acesso ao sistema de certificação de produção, onde são executados os comandos de desativação do sistema, após a sua devida identificação e autorização feita através de mecanismos nativos do sistema operacional.

Esses funcionários são identificados pelo crachá funcional emitido pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO contendo fotografia, nome e departamento do funcionário.

5.2.8. Método de destruição de chave privada

5.2.8.1. O Gerente de Criptografia da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, de posse da chave privada original e suas cópias de segurança a serem destruídas, acompanhado do Gerente de Segurança e do representante legal da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, titular do certificado, conduz cerimônia especifica, em ambiente de nível 4 de segurança, para reinicialização das mídias de armazenamento das chaves privadas, não deixando informações remanescente sensíveis nessas mídias.

5.2.8.2. Os Gerentes de Criptografia e Segurança são identificados pelo crachá funcional emitido pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO contendo fotografia, nome e departamento do funcionário. O representante legal da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é identificado através de cédula de identidade ou passaporte, se estrangeiro.

5.3. Outros Aspectos do Gerenciamento do Par de Chaves

5.3.1. Arquivamento de chave pública

5.3.1.1. As chaves públicas da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e dos titulares dos certificados de AC Subsequentes por ela emitidos, bem como as LCR emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

5.3.2. Períodos de uso para as chaves pública e privada

5.3.2.1. As chaves privadas dos titulares dos certificados de AC Subsequentes emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

5.3.2.2. O período máximo de validade admitido para o certificado desta AC é de 20 (vinte) anos e para os certificados das AC Subsequentes é de 10 (dez) anos.

5.4. Dados de Ativação

Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

5.4.1. Geração e instalação dos dados de ativação

5.4.1.1. Os dados de ativação do equipamento de criptografia que armazena as chaves privadas da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são únicos e aleatórios.

5.4.2. Proteção dos dados de ativação

5.4.2.1. A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO garante que os dados de ativação de sua chave privada são protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico;

5.4.2.2. Os dados de ativação da chave privada da entidade titular do certificado são protegidos contra o uso não autorizado.

5.5. Controles de Segurança Computacional

5.5.1. Requisitos técnicos específicos de segurança computacional

5.5.1.1. A geração do par de chaves da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO é realizada em ambiente próprio para a condução de Cerimônia de Geração de Chaves. O ambiente computacional é mantido off-line de modo a impedir o acesso remoto não-autorizado.

5.5.1.2. A geração dos pares de chaves das AC Subsequentes é realizada em ambiente próprio, protegido de modo a minimizar os riscos potenciais inerentes

desta operação. O ambiente computacional é mantido off-line para impedir o acesso remoto não-autorizado.

5.5.1.3. O ambiente computacional da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes funções:

a) Controle de acesso aos serviços e perfis da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
b) Separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
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 da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
e) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) Mecanismos para cópias de segurança (*backup*).

5.5.1.4. Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e mecanismos de segurança física;

5.5.1.5. As informações sensíveis contidas nos equipamentos são retiradas dos equipamentos para manutenção.

5.5.1.6. Os números de série dos equipamentos e as datas de envio e de recebimento da manutenção são controladas. Ao retornar às instalações da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, o equipamento que passou por manutenção é inspecionado. As informações sensíveis armazenadas, relativas à atividade da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, são destruídas de maneira definitiva nos equipamentos que deixam de ser utilizados em caráter permanente. Todos esses eventos são registrados para fins de auditoria.

5.5.1.7. Equipamentos utilizados pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são preparados e configurados como previsto na Política de Segurança da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO implementada ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade.

5.5.2. Classificação da segurança computacional

5.5.2.1. A segurança computacional da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO segue as recomendações Common Criteria.

5.6. Controles Técnicos do Ciclo de Vida

A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO não desenvolve sistemas com qualquer finalidade relacionada à operação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

5.6.1. Controles na Geração de LCR

5.6.1.1. Antes de publicadas, todas as LCR geradas pela AC são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação ao número da LCR, data/hora de emissão e outras informações relevantes.

5.7. Controles de Segurança de Rede

5.7.1. Diretrizes Gerais

5.7.1.1. Neste item são descritos os controles relativos à segurança da rede da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, incluindo firewalls e recursos similares.

5.7.1.2. Nos servidores do sistema de certificação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados;

5.7.1.3. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, switches, firewalls, e sistemas de detecção de intrusos (IDS), presentes no segmento de rede que hospeda o sistema de certificação estão localizados e operam em ambiente de nível 4;

5.7.1.4. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação;

5.7.1.5. 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.

5.7.2. Firewall

5.7.2.1. 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 AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

5.7.2.2. O software de firewall, entre outras características, implementa registros de auditoria.

5.7.3. Sistema de detecção de intrusão (IDS)

5.7.3.1. 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;

5.7.3.2. O sistema de detecção de intrusão reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com atualização da sua base de reconhecimento;

5.7.3.3. 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.

5.7.4. Registro de acessos não-autorizados à rede

5.7.4.1. 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. PERFIS DE CERTIFICADO E LCR

6.1. Diretrizes Gerais

6.1.1. Nos itens seguintes são descritos os aspectos dos certificados e LCR emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;

6.1.2. Nos itens seguintes também são especificados o formato dos certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

6.2. Perfil do Certificado

6.2.1. Todos os certificados e LCR emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8;

6.2.2. Número de versão

6.2.2.1. Todos os certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

6.2.3. Extensões de certificado

Os certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO possuem as seguintes extensões:

a) **Authority Key Identifier**, não crítica: o campo keyIdentifier contém o hash **SHA-1** da chave pública da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO;
b) **Subject Key Identifier**, não crítica: contém o *hash* **SHA-1** da chave pública da AC titular do certificado;
c) **Key Usage,** crítica: somente os bits keyCertSign e CRLSign estão ativados;;
d) **Certificate Policies**, não crítica:

d.1) o campo policyIdentifier contém:

i. o *Object Identifier* (OID) da PC da AC Subsequente.

d.2) o campo policyQualifiers contém o o endereço *Web* da DPC da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO http://acsat.imprensaoficial.com.br/repositorio/dpc/acraizsefazsp/dpc_acraizsefazsp.pdf

a) **basicConstraints, crítica**: contém o campo *cA=True*.

b) **CRL Distribution Points**, não crítica: contém o endereço Web onde se obtém a LCR da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO:

Para certificados emitidos a partir de 21/12/2012:

http://acsat.imprensaoficial.com.br/repositorio/dpc/acraizsefazsp/dpc_acraizsefazsp.pdf

6.2.4. Identificadores de algoritmo

Os certificados emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são assinados com o uso do algoritmo RSA com SHA-512 como função de hash (OID = 1.2.840.113549.1.1.13) conforme o padrão PKCS#1.

6.2.5. Formatos de nome

O nome do titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

O = Secretaria da Fazenda do Estado de Sao Paulo

CN = AC SAT SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO SP

6.2.6. Restrições de nome

6.2.6.1. Neste item são descritas as restrições aplicáveis para os nomes dos titulares de certificados.

6.2.6.2. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO são as seguintes:

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
"	22
#	23
'	27
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D

6.2.7. OID (Object Identifier) de DPC

O OID desta DPC é: 1.3.6.1.4.1.30253.2.

6.2.8. Sintaxe e semântica dos qualificadores de política

O campo **policyQualifiers** da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO http://acsat.imprensaoficial.com.br/repositorio/dpc/acraizsefazsp/dpc_acraizsefazsp.pdf

6.2.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

6.3. Perfil de LCR

6.3.1. Número(s) de versão

As LCR geradas pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

6.3.2. Extensões de LCR e de suas entradas

6.3.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO e sua criticidade.

6.3.2.2. As LCR da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO obedecem as seguintes extensões para certificados de AC:

a) **Authority Key Identifier**, contém o hash SHA-512 da chave pública da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO que assina a LCR.

b) **"CRL Number"**, não crítica: contém um número sequencial para cada LCR emitida pela AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO.

7. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

7.1. Políticas de publicação e notificação

A AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço *Web*:

(http://acsat.imprensaoficial.com.br/repositorio/dpc/acraizsefazsp/dpc_acraizsefazsp.pdf).

8. DOCUMENTOS REFERENCIADOS

8.1. Os documentos que regulamentam a criação e a operação da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO para atendimento ao SAT - Sistema Autenticador e Transmissor de Cupons Fiscais Eletrônicos (CF-e-SAT) da SEFAZ estão referenciados no site: http://www.fazenda.sp.gov.br/sat.