IMPRENSA OFICIAL DO ESTADO SA IMESP (AC IMPRENSA OFICIAL SSL)

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

VERSÃO 1.1 – 25/02/2019

HISTÓRICO DE VERSÕES

Data	*Versão*	*Observações*
15/12/2016	1.0	Redação Inicial
25/02/2019	1.1	Revisão

AVISO LEGAL

CONTEÚDO

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 Imprensa Oficial para a emissão de certificados de Servidor (AC Imprensa Oficial SSL), 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 SSL ou entidades a ela vinculadas possa vir a adotar.

1.1.3. A AC Imprensa Oficial SSL está certificada em nível imediatamente subsequente ao da Autoridade Certificadora Principal da Imprensa Oficial (AC Imprensa Oficial SP) certificada pela AC Raiz da ICP-Brasil. O certificado da AC Imprensa Oficial SSL contém a chave pública correspondente à sua chave privada, utilizada para assinar os certificados de assinatura A1, A3 e A4 e para assinar a sua Lista de Certificados Revogados (LCR).

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

1.2. IDENTIFICAÇÃO

Este documento é designado Declaração de Práticas de Certificação da Autoridade Certificadora Imprensa Oficial para a emissão de certificados de Servidor e referida a seguir como "DPC da AC Imprensa Oficial SSL".

Este documento é identificado pela seguinte informação:

INFORMAÇÃO DO DOCUMENTO	
Versão/Edição	1.1
Data de Aprovação	25/02/2019
Data de Validade	Não aplicável
OID	2.16.76.1.1.119
Localização	http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/

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 SSL".

1.3.2. AUTORIDADES DE REGISTRO

1.3.2.1. A Autoridade de Registo (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 SSL estão relacionadas em (URL): http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/

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 SSL, com respectiva data do descredenciamento;
e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC Imprensa Oficial SSL 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 SSL e/ou por intermédio das suas ARs é publicada em http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/

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 SSL mantém as informações acima sempre atualizadas.

1.3.4. TITULARES DE CERTIFICADO

As pessoas físicas ou jurídicas de direito público ou privado, nacionais ou internacionais, que atendam aos requisitos desta DPC e das PC aplicáveis podem ser Titulares de Certificado, para uso por pessoas físicas, pessoas jurídicas, em equipamentos ou aplicações.

1.3.5. APLICABILIDADE

A AC Imprensa Oficial SSL implementa as seguintes Políticas de Certificado Digital:

Para Certificados de Assinatura Digital:

Política de Certificado	Nome	OID
Política de Certificado de Assinatura Digital Tipo A1 da AC Imprensa Oficial SSL	PC A1 da AC Imprensa Oficial SSL	2.16.76.1.2.1.211
Política de Certificado de Assinatura Digital Tipo A3 da AC Imprensa Oficial SSL	PC A3 da AC Imprensa Oficial SSL	2.16.76.1.2.3.209
Política de Certificado de Assinatura Digital Tipo A4 da AC Imprensa Oficial SSL	PC A4 da AC Imprensa Oficial SSL	2.16.76.1.2.4.42

Nas PC correspondentes estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC Imprensa Oficial SSL e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

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: Certificação Digital
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 SSL.

2.1.1. OBRIGAÇÕES DA AC

As obrigações da AC Imprensa Oficial SSL são:

a) operar de acordo com esta DPC e com as PC que implementa;
b) gerar e gerenciar seus pares de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar a AC Imprensa Oficial SP, 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 SSL, 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 AR vinculadas e de usuários finais;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados emitidos;
j) emitir, gerenciar e publicar sua LCR e quando aplicável, disponibilizar consulta *online* de situação do certificado (OCSP *Online Certificate Status Protocol*);
k) publicar em sua página web esta DPC da AC Imprensa Oficial SSL e as PC que implementa;
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 registar 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 registo, com cobertura suficiente e compatível com o risco dessas atividades;
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 SSL;
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 auditorar as AR vinculadas e os prestadores de serviço que lhe sejam vinculados, em conformidade com as políticas, normas e procedimentos da ICP-Brasil; e
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 SSL 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 SSL 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 SSL 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 SSL 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 SSL e às PC aplicáveis, bem como respeitar a legislação aplicável, incluindo as regras definidas pelo CG da ICP-Brasil;
m) notificar os titulares, com antecedência mínima de 30 (trinta) dias, a expiração da validade dos certificados.

2.1.3. OBRIGAÇÕES DO TITULAR DO CERTIFICADO

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

n) fornecer, de modo completo e preciso, todas as informações necessárias para a sua identificação;
o) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
p) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
q) conhecer os seus direitos e obrigações contemplados por esta DPC, pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;
r) informar à AC Imprensa Oficial SSL o comprometimento ou suspeita de comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
s) apresentação dos originais e fornecimento de cópias autênticas dos documentos que forem exigidos para emissão do certificado;
t) verificar, no momento da aceitação do certificado, a veracidade e exatidão das informações contidas no seu certificado e notificar a AC Imprensa Oficial SSL, solicitando a imediata revogação do certificado que contiver inexatidões ou erros;
u) obedecer estritamente a esta DPC da AC Imprensa Oficial SSL e às PC aplicáveis, 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 SSL e AR;
v) assumir a responsabilidade pelo custo do processo de emissão do certificado;
w) no caso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, estas obrigações aplicam-se ao responsável pelo uso do certificado.

2.1.4. DIREITOS DA TERCEIRA PARTE (*RELYING PARTY*)

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

2.1.4.2. Constituem direitos da terceira parte:

a) recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;

b) verificar, a qualquer tempo, a validade do certificado. Um certificado emitido pela AC Imprensa Oficial SSL é considerado válido quando:
   i. não constar da LCR da AC Imprensa Oficial SSL;
   ii. não estiver expirado;
   iii. puder ser verificado através de certificado válido da AC Imprensa Oficial SSL.

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

2.1.5. OBRIGAÇÕES DO REPOSITÓRIO

As obrigações do repositório da AC Imprensa Oficial SSL são:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC Imprensa Oficial SSL e sua LCR;
b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
c) implementar os recursos necessários para a segurança dos dados nele armazenados; e
d) disponibilizar verificação on-line do status do certificado ou outro mecanismo de atualização de status aprovado pela ICP-Brasil, quando aplicável por força de contratação específica.

2.2. RESPONSABILIDADES

2.2.1. RESPONSABILIDADES DA AC

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

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

2.2.1.3. Não se aplica.

2.2.1.4. Não se aplica.

2.2.2. RESPONSABILIDADES DAS AR

A AR é responsável pelos danos a que der causa.

2.3. RESPONSABILIDADE FINANCEIRA

2.3.1. INDENIZAÇÕES DEVIDAS PELA TERCEIRA PARTE (*RELYING PARTY*)

A terceira parte responde perante a AC Imprensa Oficial SSL e ARs 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 SSL 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 SSL ou sua AR vinculada indeniza integralmente os prejuízos que, comprovadamente, der causa, quando o Titular do Certificado for pessoa física.

Caso o Titular do Certificado seja pessoa jurídica, a política de indenizações da AC Imprensa Oficial SSL e de suas AR vinculadas pelos danos a que, comprovadamente, derem causa, prevê o pagamento de indenização correspondente a 20 (vinte) vezes o valor do certificado, ou a R$ 40.000,00 (quarenta mil reais), o que for menor.

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

2.3.3. PROCESSOS ADMINISTRATIVOS

O titular do certificado que sofrer perdas e danos decorrentes do uso do certificado digital emitido pela AC Imprensa Oficial SSL tem o direito de solicitar à AC Imprensa Oficial SSL 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 SSL, 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 SSL ou à AR vinculada;

c) nos casos de erro na transcrição, o titular do certificado não pode requerer qualquer indenização quando houver aceitado o certificado.

2.4. INTERPRETAÇÃO E EXECUÇÃO

2.4.1. LEGISLAÇÃO

Esta DPC é regida pela Medida Provisória nº 2.200-02, pelas Resoluções do Comitê Gestor da ICP-Brasil e da Secretaria da Receita Federal do 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, ou por escrito e entregue à AC Imprensa Oficial SSL.

2.4.3. PROCEDIMENTOS DA SOLUÇÃO DE DISPUTA

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

2.4.3.2. Esta DPC da AC Imprensa Oficial SSL 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

Em caso de revogação do certificado por motivo de comprometimento da chave privada ou da mídia armazenadora da chave privada da AC Imprensa Oficial SSL, ou ainda quando constatada a emissão imprópria ou defeituosa imputável à AC Imprensa Oficial SSL, será emitido gratuitamente outro certificado em substituição.

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 SSL (http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/), obedecendo as regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC Imprensa Oficial SSL em serviço de diretório e/ou página web é de 99,5% (noventa e nove virgulo cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2. As seguintes informações são publicadas em serviço de diretório e/ou em página web da AC Imprensa Oficial SSL (http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/):

a) seu próprio certificado;
b) suas LCR;
c) esta DPC;
d) as PC que implementa;

e) uma relação, regularmente atualizada, contendo as AR vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;
f) 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;
g) uma relação, regularmente atualizada, dos PSS vinculados.

2.6.2. FREQUÊNCIA DE PUBLICAÇÃO

A AC Imprensa Oficial SSL atualiza as informações descritas no item anterior logo que sejam geradas, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos. As versões ou alterações desta DPC e das PC, assim como os endereços das Instalações Técnicas das AR vinculadas, são atualizadas no repositório da AC Imprensa Oficial SSL, somente após aprovação da AC Raiz da ICP-Brasil.

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 SSL 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/IMESPSSL/.

Somente a AC Imprensa Oficial SSL, 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 SSL disponibiliza 03 (três) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR:

- http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/ACIMESPSSL.crl
- http://www.digitaltrust.com.br/repositorio/IMESPSSL/ACIMESPSSL.crl
- http://repositorio.icpbrasil.gov.br/lcr/IMESP/ACIMESPSSL.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 e com os princípios e critérios definidos pelo WebTrust.

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 SSL 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 a AC Imprensa Oficial SSL – AR e PSS, também receberam auditoria prévia, para fins de credenciamento, e a AC Imprensa Oficial SSL 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 SSL 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 titulares (ou os responsáveis no caso de pessoa jurídica) dos certificados de assinatura emitidos pela AC Imprensa Oficial SSL são responsáveis pela 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 registo fornecido pelos titulares de certificado à AC Imprensa Oficial SSL 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 SSL;
b) informações corporativas ou pessoais que constem nos certificados ou em diretórios públicos;
c) as PC implementadas pela AC;
d) esta DPC;
e) versões públicas de Políticas de Segurança;
f) resultados finais de auditorias; e
g) Termo de Titularidade ou solicitação de emissão do certificado.

A AC Imprensa Oficial SSL e AR a ela vinculada tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

a) estejam na posse legítima da AC Imprensa Oficial SSL 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 SSL 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 SSL 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 SSL 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 SSL 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 registo sob a guarda da AC Imprensa Oficial SSL 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 ou 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 SSL 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 será permitida sem autorização em uma das formas supracitadas, 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 SSL 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 SSL 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 individuo: 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 apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como responsável pelo uso do certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP-Brasil 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 da documentação apresentada na etapa de validação;
   iv. antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.1.1.2. Excepcionalmente, o processo de validação poderá ser realizado fora do ambiente físico da AR, através de procedimento de validação externa, mediante o deslocamento do Agente de Registro da AR até o interessado na obtenção do certificado, observadas as hipóteses, a forma e as condições abaixo dispostas, vedada a criação de instalações físicas destinadas a tal fim, qualquer que seja a denominação utilizada, tais como, mas não limitada a, ponto de atendimento, posto de validação, parceiro, canal, agente credenciado ou agência autorizada.

3.1.1.2.1 As AR poderão adotar o procedimento de validação externa nas seguintes hipóteses:

i. Para pessoas com deficiência ou com mobilidade reduzida, conforme definido pela Lei nº 13.146, de 6 de julho de 2015, devidamente comprovado por documento hábil;
ii. Para pessoas Politicamente Expostas – PEP, conforme definido na Resolução nº 16, de 28 de março de 2007, do Conselho de Controle de Atividades Financeiras COAF/MF, devidamente comprovado por documento hábil;
iii. Para pessoas que se encontrem cumprindo pena ou detidas em estabelecimento prisional;
iv. Para pessoas com incapacidade física momentânea ou por motivo de saúde, em qualquer caso devidamente justificado e comprovado por documento hábil, estejam impedidas ou impossibilitadas de se deslocar até a instalação física da AR;
v. Para atender contratos firmados com entidades públicas cujos os editais de licitação tenham sido publicados até a data de publicação desta Resolução;
vi. Outras pessoas não citadas anteriormente, mediante solicitação expressa de validação externa pelo titular do certificado, limitado a 15% (quinze por cento) do total de certificados emitidos pela AR no mês imediatamente anterior.

Nota 1: O disposto na alínea VI, aplica-se a partir do mês subsequente à entrada em operação da AR, vedada a validação externa com base no referido dispositivo, no mês do início de sua operação.

Nota 2: Considera-se como total de certificados emitidos pela AR no mês imediatamente anterior, para fins da alínea VI, o volume de certificados

emitidos pela AR, informado na documentação encaminhada ao ITI na forma e no prazo previsto pela Instrução Normativa no 14, de 28 de novembro de 2016.

Nota 3: Acaso a AR não tenha emitido certificados no mês anterior ou não tenham sido prestadas as informações na forma ou no prazo exigidos, ficará a AR impossibilitada de emitir novos certificados com fulcro na alínea VI, somente podendo voltar a emiti-los no mês imediatamente subsequente, desde que prestadas as informações de forma tempestiva.

Nota 4: Para o cálculo da quantidade limite disposto na alínea VI, em caso de resultado fracionário, admitir-se-á o arredondamento para a unidade superior.

3.1.1.2.2. A validação externa será realizada no domicílio do titular do certificado digital, nas hipóteses previstas nos incisos I, II e IV, do item 3.1.1.2.1, ou no local que este se encontre, na hipótese do inc. III, do mesmo item.

3.1.1.2.3. Para fins do item anterior, considera-se domicílio do titular do certificado digital, o seu domicílio civil, na forma do disposto no Código Civil, Lei nº 10.406, de 10 de janeiro de 2002.

3.1.1.2.4. O local no qual a validação externa será realizada deverá ser informado no Formulário de Validação Externa, a que se refere a alínea "d" do item 3.1.1.2.5.

3.1.1.2.5. A validação fora do ambiente físico da AR deve atender ainda as seguintes condições:

a) utilizar ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR;
b) adotar aplicativo de georreferenciamento que permita rastrear o computador móvel utilizado na validação externa, sendo que a localização do equipamento deve ficar disponível no sistema da AR em que o agente de registro deva estar cadastrado previamente;
c) adotar equipamentos de coleta e verificação biométrica do titular e do agente de registro, em atendimento aos padrões da ICP-Brasil;
d) preencher o Formulário de Validação Externa, adendo ADE-ICP-05.D, o qual deverá ser assinado pelo agente de registro e pelo titular do certificado, preferencialmente assinados digitalmente;
e) em se tratando de dossiês físicos do titular de certificado, esses devem ser enviados para a Instalação Técnica em até 5 (cinco) dias úteis; e
f) utilização de equipamento específico, destinado exclusivamente para fins de validação externa, vedada a utilização, para tal fim, das estações de trabalho ou outros equipamentos empregados na instalação técnica.

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 SSL, 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. A AC Imprensa Oficial SSL disponibiliza, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

3.1.1.8. Não se aplica.

3.1.1.9. Não se aplica.

3.1.1.10. Não se aplica.

3.1.1.11. 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, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular. O certificado emitido para pessoa jurídica inclui o nome da pessoa física responsável pelo seu uso. Para todos os efeitos legais, os certificados e as respectivas chaves criptográficas são da titularidade do responsável constante do certificado.

3.1.2.2. Não se aplica.

3.1.3. NECESSIDADE DE NOMES SIGNIFICATIVOS

Os certificados emitidos pela AC Imprensa Oficial SSL exigem o uso de nomes significativos que possibilitam determinar inequivocadamente a identidade da pessoa ou 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 SSL.

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 SSL 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 AR 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) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
c) Passaporte, se estrangeiro não domiciliado no Brasil;
d) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial; e

e) mais um documento oficial com fotografia, no caso de certificados de tipos A4.
f) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11].
g) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11].

Nota 1: 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.

Nota 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguer onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

Nota 3: 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.

Nota 4: Para a identificação de indivíduo na emissão de certificado que integra o Documento RIC, deverá ser observado o disposto no item 3.1.1.6.

Nota 5: 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.

Nota 6: 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].

Nota 7: 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.

Nota 8: Para a identificação de indivíduo na emissão de certificado digital para servidor público da ativa e militar da União, deverá ser observado o disposto item 3.1.1.9.

Nota 9: É facultado aos Bancos Múltiplos e Caixa Econômica Federal autorizados a funcionar pelo BACEN, na identificação de titulares pessoa física de conta de depósito, utilizar o procedimento disposto no item 3.1.1.10.

3.1.9.2. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO

3.1.9.2.1. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:

a) nome completo, sem abreviações;
b) data de nascimento.

3.1.9.2.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, pode solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

a) Cadastro de Pessoa Física (CPF);
b) número de Identificação Social NIS (PIS, PASEP ou CI);
c) número do Registro Geral RG do titular e órgão expedidor;
d) número do Cadastro Especifico do INSS (CEI);
e) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;
f) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

3.1.9.2.3. Para tanto, o titular deve apresentar a documentação respectiva, caso a caso, em original. É mantido arquivo com as cópias de todos os documentos utilizados.

Nota 1: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

Nota 2: O cartão CPF pode ser substituído por consulta à página da Receita Federal, sendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.1.10. AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO

3.1.10.1. DISPOSIÇÕES GERAIS

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

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

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

a) apresentação do rol de documentos elencados no item 3.1.10.2;
b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado; e
c) presença física dos representantes legais e do responsável pelo uso do certificado;
d) assinatura do termo de titularidade de que trata o item 4.1.1 pelo titular ou responsável pelo uso do certificado.

NOTA 01: Poderá a AC responsável e as AR a ela vinculada solicitar uma assinatura manuscrita ao titular ou responsável pelo uso do certificado para comparação com o documento de identidade ou contrato social.

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 registado no órgão competente; e
   ii. 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. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

a) Denominação social constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações;
b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
c) Nome completo do responsável pelo certificado, sem abreviações;
d) Data de nascimento do responsável pelo certificado.

3.1.10.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.1.9.2.

3.1.11. AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO OU APLICAÇÃO

3.1.11.1. DISPOSIÇÕES GERAIS

3.1.11.1.1. Tratando-se de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

3.1.11.1.2. Se o titular for pessoa física, deverá ser feita a confirmação da sua identidade na forma do item 3.1.9.1 e esta assinará o termo de titularidade de que trata o item 4.1.1.

3.1.11.1.3. Se o titular for pessoa jurídica, 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 do responsável pelo uso do certificado e assinatura do termo de responsabilidade de que trata o item 4.1.1; e
d) presença física do(s) representante(s) legal(is) da pessoa jurídica e assinatura do termo de titularidade de que trata o item 4.1.1, ou outorga de procuração atribuindo poderes para solicitação de certificado para equipamento ou aplicação e assinatura do respectivo termo de titularidade.

3.1.11.2. PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO OU APLICAÇÃO

3.1.11.2.1. Para certificados de equipamento ou aplicação que utilizem URL no campo *Common Name*, deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele nome. Nesse caso deve ser apresentada documentação comprovativa (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

3.1.11.2.2. Não se aplica.

3.1.11.3. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO OU APLICAÇÃO

3.1.11.3.1. É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nos documentos apresentados:

a) URL ou nome da aplicação;
b) Nome completo do responsável pelo certificado, sem abreviações;
c) Data de nascimento do responsável pelo certificado;
d) Nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviaturas, se o titular for pessoa jurídica;
e) Cadastro Nacional de Pessoa Jurídica (CNPJ), se o titular for pessoa jurídica.

3.1.11.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.1.9.2.

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

Não se aplica.

3.1.13. AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTO PARA CERTIFICADO OM-BR

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 SSL 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 segundo uma das seguintes possibilidades:

a) Adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado; ou
b) A solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva, permitida tal hipótese apenas para os certificados digitais de pessoa física.

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 nas PC implementadas.

3.3.2. Não se aplica.

3.4. SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante.

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 AR vinculada possa vir a adotar.

De entre os requisitos e procedimentos operacionais estabelecidos pela AC Imprensa Oficial SSL para as solicitações de emissão de certificado, estão:

a) a comprovação de atributos de identificação constantes do certificado e o recebimento dos documentos obrigatórios exigidos para identificação dos titulares e responsáveis, conforme disposto no item 3.1;
b) a autenticação do agente de registo responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes a de um certificado de tipo A3; e
c) um termo de titularidade e responsabilidade assinado pelo titular do certificado e pelo responsável pelo uso do certificado, elaborados conforme o documento MODELO DE TERMO DE TITULARIDADE [4].

4.1.2. Não se aplica.

4.1.3. Não se aplica.

4.1.4. Não se aplica.

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.

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

4.3. ACEITAÇÃO DE CERTIFICADO

4.3.1. O titular do certificado ou pessoa física responsável verifica as informações contidas no certificado e aceita-o caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

- concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;

- 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 e do seu conteúdo é declarada, pelo titular do certificado, na primeira utilização da chave privada correspondente. O prazo para aceitação do certificado está definido no item 4.4.4 de cada PC implementada pela AC Imprensa Oficial SSL.

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 em qualquer altura 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 SSL;
d) no caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora;
e) no caso de falecimento do titular, quando pessoa física;
f) no caso de mudança na razão ou denominação social do titular, quando equipamentos, aplicações ou pessoas jurídicas;
g) no caso de extinção, dissolução ou transformação do titular do certificado, quando equipamentos, aplicações ou pessoas jurídicas;
h) no caso de falecimento ou demissão do responsável, quando equipamentos, aplicações ou pessoas jurídicas.

4.4.1.3. A AC Imprensa Oficial SSL revoga, no prazo definido no item 4.4.3, 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 SSL 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, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
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 SSL;
e) Por uma AR vinculada;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz;
g) Não se aplica;
h) Não se aplica;
i) Não se aplica;
j) 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 SSL 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 SSL;
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 SSL, quando aplicável.

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

4.4.3.4. Não se aplica.

4.4.3.5. A AC Imprensa Oficial SSL 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. A frequência para emissão de LCR referentes a certificados de usuários finais é de 1 (uma) hora, podendo ser estendida em casos excepcionais até ao limite estabelecido no item 4.4.9.2.

4.4.9.2. A frequência máxima admitida para a emissão de LCR para os certificados de usuários finais é de 6 (seis) horas.

4.4.9.3. Não se aplica.

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 SSL e do período de validade da LCR.

4.4.11. DISPONIBILIDADE PARA REVOGAÇÃO OU VERIFICAÇÃO DE STATUS ON-LINE

A AC Imprensa Oficial SSL suporta os processos de revogação de certificados de forma online quando aplicável por força de contratação específica.

A AC Imprensa Oficial SSL suporta verificação da situação de estado de certificados de forma online quando aplicável por força de contratação específica.

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

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, através de solicitação de revogação de certificado, à AR responsável 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 deve ser comunicado à AC Imprensa Oficial SSL através do formulário específico para tal fim.

4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

4.5.1. TIPOS DE EVENTOS REGISTRADOS

4.5.1.1. A AC Imprensa Oficial SSL registra em arquivos de auditoria todos os eventos relacionados com a segurança do seu sistema de certificação. Os seguintes eventos são 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 SSL;

c) mudanças na configuração dos sistemas AC Imprensa Oficial SSL ou nas suas chaves;
d) mudanças nas políticas de criação de certificados;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não-autorizadas de acesso aos arquivos do sistema;
g) geração de chaves próprias da AC Imprensa Oficial SSL ou de chaves de seus usuários finais;
h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável;
l) operações de escrita nesse repositório, quando aplicável.

4.5.1.2. A AC Imprensa Oficial SSL 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 SSL 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 SSL é armazenada, eletrônica ou manualmente, 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 SSL registam 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 SSL 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 SSL 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 SSL 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. As ferramentas disponíveis no sistema operacional liberam os acessos lógicos aos registros de auditoria somente a usuários ou aplicações autorizadas, através de permissões dadas pelo administrador do sistema de acordo com a função dos usuários ou aplicações e orientação do departamento de segurança.

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 SSL, 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 SSL 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 SSL 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 SSL, 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 SSL, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. As ações corretivas decorrentes são implementadas pela AC Imprensa Oficial SSL 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 SSL; e
g) informações de auditoria previstas no item 4.5.1.

4.6.2. PERÍODO DE RETENÇÃO PARA ARQUIVO

a) as LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;
b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade são retidos por 10 (dez) anos, a contar da data de expiração ou revogação do certificado.; e
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 SSL estabelece que uma segunda cópia de todo o material arquivado é armazenada no site *Disaster Recovery* da AC Imprensa

Oficial SSL, 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 SSL 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 SSL 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 SSL, 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. O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico, disponibilizado pela AR Responsável, por onde é encaminhado o processo de fornecimento de novo certificado.

A AR que recebeu e validou o pedido de emissão do certificado envia uma comunicação ao titular do certificado 30 (trinta) dias antes 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 SSL 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 SSL, 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 SSL o Administrador de Segurança, juntamente com o Administrador PKI da AC Imprensa Oficial SSL, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados.

A AC Imprensa Oficial SSL gerará novo par de chaves da AC Imprensa Oficial SSL, e logo que tenha sido emitido o certificado associado ao novo par de chaves gerado, a AC Imprensa Oficial SSL 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 SSL, o fato é imediatamente comunicado ao Administrador de Segurança que, juntamente com o Administrador PKI da AC Imprensa Oficial SSL, 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 SSL, 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 SSL, e logo que tenha sido emitido o certificado associado ao novo par de chaves gerado, a AC Imprensa Oficial SSL 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* da AC Imprensa Oficial SSL.

4.8.5. ATIVIDADES DAS AUTORIDADES DE REGISTRO

As AR vinculadas à AC Imprensa Oficial SSL 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 SSL, 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 SSL.

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

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 SSL. Para entrar em uma área de nível 1, cada indivíduo é identificado e registado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC Imprensa Oficial SSL transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC Imprensa Oficial SSL 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 SSL 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 SSL. 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 SSL. 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 SSL, 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 SSL 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, gazes e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - possuem proteção contra interferência eletromagnética externa.

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

5.1.2.1.11. Na AC Imprensa Oficial SSL, 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 fechadura individual. Os dados de ativação da chave privada da AC Imprensa Oficial SSL 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 SSL 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 SSL 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 SSL e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC Imprensa Oficial SSL.

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

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

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

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

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

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

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

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

5.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC Imprensa Oficial SSL 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 SSL 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 SSL, 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 SSL 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 SSL 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 SSL 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 SSL 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 SSL 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 SSL 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 SSL, 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 SSL 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 SSL tem a sua identidade e perfil verificados antes de:

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

5.2.3.2. Os certificados, contas e senhas utilizados para identificação e autenticação dos empregados:

a) são diretamente atribuídos a um único empregado;
b) não são compartilhados; e
c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC Imprensa Oficial SSL 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 SSL, 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; e
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 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 SSL 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 SSL 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 SSL e das AR vinculadas;
b) sistema de certificação em uso na AC Imprensa Oficial SSL;
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 SSL 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 SSL.

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 SSL ou de uma AR vinculada, o acesso dessa pessoa ao sistema de certificação é suspenso, é instaurado processo administrativo para apurar os fatos e, se for o caso, são tomadas as medidas administrativas e legais cabíveis.

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

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

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

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

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

5.3.7. REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

Todo o pessoal da AC Imprensa Oficial SSL 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 SSL disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas:

a) a DPC da AC Imprensa Oficial SSL;
b) as PCs que implementa;
c) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e a sua Política de Segurança;
d) documentação operacional relativa às suas atividades;
e) 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 SSL 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 SSL é gerado pela própria AC Imprensa Oficial SSL, após ter sido deferido o seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. Os pares de chaves criptográficas são gerados somente pelo titular do certificado correspondente.

6.1.1.3. Cada PC implementada pela AC Imprensa Oficial SSL define o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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 SSL entrega cópia de sua chave pública à AC Imprensa Oficial SP em formato PKCS #10.

6.1.3.2. Os procedimentos para a entrega da chave pública de um solicitante de certificado estão detalhados nas PC implementadas.

6.1.4. DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC PARA USUÁRIOS

A AC Imprensa Oficial SSL 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. Cada PC implementada pela AC Imprensa Oficial SSL define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.5.2. Não se aplica.

6.1.6. GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS

Os parâmetros de geração de chaves assimétricas da AC Imprensa Oficial adotam o padrão RSA 4096, 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 SSL são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8.2. Cada PC implementada pela AC Imprensa Oficial SSL caracteriza o processo utilizado para a geração de chaves criptográficas dos titulares dos certificados, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.9. PROPÓSITOS DE USO DE CHAVE (CONFORME O CAMPO "*KEY USAGE*" NA X.509V3)

6.1.9.1. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC Imprensa Oficial SSL, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC implementada.

6.1.9.2. A chave privada da AC Imprensa Oficial SSL 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 SSL implementa uma combinação de controles físicos, lógicos e procedimentais de forma a garantir a segurança das suas chaves privadas. As chaves privadas da AC Imprensa Oficial SSL trafegam cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento. Cada PC implementada especifica os requisitos específicos aplicáveis para a proteção das chaves privadas das entidades titulares de certificados.

6.2.1. PADRÕES PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC Imprensa Oficial adota o padrão FIPS 140-1 nível 2 (para a cadeia de certificação V0); ou FIPS 140-2 nível 2 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para as cadeias de certificação V2 e V3) e no padrão obrigatório (com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. Cada PC implementada especifica os requisitos específicos aplicáveis para a geração de chaves criptográficas dos titulares de certificado.

6.2.2. CONTROLE "N DE M" PARA CHAVE PRIVADA

6.2.2.1. A AC Imprensa Oficial SSL 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 SSL.

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 SSL mantém cópia de segurança de sua chave privada.

6.2.4.3. A AC Imprensa Oficial SSL não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido. Por solicitação do respectivo titular ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC Imprensa Oficial SSL poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico 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. As chaves privadas de sigilo são arquivadas com um nível de segurança não inferior àquele definido para a chave original. Não são arquivadas chaves privadas de assinatura digital. A AC Imprensa Oficial SSL arquiva somente chaves privadas de sigilo, e por solicitação do titular ou empresa ou órgão, quando o titular do certificado for seu empregado ou cliente.

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

6.2.6. INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

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

Cada PC implementada define, quando aplicável, os requisitos para a inserção da chave privada dos titulares de certificado em módulo criptográfico.

6.2.7. MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

A ativação das chaves privadas das AC Imprensa Oficial SSL 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.

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

6.2.8. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

A desativação das chaves privadas das AC Imprensa Oficial SSL 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.

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

6.2.9. MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

A destruição das chaves privadas das AC Imprensa Oficial SSL 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.

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

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. ARQUIVAMENTO DE CHAVE PÚBLICA

As chaves públicas da AC Imprensa Oficial SSL e dos titulares dos certificados de assinatura digital por ela emitidos, bem como as LCR emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. PERÍODOS DE USO PARA AS CHAVES PÚBLICA E PRIVADA

6.3.2.1. As chaves privadas dos titulares dos certificados de assinatura digital emitidos pela AC Imprensa Oficial SSL 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. Cada PC implementada pela AC Imprensa Oficial SSL define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.3.2.4. O período máximo de validade admitido para certificados da AC Imprensa Oficial SSL é de 8 (oito) anos.

6.4. DADOS DE ATIVAÇÃO

Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Cada PC implementada descreve os requisitos específicos aplicáveis.

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 SSL são únicos e aleatórios.

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

6.4.2. PROTEÇÃO DOS DADOS DE ATIVAÇÃO

6.4.2.1. A AC Imprensa Oficial SSL 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. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra o uso não autorizado.

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 SSL 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. Os requisitos de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC Imprensa Oficial SSL são descritos em cada PC implementada.

6.5.1.3. O ambiente computacional da AC Imprensa Oficial SSL 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 SSL;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC Imprensa Oficial SSL;
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 SSL;
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 SSL, o equipamento que passou por manutenção é inspecionado.

As informações sensíveis armazenadas, relativas à atividade da AC Imprensa Oficial SSL, são destruídas de maneira definitiva nos equipamentos que deixam de ser utilizados em caráter permanente.

Todos esses eventos são registados para fins de auditoria.

6.5.1.6. Equipamentos utilizados pela AC Imprensa Oficial SSL são preparados e configurados como previsto na Política de Segurança da AC Imprensa Oficial SSL 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 SSL segue as recomendações Common Criteria.

6.5.3. CONTROLES DE SEGURANÇA PARA AS AUTORIDADES DE REGISTRO

6.5.3.1. A AC Imprensa Oficial SSL 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 SSL 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 SSL provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC Imprensa Oficial SSL.

6.6.2. CONTROLES DE GERENCIAMENTO DE SEGURANÇA

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

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 SSL, incluindo *firewalls* e recursos similares.

6.7.1.2. Nos servidores do sistema de certificação da AC Imprensa Oficial SSL, 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 SSL.

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 intrusão provê o registro dos eventos em *logs*, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4. REGISTRO DE ACESSOS NÃO-AUTORIZADOS À REDE

As tentativas de acesso não-autorizado – em *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 utilizado para armazenamento da chave privada da AC Imprensa Oficial SSL está em conformidade com o padrão FIPS 140-2 nível 3, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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 SSL.

7.1.2. As PCs abaixo, implementadas pela AC Imprensa Oficial SSL, especificam os formatos dos certificados gerados e das correspondentes LCR. Nessas PC são incluídas informações sobre os padrões adotados, perfis, versões e extensões.

Política de Certificado	Nome	OID
Política de Certificado de Assinatura Digital Tipo A1 da AC Imprensa Oficial SSL	PC A1 da AC Imprensa Oficial SSL	2.16.76.1.2.1.211
Política de Certificado de Assinatura Digital Tipo A3 da AC Imprensa Oficial SSL	PC A3 da AC Imprensa Oficial SSL	2.16.76.1.2.3.209
Política de Certificado de Assinatura Digital Tipo A4 da AC Imprensa Oficial SSL	PC A4 da AC Imprensa Oficial SSL	2.16.76.1.2.4.42

7.1.3. Não se aplica.

7.2. PERFIL DO CERTIFICADO

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

7.2.2. EXTENSÕES DE CERTIFICADO

Não se aplica.

7.2.3. IDENTIFICADORES DE ALGORITMO

Não se aplica.

7.2.4. FORMATOS DE NOME

Não se aplica.

7.2.5. RESTRIÇÕES DE NOME
Não se aplica.

7.2.6. OID (OBJECT IDENTIFIER) DE DPC
O OID desta DPC é 2.16.76.1.1.119.

7.2.7. USO DA EXTENSÃO "POLICY CONSTRAINTS"
Não se aplica.

7.2.8. SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA
Não se aplica.

7.2.9. SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS
Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.3. PERFIL DE LCR

7.3.1. NÚMERO(S) DE VERSÃO
As LCR geradas pela AC Imprensa Oficial SSL 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 SSL, as seguintes extensões de LCR:

1. "*Authority Key Identifier*": contém o hash SHA-1 da chave pública da AC Imprensa Oficial SSL.

a) "*CRL Number*", não crítica: contém um número sequencial para cada LCR emitida pela AC Imprensa Oficial SSL.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

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

Esta DPC é atualizada sempre que uma nova PC implementada pela AC Imprensa Oficial SSL o exigir.

8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

A AC Imprensa Oficial SSL mantém disponível em repositório, para consulta pública, esta DPC (http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/).

8.3. PROCEDIMENTOS DE APROVAÇÃO

Esta DPC da AC Imprensa Oficial SSL foi submetida à aprovação, durante o processo de credenciamento da AC Imprensa Oficial SSL, 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