

IMPrensa OFICIAL DO ESTADO SA IMESP (AC IMPrensa OFICIAL SP G4)

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

VERSÃO 5.3 – 21/02/2017

HISTÓRICO DE VERSÕES

<i>Data</i>	<i>Versão</i>	<i>Observações</i>
23/10/2014	5.2	Redação Inicial
15/12/2016	5.3	Revisão

AVISO LEGAL

Copyright © Imprensa Oficial do Estado SA IMESP. Todos os direitos reservados.

Imprensa Oficial é uma marca registrada da Imprensa Oficial do Estado SA IMESP. Todas as restantes marcas, trademarks e service marks são propriedade dos seus respectivos detentores.

É expressamente proibida a reprodução, total ou parcial, do conteúdo deste documento, sem prévia autorização escrita emitida pela Imprensa Oficial.

Qualquer dúvida ou pedido de informação relativamente ao conteúdo deste documento deverá ser dirigido a certificacao@imprensaoficial.com.br.

CONTEÚDO

1. Introdução	9
1.1. Visão Geral	9
1.2. Identificação	9
1.3. Comunidade e Aplicabilidade	9
1.3.1. Autoridades Certificadoras	9
1.3.2. Autoridades de Registro	10
1.3.3. Prestador de Serviço de Suporte	10
1.3.4. Titulares de Certificado	10
1.3.5. Aplicabilidade	11
1.4. Dados de Contato	11
2. Disposições Gerais	12
2.1. Obrigações e Direitos	12
2.1.1. Obrigações da AC	12
2.1.2. Obrigações das AR	13
2.1.3. Obrigações do Titular do Certificado	13
2.1.4. Direitos da Terceira Parte (Relying Party)	14
2.1.5. Obrigações do Repositório	14
2.2. Responsabilidades	14
2.2.1. Responsabilidades da AC	14
2.2.2. Responsabilidades das AR	14
2.3. Responsabilidade Financeira	14
2.3.1. Indenizações devidas pela terceira parte (Relying Party)	15
2.3.2. Relações Fiduciárias	15
2.3.3. Processos Administrativos	15
2.4. Interpretação e Execução	15
2.4.1. Legislação	15
2.4.2. Forma de interpretação e notificação	15
2.4.3. Procedimentos da solução de disputa	16
2.5. Tarifas de Serviço	16
2.5.1. Tarifas de emissão e renovação de certificados	16
2.5.2. Tarifas de acesso ao certificado	16
2.5.3. Tarifas de revogação ou de acesso à informação de status	16
2.5.4. Tarifas para outros serviços	16
2.5.5. Política de reembolso	16
2.6. Publicação e Repositório	16
2.6.1. Publicação de informação da AC	16
2.6.2. Frequência de publicação	17

2.6.3.	Controles de acesso	17
2.6.4.	Repositórios.....	17
2.7.	Fiscalização e Auditoria de Conformidade.....	17
2.8.	Sigilo	18
2.8.1.	Disposições gerais	18
2.8.2.	Tipos de informações sigilosas	18
2.8.3.	Tipos de informações não-sigilosas	18
2.8.4.	Divulgação de informação de revogação ou suspensão de certificado	19
2.8.5.	Quebra de sigilo por motivos legais	19
2.8.6.	Informações a terceiros	19
2.8.7.	Divulgação por solicitação do Titular.....	19
2.8.8.	Outras circunstâncias de divulgação de informação	20
2.9.	Direitos de Propriedade Intelectual.....	20
3.	Identificação e Autenticação.....	21
3.1.	Registro Inicial.....	21
3.1.1.	Disposições Gerais	21
3.1.2.	Tipos de nomes.....	22
3.1.3.	Necessidade de nomes significativos	22
3.1.4.	Regras para interpretação de vários tipos de nomes	22
3.1.5.	Unicidade de nomes.....	22
3.1.6.	Procedimento para resolver disputa de nomes.....	22
3.1.7.	Reconhecimento, autenticação e papel de marcas registradas	22
3.1.8.	Método para comprovar a posse de chave privada	23
3.1.9.	Autenticação da identidade de um indivíduo	23
3.1.10.	Autenticação da identidade de uma organização.....	24
3.1.11.	Autenticação da identidade de equipamento ou aplicação.....	25
3.1.12.	Autenticação de Identificação de Equipamento para Certificado CF-e-SAT	25
3.2.	Geração de novo par de chaves antes da expiração do atual.....	25
3.3.	Geração de novo par de chaves após expiração ou revogação	26
3.4.	Solicitação de Revogação	26
4.	Requisitos Operacionais.....	27
4.1.	Solicitação de Certificado	27
4.2.	Emissão de Certificado	27
4.3.	Aceitação de Certificado	27
4.4.	Suspensão e Revogação de Certificado	28
4.4.1.	Circunstâncias para revogação	28
4.4.2.	Quem pode solicitar revogação	28
4.4.3.	Procedimento para solicitação de revogação	28

4.4.4.	Prazo para solicitação de revogação.....	29
4.4.5.	Circunstâncias para suspensão	29
4.4.6.	Quem pode solicitar suspensão	29
4.4.7.	Procedimento para solicitação de suspensão	29
4.4.8.	Limites no período de suspensão	29
4.4.9.	Frequência de emissão de LCR.....	30
4.4.10.	Requisitos para verificação de LCR	30
4.4.11.	Disponibilidade para revogação ou verificação de status on-line	30
4.4.12.	Requisitos para verificação de revogação on-line	30
4.4.13.	Outras formas disponíveis para divulgação de revogação	30
4.4.14.	Requisitos para verificação de outras formas de divulgação de revogação 30	
4.4.15.	Requisitos especiais para o caso de comprometimento de chave	30
4.5.	Procedimentos de Auditoria de Segurança	31
4.5.1.	Tipos de eventos registrados.....	31
4.5.2.	Frequência de auditoria de registros (logs)	32
4.5.3.	Período de retenção para registros (logs) de auditoria.....	32
4.5.4.	Proteção de registro (log) de auditoria	32
4.5.5.	Procedimentos para cópia de segurança (backup) de registro (log) de auditoria 32	
4.5.6.	Sistema de coleta de dados de auditoria	33
4.5.7.	Notificação de agentes causadores de eventos.....	33
4.5.8.	Avaliações de vulnerabilidade	33
4.6.	Arquivamento de Registros.....	33
4.6.1.	Tipos de registros arquivados.....	33
4.6.2.	Período de retenção para arquivo	33
4.6.3.	Proteção de arquivo	33
4.6.4.	Procedimentos para cópia de segurança (backup) de arquivo.....	33
4.6.5.	Requisitos para datação (time-stamping) de registros	34
4.6.6.	Sistema de coleta de dados de arquivo	34
4.6.7.	Procedimentos para obter e verificar informação de arquivo	34
4.7.	Troca de chave.....	34
4.8.	Comprometimento e Recuperação de Desastre	34
4.8.1.	Recursos computacionais, software, e dados corrompidos.....	34
4.8.2.	Certificado de entidade é revogado	35
4.8.3.	Chave da entidade é comprometida	35
4.8.4.	Segurança dos recursos após desastre natural ou de outra natureza	35
4.8.5.	Atividades das Autoridades de Registro.....	35
4.9.	Extinção dos serviços de AC, AR ou PSS.....	36

5.	Controles de Segurança Física, Procedimental e de Pessoal	37
5.1.	Controles Físicos	37
5.1.1.	Construção e localização das instalações.....	37
5.1.2.	Acesso físico nas instalações de AC	37
5.1.3.	Energia e ar condicionado nas instalações de AC	39
5.1.4.	Exposição à água nas instalações de AC.....	40
5.1.5.	Prevenção e proteção contra incêndio nas instalações de AC.....	40
5.1.6.	Armazenamento de mídia nas instalações de AC	41
5.1.7.	Destruição de lixo nas instalações de AC.....	41
5.1.8.	Instalações de segurança (backup) externas (off-site).....	41
5.1.9.	Instalações técnicas de AR.....	41
5.2.	Controles Procedimentais.....	41
5.2.1.	Perfis qualificados	41
5.2.2.	Número de pessoas necessário por tarefa	42
5.2.3.	Identificação e autenticação para cada perfil.....	42
5.3.	Controles de Pessoal	42
5.3.1.	Antecedentes, qualificação, experiência e requisitos de idoneidade.....	42
5.3.2.	Procedimentos de verificação de antecedentes.....	43
5.3.3.	Requisitos de treinamento	43
5.3.4.	Frequência e requisitos para reciclagem técnica.....	43
5.3.5.	Frequência e sequência de rodízio de cargos.....	43
5.3.6.	Sanções para ações não autorizadas	43
5.3.7.	Requisitos para contratação de pessoal.....	44
5.3.8.	Documentação fornecida ao pessoal.....	44
6.	Controles Técnicos de Segurança.....	45
6.1.	Geração e Instalação do Par de Chaves.....	45
6.1.1.	Geração do par de chaves	45
6.1.2.	Entrega da chave privada à entidade titular.....	45
6.1.3.	Entrega da chave pública para emissor de certificado	45
6.1.4.	Disponibilização de chave pública da AC para usuários.....	45
6.1.5.	Tamanhos de chave	46
6.1.6.	Geração de parâmetros de chaves assimétricas	46
6.1.7.	Verificação da qualidade dos parâmetros.....	46
6.1.8.	Geração de chave por hardware ou software.....	46
6.1.9.	Propósitos de uso de chave (conforme o campo "key usage" na X.509v3).....	46
6.2.	Proteção da Chave Privada	46
6.2.1.	Padrões para módulo criptográfico	47
6.2.2.	Controle "n de m" para chave privada	47

6.2.3.	Recuperação (escrow) de chave privada	47
6.2.4.	Cópia de segurança (backup) de chave privada	47
6.2.5.	Arquivamento de chave privada.....	47
6.2.6.	Inserção de chave privada em módulo criptográfico	47
6.2.7.	Método de ativação de chave privada.....	48
6.2.8.	Método de desativação de chave privada.....	48
6.2.9.	Método de destruição de chave privada.....	48
6.3.	Outros Aspectos do Gerenciamento do Par de Chaves	48
6.3.1.	Arquivamento de chave pública.....	48
6.3.2.	Períodos de uso para as chaves pública e privada	48
6.4.	Dados de Ativação	49
6.4.1.	Geração e instalação dos dados de ativação.....	49
6.4.2.	Proteção dos dados de ativação.....	49
6.4.3.	Outros aspectos dos dados de ativação.....	49
6.5.	Controles de Segurança Computacional	49
6.5.1.	Requisitos técnicos específicos de segurança computacional.....	49
6.5.2.	Classificação da segurança computacional.....	50
6.5.3.	Controles de Segurança para as Autoridades de Registro	50
6.6.	Controles Técnicos do Ciclo de Vida	50
6.6.1.	Controles de desenvolvimento de sistema.....	50
6.6.2.	Controles de gerenciamento de segurança	50
6.6.3.	Classificações de segurança de ciclo de vida.....	51
6.6.4.	Controles na Geração de LCR.....	51
6.7.	Controles de Segurança de Rede	51
6.7.1.	Diretrizes Gerais.....	51
6.7.2.	Firewall.....	51
6.7.3.	Sistema de detecção de invasão (IDS).....	52
6.7.4.	Registro de acessos não-autorizados à rede	52
6.8.	Controles de Engenharia do Módulo Criptográfico.....	52
7.	Perfis de Certificado e LCR	53
7.1.	Diretrizes Gerais.....	53
7.2.	Perfil do Certificado	53
7.2.1.	Número de versão.....	53
7.2.2.	Extensões de certificado	53
7.2.3.	Identificadores de algoritmo	54
7.2.4.	Formatos de nome.....	54
7.2.5.	Restrições de nome.....	54
7.2.6.	OID (Object Identifier) de DPC	55

7.2.7.	Uso da extensão "Policy Constraints"	55
7.2.8.	Sintaxe e semântica dos qualificadores de política	55
7.2.9.	Semântica de processamento para extensões críticas.....	55
7.3.	Perfil de LCR	55
7.3.1.	Número(s) de versão	55
7.3.2.	Extensões de LCR e de suas entradas	55
8.	Administração de Especificação	56
8.1.	Procedimentos de mudança de especificação	56
8.2.	Políticas de publicação e notificação	56
8.3.	Procedimentos de aprovação	56
9.	Documentos Referenciados	57

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos utilizados pela Autoridade Certificadora Principal da Imprensa Oficial (AC Imprensa Oficial SP), AC integrante na Infraestrutura 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 subsequente ao da AC Raiz da ICP-Brasil. O certificado da AC Imprensa Oficial SP contém a chave pública correspondente à sua chave privada, utilizada para assinar os certificados de AC de nível imediatamente subsequente (AC subsequente) ao seu e para assinar a sua Lista de Certificados Revogados (LCR).

1.1.4. Para regulamentar usos específicos dos certificados emitidos pela AC Imprensa Oficial SP são publicadas Políticas de Certificado disponíveis em página web (<http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/>).

1.2. IDENTIFICAÇÃO

Este documento é designado Declaração de Práticas de Certificação da Autoridade Certificadora Imprensa Oficial e referida a seguir como "DPC da AC Imprensa Oficial SP".

Este documento é identificado pela seguinte informação:

INFORMAÇÃO DO DOCUMENTO	
Versão/Edição	5.3
Data de Aprovação	15/12/2016
Data de Validade	Não aplicável
OID	2.16.76.1.1.26
Localização	http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. AUTORIDADES CERTIFICADORAS

O termo "Autoridade Certificadora" (AC) designa a entidade que emite e gere certificados digitais.

Esta DPC refere-se à Autoridade Certificadora "AC Imprensa Oficial SP".

1.3.2. AUTORIDADES DE REGISTRO

1.3.2.1. A Autoridade de Registro (AR) é uma entidade que desempenha o papel de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação dos seus solicitantes em nome da AC.

As ARs vinculadas à AC Imprensa Oficial SP estão relacionadas em (URL): <http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/>

O URL referido contém:

- a) relação de todas as AR credenciadas, com informações sobre as PC que implementam.
- 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 das AR que se tenham descredenciado da cadeia da AC Imprensa Oficial SP, com respetiva data do descredenciamento;
- e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respetiva data de encerramento das atividades;
- f) acordos operacionais celebrados pelas AR 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 das suas ARs é publicada em <http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/> e a seguir nomeados:

DigitalSign Certificadora Digital Ltda

1.3.3.2. Os PSS são entidades utilizadas pela AC e/ou suas ARs para desempenhar as atividades descritas nesta DPC ou nas PC e classificam-se em três categorias, conforme o tipo de atividade prestada:

- a) disponibilização de infraestrutura física e lógica;
- b) disponibilização de recursos humanos especializados; ou
- c) disponibilização de infraestrutura 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 subsequente 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 ao seu e para assinar a sua Lista de Certificados Revogados.

1.4. DADOS DE CONTATO

Imprensa Oficial do Estado SA IMESP.

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

Telefone: (55 11) 0800 0123401

Fax: (55 11) 2799 9887

Nome: João Paulo Foini

Telefone: (55 11) 2799 9800

Email: certificacao@imprensaoficial.com.br

2. DISPOSIÇÕES GERAIS

2.1. OBRIGAÇÕES E DIREITOS

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. Os requisitos específicos associados a essas obrigações estão detalhados nas PC implementadas pela AC Imprensa Oficial SP.

2.1.1. OBRIGAÇÕES DA AC

As obrigações da AC Imprensa Oficial SP são:

- 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 subsequente ao seu;
- h) informar a emissão do certificado ao respectivo solicitante;
- i) revogar os certificados emitidos;
- j) emitir, gerenciar e publicar sua LCR e quando aplicável, disponibilizar consulta *online* de situação do certificado (*OCSP Online Certificate Status Protocol*);
- k) publicar em sua página web esta DPC da AC 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, PC e Política de Segurança 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 anualmente 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 ACs de nível subsequente 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) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos;
- w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;

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

As obrigações das AR vinculadas à AC Imprensa Oficial SP são:

- 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 utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];
- 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

As obrigações dos titulares de certificados emitidos pela AC Imprensa Oficial SP são:

- a) fornecer, de modo completo e preciso, todas as informações necessárias para a 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 DPCe 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) apresentação dos originais e fornecimento de cópias autênticas dos documentos que forem exigidos para emissão do certificado;
- g) 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;

- h) 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.

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. Constituem direitos 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:
 - i. não constar da LCR da AC Imprensa Oficial SP;
 - ii. não estiver expirado;
 - iii. puder ser verificado através de certificado válido da AC Imprensa Oficial SP.

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

2.1.5. OBRIGAÇÕES DO REPOSITÓRIO

As obrigações do repositório da AC Imprensa Oficial SP são:

- 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;
- 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

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 da sua cadeia de certificação: ACs subordinadas, AR e PSS.

2.2.2. RESPONSABILIDADES DAS AR

As ARs são 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 as ACs e ARs a ela vinculadas apenas pelos prejuízos a que der causa com a prática de ato ilícito, nos termos da legislação vigente.

Essa terceira parte deverá indenizar a AC Imprensa Oficial SP e/ou os titulares dos seus certificados pelos danos a que der causa na decorrência de omissão ou ação não conforme com a legislação aplicável.

2.3.2. RELAÇÕES FIDUCIÁRIAS

A AC Imprensa Oficial SP ou sua AR vinculada indeniza integralmente os prejuízos que, comprovadamente, der causa, quando o Titular do Certificado for pessoa jurídica.

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 ACs e 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 solicitar à AC Imprensa Oficial SP 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;
- c) nos casos de erro na transcrição, o titular do certificado não pode requerer qualquer indenização quando houver aceito 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. Caso uma ou mais disposições desta DPC venha a ser, por qualquer razão, considerada inválida, ilegal, ou não aplicável por lei, tal não afeta as demais disposições, sendo esta DPC interpretada como se não contivesse tal disposição e, na medida do possível, interpretada para manter a intenção original da DPC.

Nesse caso, serão tomadas de imediato as medidas necessárias para adequar esta 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, e enviado ao endereço eletrônico indicado pelo solicitante no formulário de solicitação.

2.4.3. PROCEDIMENTOS DA SOLUÇÃO DE DISPUTA

2.4.3.1. Em caso de conflito entre esta DPC e outras declarações, políticas, planos, acordos, contratos ou outros documentos que a AC 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 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

Pela emissão e renovação do certificado será cobrado o valor estabelecido contratualmente.

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

Pela revogação ou acesso à informação de status do certificado será cobrado o valor estabelecido contratualmente.

2.5.4. TARIFAS PARA OUTROS SERVIÇOS

Pelos demais serviços será cobrado o valor estabelecido contratualmente.

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

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://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/>), 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 vírgula 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://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/>):

- a) seu 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;
- f) uma relação, regularmente atualizada, dos PSS vinculados.

2.6.2. FREQUÊNCIA DE PUBLICAÇÃO

A AC Imprensa Oficial SP atualiza as informações descritas no item anterior logo que sejam geradas, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

Os certificados são publicados após emissão.

A LCR é publicada de acordo com o disposto no item 4.4.9.

2.6.3. CONTROLES DE ACESSO

Não há qualquer restrição ao acesso para consulta às informações descritas no item 2.6.1 desta DPC.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não-autorizado.

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, através de protocolo http, e pode ser encontrado em: <http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/>

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

2.6.4.1. A AC Imprensa Oficial SP disponibiliza o seguinte repositório para distribuição de LCR:

- <http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/ACIMESPSPG4.crl>

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 ICP-BRASIL [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 ICP-BRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5. As entidades da ICP-Brasil diretamente vinculadas à AC Imprensa Oficial SP – AC subordinadas, AR vinculadas 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 da sua inteira responsabilidade.

2.8.1.2. Os responsáveis pelo uso de certificados da AC subsequente têm as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevida dessas mesmas chaves.

2.8.1.3. Não se aplica.

2.8.2. TIPOS DE INFORMAÇÕES SIGILOSAS

2.8.2.1. Como princípio geral, todos os documentos, informações ou registros fornecidos à AC ou às AR são sigilosos.

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

Não são consideradas informações sigilosas:

- a) os certificados e LCR emitidos pela AC Imprensa Oficial SP;

- b) informações corporativas ou pessoais que constem no certificados ou em diretórios públicos;
- c) esta DPC;
- d) versões públicas de Políticas de Segurança;
- e) resultados finais de auditorias.

A AC Imprensa Oficial SP e AR a ela vinculadas 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 do 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 justifiquem 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, pelo menos, através da emissão de LCR, nos termos descritos nesta DPC.

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, todos os 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 o requerer, através de instrumento devidamente constituído, estiver corretamente identificada e autorizada para o fazer.

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 dos seus registros.

2.8.7.2. Qualquer liberação de informação pela AC Imprensa Oficial SP ou AR vinculada somente será permitida mediante autorização formal do titular do certificado. Os pedidos de liberação deverão ser feitos por meio eletrônico, contendo assinatura válida garantida por certificado do mesmo tipo ou superior emitido na ICP-Brasil, ou por solicitação escrita, com firma reconhecida.

Nenhuma liberação de informação é permitida sem autorização, 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 emissão do certificado não implica a transferência, cessão ou licença de direitos de propriedade intelectual de softwares, certificados, políticas, especificações de práticas e procedimentos, nomes, chaves criptográficas e outros da AC Imprensa Oficial SP ou de AR vinculadas para o solicitante.

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 detalhe os requisitos e procedimentos utilizados pelas AR vinculadas à 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 descritos nos itens 3.1.9, 3.1.10 e 3.1.11:
 - i. confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados constam na documentação e/ou biometria 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 e/ou biometria 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 e com prazo de validade de até 90 (noventa) dias. O responsável pela utilização do certificado digital de pessoa jurídica deve comparecer presencialmente, vedada qualquer espécie de procuração para tal fim;
 - 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;
- 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 e/ou biometria 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, desde que utilizado ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado são registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC Imprensa Oficial SP, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. 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 e/ou organização. Tais cópias são mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

3.1.1.4.1. Não se aplica.

3.1.1.5. Não se aplica.

3.1.1.6. Não se aplica.

3.1.1.7. Não se aplica.

3.1.1.8. 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 subsequente 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 inequivocadamente 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

Esta DPC estabelece que identificadores do tipo "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado emitido pela AC Imprensa Oficial SP.

Para assegurar a unicidade do campo DN podem ser incluídos números ou letras adicionais ao nome de cada titular.

3.1.6. PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES

A AC Imprensa Oficial SP 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. O descrito no RFC 2510 é utilizado como referência para essa finalidade. O método de verificação utilizado é – *Proof of Possession (POP) of Private Key* – conforme o item 2.3 do documento referido.

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 e pelo processo de identificação biométrica ICP-Brasil.

3.1.9.1. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO

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

- a) Cédula de Identidade ou Passaporte, se brasileiro;
- b) Registro Nacional de Estrangeiro – RNE, 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;
- f) Ata ou Procuração conferindo poderes ao responsável, quando aplicável;
- g) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11]; e
- h) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11].

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.

É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

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

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 ICP-BRASIL [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.

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.

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. Sendo o titular do certificado uma pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada correspondente.

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;
- 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 deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

- a) Relativos à sua habilitação jurídica:
 - i. ato constitutivo, devidamente registrado no órgão competente;
 - ii. Decreto ou Lei de Criação ou Lei Orgânica do Órgão (somente para Empresas Públicas);
 - iii. documentos da eleição de seus administradores, quando aplicável;
- 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.

3.1.12. AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTO PARA CERTIFICADO CF-E-SAT

Não se aplica.

3.2. GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

3.2.1. Esta DPC estabelece 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. Este processo 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 subsequente ao da AC Imprensa Oficial SP, a AC subsequente 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. A solicitação de emissão de um Certificado Digital é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR vinculada. Todas as referências a formulário deverão ser entendidas também como referências a outras formas que a AC Imprensa Oficial SP ou AR vinculada possa vir a adotar.

Os procedimentos de solicitação incluem a assinatura de um contrato que estabelece os termos e condições de uso do certificado, bem como o fornecimento de todos os dados obrigatórios que permitam a comprovação dos atributos de identificação.

4.1.2. A solicitação de certificado para AC de nível imediatamente subsequente à 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 Subsequente 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].

4.2. 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 cópia do certificado é entregue ao representante da AC.

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 aceita-o caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o responsável pelo certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

- concorda com as responsabilidades, obrigações e deveres previstos nesta DPC;
- garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;
- afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.3.2. A aceitação do certificado de uma AC subsequente 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 do seu certificado a qualquer tempo e independentemente de qualquer circunstância.

4.4.1.2. O certificado é obrigatoriamente revogado:

- a) quando for 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 da sua mídia armazenadora; 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) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- d) pela AC Imprensa Oficial SP;
- e) pela AR que tiver recebido a solicitação;
- f) por determinação do CG da ICP-Brasil ou da AC Raiz;
- g) Não se aplica;
- h) Não se aplica.

4.4.3. PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.4.3.1. É necessária uma solicitação de revogação para que AR responsável inicie o processo de revogação.

As instruções para a solicitação de revogação do Certificado são obtidas em página web disponibilizada pela AC Imprensa Oficial SP ou pela AR Responsável.

A revogação é realizada através de formulário contendo o motivo da solicitação de revogação e mediante o fornecimento de dados indicados na solicitação de emissão do certificado, ou por formulário assinado pelo titular na falta desses dados.

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 final de revogação de um certificado termina com a geração e a publicação da LCR que contenha o certificado revogado e com a atualização do estado do certificado em resposta OCSP à base de dados da AC Imprensa Oficial SP, quando aplicável.

4.4.3.3. O prazo máximo para conclusão do processo de revogação do certificado pela AC Imprensa Oficial SP, após a conclusão do processo de aceitação e registro da solicitação de revogação é de 12 (doze) horas.

4.4.3.4. O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC, 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 entre a solicitação da sua revogação e a emissão da LCR correspondente.

4.4.3.6. Não se aplica.

4.4.4. PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.4.4.1. A solicitação de revogação deve 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, 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. FREQUÊNCIA DE EMISSÃO DE LCR

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

4.4.9.2. Não se aplica.

4.4.9.3. A frequência 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 subsequente 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 subsequente 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. É também obrigatória a verificação da autenticidade da LCR, por meio da verificação 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 deverão ser registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.4.15.2. A perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de chave pode ainda ser comunicado diretamente à 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

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 com a 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 (logout);
- 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 subsequentes;
- h) emissão e revogação de certificados;
- i) geração de LCR;
- j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
- k) operações 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) 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 em local único, de forma estruturada para facilitar o acesso e consulta nos processos de auditoria, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

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

4.5.1.7. A AC Imprensa Oficial SP define, em documento disponível nas auditorias de conformidade, o local de arquivo das cópias dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados e do termo de titularidade.

4.5.2. FREQUÊNCIA DE AUDITORIA DE REGISTROS (LOGS)

A periodicidade máxima 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, subsequentemente, 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 utilizados.

4.5.4.2. As 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 esses 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, efetuadas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas.

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 pelo seu pessoal operacional e/ou pelos 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. As 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;
- 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 são retidos 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;
- c) as demais informações, inclusive os arquivos de auditoria, são retidas por 7 (sete) 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 no site *Disaster Recovery*, 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

As informações de data e hora nos registros baseiam-se no horário Greenwich Mean Time.

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 nos 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 subsequente utilizando o mesmo procedimento utilizado para emissão do certificado inicial.

A AC Imprensa Oficial SP envia uma comunicação ao titular do certificado com 13 (treze) meses de antecedência da data de expiração do mesmo, juntamente com instruções para a solicitação de um novo certificado.

A comunicação de expiração, juntamente com as instruções para a solicitação de um novo certificado é realizada através de correio eletrônico enviado ao titular do certificado.

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 Administrador de Segurança da AC Imprensa Oficial SP, que decreta o início da fase de resposta.

Nessa fase, é realizada uma rigorosa inspeção para verificar a veracidade do fato e as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação.

Caso haja necessidade, o administrador de Segurança decretará a contingência respectiva.

4.8.2. CERTIFICADO DE ENTIDADE É REVOGADO

Em caso de revogação do certificado da AC Imprensa Oficial SP o Administrador de Segurança, juntamente com o Administrador PKI da AC Imprensa Oficial SP, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados.

A AC Imprensa Oficial SP gerará novo par de chaves da AC Imprensa Oficial SP, e logo que tenha sido emitido o certificado associado ao novo par de chaves gerado, 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 Administrador de Segurança que, juntamente com o Administrador PKI 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 a AC Imprensa Oficial SP, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados.

A AC Imprensa Oficial SP gerará novo par de chaves da AC Imprensa Oficial SP, e logo que tenha sido emitido o certificado associado ao novo par de chaves gerado, a AC Imprensa Oficial SP emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

4.8.4. SEGURANÇA DOS RECURSOS APÓS DESASTRE NATURAL OU DE OUTRA NATUREZA

Em caso de desastre natural ou de outra natureza, é notificado o Administrador de Segurança, que decreta o início da fase de resposta.

Nessa fase, é realizada uma rigorosa inspeção para verificar as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação.

Caso haja necessidade, as atividades são transferidas para o site de *Disaster Recovery*.

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 falha de equipamentos, 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. Em caso de extinção da AC Imprensa Oficial SP, AR Vinculada ou PSS serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.9.2. Os procedimentos incluem, mas não estão limitados à divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, aplicativos dedicados à certificação digital, guarda de bases de dados e registros observará os mesmos requisitos de segurança exigidos pela AC Imprensa Oficial SP.

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. Na construção das instalações da AC Imprensa Oficial SP foram considerados, entre outros, os seguintes aspectos relevantes para os controles de segurança física:

- a) 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;
- b) Instalações para sistemas de telecomunicações;
- c) Sistemas de aterramento e de proteção contra descargas atmosféricas;
- d) Iluminação de emergência.

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 das 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 e a disponibilidade à resposta a consulta OCSP. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver sendo ocupado.

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, gases 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, existe 1 (um) ambiente de quarto nível para abrigar e segregar:

- a) equipamentos de produção on-line;
- b) equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores;
- c) equipamentos de produção off-line e cofre de armazenamento.

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos estão armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre obedece às seguintes especificações:

- a) confeccionado em aço;
- b) possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) consiste em pequenos depósitos localizados no interior do cofre de 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 câmaras 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 câmaras 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 câmara 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 no ambiente de nível 4.

5.1.2.4. MECANISMOS DE EMERGÊNCIA

5.1.2.4.1. Mecanismos específicos foram 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 infraestrutura 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 anomalias.

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, 1 (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 fisicamente destruídos.

5.1.8. INSTALAÇÕES DE SEGURANÇA (BACKUP) EXTERNAS (OFF-SITE)

As instalações de backup (*Disaster Recovery*) atendem os requisitos mínimos estabelecidos por este documento. A 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 diferentes perfis para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

O detalhe dos perfis encontra-se em documento interno normativo.

5.2.1.3. Os operadores do sistema de certificação da AC Imprensa Oficial SP recebem formação específica antes de obter qualquer tipo de acesso ao sistema. O tipo e o nível de acesso estão determinados, em documento formal, 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 seus funcionários. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o funcionário devolve à AC Imprensa Oficial SP no ato de seu desligamento.

5.2.2. NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA

5.2.2.1. É requerido um controle multiusuário 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 está 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 a 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;
- 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;
- c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC Imprensa Oficial SP implementa um padrão de utilização de "senhas fortes", definido na Política de Segurança implementada e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], 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], e na Política de Segurança implementada.

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) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. FREQUÊNCIA 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. FREQUÊNCIA E SEQUÊNCIA 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) 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;
- 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] e na Política de Segurança implementada.

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] e a sua Política de Segurança;
- c) documentação operacional relativa às suas atividades;
- d) contratos, normas e políticas relevantes para as 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 deferido o seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

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

A geração do par de chaves de AC 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 à AC Raiz em formato PKCS #10. Essa entrega é realizada por representante legal constituído da AC Imprensa Oficial SP, em cerimônia específica, em data e hora previamente estabelecida.

6.1.3.2. A chave pública de uma AC Subsequente é entregue ao representante legal da AC Subsequente pela AC Imprensa Oficial SP de acordo com procedimentos internamente definidos. 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, de entre outras, através do seu diretório.

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 Subsequentes é de 4096 bits.

6.1.6. GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS

Os parâmetros de geração de chaves assimétricas da AC Imprensa Oficial 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 das AC subsequentes são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão definido no 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.509V3)

6.1.9.1. A chave privada das AC Subsequentes 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 da 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 das suas chaves privadas. Controles Lógico e Procedimental estão descritos no item 5.2. Controle de acesso físico está descrito no item 5.1.2.

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

6.2.1.2. Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS 140-1 ou FIPS 140-2, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9] ou outro de conteúdo semelhante a um destes.

6.2.2. CONTROLE “N DE M” PARA CHAVE PRIVADA

6.2.2.1. A AC Imprensa Oficial SP exige controle múltiplo do tipo “n de m” para utilização da sua chave privada.

6.2.2.2. É necessária a presença de pelo menos 2 (dois) de um grupo de 4 (quatro) 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 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. A AC Imprensa Oficial SP não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

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 Administrador PKI, implementando-se o controle “n de m”, conforme item 6.2.2 anterior. A identidade dos intervenientes é verificada por guarda armado.

6.2.8. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

A desativação das chaves privadas das AC Imprensa Oficial SP é coordenada pelo seu Administrador PKI, implementando-se o controle “n de m”, conforme item 6.2.2 anterior. A identidade dos intervenientes é verificada por guarda armado.

6.2.9. MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

A destruição das chaves privadas das AC Imprensa Oficial SP é coordenada pelo seu Administrador PKI, implementando-se o controle “n de m”, conforme item 6.2.2 anterior. A identidade dos intervenientes é verificada por guarda armado.

As mídias de armazenamento das chaves privadas são reinicializadas de forma a não restarem nelas informações sensíveis.

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 Subsequentes por ela emitidos, bem como as LCR emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

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 Subsequentes 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. A validade admitida para certificados de AC 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 dos equipamentos criptográficos que armazenam 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 de nível 4. O ambiente computacional é mantido off-line de modo a impedir o acesso remoto não autorizado.

6.5.1.2. A geração do par de chaves das AC subsequentes é realizada em ambiente próprio. O ambiente computacional é mantido off-line de modo a 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 das 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;
- 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 controlados. 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. A AC Imprensa Oficial SP implementa 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 correspondem, no mínimo, aos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA

6.6.1.1. A AC Imprensa Oficial SP utiliza preferencialmente sistemas e tecnologias certificadas. Quaisquer desenvolvimentos e/ou customizações são realizadas em ambiente de desenvolvimento/homologação antes da sua passagem a produção.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC Imprensa Oficial SP provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC Imprensa Oficial SP.

6.6.2. CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.6.2.1. A AC Imprensa Oficial SP e ARs vinculadas utilizam ferramentas e procedimentos formais para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

6.6.2.2. A AC Imprensa Oficial SP utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação da AC Imprensa Oficial SP.

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 são verificadas 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 infraestrutura e proteção de rede, tais como *routers*, *hubs*, *switches*, *firewalls* e sistemas de detecção de invasão (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 infraestrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os *routers* 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. Os 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 INVASÃO (IDS)

6.7.3.1. O sistema de detecção de invasão 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 invasão 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 invasão 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 *routers*, *firewalls* ou *IDS* – são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. 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 seguintes itens desta DPC 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

Os certificados 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

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

- a) "Authority Key Identifier", 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, contém:
 - o OID desta DPC: 2.16.76.1.1.26;
 - e o endereço web onde se encontra publicada:
http://icpbr.imprensaoficial.com.br/repositorio/media/files/Repositorio/ACP/dpc_-_imesp.pdf ;
http://io-com-icpbr.imprensaoficial.com.br/repositorio/media/files/Repositorio/ACP/dpc_-_imesp.pdf ;
http://io-com-icpbr.imprensaoficial.com.br/repositorio/media/files/Repositorio/ACP/dpc_-_imesp.pdf ;"CRL Distribution Points", não crítica: contém os endereços Web onde se obtém a LCR correspondente:

Para certificados emitidos na G1:

- <http://icp-brasil.certisign.com.br/repositorio/lcr/ACImprensaOficialSPPrincipal/LatestCRL.crl>

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>

Para certificados emitidos na G4:

- <http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSP/ACIMESPSPG4.crl>

- e) "Basic Constraints", crítica: deve conter o campo cA=True;

7.2.3. IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC Imprensa Oficial SP são assinados utilizando o algoritmo criptográfico admitido no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [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:

- C** = BR
- O** = ICP-Brasil
- OU** = <Razão social da AC subsequente>
- CN** = <Nome da AC subsequente>

7.2.5. RESTRIÇÕES DE NOME

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC Imprensa Oficial SP são as seguintes:

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Os acentos devem ser substituídos pelo caractere não acentuado;
- O "ç" deve ser substituído pelo caractere 'c';
- Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
branco	20
!	21
"	22
#	23
\$	24
%	25
&	26
'	27
(28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40

\	5C
---	----

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"

Não se aplica.

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://io-com-icpbr.imprensaoficial.com.br/repositorio/media/files/Repositorio/ACP/dpc_-_imesp.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 a sua criticidade.

7.3.2.2. A ICP-Brasil define como obrigatórias, e são implementadas pela AC Imprensa Oficial SP, as seguintes extensões de LCR:

1. "*Authority Key Identifier*": contém o hash SHA-1 da chave pública da AC Imprensa Oficial SP.
 - a) "*CRL Number*", não crítica: contém um número sequencial para cada LCR emitida pela AC Imprensa Oficial SP.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Qualquer alteração nesta DPC é submetida à aprovação do CG da ICP-Brasil.

8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

A AC Imprensa Oficial SP mantém disponível em repositório, para consulta pública, esta DPC
(http://io-com-icpbr.imprensaoficial.com.br/repositorio/media/files/Repositorio/ACP/dpc_-_imesp.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].

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 CREDENCIAMENTO DAS 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
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICPBRASIL	DOC-ICP-05.02
[11]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	DOC-ICP-05.03

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.B