Declaração de Práticas de Certificação da Autoridade Certificadora Imprensa Oficial SP

DPC DA AC Imprensa Oficial SP

Versão 6.0 - 24 de Julho de 2014

ÍNDICE

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA IMPRENSA OFICIAL 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 Imprensa Oficial SP na Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) 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 Imprensa Oficial SP ou entidades a ela vinculadas possa vir a adotar.

1.1.3. A AC Imprensa Oficial SP está certificada em nível imediatamente subseqüente ao da AC Raiz da ICP-Brasil. O seu certificado contém a chave pública correspondente à chave privada da AC Imprensa Oficial SP utilizada para assinar os certificados de AC de nível imediatamente subseqüente (AC Subseqüente) ao seu e à sua LCR (Lista de Certificados Revogados).

1.1.4. O certificado da AC Imprensa Oficial SP é usado na emissão de certificados digitais de AC Subseqüentes, com o objetivo de identificar as AC de nível imediatamente subseqüente ao seu, referidas neste documento como AC Subseqüentes. Para regulamentar usos específicos dos certificados emitidos pela a AC Imprensa Oficial SP são publicadas Políticas de Certificado disponíveis em página web (http://icp-brasil.certisign.com.br/repositorio/ac-imesp-1n/index.htm).

1.2. Identificação

Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora Imprensa Oficial SP e referida como "DPC da AC Imprensa Oficial SP ", cujo OID (*object identifier*) é 2.16.76.1.1.26.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

Esta DPC refere-se à AC Imprensa Oficial SP no âmbito da ICP-Brasil.

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pelas ACs subsequentes a AC Imprensa Oficial SP para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais de AC Subseqüentes e identificação das organizações solicitantes, são publicados em serviço de diretório e/ou em página web da prestadora de serviço e suporte (http://icp-brasil.certisign.com.br/repositorio):

a) relação de todas as ARs credenciadas;

b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;

c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;

d) relação de AR que tenham se descredenciado da cadeia da AC Imprensa Oficial SP, com respectiva data do descredenciamento;

e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;

f) acordos operacionais celebrados pelas ARs vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC Imprensa Oficial SP mantém as informações acima sempre atualizadas.

1.3.3. Prestador de Serviço de Suporte

1.3.3.1. A relação de todos os Prestadores de Serviço de Suporte – PSS vinculados diretamente a AC Imprensa Oficial SP e/ou por intermédio de suas ARs é publicada em serviço de diretório e/ou em página web da AC Imprensa Oficial SP (http://icp-brasil.certisign.com.br/repositorio/ac-imesp-1n/index.htm).

1.3.3.2. PSS são entidades utilizadas pela AC e/ou suas AR para desempenhar atividade descrita nesta DPC 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.

1.3.3.3. A AC Imprensa Oficial SP mantém as informações acima sempre atualizadas.

1.3.4. Titulares de Certificado

Apenas pessoas jurídicas podem ser titulares de certificados de AC Subseqüente emitidos pela AC Imprensa Oficial SP.

1.3.5. Aplicabilidade

Os certificados emitidos pela AC Imprensa Oficial SP tem sua utilização exclusiva para assinatura de certificados digitais de AC de nível imediatamente subseqüente (AC Subseqüente) ao seu e de sua Lista de Certificados Revogados (LCR).

1.4. Dados de Contato

Nome: Imprensa Oficial do Estado SA IMESP

Endereço: Rua da Mooca, 1921 – Mooca – São Paulo, SP

Nome: João Paulo Foini

Telefone: (11) 2799-9800 / (11) 2799-9782
E-mail: certificacao@imprensaoficial.com.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 Imprensa Oficial SP

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 a AC Raiz, 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 Imprensa Oficial 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 AC de nível imediatamente subseqüente ao seu;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados emitidos;

j) emitir, gerenciar e publicar sua LCR;

k) publicar em sua página web esta DPC da AC Imprensa Oficial SP;

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

m) publicar em sua página web informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;

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

o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

p) adotar as medidas de segurança e controle previstas nesta DPC da AC Imprensa Oficial SP e Política de Segurança da AC Imprensa Oficial SP que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

s) manter e testar regularmente seu Plano de Continuidade do Negócio;

t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas AC de nível subseqüente ao seu;

u) informar à terceira parte e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC Imprensa Oficial SP;

v) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;

w) fiscalizar e auditorar as AR vinculadas e os prestadores de serviço que lhe sejam vinculados, em conformidade com as políticas, normas e procedimentos da ICP-Brasil; e

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

2.1.2. Obrigações das AR

a) receber solicitações de emissão ou de revogação de certificados;

b) confirmar a identidade do solicitante e a validade da solicitação;

c) encaminhar as solicitações de emissão ou de revogação de certificados à AC Imprensa Oficial SP;

d) informar os titulares de certificado a emissão ou a revogação de seus certificados;

e) disponibilizar os certificados emitidos pela AC Imprensa Oficial SP aos seus respectivos solicitantes;

f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP Brasil;

g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC Imprensa Oficial SP e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];

h) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP -Brasil;

i) manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;

j) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9, 3.1.10 e 3.1.11;

k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas; e

l) obedecer estritamente a esta DPC da AC Imprensa Oficial SP, bem como respeitar a legislação aplicável, incluindo as regras definidas pelo CG da ICP-Brasil.

2.1.3. 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 por outros documentos aplicáveis da ICP-Brasil;

e) informar à AC Imprensa Oficial 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 Imprensa Oficial SP, solicitando a imediata revogação do certificado que contiver inexatidões ou erros; e

g) obedecer estritamente a esta DPC da AC Imprensa Oficial SP, bem como respeitar a legislação aplicável, incluindo as regras definidas pelo CG da ICP-Brasil e as obrigações contratuais assumidas perante à AC Imprensa Oficial SP e AR.

Estas obrigações se aplicam ao responsável pelo uso do certificado.

2.1.4. Direitos da Terceira Parte (Relying Party)

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

2.1.4.2. 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 Imprensa Oficial SP é considerado válido quando:

a) não constar da LCR da AC Imprensa Oficial SP;

b) não estiver expirado; e

c) sua validade puder ser verificada através de certificado válido da AC Imprensa Oficial SP.

2.1.4.3. O não exercício desse direito não afasta a responsabilidade da AC Imprensa Oficial SP e do titular do certificado.

2.1.5. Obrigações do Repositório

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC Imprensa Oficial 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 aprovado pela ICP-Brasil, quando aplicável por força de contratação específica;

2.2. Responsabilidades

2.2.1. Responsabilidades da AC Imprensa Oficial SP

2.2.1.1. A AC Imprensa Oficial SP responde pelos danos a que der causa.

2.2.1.2. A AC Imprensa Oficial SP responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

2.2.2. Responsabilidades das AR

A AR é responsável pelos danos a que der causa.

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (Relying Party)

A terceira parte responde perante a AC Imprensa Oficial SP e ARs vinculadas apenas pelos prejuízos a que der causa com a prática de ato ilícito, nos termos da legislação vigente.

2.3.2. Relações Fiduciárias

A política de indenizações da AC Imprensa Oficial SP e de suas AR vinculadas, pelos danos a que, comprovadamente, derem causa , prevê o pagamento de indenização correspondente à 20 (vinte) vezes o valor do certificado, ou a R$ 40.000,00, o que for menor.

As indenizações da AC Imprensa Oficial SP e de suas AR vinculadas cobrem perdas e danos decorrentes de comprometimento da chave privada da AC Imprensa Oficial SP, de erro na identificação do titular, de emissão defeituosa do certificado ou de erros ou omissões da AC Imprensa Oficial SP ou das AR vinculadas.

2.3.3. Processos Administrativos

O titular do certificado que sofrer perdas e danos decorrentes do uso do certificado digital emitido pela AC Imprensa Oficial SP tem o direito de comunicar à AC Imprensa Oficial SP que deseja a indenização prevista no item 2.3.2 acima, observadas as seguintes condições:

a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC Imprensa Oficial SP, tal comprometimento deverá ter sido comprovado por perícia realizada por perito especializado e independente;
b) nos casos de erro na identificação, o titular do certificado não pode requerer qualquer indenização quando os dados constantes no certificado corresponderem aos dados fornecidos por esse titular à AC Imprensa Oficial SP ou à AR Imprensa Oficial SP;
c) nos casos de erro na transcrição, o titular do certificado não pode requerer qualquer indenização quando houver aceitado o certificado.

2.4. Interpretação e Execução

2.4.1. Legislação

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

2.4.2. Forma de interpretação e notificação

2.4.2.1. Na hipótese de uma ou mais disposições desta DPC ser, por qualquer razão, considerada inválida, ilegal, ou conflituosa com norma da ICP-Brasil, 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, o Grupo de Práticas e Políticas da AC Imprensa Oficial SP examinará a disposição inválida e proporá à nova redação ou retirada da disposição afetada, na forma do item 8 desta DPC.

2.4.2.2. As notificações ou qualquer outra comunicação necessária, relativas às práticas descritas nesta DPC, são feitas através de mensagem eletrônica assinada digitalmente, com chave pública certificada pela ICP-Brasil, ou por escrito e entregue à AC Imprensa Oficial SP.

2.4.2.3. A DPC da AC Imprensa Oficial SP na ICP-Brasil, não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3. Procedimentos da solução de disputa

2.4.3.1. Em caso de conflito entre esta DPC da AC Imprensa Oficial SP ou outros documentos que a AC Imprensa Oficial SP adotar, prevalece o disposto nesta DPC. O contrato para emissão de certificados poderá criar obrigações específicas, limitar o uso dos certificados ou restringir valores de transações comerciais, desde que respeitados os direitos previstos nesta DPC.

2.4.3.2. Esta DPC da AC Imprensa Oficial SP não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

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

2.5. Tarifas de Serviço

2.5.1. Tarifas de emissão e renovação de certificados

Variável conforme definição interna da Imprensa Oficial SP.

2.5.2. Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

2.5.3. Tarifas de revogação ou de acesso à informação de status

Variável conforme definição interna da Imprensa Oficial SP.

2.5.4. Tarifas para outros serviços

Variável conforme definição interna da Imprensa Oficial SP.

2.5.5. Política de reembolso

Variável conforme definição interna da Imprensa Oficial SP.

2.6. Publicação e Repositório

2.6.1. Publicação de informação da AC Imprensa Oficial SP

2.6.1.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC Imprensa Oficial SP (http://icp-brasil.certisign.com.br/repositorio/ac-imesp-1n/index.htm), obedecendo as regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC Imprensa Oficial 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 Imprensa Oficial SP (http://icp-brasil.certisign.com.br/repositorio/ac-imesp-1n/index.htm):

a) seus próprio certificado;

b) suas LCR;

c) esta DPC;

d) uma relação, regularmente atualizada, contendo as AR vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;

e) uma relação, regularmente atualizada, das AR vinculadas que tenham celebrado acordos operacionais com outras AR da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado; e

f) uma relação, regularmente atualizada, dos PSS vinculados.

2.6.2. Freqüência de publicação

Certificados são publicados imediatamente após sua emissão. A publicação da LCR se dá conforme o item 4.4.9 desta DPC. As versões ou alterações desta DPC, assim como os endereços das instalações técnicas das AR vinculadas, são atualizadas no web site da AC Imprensa Oficial SP após aprovação da AC Raiz da ICP-Brasil.

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 Imprensa Oficial SP e aos endereços das instalações técnicas das AR vinculadas.

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 Imprensa Oficial 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://icp-brasil.certisign.com.br/repositorio/ac-imesp-1n/index.htm).

As publicações da AC Imprensa Oficial SP podem ser consultadas através do protocolo http.

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

2.7. Fiscalização e Auditoria de Conformidade

2.7.1. As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPC, PC, Política de Segurança e demais normas e procedimentos estabelecidos pela ICP-Brasil.

2.7.2. As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

2.7.3. Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICPBRASIL [3].

2.7.4. A AC Imprensa Oficial SP recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICPBRASIL [3]. Esse documento trata do objetivo, freqüência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5. As entidades da ICP-Brasil diretamente vinculadas a AC Imprensa Oficial SP – AC, AR e PSS, também receberam auditoria prévia, para fins de credenciamento, e a AC Imprensa Oficial SP é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

2.8. Sigilo

2.8.1. Disposições gerais

2.8.1.1. AC Imprensa Oficial 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.

2.8.1.2. Não se aplica.

2.8.1.3. Não se aplica.

2.8.1.4. O responsável pelo uso do certificado de AC Subseqüente titular de certificado emitido pela AC Imprensa Oficial SP é responsável pela geração, utilização, manutenção e sigilo da chave privada correspondente a chave pública contida no certificado.

2.8.1.5. O Titular do certificado emitido pela AC Imprensa Oficial SP responderá pelo uso que o responsável fizer de sua chave privada, bem como pela divulgação ou utilização indevida dessa chave.

2.8.2. Tipos de informações sigilosas

2.8.2.1. Como princípio geral, todo documento, informação ou registro fornecido à AC ou às AR é sigiloso.

2.8.2.2. Nenhum documento, informação ou registro fornecido pelos titulares de certificado à AC Imprensa Oficial SP será divulgado.

2.8.3. Tipos de informações não-sigilosas

As informações consideradas não-sigilosas compreendem:

a) os certificados e a LCR emitidos pela AC Imprensa Oficial SP;
b) informações corporativas que constem nos certificados ou em diretórios públicos;
c) esta DPC;
d) versões públicas de Políticas de Segurança; e
e) resultados finais de auditorias.

A AC Imprensa Oficial SP e a AR a ela vinculada tratam 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 Imprensa Oficial SP ou da AR a ela vinculada 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 Imprensa Oficial SP ou a AR a ela vinculada 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 Imprensa Oficial SP e pela AR a ela vinculada, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

2.8.4. Divulgação de informação de revogação ou suspensão de certificado

2.8.4.1. Informações sobre revogação de certificados emitidos pela AC Imprensa Oficial SP são fornecidas em sua LCR.

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

2.8.4.3. A suspensão de certificados não é admitida na ICP-Brasil.

2.8.5. Quebra de sigilo por motivos legais

A AC Imprensa Oficial SP fornecerá, mediante ordem judicial ou por determinação legal, documentos, informações ou registros sob sua guarda.

2.8.6. Informações a terceiros

Nenhum documento, informação ou registro sob a guarda da AC Imprensa Oficial 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.

2.8.7. Divulgação por solicitação do Titular

2.8.7.1. 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.

2.8.7.2. 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.

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

2.8.8. Outras circunstâncias de divulgação de informação

Não se aplica.

2.9. Direitos de Propriedade Intelectual

A Certisign Certificadora Digital S.A. ou sua licenciante VeriSign, Inc. 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 Imprensa Oficial SP nos termos dessa DPC.

Os Direitos de Propriedade terão proteção conforme a legislação aplicável.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Registro Inicial

3.1.1. Disposições Gerais

3.1.1.1. . Neste item e nos itens seguintes estão descritos em detalhes os requisitos e procedimentos utilizados pelas AR vinculadas a AC Imprensa Oficial SP para a realização dos seguintes processos:

a) Validação da solicitação de certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e 3.1.11:

i. confirmação da identidade de um individuo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados constam na documentação apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como responsável pelo uso do certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP-Brasil;

ii. confirmação da identidade de uma organização: comprovação de que os documentos apresentados referem se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;

iii. emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC;

iv. as etapas descritas acima podem ser realizadas por um ou mais agentes de validação.

b) Verificação da solicitação de certificado - confirmação da validação realizada,

observando que deve ser executada, obrigatoriamente:

i. por agente de registro distinto do que executou a etapa de validação;

ii. em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;

iii. somente após o recebimento, na instalação técnica da AR, de cópia dos da documentação apresentada na etapa de validação;

iv. antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.1.1.2. O processo de validação pode ser realizado pelo agente de registro fora do ambiente físico da AR.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado são registradas e assinadas. Tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.1.1.4. É mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de um indivíduo. Tais cópias são mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL [1].

3.1.1.5. Nos casos de certificado digital emitido para Servidores do Serviço Exterior Brasileiro, em missão permanente no exterior, assim caracterizados conforme a Lei nº 11.440, de 29 de dezembro de 2006, se houver impedimentos para a identificação conforme o disposto no subitem 3.1.1.1 deste anexo, é facultada a remessa da documentação pela mala diplomática e a realização da identificação por outros meios seguros, a serem definidos e aprovados pela AC-Raiz da ICP-Brasil.

3.1.1.6. Não se Aplica

3.1.2. Tipos de nomes

3.1.2.1. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o "*distinguished name*" do padrão ITU X.500.

3.1.2.2. Um certificado emitido para uma AC Subseqüente não inclui o nome da pessoa responsável.

3.1.3. Necessidade de nomes significativos

Os certificados emitidos pela AC Imprensa Oficial SP exigem o uso de nomes significativos que possibilitam determinar univocamente a identidade da organização titular do certificado.

3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.5. Unicidade de nomes

Identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado emitido pela AC Imprensa Oficial SP. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo DN.

3.1.6. Procedimento para resolver disputa de nomes

A AC Imprensa Oficial SP se reserva o direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrente da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas são executados de acordo com a legislação em vigor.

3.1.8. Método para comprovar a posse de chave privada

A AC verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. A RFC 2510 é utilizada como referência para essa finalidade. O método de verificação utilizado é – Proof of Possession (POP) of Private Key – conforme o item 2.3 da RFC 2510.

3.1.9. Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado, com base em documentos pessoais de identificação legalmente aceitos.

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

Deve ser apresentada a seguinte documentação, em sua versão original, para fins de identificação de um indivíduo solicitante de certificado:

a) Cédula de Identidade ou Passaporte, se brasileiro;

b) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;

c) Passaporte, se estrangeiro não domiciliado no Brasil;

d) caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data da validação presencial;

e) comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial; e

f) Ata ou Procuração conferindo poderes ao responsável, quando aplicável.

Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a CNH - Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

Deverão ser consultadas as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL [1].

Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

Os documentos que possuem data de validade precisam estar dentro do prazo.

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.9.2.1. Não se aplica.

3.1.9.2.2. Não se aplica.

3.1.9.2.3. Não se aplica.

É permitida a substituição dos documentos elencados no item anterior por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

O cartão CPF pode ser substituído por consulta à página da Receita Federal, sendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.1.10. Autenticação da identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.1.1. Neste item são definidos os procedimentos empregados pelas AR vinculadas para a confirmação da identidade de uma pessoa jurídica.

3.1.10.1.2. Em sendo o titular do certificado a pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

3.1.10.1.3. Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.1.10.2;

b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado; e

c) presença física dos representantes legais e do responsável pelo uso do certificado, e assinatura do termo de titularidade de que trata o item 4.1.1.

3.1.10.2. Documentos para efeitos de identificação de uma organização

A confirmação da identidade de uma pessoa jurídica é feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos a sua habilitação jurídica:
i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;

ii. se entidade privada:
1. ato constitutivo, devidamente registrado no órgão competente; e
2. documentos da eleição de seus administradores, quando aplicável registrado no órgão competente;

b) Relativos a sua habilitação fiscal:
i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
ii. prova de inscrição no Cadastro Específico do INSS – CEI.

3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.10.3.1. Não se aplica.

3.1.10.3.2. Não se aplica.

3.1.11. Autenticação da identidade de equipamento ou aplicação

3.1.11.1. Disposições Gerais

3.1.11.1.1. Não se aplica.

3.1.11.1.2. Não se aplica.

3.1.11.1.3. Não se aplica.

3.1.11.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação

Não se aplica.

3.1.11.3. Informações contidas no certificado emitido para um equipamento ou aplicação

3.1.11.3.1. Não se aplica.

3.1.11.3.2. Não se aplica.

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

3.2.1. No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC Imprensa Oficial SP para a geração de novo par de chaves e de seu correspondente certificado, antes da expiração do certificado vigente.

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

3.2.3. Não se aplica.

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

3.3.1. 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.

3.3.2. Após a expiração ou revogação de certificado de AC de nível imediatamente subseqüente ao da AC Imprensa Oficial SP, a AC Subseqüente executa os processos regulares de geração de seu novo par de chaves.

3.4. Solicitação de Revogação

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

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 AR. As solicitações de revogação de certificado são registradas.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado

4.1.1. Para atender à solicitação de emissão de certificados a AC Imprensa Oficial SP exige que a AR tenha provido:

a) a comprovação de atributos de identificação constantes do certificado e o recebimento dos documentos obrigatórios exigidos para identificação dos titulares e responsáveis, conforme item 3.1;

b) a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes a de um certificado de nível A3;

c) um termo de titularidade assinado pelo titular do certificado e pelo responsável pelo uso do certificado, no caso de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico.

4.1.2. A solicitação de certificado para AC de nível imediatamente subseqüente a AC Imprensa Oficial SP somente é possível após o processo de credenciamento e autorização de funcionamento da AC em questão, conforme documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.3. A AC Subseqüente encaminha a solicitação de seu certificado à AC Imprensa Oficial SP por meio de seu(s) representante(s) legal(is), utilizando protocolo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

4.1.4. Nos casos previstos no item 4.1.2., a AC subsequente deverá encaminhar a solicitação de certificado à AC emitente por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

4.2. Emissão de Certificado

4.2.1. A emissão de certificado depende do correto preenchimento de formulário de solicitação, do recebimento do "Termo de Titularidade", no caso de certificados de pessoas jurídicas, equipamentos ou aplicações e dos demais documentos exigidos. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido e Titular é notificado, por e-mail, da emissão e do método para a retirada do certificado.

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

4.3. Aceitação de Certificado

4.3.1. A pessoa física responsável, verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, 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.
d) Torna-se responsável por todos os atos praticados perante a RFB utilizando a chave privada correspondente à chave pública contida no certificado e-CPF e e-CNPJ.

4.3.2. A aceitação do certificado de uma AC Subseqüente é declarada por seu responsável através da assinatura do Termo de Aceitação.

4.3.3. Não se aplica.

4.4. Suspensão e Revogação de Certificado

4.4.1. Circunstâncias para revogação

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

4.4.1.2. 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 Imprensa Oficial SP;
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.

4.4.1.3. A AC Imprensa Oficial SP revoga, no prazo definido no item 4.4.4, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil.

O CG da ICP-Brasil ou AC Raiz determina a revogação do certificado da AC Imprensa Oficial SP quando essa deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

4.4.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

a) por solicitação do titular do certificado;

b) por solicitação do responsável pelo certificado;

c) pela AC Imprensa Oficial SP;

d) pela AR que tiver recebido a solicitação;

e) por determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3. Procedimento para solicitação de revogação

4.4.3.1. Uma solicitação de revogação é necessária para que AR responsável 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 Imprensa Oficial SP ou pela AR Responsável.

4.4.3.2. 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 Imprensa Oficial 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.

4.4.3.3. Não se aplica.

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

4.4.3.5. A AC Imprensa Oficial 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.

4.4.3.6. Não se aplica.

4.4.4. Prazo para solicitação de revogação

4.4.4.1. A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 4.4.1 desta DPC.

O prazo para aceitação do certificado pelo seu titular é de 3 (três) dias úteis, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa de revogação.

4.4.4.2. Não se aplica.

4.4.5. Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.6. Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.7. Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.8. Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.9. Freqüência de emissão de LCR

4.4.9.1. Neste item é definida a freqüência para a emissão de LCR referente a certificados de AC de nível imediatamente subseqüente a AC Imprensa Oficial SP.

4.4.9.2. Não se aplica.

4.4.9.3. A freqüência máxima admitida para a emissão de LCR referente a certificados de AC Subseqüente é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC de nível imediatamente subseqüente a AC Imprensa Oficial SP, é emitida nova LCR no prazo previsto no item 4.4.3 e notificada a todas as AC de nível imediatamente subseqüente ao seu.

4.4.9.4. Não se aplica.

4.4.10. Requisitos para verificação de LCR

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

4.4.10.2. Também é obrigatória a verificação da autenticidade da LCR, por meio das verificações da assinatura da AC Imprensa Oficial SP e do período de validade da LCR.

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

Não se aplica.

4.4.12. Requisitos para verificação de revogação on-line

Não se aplica.

4.4.13. Outras formas disponíveis para divulgação de revogação

Não se aplica.

4.4.14. Requisitos para verificação de outras formas de divulgação de revogação

Não se aplica.

4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.4.15.1. O titular de certificado deve notificar imediatamente, à AC Imprensa Oficial SP 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 4.4.3.

4.4.15.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente na AR Responsável da forma do item 4.4.3 desta DPC.

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

4.5. Procedimentos de Auditoria de Segurança

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC Imprensa Oficial SP com o objetivo de manter um ambiente seguro.

4.5.1. Tipos de eventos registrados

4.5.1.1. A AC Imprensa Oficial 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 Imprensa Oficial SP;

c) mudanças na configuração dos sistemas AC Imprensa Oficial 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 Imprensa Oficial SP ou de chaves das AC Subseqüentes;

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.

4.5.1.2. A AC Imprensa Oficial 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.

4.5.1.3. As informações registradas pela AC Imprensa Oficial SP são todas as descritas nos itens acima.

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

4.5.1.5. A documentação relacionada aos serviços da AC Imprensa Oficial SP é armazenada, eletrônica ou manualmente, em local único, de forma estruturada para facilitar o acesso e consulta nos processos de auditoria, para atender a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.1.6. As AR vinculadas à AC Imprensa Oficial SP registram manualmente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) os agentes de registro que realizaram as operações;

b) data e hora das operações;

c) a associação entre os agentes que realizaram a validação e aprovação e o certificado gerado;

d) a assinatura do executante.

4.5.1.7. A AC Imprensa Oficial SP 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.

4.5.2. Freqüência de auditoria de registros (logs)

A periodicidade com que os registros de auditoria da AC Imprensa Oficial SP são analisados pelo pessoal operacional é de uma semana.

Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

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

A AC Imprensa Oficial SP mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses e, subseqüentemente, armazena-os da maneira descrita no item 4.6.

4.5.4. Proteção de registro (log) de auditoria

4.5.4.1. 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.

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

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

4.5.4.3. Os mecanismos de proteção descritos obedecem à Política de Segurança da AC Imprensa Oficial SP, em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

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

Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela AC Imprensa Oficial SP têm cópias de segurança semanais, feitas, automaticamente pelo

sistema ou manualmente pelos administradores de sistemas. Estas cópias são enviadas ao departamento de segurança.

4.5.6. Sistema de coleta de dados de auditoria

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

4.5.7. Notificação de agentes causadores de eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC Imprensa Oficial SP, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8. Avaliações de vulnerabilidade

Os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC Imprensa Oficial SP, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC Imprensa Oficial SP e registradas para fins de auditoria.

4.6. Arquivamento de Registros

4.6.1. 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 Imprensa Oficial SP; e

g) informações de auditoria previstas no item 4.5.1.

4.6.2. 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.

4.6.3. Proteção de arquivo

Todos os registros são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

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

4.6.4.1. A AC Imprensa Oficial SP estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC Imprensa Oficial SP, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

4.6.4.3. A AC Imprensa Oficial SP verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

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

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.

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

4.6.6. Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Imprensa Oficial SP em seus procedimentos operacionais são automatizados e manuais e internos.

4.6.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC Imprensa Oficial SP, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

4.7. Troca de chave

4.7.1. A AC Imprensa Oficial SP fornece novo certificado a AC Subseqüente utilizando o mesmo procedimento utilizado para emissão do certificado inicial. A AC Imprensa Oficial SP comunica o titular do certificado, 13 (treze) meses antes da expiração do certificado, junto com instruções para a solicitação de um novo certificado. A comunicação de expiração e solicitação de renovação é realizada através de email.

4.7.2. Não se aplica.

4.8. Comprometimento e Recuperação de Desastre

A AC Imprensa Oficial SP possui um Plano de Continuidade de Negócios testado anualmente para garantir a continuidade de seus serviços críticos.

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

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

4.8.2. Certificado de entidade é revogado

Em caso de revogação do certificado da AC Imprensa Oficial SP o Gerente de Segurança, juntamente com o Gerente de Criptografia da AC Imprensa Oficial SP, revogará todos os certificados subseqüentes. Os titulares dos certificados revogados serão informados. A AC Imprensa Oficial SP emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

4.8.3. Chave da entidade é comprometida

Em caso de suspeita de comprometimento de chave da AC Imprensa Oficial SP, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com o Gerente de Criptografia da AC Imprensa Oficial SP, decretam o início da fase resposta e seguirão 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 Imprensa Oficial SP estiver encerrando suas atividades – DPC Item 4.9.

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

Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, 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 Imprensa Oficial 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.

4.8.5. Atividades das Autoridades de Registro

As AR vinculadas à AC Imprensa Oficial SP possuem um Plano de Continuidade de Negócios testado anualmente para garantir a recuperação, total ou parcial das atividades das AR, contendo, no mínimo as seguintes informações:

a) identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo inundações e incêndios;

b) identificação e concordância de todas as responsabilidades e procedimentos de emergência;

c) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial é dada à avaliação da recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;

d) documentação dos processos e procedimentos acordados;

e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;

f) teste e atualização dos planos.

4.9. Extinção dos serviços de AC, AR ou PSS

4.9.1. Observado o disposto no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], este item descreve os requisitos e procedimentos adotados nos casos de extinção dos serviços da AC Imprensa Oficial SP ou de uma AR ou PSS a ela vinculados.

4.9.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC Imprensa Oficial SP segue os requisitos e procedimentos descritos no documento Plano de Encerramento. Esse plano tem abordagem multidisciplinar envolvendo aspectos de varias áreas da companhia, como jurídico, comercial, técnicos/tecnológicos, entre outros. De acordo com esse plano a AC Imprensa Oficial SP:

a) Comunicará publicamente a extinção dos serviços da AC Imprensa Oficial SP, através de publicação em jornal de grande circulação.
b) Revogará todos os certificados gerados pela AC Imprensa Oficial SP nos prazos estipulados nesta DPC após a publicação e comunicará às 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 Imprensa Oficial SP extinta seguindo o procedimento descrito na DPC Item 6.2.9.

f) Transferirá os dados e gravações da AC Imprensa Oficial SP para a Autoridade Certificadora sucessora, aprovada pela AC Raiz. O período no qual os mesmos ficarão armazenados está descrito na DPC item 4.6.

g) Transferirá as chaves públicas dos certificados emitidos pela AC Imprensa Oficial 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 Imprensa Oficial 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 AC Raiz.

h) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC Imprensa Oficial SP.

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

No caso de encerramento das atividades como AR vinculada a AC Imprensa Oficial SP a AR deverá seguir os seguintes requisitos e procedimentos :

a) Comunicará publicamente a extinção dos serviços de AR vinculada AC Imprensa Oficial SP, através de publicação em jornal de grande circulação.

b) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados;

c) Ficará responsável pela guarda dos documentos, dados e registros relativos aos pedidos de emissão de certificados para a AC Imprensa Oficial SP, devendo fornecê-los sempre que solicitada pelo Titular, ou pela AC Imprensa Oficial SP. O período no qual os mesmos ficarão armazenados está descrito na DPC item 4.6.

Em caso de falência ou extinção da AR a documentação e registros relativos à emissão de certificados deverá ser entregue para guarda da AC Imprensa Oficial SP.

No caso de encerramento das atividades como PSS vinculada a AC Imprensa Oficial SP, diretamente ou por intermédio da AR, 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.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

5.1. Controles Físicos

5.1.1. Construção e localização das instalações

5.1.1.1. A localização e o sistema de certificação da AC Imprensa Oficial 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.

5.1.1.2. 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.

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

Existem sistemas de aterramento e de proteção contra descargas atmosféricas

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

5.1.2. Acesso físico nas instalações de AC

A AC Imprensa Oficial SP possui sistema de controle de acesso físico que garante a segurança de suas instalações conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e os requisitos que seguem.

5.1.2.1 Níveis de acesso

5.1.2.1.1. A AC Imprensa Oficial SP possui 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 2 (dois) níveis de proteção da chave privada da AC Imprensa Oficial SP;

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

Nenhum tipo de processo operacional ou administrativo da AC Imprensa Oficial SP é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC Imprensa Oficial 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.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC Imprensa Oficial SP. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá.

5.1.2.1.5. O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da AC Imprensa Oficial 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.

5.1.2.1.6. No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: identificação individual, por meio de cartão eletrônico, e identificação biométrica.

5.1.2.1.7. Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC Imprensa Oficial SP, não são admitidos a partir do nível 3.

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC Imprensa Oficial SP 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.

5.1.2.1.9. 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.

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

5.1.2.1.11. Na AC Imprensa Oficial 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);

5.1.2.1.12. 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 superior.

5.1.2.1.13. 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.

5.1.2.1.14. 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 Imprensa Oficial SP são armazenados nesses depósitos.

5.1.2.2 Sistemas físicos de detecção

5.1.2.2.1. 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.

5.1.2.2.2. 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.

5.1.2.2.3. 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.

5.1.2.2.4. 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.

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

5.1.2.2.6. 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.

5.1.2.3 Sistema de controle de acesso

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

5.1.2.4 Mecanismos de emergência

5.1.2.4.1. Mecanismos específicos são implantados pela AC Imprensa Oficial 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.

5.1.2.4.2. 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.

5.1.3. Energia e ar condicionado nas instalações de AC

5.1.3.1. A infra-estrutura do ambiente de certificação da AC Imprensa Oficial 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 Imprensa Oficial SP e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC Imprensa Oficial SP.

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

5.1.3.3. Existem tubulações, dutos, calhas, quadros e caixas – de passagem, distribuição e terminação – projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, telefonia e dados.

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

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

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

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

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

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

5.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC Imprensa Oficial 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.

5.1.4. 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.

5.1.5. Prevenção e proteção contra incêndio nas instalações de AC

5.1.5.1. 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.

5.1.5.2. Nas instalações da AC Imprensa Oficial SP não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. 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.

5.1.5.4. Em caso de incêndio nas instalações da AC Imprensa Oficial 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.

5.1.6. Armazenamento de mídia nas instalações de AC

A AC Imprensa Oficial SP atende às normas NBR 11.515 e NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados ").

5.1.7. Destruição de lixo nas instalações de AC

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

5.1.7.2. Todos os dispositivos 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.

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

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.

5.1.9. Instalações técnicas de AR

As instalações técnicas de AR atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.1.1. A AC Imprensa Oficial 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.

5.2.1.2. A AC Imprensa Oficial 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 Imprensa Oficial SP;
  - gerenciamento e controle da tecnologia empregada nos serviços de certificação da AC Imprensa Oficial SP;
  - controle de acesso dos funcionários à rede AC Imprensa Oficial SP;
  - gerenciamento dos operadores da AC Imprensa Oficial SP;
  - controle de acesso ao sistema de certificação.
- Gerência de Segurança:
  - implementação da Política de Segurança da AC Imprensa Oficial SP;
  - verificação dos registros de auditoria;
  - supervisão do cumprimento das práticas e procedimentos determinados na Política de Segurança da AC Imprensa Oficial 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 Imprensa Oficial 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.

5.2.1.3. Os operadores do sistema de certificação da AC Imprensa Oficial 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 Imprensa Oficial SP), com base nas necessidades de cada perfil.

5.2.1.4. A AC Imprensa Oficial 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 Imprensa Oficial SP no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC Imprensa Oficial SP, conforme o descrito em 6.2.2.

5.2.2.2. Todas as tarefas executadas no ambiente onde esta localizado o equipamento de certificação da AC Imprensa Oficial 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.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC Imprensa Oficial SP tem sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso às instalações da AC Imprensa Oficial SP;

b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC Imprensa Oficial SP;
c) receber um certificado para executar suas atividades operacionais na AC Imprensa Oficial SP; e
d) receber uma conta no sistema de certificação da AC Imprensa Oficial SP.

5.2.3.2. 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.

5.2.3.3. A AC Imprensa Oficial SP adota padrão de utilização de "senhas fortes", definido na sua Política de Segurança e em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Todos os empregados da AC Imprensa Oficial SP, das AR 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 da ICP-Brasil;

c) o compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC Imprensa Oficial SP e das AR vinculadas 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 DA ICP-BRASIL [8].

5.3.2. Procedimentos de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC Imprensa Oficial SP e das AR vinculadas 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.

5.3.2.2. Não se aplica.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC Imprensa Oficial SP e das AR vinculadas 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 Imprensa Oficial SP e das AR vinculadas;
b) sistema de certificação em uso na AC Imprensa Oficial SP;
c) procedimentos de recuperação de desastres e de continuidade do negócio;
d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma dos itens 3.1.9, 3.1.10 e 3.1.11; e
e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Freqüência e requisitos para reciclagem técnica

O pessoal da AC Imprensa Oficial SP e das AR vinculadas 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 Imprensa Oficial SP.

5.3.5. Freqüência e seqüência de rodízio de cargos

Não estabelecido.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC Imprensa Oficial SP ou de uma AR vinculada, 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 e legais cabíveis.

5.3.6.2. O processo administrativo referido acima contém, no mínimo, os seguintes itens:

a) relato da ocorrência com "modus operandis";
b) identificação dos envolvidos;
c) eventuais prejuízos causados;
d) punições aplicadas, se for o caso; e
e) conclusões.

5.3.6.3. Concluído o processo administrativo, a AC Imprensa Oficial SP encaminha suas conclusões à AC Raiz.

5.3.6.4. As punições passíveis de aplicação, em decorrência de processo administrativo, são:

a) advertência;
b) suspensão por prazo determinado; ou
c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da AC Imprensa Oficial SP e das AR vinculadas 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 DA ICP-BRASIL [8].

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC Imprensa Oficial SP disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas:

a) A DPC da AC Imprensa Oficial SP;
b) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];

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

5.3.8.2. A documentação fornecida é classificada segundo a política de classificação de informação definida pela AC Imprensa Oficial SP e é mantida atualizada.

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas da AC Imprensa Oficial SP é gerado pela própria AC Imprensa Oficial SP, após ter sido credenciada e autorizada a funcionar no âmbito da ICP-Brasil.

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

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

O par de chaves da AC Imprensa Oficial SP é gerado em módulos criptográficos de hardware, conforme definido no DOC-ICP-01.01, com padrão de segurança 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 cadeia de certificação V2 e V3).

6.1.1.2. Pares de chaves das AC Subseqüente são gerados somente pelas AC Subseqüente, 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 Subseqüente é realizada em processo verificável, obrigatoriamente na presença de funcionários de confiança da AC Subseqüente treinados para a função. A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves das AC Subseqüente é gerado e armazenado em módulo criptográfico de hardware, conforme definido no DOC-ICP-01.01, com padrão de segurança 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 cadeia de certificação V2 e V3).

6.1.1.3. Não se aplica.

6.1.2. Entrega da chave privada à entidade titular

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

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. A AC Imprensa Oficial 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 Imprensa Oficial SP, em cerimônia especifica, em data e hora previamente estabelecida.

6.1.3.2. A chave pública de uma AC Subseqüente é entregue pelo representante legal da AC Subseqüente, em cerimônia específica, em data e hora previamente estabelecidas pela AC Imprensa Oficial SP. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

6.1.4. Disponibilização de chave pública da AC para usuários

A AC Imprensa Oficial SP disponibiliza o seu certificado e todos os certificados da cadeia de certificação para os usuários da ICP-Brasil, através endereço Web: http://icp-brasil.certisign.com.br/repositorio/ac-imesp-1n/index.htm.

6.1.5. Tamanhos de chave

6.1.5.1. Não se aplica.

6.1.5.2. O tamanho mínimo das chaves criptográficas associadas aos certificados de AC Subseqüentes é de RSA 2048 bits (V1), RSA 4096 bits (V2), conforme definido no DOC-ICP-01.01.

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC Imprensa Oficial SP adotam 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), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8. Geração de chave por *hardware ou software*

6.1.8.1. As chaves da AC Imprensa Oficial SP são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo 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), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8.2. As chaves criptográficas das AC Subseqüentes são geradas, armazenadas e utilizadas dentro de hardware específico, compatível com os requisitos da norma 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 cadeia de certificação V2 e V3), conforme definido no DOC-ICP-01.01, baseado nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

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

6.1.9.2. A chave privada da AC Imprensa Oficial SP é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

6.2. Proteção da Chave Privada

A AC Imprensa Oficial SP implementa uma combinação de controles físicos lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas. Controles Lógico e Procedimental estão descritos no item 5.2. Controle de acesso físico está descrito no item 5.1.2.

A chave privada da AC Imprensa Oficial 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 Imprensa Oficial 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.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC Imprensa Oficial SP adota o padrão FIPS (Federal Information Processing Standards) 140-2, level

3, padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. Não se Aplica

6.2.2. Controle "n de m" para chave privada

6.2.2.1. A AC Imprensa Oficial SP exige controle múltiplo para utilização da sua chave privada.

6.2.2.2. 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 Imprensa Oficial SP.

6.2.3. Recuperação (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, 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.

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

6.2.4.1. Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua chave privada.

6.2.4.2. A AC Imprensa Oficial SP mantém cópia de segurança de sua chave privada.

6.2.4.3. Não se aplica.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo 3DES – 112 bits ou AES – 128 ou 256 bits, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1. Não se aplica.

6.2.5.2. Não se aplica.

6.2.6. Inserção de chave privada em módulo criptográfico

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

6.2.7. Método de ativação de chave privada

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

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

6.2.8. Método de desativação de chave privada

A chave privativa da AC Imprensa Oficial 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 Imprensa Oficial SP.

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 Imprensa Oficial SP contendo fotografia, nome, e departamento do funcionário.

6.2.9. Método de destruição de chave privada

O Gerente de Criptografia da AC Imprensa Oficial 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 Imprensa Oficial 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.

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

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da AC Imprensa Oficial SP e dos titulares dos certificados de AC Subseqüentes 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.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas dos titulares dos certificados de AC Subseqüentes emitidos pela AC Imprensa Oficial 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.

6.3.2.2. Não se aplica.

6.3.2.3. Não se aplica.

6.3.2.4. O período máximo de validade admitido para certificado da AC Imprensa Oficial SP é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4. Dados de Ativação

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

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação do equipamento de criptografia que armazena as chaves privadas da AC Imprensa Oficial SP são únicos e aleatórios.

6.4.1.2. Não se aplica.

6.4.2. Proteção dos dados de ativação

6.4.2.1. A AC Imprensa Oficial 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.

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

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A geração do par de chaves da AC Imprensa Oficial 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.

6.5.1.2. A geração dos pares de chaves das AC Subseqüentes 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.

6.5.1.3. O ambiente computacional da AC Imprensa Oficial 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 Imprensa Oficial SP;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC Imprensa Oficial 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 Imprensa Oficial SP;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) mecanismos para cópias de segurança (*backup*).

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

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

Os números de série dos equipamentos e as datas de envio e de recebimento da manutenção são controladas. Ao retornar às instalações da AC Imprensa Oficial SP, o equipamento que passou por manutenção é inspecionado. As informações sensíveis armazenadas, relativas à atividade da AC Imprensa Oficial 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.

6.5.1.6. Equipamentos utilizados pela AC Imprensa Oficial SP são preparados e configurados como previsto na Política de Segurança da AC Imprensa Oficial SP

implementada ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A segurança computacional da AC Imprensa Oficial SP segue as recomendações Common Criteria.

6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. Neste item estão descritos os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas AR para os processos de validação e aprovação de certificados.

6.5.3.2. Os requisitos abaixo correspondem aos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL [1]:

a) controle de acesso lógico ao sistema operacional;

b) exigência de uso de senhas fortes;

c) diretivas de senha e de bloqueio de conta;

d) logs de auditoria do sistema operacional ativados, registrando:

i. iniciação e desligamento do sistema;

ii. tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;

iii. mudanças na configuração da estação;

iv. tentativas de acesso (login) e de saída do sistema (logoff);

v. tentativas não-autorizadas de acesso aos arquivos de sistema;

vi. tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.

e) antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;

f) firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo;

g) proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;

h) sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);

i) utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;

j) impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;

k) utilização da data e Hora Legal Brasileira.

6.6. Controles Técnicos do Ciclo de Vida

A AC Imprensa Oficial SP não desenvolve sistemas com qualquer finalidade relacionada à operação da AC Imprensa Oficial SP ou da AR Imprensa Oficial SP.

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. Não se aplica.

6.6.1.2. Não se aplica.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. Não se aplica.

6.6.2.2. Não se aplica.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

Antes de publicadas, todas as LCR geradas pela AC devem ser 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.

6.7. Controles de Segurança de Rede

6.7.1. Diretrizes Gerais

6.7.1.1. Neste item são descritos os controles relativos à segurança da rede da AC Imprensa Oficial SP, incluindo firewalls e recursos similares.

6.7.1.2. Nos servidores do sistema de certificação da AC Imprensa Oficial SP, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.

6.7.1.3. Todos os servidores e elementos de infra-estrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls, e sistemas de detecção de intrusos (IDS), localizados no segmento de rede que hospeda o sistema de certificação estão localizados e operam em ambiente de nível 4.

6.7.1.4. 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.

6.7.1.5. 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.

6.7.2. Firewall

6.7.2.1. 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 Imprensa Oficial SP.

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

6.7.3. Sistema de detecção de intrusão (IDS)

6.7.3.1. 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.

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

6.7.3.3. 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.

6.7.4. Registro de acessos não-autorizados à rede

As tentativas de acesso não-autorizado – em roteadores, firewalls ou IDS – são registradas em arquivos para posterior análise. A freqüência de exame dos arquivos de

registro é diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico de geração de chaves assimétricas da AC Imprensa Oficial SP adota o padrão FIPS (Federal Information Processing Standards) 140-2, level 3.

7. PERFIS DE CERTIFICADO E LCR

7.1. Diretrizes Gerais

7.1.1. Nos itens seguintes são descritos os aspectos dos certificados e LCR emitidos pela AC Imprensa Oficial SP.

7.1.2. Não se aplica.

7.1.3. Nos itens seguintes também são especificados o formato dos certificados emitidos pela AC Imprensa Oficial SP.

7.2. Perfil do Certificado

Todos os certificados e LCR emitidos pela AC Imprensa Oficial SP estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.2.1. Número de versão

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

7.2.2. Extensões de certificado

Para os certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira:

Os certificados emitidos pela AC Imprensa Oficial SP obedecem a ICP - Brasil, que define como obrigatórias as seguintes extensões:

a) **Authority Key Identifier**, não crítica: não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Imprensa Oficial SP;
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 OID da DPC da AC titular do certificado, se essa AC emite certificados para outras ACs (OID = 2.16.76.1.1.26);

d.2) o campo policyQualifiers contém o o endereço *Web* da DPC da AC Imprensa Oficial SP (http://icp-brasil.certisign.com.br/repositorio/dpc/AC_IMESP_1n/DPC_AC Imprensa Oficial SP.pdf).

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

f) **CRL Distribution Points**, não crítica: contém o endereço Web onde se obtém a LCR da AC Imprensa Oficial SP:

Para certificados emitidos na G2:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACImprensaOficialSPPrincipalG2/LatestCRL.crl

Para certificados emitidos na G3:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACImprensaOficialSPPrincipalG3/LatestCRL.crl

7.2.3. Identificadores de algoritmo

Os certificados emitidos pela AC Imprensa Oficial SP são assinados com o uso do algoritmo RSA com SHA-1 como função de hash (OID = 1.2.840.113549.1.1.5) nas hierarquias V0 e V1, e algoritmo RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11) ou algoritmo RSA com SHA-512 como função de hash (OID = 1.2.840.113549.1.1.13) na hierarquia V2 conforme o padrão PKCS#1.

7.2.4. 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:

C = BR

O = ICP-Brasil

OU = Razão Social da AC Subseqüente

CN = nome da AC Subseqüente

7.2.5. Restrições de nome

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

7.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC Imprensa Oficial SP 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 (hexadeciamal)
Branco	20
"	22
#	23
'	27
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D

7.2.6. OID (Object Identifier) de DPC

O OID desta DPC é: 2.16.76.1.1.26.

7.2.7. Uso da extensão "Policy Constraints"

Item não aplicável.

7.2.8. Sintaxe e semântica dos qualificadores de política

O campo **policyQualifiers** da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC Imprensa Oficial SP (http://icp-brasil.certisign.com.br/repositorio/dpc/AC_IMESP_1n/DPC_AC Imprensa Oficial SP.pdf)

7.2.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.3. Perfil de LCR

7.3.1. Número(s) de versão

As LCR geradas pela AC Imprensa Oficial SP implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.3.2. Extensões de LCR e de suas entradas

7.3.2.1. Neste item estão descritas todas as extensões de LCR utilizadas e sua criticidade.

7.3.2.2. As LCR da AC Imprensa Oficial SP obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões para certificados de AC:

a) "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC Imprensa Oficial SP que assina a LCR.

b) "CRL Number", não crítica: contém um número seqüencial para cada LCR emitida pela AC Imprensa Oficial SP.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

Alterações nesta DPC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC Imprensa Oficial SP. A aprovação e conseqüente adoção de nova versão estarão sujeitas à autorização do CG da ICP-Brasil.

8.2. Políticas de publicação e notificação

A AC Imprensa Oficial SP mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço *Web*: http://icp-brasil.certisign.com.br/repositorio/dpc/AC_IMESP_1n/DPC_AC Imprensa Oficial SP.pdf

8.3. Procedimentos de aprovação

Esta DPC da AC Imprensa Oficial SP foi submetida à aprovação, durante o processo de credenciamento da AC Imprensa Oficial SP, conforme o determinado CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

9. DOCUMENTOS REFERENCIADOS

9.1 Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTODAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

9.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio Http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

9.3 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

Ref.	Nome do documento	Código
[4]	MODELO DE TERMO DE TITULARIDADE	ADE-ICP-05.A