Declaração de Práticas de Certificação

da Autoridade Certificadora SAT SEFAZ SP

DPC DA AC SAT SEFAZ SP

Versão 1.1 – abril de 2015

ÍNDICE

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA SAT SEFAZ SP

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 SAT SEFAZ SP, na execução dos seus serviços de certificação digital.

1.1.2. 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 SAT SEFAZ SP ou entidades a ela vinculadas possa vir a adotar.

1.1.3. A AC SAT SEFAZ SP está certificada em nível imediatamente subsequente ao da AC RAIZ DA SECRETARIA DA FAZENDA DO ESTADO DE SAO PAULO. O certificado da AC SAT SEFAZ SP contém a chave pública correspondente à sua chave privada, utilizada para assinar os certificados de assinatura A3 e para assinar a sua Lista de Certificados Revogados (LCR).

1.1.4. Para regulamentar usos específicos dos certificados emitidos pela a AC SAT SEFAZ SP 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 SAT SEFAZ SP e referida como "DPC da AC SAT SEFAZ SP", cujo OID (*object identifier*) é 1.3.6.1.4.1.30253.3.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

Esta DPC refere-se à AC SAT SEFAZ SP.

1.3.1.1. A AC SAT SEFAZ SP mantém as informações acima sempre atualizadas.

1.3.2. Prestadores 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 SEFAZ SP http://acsat.imprensaoficial.com.br/repositorio.

1.3.3.2. PSS são entidades utilizadas pela AC 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

Apenas pessoas jurídicas podem ser titulares de certificados emitidos pela AC SAT SEFAZ SP.

1.3.4. Aplicabilidade

A AC SAT SEFAZ SP implementa as seguintes Políticas de Certificado Digital para Certificados de Assinatura Digital:

1.3.4.1. Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora SAT SEFAZ SP, PC A3 da AC SAT SEFAZ SP, OID 1.3.6.1.4.1.30253.3;

1.3.4.2. Na PC correspondente estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC SAT SEFAZ SP e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

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. Os requisitos específicos associados a essas obrigações estão detalhados nas PC implementadas pela AC SAT SEFAZ SP.

2.1.1. Obrigações da AC SAT SEFAZ SP

a) Operar de acordo com esta DPC e com as PC que implementa;

b) Gerar e gerenciar seus pares de chaves criptográficas;

c) Assegurar a proteção de suas chaves privadas;

d) Notificar a AC SEFAZ, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;

e) Notificar os usuários quando ocorrer suspeita de comprometimento da chave privada da AC SAT SEFAZ SP, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

f) Distribuir seu próprio certificado;

g) Emitir, expedir e distribuir os certificados de usuários finais;

h) Informar a emissão do certificado ao respectivo solicitante;

i) Revogar os certificados emitidos;

j) Emitir, gerenciar e publicar sua LCR e quando aplicável, disponibilizar consulta online de situação do certificado (OCSP Online Certificate Status Protocol);

k) Publicar em sua página web esta DPC da AC SAT SEFAZ SP e as PC que implementa;

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

m) Utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;

n) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pela legislação vigente;

o) Adotar as medidas de segurança e controle previstas nesta DPC da AC SAT SEFAZ SP, nas PC e Política de Segurança da AC SAT SEFAZ SP que implementar , envolvendo seus processos, procedimentos e atividades;

p) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da legislação vigente;

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

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

s) Informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos;

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

u) 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 na PC correspondente;

d) Conhecer os seus direitos e obrigações contemplados por esta DPC, pela PC correspondente e por outros documentos aplicáveis da legislação vigente;

e) Informar à AC SAT SEFAZ SP o comprometimento ou suspeita de comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;

f) Verificar, no momento da aceitação do certificado, a veracidade e exatidão das informações contidas no seu certificado e notificar a AC SAT SEFAZ SP, solicitando a imediata revogação do certificado que contiver inexatidões ou erros; e

g) Obedecer estritamente a esta DPC da AC SAT SEFAZ SP e às PC aplicáveis, bem como respeitar a legislação aplicável, incluindo as regras definidas pela legislação vigente.

Estas obrigações se aplicam ao responsável pelo uso do certificado.

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 na PC correspondente;

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

Um certificado emitido pela AC SAT SEFAZ SP é considerado válido quando:

a) Não constar da LCR da AC SAT SEFAZ SP;

b) Não estiver expirado; e

c) Sua validade puder ser verificada através de certificado válido da AC SAT SEFAZ SP.

2.1.3.3. O não exercício desse direito não afasta a responsabilidade da AC SAT SEFAZ SP e do titular do certificado.

2.1.4. Obrigações do Repositório

a) Disponibilizar, logo após a sua emissão, os certificados emitidos pela AC SAT SEFAZ SP 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 por força de contratação específica;

2.2. Responsabilidades

2.2.1. Responsabilidades da AC SAT SEFAZ SP

2.2.1.1. A AC SAT SEFAZ SP responde pelos danos a que der causa.

2.2.1.2. A AC SAT SEFAZ SP responde solidariamente pelos atos das entidades de sua cadeia de certificação: PSS.

2.3. Interpretação e Execução

2.3.1. Forma de interpretação e notificação

2.3.1.1. 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.

2.3.1.2. 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.

2.3.2. Procedimentos da solução de disputa

2.3.2.1. 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.

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

2.4. Tarifas de Serviço

2.4.1. Tarifas de emissão e renovação de certificados

Não serão cobradas tarifas para emissão e renovação de certificados.

2.5. Publicação e Repositório

2.5.1. Publicação de informação da AC SAT SEFAZ SP

2.6.1.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC SAT SEFAZ SP (http://acsat.imprensaoficial.com.br/repositorio), obedecendo as regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC SAT SEFAZ SP 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 SAT SEFAZ SP (http://acsat.imprensaoficial.com.br/repositorio):

a) Seus próprios certificados;

b) Suas LCRs;

c) Esta DPC;

d) As PC que implementa;

2.5.2. Frequência de publicação

Certificados são publicados imediatamente após sua emissão. A publicação da LCR se dá conforme o item 3.4.5 da PC correspondente. As versões ou alterações desta DPC e da PC são atualizadas no web site da AC SAT SEFAZ SP.

2.5.3. Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC SAT SEFAZ SP e à PC implementada.

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.

2.5.4. Repositórios

O repositório da AC SAT SEFAZ SP 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 SAT SEFAZ SP podem ser consultadas através do protocolo http.

Somente a AC SAT SEFAZ SP, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar as atualizações nas informações por ela publicadas no seu repositório.

2.6. Sigilo

2.6.1. Disposições gerais

2.6.1.1. AC SAT SEFAZ SP 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.

2.6.1.2. O titular ou responsável pelo uso dos certificados de assinatura digital e de sigilo emitidos pela AC SAT SEFAZ SP é responsável pela geração, manutenção e sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevida dessas chaves.

2.6.1.3. No intuito de preservar o sigilo da sua chave privada o titular pelo certificado deve tomar todas as medidas para a proteção da mesma.

O sigilo da chave privada do certificado é garantido através de senha de acesso à chave privada. Esta senha será definida pelo usuário no momento da instalação do certificado. A criação e utilização dessa senha para acesso à aplicação são de responsabilidade do usuário.

O Titular pelo Certificado deve observar procedimentos básicos de segurança, tais como:

1) Nunca fornecer a senha a terceiros;

2) Utilizar senha de, no mínimo, 8 caracteres;

3) Não utilizar senha fraca ou óbvia, conforme definido na Política de Segurança da AC SAT SEFAZ SP;

4) Montar senha com caracteres alfanuméricos;

5) Não compartilhar a senha.

2.6.2. Tipos de informações sigilosas

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

2.6.2.2. Nenhum documento, informação ou registro fornecido pelos titulares de certificado à AC SAT SEFAZ SP será divulgado.

2.6.3. Tipos de informações não-sigilosas

As informações consideradas não-sigilosas compreendem:

a) os certificados e a LCR emitidos pela AC SAT SEFAZ SP;

b) informações corporativas ou pessoais que constem no certificados ou em diretórios públicos;

c) a PC correspondente;

d) esta DPC;

e) versões públicas de Políticas de Segurança; e

f) Termo de Titularidade ou solicitação de emissão do certificado.

A AC SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

2.6.4. Divulgação de informação de revogação ou suspensão de certificado

2.7.4.1. Informações sobre revogação de certificados emitidos pela AC SAT SEFAZ SP são fornecidas em sua LCR.

2.7.4.2. A razão para a revogação de certificado é informada ao titular do certificado e será tornada pública, desde que autorizada a divulgação pelo mesmo.

2.6.5. Quebra de sigilo por motivos legais

2.7.5.1. A AC SAT SEFAZ SP fornecerá, mediante ordem judicial ou por determinação legal, documentos, informações ou registros sob sua guarda.

2.6.6. Informações a terceiros

2.7.6.1. Nenhum documento, informação ou registro sob a guarda da AC SAT SEFAZ SP é fornecido a qualquer pessoa, exceto quando a pessoa que requerer, através de instrumento devidamente constituído, estiver corretamente identificada e autorizada para fazê-lo.

2.6.7. 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 e identificações 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 do mesmo tipo ou superior emitido na ICP-Brasil;

b) Por solicitação escrita, com firma reconhecida.

Nenhuma liberação de informação é permitida sem autorização numa das formas acima, exceto nos casos do item 2.8.5.

2.7. Direitos de Propriedade Intelectual

A SEFAZ SP detém todos os direitos de propriedade intelectual sobre as idéias, 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.

Os Direitos de Propriedade terão proteção conforme a legislação aplicável.

2.8. Geração de novo par de chaves antes da expiração do atual

2.9.1. No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC SAT SEFAZ SP 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.

2.9. 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 nas PC implementadas.

2.10. Solicitação de Revogação

2.10.1. A solicitação de revogação de certificado é realizada através web site disponibilizado pela SEFAZ;

2.10.2. 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 O titular do certificado fará a solicitação do certificado através do equipamento SAT-CF-e de forma automatizada durante a inicialização do equipamento;

3.2. Emissão de Certificado

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

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

3.3. Aceitação de Certificado

3.3.1. Ao aceitar o certificado, o titular do certificado:

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

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 e do seu conteúdo é declarada, pelo titular do certificado, na primeira utilização da chave privada correspondente.

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 SAT SEFAZ SP;

d) No caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora;

e) No caso de mudança na razão ou denominação social do titular - equipamentos, aplicações e pessoas jurídicas;

f) No caso de extinção, dissolução ou transformação de equipamentos, aplicações e pessoas jurídicas; ou

3.4.1.3. A AC SAT SEFAZ SP revoga, no prazo definido no item 3.4.4, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas pela legislação.

3.4.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

a) Por solicitação do responsável pelo certificado;

b) Pela AC SAT SEFAZ SP;

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 SAT SEFAZ SP.

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 SAT SEFAZ SP;

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 e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC SAT SEFAZ SP.

3.4.3.3. O prazo máximo admitido para a conclusão do processo de revogação dos certificados emitidos pela AC SAT SEFAZ SP, após o recebimento da respectiva solicitação é de 12 (doze) horas.

3.4.3.4. A AC SAT SEFAZ SP 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 emitidos pela AC SAT SEFAZ SP.

3.4.5.2. A frequência para emissão da LCR é de 1 (uma) hora.

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 SAT SEFAZ SP e do período de validade da LCR.

3.4.7. Disponibilidade para revogação ou verificação de status on-line

3.4.7.1. A AC SAT SEFAZ SP suporta os processos de revogação de certificados de forma on-line quando aplicável;

3.4.7.2. A AC SAT SEFAZ SP, suporta verificação da situação de estado de certificados de forma on-line quando aplicável;

3.4.7.3. A verificação da situação de um certificado deverá ser feita diretamente na AC SAT SEFAZ SP, por meio do protocolo OCSP (On-line Certificate Status Protocol).

3.4.8. Requisitos especiais para o caso de comprometimento de chave

3.4.8.1. O titular de certificado deve notificar imediatamente, através de solicitação on-line de revogação de certificado, 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.

3.4.8.2. 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;

3.4.8.3. 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 SAT SEFAZ SP com o objetivo de manter um ambiente seguro.

3.5.1. Tipos de eventos registrados

3.5.1.1. A AC SAT SEFAZ SP 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 SAT SEFAZ SP;

c) Mudanças na configuração dos sistemas AC SAT SEFAZ SP 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 SAT SEFAZ SP ou de chaves de seus usuários finais;

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 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 SAT SEFAZ SP também registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

a) Registros de acessos físicos;

b) Manutenção e mudanças na configuração de seus sistemas;

c) Mudanças de pessoal e perfis qualificados;

d) Relatórios de discrepância e comprometimento; e

e) 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 SAT SEFAZ SP 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 SAT SEFAZ SP define, em documento disponível nas auditorias de conformidade, as informações para identificação registradas 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 SAT SEFAZ SP 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 SAT SEFAZ SP mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) anos 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;

3.5.4.4. Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela AC SAT SEFAZ SP têm cópias de segurança periódicas, feitas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas. Estas cópias são enviadas ao departamento de segurança.

3.5.5. Sistema de coleta de dados de auditoria

3.5.5.1. O sistema de coleta de dados de auditoria interno à AC SAT SEFAZ SP 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 SAT SEFAZ SP, 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 SAT SEFAZ SP, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC SAT SEFAZ SP 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 SAT SEFAZ SP; 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) 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.

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

3.6.4.1. A AC SAT SEFAZ SP estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC SAT SEFAZ SP, 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 SAT SEFAZ SP 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 SAT SEFAZ SP em seus procedimentos operacionais são automatizados e 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 SAT SEFAZ SP, 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 SEFAZ iniciará o processo de renovação do certificado quanto tiver transcorrido, no mínimo, 85% (oitenta e cinco porcento) do tempo de sua vida útil.

3.8. Comprometimento e Recuperação de Desastre

3.8.1. A AC SAT SEFAZ SP possui um Plano de Continuidade de Negócios testado anualmente para garantir a continuidade de seus serviços críticos.

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 SAT SEFAZ SP, 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 SAT SEFAZ SP o Gerente de Segurança, juntamente com o Gerente de Criptografia da AC SAT SEFAZ SP, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados. A AC SAT SEFAZ SP emitirá certificados em substituição aos revogados com data de expiração coincidente ou superior 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 SAT SEFAZ SP, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com o Gerente de Criptografia da AC SAT SEFAZ SP, 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;

b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a AC SAT SEFAZ SP 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 Infra-estrutura, 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 SAT SEFAZ SP;

b) Monitorar e controlar o foco da contingência;

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

3.9. Extinção dos serviços de AC ou PSS

3.9.1. No caso de encerramento das atividades como AC, a AC SAT SEFAZ SP 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 SAT SEFAZ SP:

a) Comunicará publicamente a extinção dos serviços da AC SAT SEFAZ SP, através do Diário Oficial;

b) Revogará todos os certificados gerados pela AC SAT SEFAZ SP nos prazos estipulados nas PC implementadas 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 SAT SEFAZ SP extinta seguindo o procedimento descrito na DPC Item 5.2.8;

f) Transferirá os dados e gravações da AC SAT SEFAZ SP 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) Transferirá as chaves públicas dos certificados emitidos pela AC SAT SEFAZ SP 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 SAT SEFAZ SP. 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 SAT SEFAZ SP;

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

3.9.2. No caso de encerramento das atividades como PSS vinculada a AC SAT SEFAZ SP a AC SAT SEFAZ SP, 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 SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP possui 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 2 (dois) níveis de proteção da chave privada da AC SAT SEFAZ SP;

4.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC SAT SEFAZ SP. 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 SAT SEFAZ SP transitam devidamente identificadas e acompanhadas.

Nenhum tipo de processo operacional ou administrativo da AC SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP. 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 SAT SEFAZ SP;

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 SAT SEFAZ SP, 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 SAT SEFAZ SP tais como emissão e revogação de certificados e emissão de LCR e a disponibilidade à resposta a consulta OCSP. 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 SAT SEFAZ SP, 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 - (Data Center);

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 Data Center. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superio;.

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 SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC SAT SEFAZ SP;

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 baseados na Política de Segurança da ICP-Brasil. 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 condicionando 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 SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP, 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 SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP estabelece 4 perfis distintos para sua operação, atribuídos às seguintes gerências:

- Gerência de Operações:

- Configuração e manutenção do hardware e do software da AC SAT SEFAZ SP;
- Gerenciamento e controle da tecnologia empregada nos serviços de certificação da AC SAT SEFAZ SP;
- Controle de acesso dos funcionários à rede AC SAT SEFAZ SP;
- Gerenciamento dos operadores da AC SAT SEFAZ SP;
- Controle de acesso ao sistema de certificação.

- Gerência de Segurança:

- Implementação da Política de Segurança da AC SAT SEFAZ SP;
- Verificação dos registros de auditoria;
- Supervisão do cumprimento das práticas e procedimentos determinados na Política de Segurança da AC SAT SEFAZ SP;
- 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 SAT SEFAZ SP;
- 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 SAT SEFAZ SP 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 SAT SEFAZ SP), com base nas necessidades de cada perfil;

4.2.1.4. A AC SAT SEFAZ SP 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 SAT SEFAZ SP 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 SAT SEFAZ SP;

4.2.2.2. Todas as tarefas executadas no ambiente onde esta localizado o equipamento de certificação da AC SAT SEFAZ SP 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 SAT SEFAZ SP tem sua identidade e perfil verificados antes de:

a) Ser incluído em uma lista de acesso às instalações da AC SAT SEFAZ SP;

b) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC SAT SEFAZ SP;

c) Receber um certificado para executar suas atividades operacionais na AC SAT SEFAZ SP; e

d) Receber uma conta no sistema de certificação da AC SAT SEFAZ SP.

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 SAT SEFAZ SP adota padrão de utilização de "senhas fortes", em conformidade com a Política de Segurança da AC SAT SEFAZ SP, juntamente com procedimentos de validação dessas senhas.

4.3. Controles de Pessoal

Todos os empregados da AC SAT SEFAZ SP 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

4.3.1.1. Todo o pessoal da AC SAT SEFAZ SP envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme baseado na Política de Segurança da AC SAT SEFAZ SP.

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 SAT SEFAZ SP 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

Todo o pessoal da AC SAT SEFAZ SP 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 SAT SEFAZ SP;
b) Sistema de certificação em uso na AC SAT SEFAZ SP;
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 SAT SEFAZ SP 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 SAT SEFAZ SP.

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 SAT SEFAZ SP, 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 SAT SEFAZ SP encaminha suas conclusões à AC Raiz.

4.3.6. Requisitos para contratação de pessoal

4.3.6.1. Todo o pessoal da AC SAT SEFAZ SP envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme estabelecido na Política de Segurança da AC SAT SEFAZ SP.

4.3.7. Documentação fornecida ao pessoal

4.3.7.1. A AC SAT SEFAZ SP disponibiliza para todo o seu pessoal:

a) A DPC da AC SAT SEFAZ SP;
b) A PC correspondente;
c) Documentação operacional relativa a suas atividades; e
d) 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 SAT SEFAZ SP 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 SAT SEFAZ SP é gerado pela própria AC SAT SEFAZ SP.

A geração do par de chaves de AC SAT SEFAZ SP é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC SAT SEFAZ SP, treinados para a função.

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

O par de chaves da AC SAT SEFAZ SP é gerado em módulos criptográficos de hardware com padrão de segurança FIPS 140-2 nível 3.

Somente os titulares dos certificados emitidos pela AC SAT SEFAZ SP geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC SAT SEFAZ SP.

5.1.1.2. Cada PC implementada pela AC SAT SEFAZ SP define o meio utilizado para armazenamento da chave privativa.

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 SAT SEFAZ SP entrega cópia de sua chave pública para a AC Raiz em formato PKCS #10. Essa entrega é feita por representante legal constituído da AC SAT SEFAZ SP, em cerimônia especifica, em data e hora previamente estabelecida;

5.1.3.2. Os usuários finais enviam suas chaves públicas a AC SAT SEFAZ SP por meio eletrônico em formato PKCS#10, através de uma sessão segura fixada pelo Secure Socket Layer (SSL).

Os procedimentos específicos aplicáveis estão detalhados nas PCs implementadas.

5.1.4. Disponibilização de chave pública da AC para usuários

A AC SAT SEFAZ SP disponibiliza o seu certificado e todos os certificados da cadeia de certificação para os usuários, através 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 bits.

5.1.6. Geração de parâmetros de chaves assimétricas

5.1.6.1. Os parâmetros de geração de chaves assimétricas da AC SAT SEFAZ SP 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 SAT SEFAZ SP 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. Cada PC implementada pela AC SAT SEFAZ SP caracteriza o processo utilizado para a geração de chaves criptográficas privativas dos titulares dos certificados, com base nos requisitos aplicáveis estabelecidos pela legislação em vigor.

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

5.1.8.1. Os certificados de assinatura emitidos pela AC SAT SEFAZ SP têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment;

5.1.8.1.2. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC SAT SEFAZ SP, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC que implementa.

5.1.8.3. A chave privada da AC SAT SEFAZ SP é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

5.2. Proteção da Chave Privada

A AC SAT SEFAZ SP implementa uma combinação de controles físicos , lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas.

A chave privada da AC SAT SEFAZ SP 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 SAT SEFAZ SP, 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 SAT SEFAZ SP adota o padrão FIPS 140-1 nível 2 (para a cadeia de certificação V0); ou FIPS 140-2 nível 2 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para as cadeias de certificação V2 e V3);

5.2.2. Controle “n de m” para chave privada

5.2.2.1. A AC SAT SEFAZ SP 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 SAT SEFAZ SP.

5.2.3. Recuperação (*escrow*) de chave privada

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 SAT SEFAZ SP mantém cópia de segurança de sua chave privada;

5.2.4.2. A AC SAT SEFAZ SP não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido;

5.2.4.3. 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. Arquivamento de chave privada

5.2.5.1. As chaves privadas de sigilo são arquivadas com um nível de segurança não inferior àquele definido para a chave original. Não são arquivadas chaves privadas de assinatura digital.

5.2.5.2. Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

5.2.6. Inserção de chave privada em módulo criptográfico

5.2.6.1. A AC SAT SEFAZ SP gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

5.2.7. Método de ativação de chave privada

5.2.7.1. A ativação das chaves privadas das AC SAT SEFAZ SP é coordenada pelo seu Gerente de Criptografia, onde 3 de um grupo de 10 funcionários com perfis qualificados da AC SAT SEFAZ SP, detentores de partição da chave de ativação do equipamento criptográfico (PIN), apresentam tais componentes em cerimônia específica;

5.2.7.2. Esses funcionários são identificados pelo crachá funcional emitido pela AC SAT SEFAZ SP contendo fotografia, nome, e departamento do funcionário;

5.2.7.3. Cada PC implementada descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

5.2.8. Método de desativação de chave privada

5.2.8.1. A chave privativa da AC SAT SEFAZ SP, 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 SAT SEFAZ SP.

5.2.8.2. 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.

5.2.8.3. Esses funcionários são identificados pelo crachá funcional emitido pela AC SAT SEFAZ SP contendo fotografia, nome, e departamento do funcionário.

5.2.8.4. Cada PC implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

5.2.9. Método de destruição de chave privada

5.2.9.1. O Gerente de Criptografia da AC SAT SEFAZ SP, 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 SAT SEFAZ SP, 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.

5.2.9.2. Os Gerentes de Criptografia e Segurança são identificados pelo crachá funcional emitido pela AC SAT SEFAZ SP contendo fotografia, nome, e departamento do funcionário. O representante legal da AC SAT SEFAZ SP é identificado através de cédula de identidade ou passaporte, se estrangeiro.

5.2.9.3. Cada PC implementada descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

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 SAT SEFAZ SP e dos titulares dos certificados de assinatura digital 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 assinatura digital emitidos pela AC SAT SEFAZ SP 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. Os períodos de uso das chaves correspondentes aos certificados de sigilo emitidos pela AC SAT SEFAZ SP são definidos nas respectivas PCs.

5.3.2.4. O período máximo de validade admitido para certificados da AC SAT SEFAZ SP 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. Cada PC implementada descreve os requisitos específicos aplicáveis.

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 SAT SEFAZ SP são únicos e aleatórios;

5.4.1.2. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

5.4.2. Proteção dos dados de ativação

5.4.2.1. A AC SAT SEFAZ SP 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. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, 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 SAT SEFAZ SP 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. Os requisitos de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC SAT SEFAZ SP são descritos em cada PC implementada;

5.5.1.3. O ambiente computacional da AC SAT SEFAZ SP 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 SAT SEFAZ SP;
b) Separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC SAT SEFAZ SP;
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 SAT SEFAZ SP;
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 SAT SEFAZ SP, o equipamento que passou por manutenção é inspecionado. As informações sensíveis armazenadas, relativas à atividade da AC SAT SEFAZ SP, 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 SAT SEFAZ SP são preparados e configurados como previsto na Política de Segurança da AC SAT SEFAZ SP implementada ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade;

5.5.2. Classificação da segurança computacional

A segurança computacional da AC SAT SEFAZ SP segue as recomendações Common Criteria.

5.6. Controles Técnicos do Ciclo de Vida

A AC SAT SEFAZ SP desenvolve sistemas apenas com finalidade relacionada à operação dos certificados de usuário final.

5.6.1. Controles de desenvolvimento de sistema

5.6.1.1. A AC SAT SEFAZ SP utiliza um modelo clássico espiral no desenvolvimento dos sistemas. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC SAT SEFAZ SP utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos informais;

5.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC SAT SEFAZ SP fornecem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC SAT SEFAZ SP.

5.6.2. Controles de gerenciamento de segurança

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

5.6.2.2. A AC SAT SEFAZ SP utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

5.6.3. Controles na Geração de LCR

5.6.3.1. 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 a 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 SAT SEFAZ SP, incluindo firewalls e recursos similares;

5.7.1.2. Nos servidores do sistema de certificação da AC SAT SEFAZ SP, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados;

5.7.1.3. Todos os servidores e elementos de infra-estrutura 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 infra-estrutura 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 SAT SEFAZ SP.

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 seguintes itens desta DPC são descritos os aspectos dos certificados e LCR emitidos pela AC SAT SEFAZ SP.

6.1.2. A seguinte PC:

PC A3 da AC SAT SEFAZ SP, OID 1.3.6.1.4.1.30253.3;

Implementada pela AC SAT SEFAZ SP especifica o formato dos certificados gerados e das correspondentes LCR. Nessas PCs são incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

6.2. Perfil do Certificado

Os certificados emitidos pela AC SAT SEFAZ SP estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

6.2.1. Número de versão

6.2.1.1. Todos os certificados emitidos pela AC SAT SEFAZ SP implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

6.2.2. OID (Object Identifier) de DPC

6.2.2.1. O OID desta DPC é 1.3.6.1.4.1.30253.3.

6.3. Perfil de LCR

6.3.1. Número(s) de versão

As LCR geradas pela AC SAT SEFAZ SP 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 SAT SEFAZ SP e sua criticidade;

6.3.2.2. As LCR da AC SAT SEFAZ SP obedecem as seguintes extensões para certificados de AC:

a) **Authority Key Identifier**, contém o hash SHA-512 da chave pública da AC SEFAZ SP que assina a LCR;

b) **"CRL Number"**, não crítica: contém um número sequencial para cada LCR emitida pela AC SAT SEFAZ SP.

7. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

7.1. Procedimentos de mudança de especificação

Alterações nesta DPC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC SAT SEFAZ SP.

Esta DPC é atualizada sempre que uma nova PC implementada pela AC SAT SEFAZ SP o exigir.

7.2. Políticas de publicação e notificação

A AC SAT SEFAZ SP 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.

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.